LA COMUNITÀ INTERNAZIONALE

Rivista Trimestrale della Società Italiana per l'Organizzazione Internazionale

QUADERNO 29

Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives

Edited by
Pietro Gargiulo, Davide Giovannelli, Annita Larissa Sciacovelli

With a preface by
Riccardo Sessa and Mart Noorma

EDITORIALE SCIENTIFICA
Napoli

LA COMUNITÀ INTERNAZIONALE

RIVISTA TRIMESTRALE DELLA

SOCIETÀ ITALIANA PER L'ORGANIZZAZIONE INTERNAZIONALE

QUADERNI (Nuova Serie)

29

SOCIETÀ ITALIANA PER L'ORGANIZZAZIONE INTERNAZIONALE

CYBERSECURITY GOVERNANCE AND NORMATIVE FRAMEWORKS: NON-WESTERN COUNTRIES AND INTERNATIONAL ORGANIZATIONS PERSPECTIVES

Edited by
Pietro Gargiulo, Davide Giovannelli, Annita Larissa Sciacovelli

With a preface by
Riccardo Sessa and Mart Noorma

EDITORIALE SCIENTIFICA
Napoli

This publication was financed by the
NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Manuscripts have been subjected to a peer review process prior to publication

Via San Biagio dei Librai, 39
89138 - Napoli
ISBN 979-12-5976-999-2

SUMMARY

PREFACE

Information and communications technologies (ICTs) are not anymore a new phenomenon, they are part of day-to-day life. Legal discussion over ICTs, however, is still, ongoing, despite a wide consensus on the applicability of international law to cyberspace. How international law applies to ICTs is still a matter of discussion by States, as disagreements and uncertainties have not been overcome yet.

In the international discussion on how international law applies to cyberspace, two fronts have emerged that are often described as 'the West and the Rest'. The first includes North-American and European countries which share common and rather coherent understanding of the key issues of international law applicable to cyber operations. The other category is broader and more diverse. Yet, in the legal discourse, the non-Western countries are often addressed in an over-simplifying manner that fails to consider the nuances between the opposing interpretations and legal positions.

Thus, this book aims to bring together perspective of Non-Western States and international organizations, in order to analyse and bring forward the different approaches to international law and cyberspace from a comparative perspective.

With reference to the domestic legal framework of the States' concern, the main purpose of this book is to provide sound analyses of domestic regulatory framework on cyber operations, as well as insights into oversight on surveillance technologies. With reference to the international organizations concern, instead, the main purpose of this book is to illustrate the how those international organizations are contributing to the ongoing discussion on how international law applies to cyberspace.

This book is a joint project between the *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) and the *Società Italiana per l'Organizzazione Internazionale* (SIOI) and it shall be also available as Open Access on website of the mentioned organizations.

We hope that this book will be of interest to anyone concerned with international law studies or working in areas where such issues are relevant – whether in circles of academics or practitioners – and we also hope that book may offer an engaging, helpful, and thought-provoking read.

Ambassador RICCARDO SESSA
President of the SIOI

Dr. MART NOORMA
Director of the CCDCOE

INTRODUCTION

The military conflict between Russia and Ukraine is yet another reminder that, when it comes to the understanding on the role, and interpretation of international law, there is still a significant gap between 'the West and the Rest'. This gap is also evident in relation to the discussion on how international law applies to cyberspace and cyber operations, in a way that creates disagreements on values (e.g. privacy v social stability, or competitiveness v equality) and on the interpretation of the law (e.g. the definition of a cyberattack v information warfare).

The 'West' camp, sometimes also referred as 'Global North', includes North-American and European countries, which share common and rather coherent understanding of the key issues of international law applicable to cyber operations. The other category, or the 'Rest', often also referred as 'Global Majority', is broader in its geographic scope and more diverse in its values. When focusing on the legal discourse, nevertheless, the non-Western countries are often addressed in an over-simplifying manner that fails to consider the nuances between the opposing interpretations and legal positions.

That is what this book is about. Entitled "Cybersecurity Governance and Normative Frameworks: Non-Western Countries and International Organizations Perspectives" this book divided in three parts and presents a series of case studies and legal analyses in order to bring forward the different approaches to international law and cyberspace from a comparative perspective.

In the first general part Annita Larissa Sciacovelli examines the notion of cyber hostile activities and malicious cyber operations in the context of international Law, while Sebastiano La Piscopia provides a doctrinal contribution on the regulatory definition of the tools for cyber offensive operations.

In the second part, the domestic governance architecture for cyber security is analysed. Arindrajit Basu and Bharath Gururagavendran address India, while Keiko Kono and Isaac Morales Tenorio and Mariana Salazar Albornoz address Japan and Mexico, respectively. In addition, Tal Mimran and Lior Weinstein paper discuss the specific topic of oversight on surveillance technologies in Israel.

In the third part, instead, the point of views of international organizations on cyber security is considered. Pietro Gargiulo describes United Nations, Ivan Ingravallo and Elena Drago condensers the Council of Europe, Elisa Tino analyses the ASEAN, Antonio Mariconda and Pierfrancesco Rossi examine the Shanghai Cooperation Organization and Silvia Venier discusses the African Union.

In assembling these selected papers, the main purpose has been to develop a closer comparative look into the approaches to international law and states behaviour in cyberspace in different geographic regions of the globe. While the Global North has maintained so far the initiative and leadership in the context of the discussion on how international law applies to cyberspace and cyber operations, any concrete step forward in that respect needs also to pay attention to Global Majority's specific concerns. This book, thus, is aimed at facilitating such exchanges of views.

DAVIDE GIOVANNELLI
Commander, Italian Navy
Researcher, Law Branch

GENERAL ASPECTS

MALICIOUS CYBEROPERATIONS COMMITTED BY STATE AND NON-STATE ACTORS: THE INTERNATIONAL LEGAL LANDSCAPE

ANNITA LARISSA SCICOVELLI

1. The recent exponential increase in malicious cyberoperations by both state and non-state actors is undermining national and international peace and security, and delicate geo-strategic balances[1]. This rise in threats in cyber space has become a critical global security issue, as highlighted in the "Concept Note for the Security Council of the United Nations" on "Maintenance of international peace and security: addressing evolving threats in cyberspace", of June 10, 2024[2], necessitating significant international attention from the international community.

---

[1] This publication is the result of the research conducted within the European Union co-financing-Next Generation EU: NRRP Initiative, Mission 4, Component 2, Investment 1.3 - Partnerships extended to universities, research centres, companies and research D.D. MUR n. 341 del 15.03.2022 –Next Generation EU (PE0000014-"SEcurity and Rights in the CyberSpace-SERICS"-CUP: H93C22000620001). On this topic see the contributions of H.S. LIN, *Offensive Cyber Operations and the Use of Force*, in *Journal of National Security Law and Policy*, 2010, 4; H. DINNISS, *Cyber Warfare and the Laws of War*, Cambridge, 2012, 74; M.N. SCHMITT, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge, 2013; L. BAUDIN, *Les cyber-attaques dans les conflits armés*, Paris, 2014; M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014; K. KITTICHAISAREE, *Public International Law of Cyberspace*, Cham, 2017; N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook on International Law and Cyberspace*, Cheltenham, Northampton, 2021; H. LAHMANN, *Unilateral Remedies to Cyber Operations*, Cambridge, 2020.

[2] See United Nations (UN) Security Council, Concept note for the Security Council high-level open debate on "Maintenance of international eace and sSecurity: Addressing Evolving Threats in Cyberspace", UN Doc. S/2024/446; Permanent Mission of the Republic of Korea at the UN, Arria-Formula Meeting on Cyber Security Evolving Cyber Threat Landscape and its Implications for the Maintenance of International Peace and Security, https://www.securitycouncilreport.org/. See in this book, GARGIULO, *The United Nations and*

Malicious cyberoperations are complex, committed with a high speed and technical sophisticated and they target - and sometimes severely impact - the information and communication technologies systems (ICTs) of private companies, public entities, and critical infrastructures within national cybersecurity perimeters[3]. These targets include, *inter alia*, healthcare systems, banking and financial services, large automated industrial complexes such as energy and manufacturing sectors, transportation, telecommunications (including satellites), and water plants, to cite a few.

Following the rapid evolution of digitalization after the Covid-19 pandemic, these entities and infrastructures have become essential for the regular functioning of governmental activities that provides essential civil, social, political, and economic services. Thus, malicious cyberoperations are a new form of intrusion into the sovereign prerogatives of states, making the protection of ICTs and the digital data stored in them crucial elements of national and international (cyber)security.

The aims of these malicious activities are to alter, degrade, destroy, or interrupt the correct functioning of ICTs, either partially or completely, and to alter, destroy or compromise, even irreversibly, the confidentiality, integrity, and availability of digital data that are essential for the cited services[4]. The impact of these activities is evident in both the digital and physical worlds.

These malicious activities are mainly transnational and are driven by the military, geopolitical, and financial interests of the various

---

Cybersecurity; S. LA PISCOPÌA, *The Regulatory Relevance of the Fifth Domain's Weapons Definition*.

[3] See the UN General Assembly resolution, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures*, December 23, 2003, n. 58/199, UN Doc. A/RES/58/199. See GEE, Report *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 14 July, 2021, UN Doc. A/76/135, para. 7, 14. See S. HAATAJA, *Cyber Operations Against Critical Infrastructure Under Norms of Responsible State Behavior and International Law*, in *International Journal of Law and Information Technology*, 2022, 423.

[4] See E.T. JENSEN, *Cyber Warfare and Precautions Against the Effects of Attacks*, in *Texas Law Review*, 2010, 88; O.A. HATHAWAY, *The Law of Cyber-Attack*, in *California Law Review*, 2012, 817; K. MAČÁK, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law,* in *Israel Law Review*, 2015, 55; M.N. SCHMITT, *The Notion of 'Objects' During Cyber Operations: A Riposte in Defence of Interpretive Precision*, ivi, 81; R. GEISS, H. LAHMANN, *Protection of Data in Armed Conflict*, in *International Law Studies*, 2021, 556.

actors acting in cyberspace, such as states and non-state entities[5]. Therefore, cyberoperations can be part of broader and complex strategies reflecting the states' agendas, potentially causing or exacerbating international crises and threatening international peace and security.

A notable example of such an operation is the cyber-attack on Viasat Inc.'s KA-SAT satellite, which disrupted Ukrainian civil and military communications just hours before the Russian military aggression on February 24, 2022[6]. This incident marks the Russian-Ukrainian conflict as the first to start in the cyber domain.

In the past, other hostile actions in cyber space were carried out, likely again by the Russian Federation, against Georgia in 2019, and against Ukraine during the Crimean War in 2014[7].

In this regard, the Council of the European Union (EU), in March 2022, adopted the *EU Strategic Compass for Security and Defense*, emphasizing that cyberoperations against European and Ukrainian network infrastructures were a significant part of Russia's hybrid

---

[5] Cyber space is made up of three segments: the first is physical and is made up of hardware systems and physical network infrastructures (computers, cables, servers); the other two segments are virtual and, specifically, one is composed of the software and other programs thanks to which the previous level can function, and the other consists of digital data that are stored in the hardware. For a definition of cyber space, see M.N. SCHMITT, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge, 2017, 564, and U.S. Dept. of Defense, *Law of War Manual*, 2023, 1025, according to which it is a «global domain within the information environment consisting of interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers». About the motivations behind cyberoperations see C. HEFFELFINGER, *The Risks Posed by Jihadist Hackers*, in *CTC Sentinel*, 2013, 32 ff; M. COHEN, F. CHUCK, G. SIBONI, *"Four Big "Ds" and a Little "r": A New Model for Cyber Defense*, in *Cyber, Intelligence, and Security*, 2017, 21 ff; F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, 11 ff; NATO, *Summit of Warsaw Communiqué*, 2016, that states that «[T]he Alliance faces a range of security challenges and threats that originate (…) from state and non-state actors; from military forces and from terrorist, cyber, or hybrid attacks».

[6] See P.H. O'NEILL, *Russia Hacked an American Satellite Company One Hour Before the Ukraine Invasion. The Attack on Viasat Showcases Cyber's Emerging Role in Modern Warfare*, 2022, https://www.technologyreview.com; MICROSOFT, *Microsoft Digital Defense Report 2022, Russian State Actors' Wartime Cyber Tactics Threaten Ukraine and Beyond*, 41 ff; M. ORENSTEIN, *Russia's Use of Cyberattacks: Lessons from the Second Ukraine War*, in *Foreign Policy Research Institute,* 2022; J.A. LEWIS, *Cyber War and Ukraine*, 2022, https://csis-website-prod.s3.amazonaws.com.

[7] See G. NAKASHIDZE, *Cyberattack Against Georgia and International Response: Emerging Normative Paradigm of 'Responsible State Behavior in Cyberspace'?*, in *EJILTalk!*, 2020; P. ROGUSKI, *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*, 2020, www.justsecurity.org.

warfare toolkit, therefore the need to create an EU cyber defense policy[8].

Additionally, it is worth mentioning the cyberoperations against Albania in July and September 2022, allegedly conducted by Iranian hackers, aimed to completely shut down the government's ICTs and erase the digital data stored in them[9]. These cyber-attacks have been defined by the Albanian Prime Minister a state aggression and they prompted a statement from the North Atlantic Treaty Organization (NATO) on September 8, 2022, acknowledging them as state cyber aggression likely orchestrated by Iran[10]. Following the technical and legal attribution of these operations, NATO's Secretary General did not rule out invoking Article 5 of the North Atlantic Treaty, which pertains to collective defense actions to protect its member states[11].

These cases highlight the dangers of cyber weapons used also in conjunction with kinetic armed conflicts and underscore the importance of an analysis of the current complex landscape of threat actors, of the hostile activities in cyberspace, and of the international legal obligations of states.

Aim of this paper is to focus on cyberoperations during peacetime, and to serve as a preliminary foundation for the subsequent chapters of this book, which will explore both the normative frameworks and positions of non-Western countries in cyberspace, and the roles of international organizations in promoting common understandings, collaboration and international cooperation for the sake of an open, secure, stable, accessible and peaceful digital environment.

---

[8] See Council of the European Union, Strategic Compass for Security and Defense and for a European Union that Protects its Citizens, its Values and its Interests and Contributes to International Peace and Security, 2022, paras. 3, 5, 6, and 7; ID., *European Union Strategic Compass for Security and Defence*, 2022, https://www.eeas.europa.eu.

[9] See NATO, *Statement by the North Atlantic Council Concerning the Malicious Cyber Activities against Albania*, September 8, 2022; CCDCOE, *Homeland Justice Operations Against Albania*, 2022, https://cyberlaw.ccdcoe.org/wiki/Homeland_Justice_operations_against_Albania_(2022). Let it be permitted to refer to A.L. SCIACOVELLI, *Taking cyber-attacks seriously: the (likely) Albanian cyber aggression and the Iranian responsibility*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana*, 2023, www.osorin.it.

[10] https://www.voanews.com/a/6734763.html; https://www.nato.int/cps/en/natohq/official_texts_207156.htm

[11] https://www.nato.int/cps/en/natohq/news_207552.htm?selectedLocale=en; https://www.nato.int/cps/en/natohq/official_texts_17120.htm.

This paper is structured as follows: it examines the most prominent types of cyberoperations below and above the use-of-force threshold of the prohibition of the use of force committed by states; it identifies the legal and technical challenges of their attribution to states, and it traces the possible solutions to the problem of international responsibility of states regarding the use of proxies to commit wrongful acts in cyberspace.

2. States often conduct illicit cyberoperations using their military and intelligence apparatus. However, in many cases, they prefer to use groups of professional criminal hackers, known as non-state actors. These include individuals, groups, or private security companies acting as *proxies* in executing hostile activities in cyberspace.

The UN Working Group on Mercenaries, in its 2021 report on cyber mercenaries, highlighted the increasing involvement of private actors in the cyber domain, such as cyber militias and Advanced Persistent Threat (APT) groups[12]. Cyber mercenaries are private actors engaged by states to conduct offensive or defensive cyberoperations to weaken or undermine the military capacities of adversary forces.

As outlined by the UN Open-Ended Intergovernmental Working Group on the use of mercenaries as a means of violating human rights and impeding the exercise of the right of peoples to self-determination (OEIWG) in its Progress Report of 2024, one of the consequences of the use of cyber militias is the asymmetric nature of modern armed conflicts[13]. This has led to the proliferation of and military companies exacerbating conflicts dynamics and exposing the civilian population to the violation of human rights. These militias provide inherently covert opportunities to product, store, transfer, and deploy significant military capabilities with minimal organizational, financial and human resources compared to traditional industrial warfare. Recently, these

[12] See the *UN Working Group Report on the Use of Mercenaries as a Means of Violating Human Rights and Impeding the Exercise of the Right of Peoples to Self-Determination*, July 15, 2021, UN Doc. A/76/151.

[13] See Chair-Rapporteur of the UN Human Rights Council, *Progress Report on the fifth session of the Open-Ended Group Intergovernmental Working Group to Elaborate the Content of an International Regulatory Framework on the Regulation, Monitoring and Oversight of the Activities of the Private Military Companies* (*OEIWG Report 2024*), UN Doc. A/HCR/57/53.

APT have developed a cyber arsenal sometimes superior to the ones of the states[14].

Generally, non-state actors operating in cyber space are highly organized and have criminal affiliations in other states. They possess their own intelligence agencies, help desks and they purchase cheap cyber weapons kits and subscriptions to commit cybercrimes on digital platforms on behalf of their clients, such as states (crime-as-a-service).

Previously, these offensive capabilities were only available to states and this recent shift is partly due to the cheap commercial availability of cybercrime and ransomware tools, leading to the *privatization* of offensive cyber capabilities.

These criminal groups use sophisticated digital tools to exploit artificial intelligence[15]. This allows them to expand digital attack surfaces by exploiting the vulnerabilities of ICTs' systems and the weaknesses of human factors, i.e. using social engineering. Soon probably non-state actors will use post quantum computing to better prepare their malicious activities in cyberspace[16].

The goals pursued by criminal hackers are primarily economic and political. Economic motivations stem from the potentiality to realize huge profits from computer crimes, ranging from hundreds to millions of dollars, which allow for the self-financing of the criminal group. Political motivations are often linked to ideological choices (as with hacktivists and cyber terrorists) or to states' geopolitical strategies in the cyber arena. Examples include collectives online acting in international conflicts (e.g., Russia and Ukraine), in regional rivalries (e.g., India and Pakistan) and regional conflicts (e.g., Israel and Hamas, Israel and Palestine)[17].

---

[14] See *OEWG Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2021, Annex I, para. 19 (*OEWG Report 2021)*, par. 16; M. N. SCHMITT, S. WATTS, *Beyond State-Centrism: International Law and Non-State Actors in Cyberspace*, in *Journal of Conflicts&Security Law*, 2016, 595 ff; E. D. BORGHARD, S.W. LONERGAN, *Cyber Operations as Imperfect Tools of Escalation*, in *Strategic Studies Quarterly*, 2019, 122 ss.; J. BLESSING, *The Global Spread of Cyber Forces, 2000–2018*, 2021, https://ccdcoe.org.

[15] See *OEIWG Report 2024*, cit., 3.

[16] See *OEWG Report 2021*, cit., par. 16; R.J. BUCHAN, *Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm*, in *Journal of Conflict & Security Law*, 2016, 429 ff; K. MAČÁK, *Unblurring the Lines: Military Cyber Operations and International Law,* in *Journal of Cyber Policy*, 2021, 411 et seq.

[17] See M. BLAEZNER, *Hotspot Analysis: Regional Rivalry Between India-Pakistan: Tit-for-tat in Cyberspace*, Center for Security Studies, ETH Zurich, 2018; T. MIMRAN, *Israel-Hamas 2023 Symposium, Cyberspace, the Hidden Aspect of the Conflict*,

Despite their role as guarantors of international law within their boundaries, states often tolerate, sponsor, or even coordinate the activities of criminal hackers operating from the digital networks of their territories. Therefore, a significant challenge in international law is how to hold a sponsor state internationally responsible for the illegal conduct of non-state actors in cyberspace[18].

3. Hostile cyberoperations vary widely in nature, scale, and scope. The most prominent and frequent types include distributed denial of service (DDoS), ransomware, which can also be destructive, and cyber espionage[19]. The first two should be distinguished from cyber espionage, which usually serves informational and retaliatory tactics. Cyber espionage involves extracting information from networks without disrupting their functionality. It violates state's domestic laws, and generally does not violate international law, unless it is part of a complex and coordinated military operation[20].

---

https://lieber.westpoint.edu/cyberspace-hidden-aspect-conflict. On the nature of the conflicts between Israel and Hamas, and between Israel and Palestine, see A.A. KARIM, Press Statement of May 20, 2024, of the International Criminal Court Prosecutor. See K.C. KHAN, *Applications for Arrest Warrants in the Situation in the State of Palestine*, 2024, https://www.icc-cpi.int/news/statement-icc-prosecutor-karim-aa-khan-kc-applications-arrest-warrants-situation-state; J.B. QUIGLEY, *Karim Khan's Dubious Characterization of the Gaza Hostilities*, 2024, in https://www.ejiltalk.org.

[18] See V. M. BENATAR, *The Use of Cyber force: Need for Legal Justification?*, in *Goettingen Journal of International Law*, 2009, 378 ff; V. WOLTAG, J. CHRISTOPH, *Cyber Warfare*, in *Max Planck Encyclopedia of Public International Law*, Oxford, 2015, 7 ff; M. FINNEMORE, D. HOLLIS, *Beyond Naming and Shaming: Accusations and International Law in Cybersecurity*, in *The European Journal of International Law*, 2020, 970; F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, 11-12.

[19] For a definition of cyber-attack, see M.N. SCHMITT, *Tallinn Manual 2.0*, cit., Rule 92, 415, a «cyber operation, whether offensive or defensive, […] is reasonably expected to cause injury or death to persons or damage or destruction of objects». The cited rule seems inspired by the notion of kinetic attack pursuant to Art. 49, par. 1, of the I Additional Protocol to the four Geneva Conventions of August 12, 1949, relating to the protection of victims of international armed conflicts, adopted in Geneva June 8, 1977, which states «[T]he expression "attacks" means acts of violence against the adversary, whether such acts are carried out for the purpose of offense or defense». M.N. SCHMITT, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in *Columbia Journal of Transnational Law*, 1999, 885; M. ROSCINI, *Cyber*, cit., 10-18; J. BILLER, *The Strategic Use of Ransomware Operations*, in *International Law Studies*, 2023, 484.

[20] For O. A. HATHAWAY, R. CROOTOF, *The Law of Cyber-Attack*, in *California Law Review*, 2012, 829, cyber espionage is «the science of covertly capturing e-mail traffic, text messages, other electronic communications, and corporate data for the purpose of gathering national-security or commercial intelligence». On cyber espionage and international law see also M. N. SCHMITT, *Tallinn Manual 2.0*, cit., Rule 32, 168; R. BUCHAN, *Cyber Espionage and International Law*, Oxford-New York, 2019.

Specifically, cyberoperations are characterized by their multistage nature. Unlike conventional military or criminal acts, where effects are apparent shortly after the weapons are used, cyber weapons (such as logic bombs, worms, trojans, and malware etc.) can stay dormant for significant periods, can secretly alter data and can clandestinely compromise a network's operation. It often takes months to detect them and this ability to avoid detection distinguishes cyber from kinetic weapons and operations[21].

Other differences include the transnational nature of the cyber domain, which lacks physical borders, grants almost total anonymity to actors, and involves complex operations that are also often widespread and decentralized from a geographical point of view.

An example is the use of hundreds of thousands of botnets (zombies) by an actor (state or otherwise) to infect computers and Internet of Things (IoT) devices in another state, as seen in the operation against Estonia in 2007 conducted from the territories of many states and presumably backed by the Russian Federation[22].

Moreover, hostile digital activities are often carried out through the ICTs of multiple states, sometimes without their knowledge. This includes the state(s) of the launch of the operation, the state(s) whose ICTs are used for the malware transit, and the state(s) where the criminal offenses take place.

---

[21] See D.D. CLARK, S. LANDAU, *Untangling Attribution*, in *Harvard National Security Journal*, 2011, 531 and 533.

[22] A botnet is a network of computers infected with malicious software (malware) to be controlled remotely by a single actor - called bot master - to attack a target, without the real owners of the computers being aware of it, hence they are called zombies, thus increasing the resources and offensive capabilities at its disposal. Computers are forced to send spam, spread viruses, or launch DDoS attacks. In the case of Estonia, the attack was launched in conjunction with the Estonian Government's decision to remove the bronze statue of the unknown Soviet soldier from the main square of Tallinn, hence its attribution to the Russian Federation on the basis of elements collected by intelligence. These attacks led to the interruption of the functioning of the main ICT systems of public, financial and media bodies, causing an economic loss quantified between twenty-seven and forty million dollars. Specifically, the DDoS attack consists of sending a series of requests for information to an entity's information and communication system in order to block it. See R. SHACKELFORD, *An Introduction to the Law of Cyber War and Peace, in Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace*, Cambridge, 2014, 263; I. ZAHRA, I. HANDAYANI, D.W. CHRISTIANTI, *Cyber-attack in Estonia: A New Challenge in the Applicability of International Humanitarian Law*, in *Yustisia*, 2021, 48; D. BROEDERS, F. DE BUSSER, F. CRISTIANO, T. TROPINA, *Revisiting Past Cyber Operations In Light of New Cyber Norms and Interpretations of International Law: Inching Towards Lines in the Sand?*, in *Journal of Cyber Policy*, 2022, 108.

Currently, there is unanimous consensus among states about the applicability of international law to cyberspace, and first of the essential principle of the respect of state's sovereignty, whose application extends to the digital dimension as well[23]. However, differing positions have emerged among member states on whether it is necessary also to draft specific provisions for cyberoperations.

Specifically, the international legal framework for cyberspace was developed within the UN since the late 1990s. This international organization has been committed to promoting a shared vision among member states for an open, accessible, and peaceful digital ecosystem. The UN has also emphasized the safe and responsible use of ICTs, in accordance with international law and the UN Charter.

Starting in 2003, the UN Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (hereinafter, GGE) and, subsequently, from 2019, the UN Open-Ended Working Group on Security of and in the Use of Information and Communication Technologies (hereinafter, OEWG) have produced a series of reports outlining the principles of international law applicable by consensus to cyberspace[24].

These reports are the principal reference for states on the application of international law, and specifically on international responsibility in cyberspace. They are the result of extensive diplomatic efforts and of the reflection of geopolitical tensions arising from the composition of the two UN working groups. The first group was established by the United States and the second one was the outcome of China and Russian Federation will. These groups are actively engaged in the elaboration of cyberspace principles that are enshrined, since 2015, in a decalogue of eleven voluntary non-binding

[23] See GEE, *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, July 22, 2015, UN Doc. A/70/174, 27 (*GEE Report 2015*); NATO, *Cyber Defence Pledge*, https://www.nato.int; Rapporteur of the Organization of American States, D.B. HOLLIS, *Improving Transparency – International Law and State Cyber Operations: Fourth Report*, OAS Doc. OEA/Ser.Q, CJI/doc 603/20 rev.1, 2020; UN General Assembly, *Program of Action to Advance Responsible State Behavior in the Use of Information and Communications Technologies in the Context of International Security*, res. of October 13, 2022, UN Doc. A/C.1/77/L.73.

[24] See UN General Assembly resolutions of 18 December 18, 2003 (UN Doc. A/RES/58/32), December 8, 2005 (UN Doc. A/RES/60/45), December 13, 2011 (UN Doc. A/RES/66/24), June 24, 2013 (UN Doc. A/68/98), January 9, 2014 (UN Doc. A/RES/68/243), December 30, 2015 (UN Doc. A/RES/70/237) January 2, 2019 (UN Doc. A/RES/73/266), July 14, 2021 (UN Doc. A/76/135), and October13, 2022 (UN Doc A/C.1/77/L.73).

norms of responsible state behavior in the use of Information and Communications Technologies (UN non-binding norms)[25].

This decalogue concerns with the maintenance of international peace and security in cyberspace in line with the principles of the UN Charter; the ban on using the state territory for internationally prohibited activities; the peaceful use of ICTs also in compliance with human rights; the respect for state sovereignty; the peaceful resolution of international disputes and the non-intervention in the internal and external affairs of a state through ICTs.

This decalogue enshrine obligations and principles of customary international law, particularly those embedded in the UN Charter, and it represents the essential, consolidated, cumulative, and evolving framework for conducts in the digital domain and to which reference will be made in this chapter[26]. As it will emerge in these pages and in the following chapters of this book, the specific contents and the practical application of the obligations and principle contained in the decalogue are still under evolution and evaluation particularly because of their recent articulation about the state's international responsibility in cyberspace.

Specifically, upon closer examination, it is evident that this framework lacks specific guidelines regarding illicit digital operations that may fall under the prohibition in Article 2, Paragraph 4 of the UN Charter. This norm prohibits the threat and use of armed force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the UN[27]. Furthermore, it does not address the exercise of the right of self-defense in response to a cyber-attack.

From a legal perspective, depending on the extent of their intrusion or on their effects, cyberoperations may violate the principles of state's sovereignty, of non-intervention or even the of the prohibition of the threat or use of force in international relations.

---

[25] GEE, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 22 July, 2015, UN Doc. A/70/150, 12; OEWG, *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2021, UN Doc. 75/816; *Ibidem*, *Report of the on Security of and in the Use of Information and Communications Technologies 2021–2025*, August 8, 2022, UN Doc. A/77/275 (*Report 2022*). See also in this book, GARGIULO, *The United Nations and Cybersecurity*, cit.

[26] See *Report OEWG 2022*, cit., par. 15 f., 10 f.

[27] See M.N. SCHMITT, *Classification of Cyber Conflict*, in *Journal of Conflict & Security Law*, 2012, 251.

Therefore, cyberoperations mainly may be categorized in operations i) that are *above* and ii) that fall *below* the use-of-force threshold enshrined in Article 2, Paragraph 4 of the UN Charter[28]. The choice of this categorization is due to the different legal consequences whether the cyberoperation falls in one of the two categories.

Starting from the type of cyberoperations whose effects are *below* the use-of-force threshold (and dealing with the 'above threshold' operations in the next paragraph), they might constitute a violation of the principle of territorial sovereignty (as it extends to the ICTs infrastructures located within its territory) and of other international norms and principles that flow from it[29].

Unauthorized intrusion of the ICTs of a State itself constitutes a violation of its territorial sovereignty along with accessing to i) to steal, manipulate, or destroy data that resides in the target information systems, and ii) to disrupt the ICTs functions. As suggested by the arbitration ruling on the *Island of Palmas* (1928), territorial sovereignty involves a state's exclusive right to exercise power over a specific area[30].

---

[28] See M.C. WAXMAN, *Cyber Attacks as "Force" Under UN Charter Article 2(4)*, in *International Law Studies*, 2011, 43; S. WATTS, *Low-Intensity Cyber Operations and the Principle of Non-Intervention*, in J.D. OHLIN, K. GOVERN (eds), *Cyber War and Ethics for Virtual Conflicts*, Oxford, 2015; M. ROSCINI, *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, Oxford, 2024, 374 ff.

[29] According to Rule 1 of the *Tallinn Manual 2.0*, cit., «[t]he principle of State sovereignty applies in cyberspace». GEE *Report 2015*, paras. 27-28. According to M.N. SCHMITT, *Tallin Manual 2.0,* cit., Rule 4, 12 ff, «[C]yber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law» on the assumption that «States enjoy sovereignty over cyber infrastructure, persons, and cyber activities located on their territory. This includes both public and private cyber infrastructure». The 'sub-threshold' operations might also represent the instrument of a military strategy: the hybrid warfare. Hybrid warfare is based above all on the use of unconventional tools, such as IT and disinformation campaigns, interference in electoral processes and the exploitation of irregular migratory flows, to name a few examples. It is an offensive strategy whose objective is to undermine the national security of a country. On this topic see M.N. SCHMITT, S. WATTS, *Beyond State-Centrism*, cit., 600; F.G. HOFFMAN, *Conflict in the 21st Century: The Rise of Hybrid Wars*, 2007, www.potomacinstitute.org; M. CLARK, *Russian Hybrid Warfare*, 2020, https://www.understandingwar.org; G. Simons, Y. DANYKM, T. MALIARCHUK, *Hybrid War And Cyber-Attacks: Creating Legal and Operational Dilemmas, Global Change*, in *Peace & Security*, 2020, 337 ff; NATO, *NATO's Response to Hybrid Threats*, 2021, www.nato.int; on the notion of cyber intervention see I. KILOVATY, *The International Law of Cyber Intervention*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook*, cit., 99 ff.

[30] Permanent Court of Arbitration, *Island of Palmas* (The Netherlands v. United States of America), arbitration award April 4, 1928, 838-839; see Rule 4 of *Tallin Manual 2.0,* cit., on "Violation of sovereignty" states «[A] State must not conduct cyber operations that violate the sovereignty of another State», 17.

For instance, a cyberoperation that affects the confidentiality, integrity, or availability of data or disrupts the functioning of computer systems and produces physical effects constitutes such a violation, such as impacting critical infrastructures (e.g., power utilities, water supplies), causing widespread effects (e.g., power outages), or interfering with the functioning of public or private healthcare facilities (e.g., hospitals).

It is noteworthy to distinguish between two approaches to find a violation of sovereignty: the *de minimis* approach, that requires a sufficient degree of infringement of the target state's territorial integrity that might be caused by the disruption of ICTs, or by an interference with/or by the usurpation of its inherently governmental functions and the presence of physical damages, and the penetration-based approach, that argues that every penetration of computer networks within a state's territory violates its sovereignty[31].

Moreover, a cyberoperation attributable to a state may constitute a violation of the *principle of non-intervention* in internal affairs of a state when it involves an act of coercion within its domestic jurisdiction, potentially constituting an internationally wrongful act.

The principle of non-intervention is clearly stated in some UN General Assembly declarations[32], and in the light of the international Court of Justice (ICJ) jurisprudence the violation of this principle can occur when two conditions are met cumulatively: the action constitutes a coercive interference into the domestic jurisdiction[33].

---

[31] Few states adhere to the latter approach, for instance according to the Ministry of Defence of France, *International Law Applied to Operations in Cyberspace*, 2019, «any cyber-attack against French digital systems or any effects produced on French territory by digital means by a State organ [or otherwise attributable to a State] constitutes a breach of sovereignty», https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Due_diligence. For the *de minimis* approach see Rule 4, *Tallinn Manual 2.0*, cit., 20.

[32] See the Principles III and VI of the UN General Assembly Declaration on Principle of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the UN Charter UN Doc. A/Res/2526(XXV), of October 24, 1970, UN Doc. A/Res/2526; the Declaration on the enhancement of the effectiveness *of the* principle of refraining from the threat or use of force in international relations, of November 18, 1987, UN Doc. A/Res/42/22; the Principles I and VI of the Final Act of the Helsinki Conference on Security and Cooperation in Europe, August 1, 1975. See M. ROSCINI, *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles*, Oxford, 2024, 374 ff.

[33] See International Court of Justice, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua* v. *United States of America) (Nicaragua case), Merits,* Judgment June 27, 1986, in *ICJ Reports*, 1986, 98 ff, paras. 187 ff, 106, para. 202; Id., case *Armed Activities on the Territory of the Congo* (*Democratic Republic* of the *Congo v. Uganda*), Judgment

Starting with the first criterion, coercion can involve forcing another state to do or refrain from doing something under threat of specific, serious, and credible harm, or taking control of a certain situation and forcibly imposing a certain action.

The second criterion involves the domestic jurisdiction, which consists of coercion of the target state in matters where it has no obligations under international law, either customary or conventional. Examples include «the choice of a political, economic, social and cultural system, and the formulation of foreign policy»[34].

In cyberspace questions remain about which affairs fall into the domestic jurisdiction of a state, and how to define the element of coercion. It may be the case of cyberoperations which disrupt the capacity of a state to conduct an electoral process, or which alter its results through manipulation of electronic voting infrastructures.

Corollary of the principle of state sovereignty is the *due diligence* principle under which every state is under an obligation «not to allow knowingly its territory to be used for acts contrary to the rights of other States», in accordance with the ICJ *Corfu Channel* case (1949)[35]. The *due diligence* principle is enshrined in Norm C of the UN non-binding norms that emphasizes that states should not knowingly permit their territory to be used for wrongful acts via ICTs[36].

Furthermore, under Norm F of the cited UN non-binding norms states should also «not conduct or knowingly support ICT activity

---

December 19, 2005, in *ICJ Reports*, 2005, 164. See also Rule 66 of the *Tallinn Manual 2.0*, cit., which states: «[A] State may not intervene, including by cyber means, in the internal or external affairs of another State», 312.

[34] ICJ, *Nicaragua* case, cit., para. 202.

[35] ICJ, The *Corfu Channel Case* (*United Kingdom* v. *Albania*), Judgment of April 9, 1949, ICJ Reports, 22; Id., Case *Pulp Mills on the River Uruguay* (*Argentina* v. *Uruguay*), Judgment of April 20, 2010, *ICJ Reports*, 2010, para. 101.

[36] See GEE *Report of 2015*, para. 13 (c); N.M. SCHMITT, *In Defense of Due Diligence in Cyberspace*, in *Yale Law Journal Forum*, 2015, 68; Rule 6, *Tallinn Manual 2.0*, cit., 30, that reads as follows: «[A] State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States». On this subject see C. BANNELIER-CHRISTAKIS, *Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?*, in *Baltic Yearbook of International Law*, 2014, 23, 37; K. KITTICHAISAREE, *Public International Law of Cyberspace*, cit., 33; I. COUZIGOU, *Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations*, 2018, 37, https://aura.abdn.ac.uk; A. COCO, T. DE SOUZA DIAS, "*Cyber Due Diligence": A Patchwork of Protective Obligations in International Law*, in *European Journal of International Law*, 2021, 771; ID., *Cyber Due Diligence in International Law*, Oxford, 2022, 47.

contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public» of other states[37].

This means that a state is obliged to prevent harmful cyber activities, that reaches the requisite threshold of harm[38], and that are originating from, passing through, or occurring in any area under its exclusive control (e.g. for the misuse of its ICTs) when it knows - or should have known - about such activities, especially when they infringe on the rights of another state. Knowledge can be determined by the notification by the victim-state that has identified the state or states from the territories of which the malicious cyber transmissions occur. Therefore, the notified state is expected to take reasonable, proportionate, and effective measures to prevent, halt, respond, and address the harmful transboundary cyberoperations that can be committed by its organs or by non-state, even if the identity of the hostile operation's initiator is unknown[39]. The latter notion should include unregulated (national or international) security companies that should be held accountable for their activities in cyberspace to avoid impunity for their actions[40]. Thus, a state may be responsible for harmful international for its failure to prevent illicit cyberoperations. However, it is not expected that the state should monitor all the ICTs activities within its territory, as it is an 'expectation of means', but it should respect the duty of prevention and vigilance[41].

4. The cyberoperations whose effects are *above* the use-of-force threshold are one of the most complex issues in international cyber law.

---

[37] Norm F of the UN non-binding norms. See R.J. BUCHAN, *Cyberspace, Non-State Actors*, cit., 451 ff.

[38] ICJ, Case *Pulp Mills on the River Uruguay*, cit., parr. 30-34.

[39] See the UN International Law Commission Draft Articles on the Prevention of Trans–Boundary Harm from Hazardous Activities that states that the standard of due diligence to assess the conduct of a state would be that which would be deemed «appropriate and proportional to the degree of risk of trans-boundary harm in the particular instance» (2001) A/56/10, 154.

[40] Also noteworthy is the OEWG Working paper, Multiple states' views on best practices relating to the implementation of norm 13(c), 2024, 2, which clarifies context and content of the *due diligence* principle, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/OEWG_Working_paper_-_Best_practices_relating_to_the_implementation_of_norm_13(c).pdf.

[41] See GGE, Report of the 2019-2021, UN Doc. A/76/135, par. 30 a.

As anticipated, this prohibition is regulated in Art. 2, para. 4 of the UN Charter and in numerous Declarations of principles of the UN General Assembly. They define the interpretative and applicative contours of the prohibition of the use of force, and the threat of the use of force, in international relations[42]. Initially, the ban was recognized as a norm of conventional international law, but subsequently the ICJ recognized its nature as both a customary norm and as a *jus cogens* norm[43]. The only agreed exception to the prohibition in question is the individual and the collective legitimate defense, which is regulated by Art. 51 of the UN Charter[44].

Specifically, the use of armed force implies a violation of Art. 2, para. 4 of the UN Charter if it reaches a certain threshold in terms of extent, duration and physical destruction, as stated by the ICJ. The Court distinguished the most serious forms of use of force - qualified as an armed attack - from the less serious forms, qualified as a mere use of force, such as border clashes/incidents[45]. The Ethiopia-Eritrea Complaints Commission reached a similar assessment in its decision (2005), in which it stated that minor border incidents, while constituting a violation of the rules relating to the prohibition of the use of force, are not comparable to an armed attack and, therefore, do not give the right to react in self-defense[46].

---

[42] On this topic see the contributions of V. STARACE, *Uso della nell'ordinamento internazionale*, in *Enciclopedia Giuridica*, vol. XXXII, Roma, 1994, 1 ff; B. SIMMA (ed.), *The Charter of the United Nations, A Commentary*, 2° ed., vol. 1, Oxford, 2002, 794; A. CASSESE, *International Law*, Oxford, 2005, 56; P. GARGIULO, *Uso della forza (Diritto internazionale)*, in *Enciclopedia del Diritto*, *Annali*, vol. V, Milano, 2012, 1376-1430; A. LANCIOTTI, A. TANZI, *Uso della Forza e legittima difesa nel diritto internazionale contemporaneo*, Napoli, 2012; O. GÖRR, *Use of Force, Prohibition of*, in *Max Planck Encyclopedia of Public International Law*, Oxford, 2019, 1; B. CONFORTI, M. IOVANE, *Diritto internazionale*, Napoli, 2022, 209; E. CANNIZZARO, *Diritto internazionale*, Torino, 2022, 21; U. VILLANI, *Lezioni di diritto internazionale*, Bari, 2023, 243.

[43] *Nicaragua* case, cit., parr. 65, 99 s., 109, 115 e 190. See M.N. SCHMITT, M. WELLER, (eds.), *The Use of Cyber Force and International Law, The Oxford Handbook of the Use of Force in International Law*, Oxford, 2015, 1110; D. AKANDE, A. COCO, T. DE SOUZA DIAS, *Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies*, in *International Law Studies*, 2022, 4.

[44] V. M. HOISINGTON, *Cyberwarfare and The Use of Force Giving Rise to The Right of Self-Defense*, in *Boston College International and Comparative Law Review*, 2009, 439-440; O. KESSLER, W. WERNER, *Expertise, Uncertainty, and International Law: A Study of the Tallinn Manual on Cyberwarfare*, in *Leiden Journal of International Law*, 2013, 807.

[45] ICJ, *Nicaragua* case, cit., 101, para. 191.

[46] See Eritrea Ethiopia Claims Commission, Partial Award, *Jus ad Bellum*, Ethiopia's Claims 1-8, December 19, 2005, para. 11; see N. RONZITTI, *Diritto internazionale dei conflitti armati*, 6° ed., Torino, 2017, 37.

Specifically, given the *sui generis* nature of the digital domain regarding the maintenance of international peace and security, it is necessary to verify the outcome of the application of the existing obligations of international law, that have been shaped for the physical world. The issue primarily concerns the qualification of a transnational malicious cyberoperation as an "armed attack", considering that, according to the ICJ, only the most severe forms of force, in terms of intensity and gravity, and physical destruction can be classified as such[47].

In the absence of an official definition of a cyber-attack in international law, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (hereinafter, Tallinn Manual 2.0) provides useful guidance. In digital space, crossing the threshold of the use of force depends not on the target of the attack (the target-based approach), nor on the digital means employed, that are digital codes (the weapons-based approach), but rather on the effects of the cyberoperation from a *quantitative* and *qualitative* perspective (the so-called *effects-based approach,* Rule 92).

In the *quantitative* approach, the *Manual* (Rule 69) suggests that a cyberoperation constitutes a violation of the prohibition on the use of force if its *scope* and *effects* are comparable to those of a "above threshold" kinetic operation[48]. Additionally, about the weapon used, in the ICJ advisory opinion on the *Lawfulness of the Threat or Use of Nuclear Weapons* (1996), the prohibition on the use of force is regardless of the type of weapons used, since this prohibition refers to any type of force, even immaterial[49].

Regarding the *qualitative* approach, the *Tallinn Manual 2.0* specifies that for a malicious cyberoperation to be considered an armed attack, damage to tangible and intangible assets (including digital data) must be such - or may reasonably likely be as such - that

---

[47] On this topic see Y. DINSTEIN, *Computer Network Attacks and Self-Defense*, in M.N. SCHMITT, B.T. O'DONNELL (eds.), *Computer Network Attack and International Law*, 2002, 38, https://digital-commons.usnwc.edu; D.B. SILVER, *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter*, in *International Law Studies Series US Naval War College*, 2002, 73; M. ROSCINI, *Cyber operations as a use of force*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research Handbook*, cit., 301 ff.

[48] See ICJ, case *Oil Platforms*, (*Islamic Republic of Iran* v. *United States of America*), Judgment of November 6, 2003, *ICJ Reports*, 2003, par. 51 and 72, which does not exclude the possibility that even a single attack (such as one against a warship), could justify the exercise of the right to self-defense.

[49] See S. LA PISCOPÌA, *Necessità di una definizione delle armi cibernetiche*, in *Eurasia*, 2022, 37, and in this book, ID., *The Regulatory Relevance*, cit.

it alters their normal use and functioning that could lead to the death and wounding of people or the destruction of property. An example would be tampering with the ICT systems of critical infrastructures, particularly in the operational technology (OT) sector, such as dams, electrical grids, or nuclear power plants. Malfunctions or tampering in these areas could cause widespread destruction or fires, resulting in physical effects—both direct and indirect—on the civilian population and the security of a state. To this end, it is advisable that the requirement of *kinetic equivalence* is respected, that is if a malicious operation causes – or is reasonably likely to cause - deaths, injuries, and significant material damages comparable to those normally resulting from an kinetic armed attack. For example, consider tampering with the IT systems of a dam downstream of a densely populated area, which results in the dam's opening and subsequently leads to the destruction of the inhabited areas and the death of the residents.

The first instance of this type of operation occurred following the *Stuxnet* attack in 2010, which was likely carried out with the aim of disrupting Iran's nuclear program. In this case, the introduction of a virus called Stuxnet into the computer system of the Natanz nuclear power plant in Iran caused the 1,000 cooling turbines of the plant to malfunction, leading to the shutdown of the facility[50]. This event highlights the *potential* consequences in the physical world if the cyber sabotage had not been limited to merely disabling the turbines, but instead had been aimed at causing an explosion at the nuclear power plant.

5. Once the cyberoperation has been qualified as a violation of a norm of international law, it should be attributed to a state eventually to declare its international responsibility. The activity of determining the responsibility for a cyber activity or operation to a state - called

[50] For Y. DINSTEIN, *War, Aggression and Self-Defence*, 5° ed., Cambridge, 2011, 105, «[T]he most egregious case is the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighboring areas are densely populated. In all these cases, the Computer Network Attack would be deemed an armed attack». See D.B. HOLLIS, *Could Deploying Stuxnet Be a War Crime?*, in *OpinioJuris.org*, 2011; S. HAATAJA, N. SAMULI, A. AKHTAR-KHAVARI, *Stuxnet and International Law on the Use of Force: an Informational Approach*, in *Cambridge International Law Journal*, 2018, 79; P. SINGER, *Stuxnet and Its Hidden Lessons on The Ethics of Cyberweapons*, in *Case Western Reserve Journal of International Law*, 2015, 132.

attribution - is a complex procedure due to the near-complete anonymity provided by cyberspace and other technical issues, especially when the cyberoperation has been committed by non-state actors. Attribution is a state's prerogative and involves establishing the connection between an agent's conduct (action or omission) and a state. This process involves three distinct sub-procedures: the technical sub-procedure, the legal and the political one.

The challenges of technical attribution in cyber activities revolve around identifying technical indicators and collecting the evidence that are needed to attribute cyber conduct to a state.

The *technical sub-procedure* involves a factual investigation aimed at identifying, with a certain degree of certainty, the source and the author of a cyberoperation, the associated network infrastructure, and the cyber tools used. It is based on a scientific examination of the digital and factual evidence of the conduct.

The identification of the source or the computer(s) used by the criminal hacker is possible identifying its Internet Protocol (IP) that gives also its location, while it is very difficult to identify the person operating it. This may be established thanks to confidential information disclosed by the intelligence agencies that may act alone or in cooperation with cyber security companies. It is well known that criminal hackers use sophisticated techniques to erase identifying evidence (fingerprints), and to obscure the source of the attack, and they orchestrate additional attack phases at different times and from various network infrastructures across multiple states[51]. For example, they anonymize their IP addresses using The Onion Router (Tor) and Virtual Private Networks (VPNs), and they encrypt their communications using servers, that can be located in a third country[52].

---

[51] See The NATO Cooperative Cyber Defence Centre of Excellence, *Mitigating Risks Arising from False-Flag and No-Flag Cyber Attacks*, https://ccdcoe.org, that states «[I]t is not enough to just locate a source IP address (unless looking solely at active defence): the identity of the attackers must be determined, as well as the parties they were acting on behalf of must also be unmasked». R. Cohen, *Cyberspace as/and Space*, in *Columbia Law Review*, 2007, 210 ff.; E. JENSEN, *Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense*, in *Stanford Journal of International Law*, 2002, 207; E.D. GRAHAM, *Cyber Threats and the Law of War*, in *Journal of National Security Law and Policy*, 2010, 89; H. PIHELGAS, *Back-Tracing and Anonymity in Cyberspace*, K. ZIOLKOWSKI (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCDCOE Publication, Tallinn, 2013, 31, https://ccdcoe.org; N. TSAGOURIAS, *The Legal Status of Cyberspace*, N. TSAGOURIAS, R. BUCHAN (eds), *Research Handbook*, cit., 13 ff.

[52] See S. KANUCK, *Sovereign Discourse on Cyber Conflict Under International Law*, in *Texas Law Review*, 2010, 1573–5; D.D. CLARK, S. LANDAU, *Untangling Attribution*, cit., 530;

Another example is when malicious cyberoperations are conducted by one or more bot-masters who infiltrate network infrastructures in different states to coordinate simultaneous malicious activities against a target state using botnets (employing IT systems owned by third parties). In such cases, it is extremely challenging to trace the bot-master, especially when actions cross multiple jurisdictions[53].

Additionally, malicious cyberoperations can be intentionally falsely attributed by criminal hackers to an APT (that usually is state sponsored) through the spoofing techniques, for instance using malware codes that have been previously employed by the APT thus creating a *false flag* operation. Such operations pose the risk of prompting the victim state to react against an innocent third state.

Once the perpetrator has been identified based on the available digital evidence, the *legal sub-procedure* establishes the degree of the international responsibility of the state that has directed, orchestrated or sponsored the cyberoperations.

In this context, it might arise the issue of the lack of sufficient evidence due to the *sui generis* nature of cyberspace.

According to the UN General Assembly, the indication that a cyber illicit activity can be traced back to or originates from the territory of a state (or its network infrastructures), or that the codes appear traceable to that state, may not constitute sufficient evidence to attribute the operation to the state[54]. For the ICJ «claims against a State involving charges of exceptional gravity must be proven by

---

J.S. DAVIS II, *Stateless Attribution: Toward International Accountability in Cyberspace*, in *UCLA Law Review,* 2017, 9, www.rand.org; C. PAYNE, L. FINLAY, *Addressing Obstacles to Cyber-Attribution: A Model Based on State Response to Cyber-Attack*, in *George Washington International Law Review*, 2017, 49 ff.

[53] See P. ROGUSKI, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, in *Policy Brief, The Hague Program for Cyber Norms*, 2020, https://www.thehaguecybernorms.nl.

[54] UN General Assembly, Resolution on the *Developments in the Field of Information and Telecommunications in the Context of International Security*, December 11, 2018, UN Doc. A/RES/73/27, par. 1.2. See *Tallinn Manual 2.0*, cit., 82 and 91; M.J. SKLEROV, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses Against States Who Neglect Their Duty to Prevent*, in *Military Law Review*, 2009, 12, that affirms the objective State's responsibility; W. HEINTSCHEL VON HEINEGG, *Territorial Sovereignty and Neutrality in Cyberspace*, in *International Law Studies*, 2013, 123; M. ROSCINI, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, in *Texas International Law Journal*, 2015, 233 ff; M. FINNEMORE, D.B. HOLLIS, *Beyond Naming and Shaming*, cit., 571 ff.

evidence that is fully conclusive»[55]. Although in some cases an additional problem might arise due to the lack by developing states of the necessary technological resources and expertise to conduct the technical attribution process effectively.

A solution has been proposed by the GEE that encourages states to facilitate the tracing of hostile activities on critical information infrastructures and, when appropriate, disclose this information to other states. In case of an ICT incident, the affected state should notify the state from which the hostile activity is emanating, although the receiving of the notification does not imply the acknowledgment of the responsibility on the receiving state[56].

At the conclusion of these two sub-procedures, the state decides whether to declare (publicly or otherwise) the responsibility of the state actor for the sponsorship or direction of the cyberoperation (the political *sub-procedure*)[57].

6. In international law attribution is «the operation of attaching a given act or omission to a State» and to this end it is worth mentioning the Draft Articles on the Responsibility of States for Internationally Wrongful Acts of 2001 (herein after ARSIWA), developed by the UN International Law Commission, that relies on the relationship between individuals with a particular state[58]. In this regard, the ARSIWA's

[55] ICJ, case *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, (*Bosnia and Herzegovina* v. *Serbia and Montenegro*), Judgment February 26, 2007, *ICJ Reports*, 2007, parra. 43, 208 and 90; case *Oil Platforms*, cit., parr. 161, 189 e 190, and see the separated opinion of Judge R. Higgins that states that «the more grave the charge the more confidence there must be in the evidence», parra. 30-39. See the states' positions in GEE, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution* 73/266, July 13, 2021, 84, UN Doc. A/ 76/136. See A. GHAPPOUR, *Tallinn, Hacking, and Customary International Law*, in *American Journal of International Law Unbound*, 2017, 224; J.N. MADUBUIKE-EKWE, *Cyberattack and the Use of Force in International Law*, in *Beijing Law Review,* 2021, 223 ff.

[56] See OEWG *Report 2021*, cit., para. 71 (g).

[57] See E.M. MUDRINICH, *Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem*, in *Air Force Law Review*, 2012, 167; K. EICHENSEHR, *The Law & Politics of Cyberattack Attribution*, in *University of California Los Angeles Law Review*, 2020, 67; N. TSAGOURIAS, M.D. FARRELL, *Cyber Attribution: Technical and Legal Approaches and Challenges*, in *European Journal of International Law*, 2020, 941.

[58] See *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, in *Yearbook of the International Law Commission*, 2001, vol. II, Part 2, 26 ff and 47 f. See C. ANTONOPOULOS, *State Responsibility in Cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.),

rules might be applied to malicious operations carried out in cyberspace, given the customary nature of most of them, although with certain difficulties.

To satisfy the evidentiary requirements for the attribution procedure it is fundamental to identify the link between the non-state actors that conducted the cyberoperation and the state that has organized, sponsored, or coordinated them. As already said, states are *outsourcing* military activities in cyberspace to avoid direct responsibility for violating the prohibitions of international law, like the practices seen in the sponsorship of international terrorism.

In the ARSIWA it is affirmed that the international responsibility of a state arises when the international offense is committed by its officials or, in specific cases, by private citizens. Specifically, Article 4 of the ARSIWA addresses conduct carried out by state bodies in an official capacity as *de jure* state organs[59]. For example, this includes malicious cyberoperations conducted by the National Cyber Security Center or by intelligence and military combat units organized[60].

According to Article 5 of the ARSIWA, the international responsibility of a state can also be asserted if persons or entities exercise governmental functions act on its behalf [61].

Additionally, under Article 11 of the ARSIWA, a state is internationally responsible for acts carried out by non-state actors if it recognizes these acts as its own, as confirmed by the ICJ's jurisprudence[62], and, *ex* Article 8 of the ARSIWA, a state is

---

Research Handbook, cit., 113 ff; A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023, 119 ff.

[59] See Art. 4, para. 1, of the ARSIWA, cit., named "Conduct of organs of a State", reads: «[T]he conduct of any State organ shall be considered an act of that State under international law, whether the organ exercises legislative, executive, judicial or any other functions, whatever position it holds in the organization of the State, and whatever its character as an organ of the central Government or of a territorial unit of the State». See Rule 15 of the *Tallinn Manual 2.0*, cit.

[60] See U.S. Congressional Research Service, *Russian Cyber-Units*, 2022, https://crsreports.congress.gov.

[61] Under Art. 5 of the ARSIWA, cit., named "Conduct of persons or entities exercising elements of governmental authority", «[T]he conduct of a person or entity which is not an organ of the State under article 4 but which is empowered by the law of that State to exercise elements of the governmental authority shall be considered an act of the State under international law, provided the person or entity is acting in that capacity in the particular instance»; see Rule 15, *Tallinn Manual 2.0*, cit.

[62] According to Art. 11 of the ARSIWA, cit., "Conduct acknowledged and adopted by a State as its own", states that: «[C]onduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its

responsible if it provides non-state actors with instructions for carrying out operations, or if it directs or controls them. In this case, non-state actors or entities are 'elevated' to *de facto* state agents or organs[63].

For the ICJ the *de facto* states organs can be identified as «persons, groups of persons or entities [that], may for purposes of international responsibility, be equated with state organs even if that status does not follow from internal law», if they «act in 'complete dependence' on the respondent State of which they are ultimately the instrument». It means that a state must exercise effective control through instructions over each individual operation and throughout the entire duration of the operation (the "effective control" test)[64].

This might establish a scenario of 'indirect' aggression, as outlined in the UN General Assembly's resolution on the definition of aggression (Resolution 3314(XXIX))[65].

---

own». Regarding the case of the *United States Diplomatic and Consular Staff in Tehran*, (*United States of America* v. *Islamic Republic of Iran*), judgment of May 24, 1980, *CIJ Reports*, 1980, Ayatollah Khomeini had approved the occupation of the American embassy and consulate premises and the taking of the staff hostages by Islamic students among the 1979 and 1981. Thus, according to the ICJ, in this case, «[T]he approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State. The militants, authors of the invasion and jailers of the hostages, had now become agents of the Iranian State for whose acts the State itself was internationally responsible», par. 74.

[63] Art. 8 of the ARSIWA, named "Conduct directed or controlled by a State", affirms: «[T]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct». See Rule 17, a), of the *Tallinn Manual 2.0*, cit.; M.N. SCHMITT, L. VIHUL, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution*, in *Fletcher Security Review*, 2014, 53; K. MAČÁK, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors*, in *Journal of Conflict and Security Law*, 2016, 405; W. BANKS, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, in *Texas Law Review*, 2017, 1487 ss.

[64] ICJ, *Nicaragua* case, cit., parr. 64 f, 106, 109, 112, 115, and the case on *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, cit., parr. 201, 205, 211-215, 396, and 400-407. For M.N. SCHMITT, *Tallinn Manual 2.0*, cit., 328, "[T]he Court sees no reason to deny that, in customary law, the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces Nicaragua", 93 par. 195. See also L. BLANK, *International Law and Cyber Threats from Non-State Actors*, in *Israel Yearbook on Human Rights*, 2013, 111.

[65] See UN General Assembly, Resolution on the definition of aggression (Resolution 3314(XXIX)) adopted by *consensus* on December 14, 1974, Art. 3. On this topic see C. KRESS, *Gewaltverbot und Selbstverteidigungsrecht nach der Satzung der Vereinten Nationen*

On this topic a different approach was taken by the Appeals Chamber of the UN *ad hoc* International Criminal Tribunal for crimes committed in former Yugoslavia in the *Tadić* case (1999). The Tribunal held that acts carried out by a military or paramilitary group could be considered acts of *de facto* organs of the state, thereby implicating the state's responsibility, if the group is under the overall control of the state. This approach (known as the "overall control" test) applies beyond «the mere financing or equipping […] and involv[es] also participation in the planning and supervision of military operations»[66].

It should be noted that these two approaches to legal attribution (the effective control and the overall one) are both challenging to be satisfied due to the technical difficulties in demonstrating the factual connection between the state and criminal hackers. As a matter of fact, a cyberoperation rarely can be reliably attributed, as it often can be only geolocated. Specifically, it is difficult to demonstrate a state's effective control over the hacker groups if it is based on factors such as the provision of weapons, training, intelligence sharing, target selection, operational, logistic and financial support, and the guarantee of a safe haven in the state's territory[67]. All these requirements for evidence are difficult to prove due to the intangible nature of ICT tools, to the virtual nature of training, to the encrypted communications, and to the use of cryptocurrencies to provide economic support, which are often untraceable, just to cite a few.

---

bei staatlicher Verwicklung in Gewaltakte Privater, Berlin, 1995, 314–19, who supports the existence of a *lex specialis* on attribution based on the 'substantial involvement-limb' in Art. 3(g) of the 1974 Definition of Aggression.

[66] See International Criminal Tribunal *ad hoc* for crimes committed in the Former Yugoslavia, Appeals Chamber, *Prosecutor* v. *Tadić*, Case No IT-94-1-A, Judgment July 15, 1999, 118-122, 131, 137, 145, and 154. In this case the Appeals Chamber found that Serbia had supported and coordinated the general planning of the military activity of the Bosnian Serb paramilitary troops materially and with funding. For the Appeals Chamber a state «wields overall control over the group, not only by equipping and financing the group, but also by coordinating or helping in the general planning of its military activity». In this case, «it is not necessary that, in addition, the State should also issue, either to the head or to members of the group, instructions for the commission of specific acts contrary to international law», par. 131. See Y. DINSTEIN, *War, Aggression*, cit., 104.

[67] UN General Assembly, January 22, 2001, invites member states to «eliminate safe havens for cybercriminals», par. 1(a), U.N. Doc. A/RES/55/63, and ICJ, *Nicaragua* case, cit., parr. 95-97, 99, 104, 106, 109, 112, 115. W. BANKS, *State Responsibility*, cit., 1490. On the notions of effective, general and indirect control operated by the State on *de facto* agents and which has emerged in international law and jurisprudence, see J. KURBALIJA, *State Responsibility in Digital Space*, in *Swiss Review of International and European Law*, 2016, 15.

Additionally, there is often a lack of will on the part of states to control the activities of online criminal groups. This reluctance is due to outsourcing of the commission of malicious cyberoperations that partly occurs because states lack the necessary technological tools, expertise, or the capability to keep pace with the rapid developments in information technology.

According to the UN Working Group on Mercenaries, this 'dissociation' of cyberoperations from the states that coordinate them makes it difficult to identify the responsible entities, the scope of the operations, their material and temporal dimensions, unlike what happens in the case of kinetic military or paramilitary operations.

Considering the technical and legal challenges in gathering evidence to attribute the actions of hacker groups to a state, a 'overall digital control' regime would be advisable[68]. This regime relies on the degree of the organization and coordination of the entire cyber-operation, and it is in line with the UN non-binding norms which states that, for the purposes of attributing cyber incidents, states should consider «all relevant information, including the larger context of the event, the challenges of attribution in the Information and Communication Technology (ICT) environment, and the nature and extent of the consequences» (para. 13, letter b)[69].

In this vein, the 2021 GGE report acknowledges the complex nature of the attribution process, noting that «a broad range of factors should be considered before establishing the source of an ICT incident»[70]. The report adds that these factors must be substantiated by factual elements related to the extent and technical characteristics of the operation, its target, the impact on international peace and security, and the outcome of consultations between states, with particular regard to the obligation of peaceful resolution of international disputes.

This might have been the outcome of the attribution to Iran of the cyber-attacks to Albania that, after attributing them to Iran, preferred to declare members of the Iranian diplomatic corps *personae non grata*, rather than reacting in self-defense, probably due to uncertainty

[68] See C. ANTONOPOULOS, *State Responsibility in Cyberspace*, cit., 123, for whom attribution may rest on a presumption that introduces a reversal of the burden of proof.

[69] See OEWG *Report 2021*, cit., 7.

[70] See GEE *Report 2021*, cit., parr. 23-25.

in evidence[71]. This response aligns with the caution advised by the GGE within the UN, to avoid the risk of military escalation between states[72].

7. The evolving landscape of cyberoperations and the increasing offensive capabilities of non-state actors necessitate an adaptive approach by international cyber law. The traditional understanding of armed attacks, rooted in the physical effects of armed force as outlined in the UN Charter, must evolve to encompass the complex and often intangible damages caused by cyber activities. This includes the disruption of critical infrastructures, alteration and cancellation of digital data, and the potential for widespread harm to national security and to international peace and security[73].

To address these challenges, a new multidimensional concept of armed attack in cyber space is essential. This concept should also account for emerging threats such as the malicious use of artificial intelligence and hybrid warfare[74]. It is also necessary to draft an international regulatory framework to hold the private military companies accountable for their illicit activities[75]. This framework should also provide guidelines on the pertaining jurisdiction.

Additionally, the development of a detailed taxonomy of cyber-attacks and clear attribution criteria is crucial. Such criteria should be based on uniform and impartial evidentiary standards to support fair and accurate attribution.

This will ensure a transparent and credible attribution process that will facilitate a global understanding of state practices in cyberspace. Moreover, the UN's initiative to create specific discussion subgroups and Points of Contact (PoC) directories will enhance cooperation and

---

[71] See DEUTSCHE WELLE, *Albania Blames Iran for Cyberattacks*, 16 September, 2022, https://www.dw.com; https://www.reuters.com/world/albania-cuts-iran-ties-orders-diplomats-go-after-cyber-attack-pm-says-2022-09-07/.

[72] See GEE *Report 2021*, cit., par. 22 ff and 71 (g).

[73] See G. CORN, *Sovereignty in the Age of Cyber*, in *American Journal of International Law Unbound*, 2018, 207; P. MICHAEL, F. ISCHERKELLER, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, 2023, https://ndupress.ndu.edu.

[74] SEE OEWG *Report 2022*, cit., parr. 15, a), and 9. On this topic see F.G. HOFFMAN, *Conflict in the 21st Century: The Rise of Hybrid Wars*, 2007, www.potomacinstitute.org; M. CLARK, *Russian Hybrid Warfare*, 2020, https://www.understandingwar.org; G. SIMONS, Y. DANYKM, T. MALIARCHUK, *Hybrid War And Cyber-Attacks: Creating Legal and Operational Dilemmas*, *Global Change*, in *Peace & Security*, 2020, 337 ff; NATO, *NATO's Response to Hybrid Threats*, 2021, www.nato.int.

[75] See OEWG, *Report 2024*, cit., 2.

coordination among states, reducing the risk of misunderstandings and unintended escalations of incidents in international crisis in cyber space[76]. On this topic the OEWG suggests the use by states of multilateral, regional, bilateral platforms to share information on national approaches to attribution, including how states can distinguish between different types of attribution, and ICTs' threats and incidents[77].

It is worth noting the recent proposal of the Program of Action by the UN, along with the suggestion for a Permanent Mechanism by the OEWG's Chair, that underscores the need for continuous dialogue and regulatory oversight[78]. These initiatives aim to establish a robust framework for the application of international law in the context of ICTs use, particularly in response to state-attributable malicious cyber activities.

In conclusion, the international community must work towards developing a uniform legal framework in completion with the recently adopted UN convention against cybercrime[79]. In the meantime, by operationalizing the UN non-binding norms on responsible behavior in cyberspace, states can effectively and efficiently enhance cybersecurity and promote international peace and security in the digital domain[80].

In this context, it is essential to consider the positions of non-Western countries governing the conduct in cyber space because the predictability of states' behavior might clarify the consequences of

---

[76] See GEE, *Report 2021*, cit., para 77 ff; OEWG, *Report 2022*, cit., 5.

[77] See Letter from OEWG Chair of May 29, 2024. Let it permitted to cite A.L. SCIACOVELLI, *Reflexions on the Hostile Activities in Cyberspace and the International Legal Landscape Promoted by the United Nations*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana OSORIN*, 2024, www.osorin.it.

[78] Letter from the Chair of the OEWG on Security of and in the Use of Information and Communications Technologies, 2021-2025, February 20, 2024, 6. On this aspects see B. ALERIANO, B. JENSEN, *De-escalation Pathways and Disruptive Technology: Cyber Operations as Off-Ramps to War*, in S. Shackelford, F. DOUZET, C. ANKERSEN (eds.), *Cyber Peace: Charting a Path Toward a Sustainable, Stable, and Secure Cyberspace*, Cambridge, 2022, 64-93; M. WALZER, *Cyber Warfare, Media Warfare, and Lawfare*, in M. GROSS, T. MEISELS (eds.), *Soft War: The Ethics of Unarmed Conflict*, Cambridge, 2017, 77 ff.

[79] See UN General Assembly, UN Convention Against Cybercrime, August 7, 2024, UN Doc. A/AC.291/L.15.

[80] GEE, *Official Compendium of Voluntary National Contributions*, cit.; UN *Program of Action to Advance Responsible State Behavior in the Use of Information and Communications Technologies in the Context of International Security*, October 13, 2022, UN Doc. A/C.1/77/L.73. See K. MAČÁK, F*rom Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers*, in *Leiden Journal of International Law*, 2017, 879.

unlawful state behavior in cyberspace and reduce the risk of miscalculation in attributing cyber activities.

THE REGULATORY RELEVANCE OF THE FIFTH DOMAIN'S WEAPONS DEFINITION

SEBASTIANO LA PISCOPÌA*

1. «The development of new technologies makes it more difficult to identify what constitutes a "weapon"»[1].

This statement, could seem, *prima facie*, the result of a consideration bordering on the obvious, but it highlights, upon closer analysis, the depth of thought of the most established international doctrine which, starting from the «virtual concreteness» of cyber warfare, crystallizes the cogency of a serious, current and unescapable problem: the definition of cyber weapons.

As recalled in the literature[2], just because a cyber attack does not equate to an armed attack, it does not mean that international law does not have regulatory tools to counteract such violations. The interference with the economic sphere, air, sea or territorial space of a state, even if not prohibited by international law, it is prohibited under the general principle of non-intervention. This point clearly appears in various treaties, United Nations resolutions and decisions of the International Court of Justice, which condemn coercion, interference or intervention that does not involve the use of force[3].

However, in the cyber realm, the most pressing issue concerns cyber operations that constitute the use of force.

---

* The author expresses here his own personal analyses and considerations as a free scholar. Therefore, his views do not represent those of the Italian Ministry of the Defence, which disclaims any responsibility, nor those of the academic or legal institutions to which he belongs.

[1] F. DELERUE, *Cyber Operations and International Law*, Cambridge, 2020, 286.

[2] A. SHULL, *Cyber Espionage and International Law*, GigaNet: Global Internet Governance Academic Network, Annual Symposium, Bali 2013, July 17, 2016, 6, note 18.

[3] M. E. O'CONNELL, *Cyber Security without Cyber War*, in *Journal of Conflict & Security Law*, CLXXXVII/2, 2012, 187, 202.

In more detail, before analysing the related legitimacy profiles, it would be appropriate to analyse the offensive threshold[4], verifying whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law.

As known, the art. 2 para 4 of the United Nations Charter[5] prohibits both, the use of force and the mere threat of its use. The term «force», in fact, appears both in the Preamble of the Charter and in Articles 41 and 46, but it is the Art. 44[6], which refers clearly to the «armed force» and that allows an overall reading with the Art. 31, para. 1 of the Vienna Convention on the Law of Treaties (1969)[7].

As we remember, in fact, the principle of non-intervention, which also extends to other instruments of coercion, or of international pressure, is quite different from the use of force pursuant to the aforementioned Art. 2 para. 4.

It is noted, in this regard, that the main analytic approaches regarding the relevance of applicability of the above mentioned Art. 2 para. 4 to cyber operations[8] are:

- the *instrument-based approach*, that focus on the means used to carry out the attack, which has its clear limits in the inherent physical characteristics of the used means;

- the *target-based approach* that argues that cyber operations reach the threshold of the use of armed force when they are conducted against the so-called national critical infrastructures, which has its discussed limits in the vagueness resulting from the different national definitions and in the related excessive inclusiveness (up to the indefinite threshold of inconvenience for the civilian population);

---

[4] A. L. SCIACOVELLI, *International Law Aspects of Information Warfare in the Digital Age*, in *La Comunità Internazionale*, 2023, 197 ff.

[5] «All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations».

[6] «The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations».

[7] Vienna Convention on the Law of Treaties, 23 May 1969, art. 31: «1. A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose».

[8] M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014, 46-48.

- the *effect-based approach* focused on the effects of the action that recalls the *kinetic equivalence principle* according to which, if the effects of the cyber operation are comparable to those achievable by the use of kinetic force, then they violate Art. 2, para 4 of the UN Charter.

In this regard, while respecting the relevance of the eight factors allegedly not legal, identified by Michael Schmitt[9], to guide the identification of a plausible kinetic equivalence (*i.e.*, severity, immediacy, directness, invasiveness, measurability of effects, military character, state involvement and presumptive legality, it seems justified to state that, from a legal point of view), it must be the instrument used to identify the nature of the operation.

If this instrument reaches the threshold of offensiveness of a cyber weapon, then there arises the need to define it and pending an international agreed definition that uniquely identifies what a cyber weapon is, it would seem acceptable to describe it as a «mean used or designed to commit acts of violence against enemy forces or material assets»[10].

Indeed, in accordance with the advisory opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons[11], it is believed that Articles 2 para 4, 51 and 42 of the UN Charter do not refer to some specific weapons, but should apply to any use of force, regardless of the weapons used.

In this regard, the international debate on the issue offered other plausible and more detailed definitions of cyber weapons such «software and information technology (IT) systems that, through ICT networks, cause destructive effects and have no other possible uses»[12].

This definition, starting from the assumption of the typical *dual use* nature of cyber weapons, theorized the possible use of the definitional criterion adopted by the international conventions on the prohibition of biological and chemical weapons.

---

[9] M. N. SCHMITT, *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, 334-336.

[10] *See* International Committee of the Red Cross (ICRC), *Customary International Humanitarian Law: Interpretive Guidance*, Cambridge, 2005.

[11] International Court of Justice, *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, 8 July 1996, ICJ Reports 1996, para. 39.

[12] T. UREN, B. HOGEVEEN and F. HANSON, *Defining offensive cyber capabilities*, Australian Strategic Policy Institute website, 2018, www.aspi.org.au/report/defining-offensive-cyber-capabilities.

These last, as known, represent dual use[13] weapons of mass destruction and belong to the physical domain[14]. This criterion represents a sort of *trait d'union* between the destructive power of such weapons and the inability to use them for peaceful uses.

This doctrinal position – which opens up to an approach based on the «method of the previous», typical of the organizational sciences – has the credit of identifying some interesting assumptions that opens to a wider international debate.

Thomas Rid, despite his sceptical view, having a similar approach starting from the engineering of the tool, defines a cyber weapon as «a computer code that is used, or designed to be used, with the aim of threatening or causing physical, functional, or mental harm to structures, systems, or living beings»[15].

It does appear relevant to observe, moreover, that even the Tallinn Manual[16], does not literally mention cyber weapons in Rule 110 (weapons review), specifying, only in the subsequent comments, that «This rule extends to any cyber weapon acquired or used by a State. It encompasses, *inter alia*, cyber weapons designed as such that are procured by States, cyber weapons developed by the armed forces in order to exploit vulnerabilities, and malicious software not originally developed for military purposes that is subsequently acquired by States for use in armed conflict».

In this regard, it is useful to highlight that no shared definition has been coined by international experts, but it is even more interesting to observe that, in this part of the Manual (that deals with the *ius in bello* and specifically to the conduct of hostilities[17]), a cyber weapon is described just in the comment to the rule.

More precisely, the comment states: «This rule extends to any cyber weapon acquired o used by a State. It encompasses, *inter alia*, cyber weapons designed as such that are procured by States, cyber weapons developed by the armed forces in order to exploit vulnerabilities, and malicious software not originally developed for

[13] Unlike nuclear weapons.

[14] Which includes small arms and light weapons, conventional weapons and weapons of mass destruction. *See* United Nations Office of Disarmament Affairs, https://disarmament.unoda.org/wmd/.

[15] T. RID, *Cyber War Will Not Take Place*, Glasgow, 2017, 37.

[16] M. N. SCHMITT, *Tallin Man.*, cit., Rule 110, 464 ff.

[17] Extended to both kind of conflicts of the Additional Protocol I and II to the Geneva Conventions.

military purposes that is subsequently acquired by States for use in armed conflict».

This point, as better clarified hereafter, characterizes these offensive tools, starting from their potential dual use peculiarity.

This approach assumes great relevance, as it clearly highlights the possible emerging critical issues in the field of arms counter-proliferation, underlying the compelling need to define these kind of weapons.

In this context, it seems reasonable to believe, according with Marco Roscini[18] that the use of armed force requires the use of a weapon and that, therefore, it is necessary to answer to the question of whether worms, viruses, botnet codes and other malware can be considered real weapons[19]. Even taking into account the foresight of international humanitarian law towards the «incoming weapons», the answer to the above-mentioned question is directly related to the concrete use of the potential cyber weapons.

Taking into account Rule 92 of the Tallinn Manual, which defines a cyberattack as an offensive or defensive operation that could reasonably cause personal injury or death, or damage or destruction to tangible property[20], it is necessary to carefully take into account the danger threshold and the destructive capacity of these weapons.

The need for this caution is related to their possible use on dual use targets, such as power plants, nuclear power plants or oil pipelines, dams, hospitals, aqueducts, swing bridges, air, rail or subway traffic control systems *etc*.

2. There are school scenarios that attempt to define the so-called limit measurement that identifies the difference between a cybernetic intrusion which, for example, temporarily blocks the supply of electricity, from a real cyber attack that creates serious damage to vital infrastructure and loss of human life[21].

---

[18] M. ROSCINI, *op. cit*., 49.

[19] Y. DINSTEIN, *The conduct of hostilities under the law on international armed conflicts*, 2nd edition, Cambridge, 2010, 1.

In this regard, the author defined weapons as any weapon, ammunition and other devices, components or mechanisms intended to destroy, disable or injure enemy personnel, tangible assets or property.

[20] M. N. SCHMITT, *Tallin Man.*, cit., 415.

[21] R.W. ALDRICH, *The International Legal Implications of Information Warfare*, US Airforce Academy, Colorado, 1996, where a physical manifestation of the effects such as an explosion is deemed necessary.

https://apps.dtic.mil/sti/pdfs/ADA365379.pdf.

It should also be noted that in the realm of the fifth dimension, it is extremely complex to compose a modern regulatory framework that can adapt itself in a «modular way» to cyber offensive operations.

The reason should be sought in the difficulty to identify *ex ante* the effects of a potentially offensive cyber operation, distinguishing between those caused by a cyber attack (according to the criteria of the theory of damage identified by the living scientific literature) and those used for information purposes with the sole intention of obtaining military secrets [22].

On this focal point of the question, the Jack Goldsmith's perspective seems particularly sophisticated: «no nation can tell for sure whether the logic bombs[23] and related agents it finds in its civilian infrastructure networks are agents of exploitation or attack – until, of course, they are used for attack. If these agents turn out to be used for attack, our complacency about the agents of exploitation – and about international law's non-regulation of digital spying and digital theft – will surely change»[24].

Doctrine discusses whether an attack on a critical national infrastructure, such as a dam or a nuclear power plant that would not cause deaths, injuries or destruction would in any case represent an attack.

This cyber operation conducted with cyber weapons would qualify them as instruments potentially capable of carrying out an indiscriminate attack that violate, *inter alia*, art. 51 (1) of the Additional Protocol I to the Geneva Conventions, as well as art. 3 common to the Geneva Conventions[25].

But that might not be enough. On this point, the position expressed by prevailing doctrine[26] which start from geographically assumable scope of the armed attack that can trigger legitimate self-

[22] S. LA PISCOPÌA and S. SETTI, *Cybernetic espionage, profiles of international law*, Rome, 2021, 91.

[23] R. A. CLARKE & R. C. KNAKE, *Cyber war: The Next Threat to National Security and What to Do About It*, New York, 2010, 287 where a logic bomb is defined as «a software application or set if instructions that cause the shutdown of a system or network and/or the deletion of all data or software on the network».

[24] J. GOLDSMITH, *How Cyber Changes the Laws of War,* in *The European Journal of International Law*, XXIV/1, 2013, 135.

[25] M. N. SCHMITT, *Tallin Man.*, cit., 529. In particular, Rule n. 140, Duty of care during attacks on dams, dykes, and nuclear electrical generating stations, prescribes the use of «particular care» in these types of attacks.

[26] K. KITTICHAISAREE, *Public International Law of Cyberspace*, Cham, 2017, 171.

defence, arrives at the assertion that[27]: «Therefore, cyber activities that are akin to cyber weapons used against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations, would violate Article 2(4) of the UN Charter and would give rise to the right of self-defence under Article 51 of the Charter and customary international law by the victim State in the scale and effects thereof are "most grave", as objectively determined in light of the prevailing circumstances of each case»[28].

In other words, there is a reaffirmation of the imperative need to carry out an assessment of the use of the cyber weapon, taking into account the seriousness of the scale of the attack and the effects caused by the weapon itself.

However, in the author's humble opinion, there is a substantial difference between conventional weapons, even defensive ones, such as anti-tank or marine mines and a logic bomb that has infected, for example, the operating system of a dam. In this regard, in order to distance oneself from mere hypothetical catastrophism, the following news is provided by way of example: «The United States has been the subject of repeated cyberattacks in the past few years. The U.S. Army Corps of Engineers lost sensitive information on 85,000 dams in 2013, and the Nuclear Regulatory Commission lost information on nuclear plants the following year». Those data included their location, condition, and number of possible victims if dam control computer systems were breached, according to a frank report on the Department of Homeland Security by Senator Tom Coburn, the former top Republican on the US Senate National Safety Committee[29].

Returning to our conceptual comparison between the laying of mines and the contagion of a logic bomb, it must be said that the laying of mines does not actually constitute an offensive operation, nor an attack[30].

---

[27] E. WILMSHURST, *Principles of International Law on the Use of Force by States in Self-Defence, Royale Institute of International Affairs*, London, 2005, 6.

[28] In this sense also H. H. DINNISS, *Cyber Warfare and the Laws of War*, Cambridge, 2012, 74, 76-81.

[29] J. ZHOU, *Outgoing Senator Describes Dysfunction at DHS*, *The Epoch Times*, 1st June 2015, Available on https://www.theepochtimes.com/article/outgoing-senator-describes-dysfunction-at-dhs-1180526.

[30] *See Commentary of the International Committee of the Red Cross on the Additional Protocols to the Geneva Conventions*, Geneve, 1987, 603, para. 1881.

On the contrary, the possibility for state A to activate the aforementioned logic bomb (in the event that state B does not yield to a specific security threat), represent an offensive operation manifested through the crystallization of the potential imminence of an attack.

It is noted, in more detail, that NATO defines the attack as follows: «in military operations, to take offensive action against a specified objective», while the mentioned Art. 49 of the Additional Protocol I defines it: «acts of violence against the adversary, whether in offence or in defence». According to NATO language, more extensive than the living treaty law, a logic bomb represents in itself an offensive action, even if in the temporary absence of manifestation of violent actions. Anyway, the logic bomb in our example could remain latent and justify a similar counter-offensive operation – in compliance with the principles of necessity and proportionality – but it could also activate the dam locks and, even without visible physical actions, concretizing a war crime in violation of Art. 56 of the aforementioned Additional Protocol I[31].

In this regard, the author reports a shared doctrinal position on installations containing dangerous forces: «This category presents an interesting issue as the prohibition in Additional Protocol I, Article 56, is against the attack of "installations containing dangerous forces, namely dams, dykes, and nuclear electrical generating stations (…) if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population". Whereas this provision appears to lead the analysis back to questions of attacks in the cyber context, the issue here resolves itself. If a ransomware operation were to somehow result in the release of dangerous forces and severe losses to the civilian population, the ransomware operation would resultantly qualify as an attack. Again, if any cyber operation results in violence»[32].

[31] Art. 56 Protection of works and installations containing dangerous forces:

«1.1. Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population. Other military objectives located at or in the vicinity of these works or installations shall not be made the object of attack if such attack may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population».

[32] J. BILLER, *The Strategic Use of Ransomware Operations as a Method of Warfare,* in *International Law Studies*, Vol. 100, 2023, 2023, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3052&context=ils.

This highlights the extraordinary insidiousness of cyber weapons that, by targeting critical dual use infrastructures require a definition effort, as soon as possible, not only from the international scientific community, but also from states.

Moreover, as already highlighted, international law not only prohibits the use of force, but also the threat of its use and, with reference to our example, a logic bomb represents, most likely, a real threat of use of force.

Indeed, there is a concrete possibility that a logic bomb[33] on military command and control computer systems could be concretely used to pursue deterrent policies against a state concerning, for instance, contentious territorial claims or threatening expansive nuclear policies. In this case, there would also be a violation of Rule No. 68 of Tallinn Manual: «a cybernetic operation which constitutes a threat of the use of force against the territorial integrity or political independence of a State, or which in any other way is inconsistent with the purposes of the United Nations, is illegal».

In any case, wanting to temper the international regulatory requirement with the *status quo*, it seems appropriate to report the position of authoritative doctrine on the matter[34]: «(…) arguments that products non-physical harm must be regarded as articulation of *lex ferenda* rather than *lex lata*: In light of the ever-increasing reliance of society on computers and computer networks, many readers, like the author, will find the "physical consequences" standard [of Art. 2(4) UN Charter] too narrow. But it does represent the *lex lata*, that is, the law that currently exists»[35].

3. Moving from a theoretical approach to an empirical one, one might wonder if, in the practical case of the aforementioned logic bomb, it would be possible to act in self-defence before the final offensive act of opening the dam occurs.

---

[33] R. A. CLARKE & R. C. KNAKE, *Cyber War: The Next (...), op. cit.*, 287 where a logic bomb is defined as: «a software application or set of instructions that cause the shutdown of a system or network and/or the deletion of all data or software on the network».

[34] R. BUCHAN, *Cyber Espionage and International Law*, Oxford, 2019, 68. It should be noted that the author expressly refers to the Schmitt's position in footnote 103 (shown below).

[35] M. N. SCHIMTT, *Attack, as a Term of Art in International Law: The Cyber Operations Context*, in C. CZOSSECK, R. OTTIS and K. ZIOLKOWSKI, *International Conference of Cyber Conflict*, 2012, 288.

International legal doctrine often refers to the famous *Caroline case*[36], allowing for the possibility of pre-empting a defensive action to the point of carrying it out before the attack, even going so far as to include almost preparatory acts. From this event, prevailing doctrine has identified three essential elements to invoke the legitimacy of self-defence as the use of force in anticipation of an imminent attack (hence the *Caroline Test*).

These elements are necessity, meaning the impossibility of pursuing alternative means to politically or diplomatically resolve the dispute, proportionality, understood as a response proportionate to the threat, and imminence, where, to exemplify, a state has reasonable grounds to believe it is about to be attacked.

Based on the above, a state can anticipate its action against an armed attack when the attacker is clearly engaged in launching such an offensive, reaching the last available window of opportunity before definitively losing its ability to defend itself effectively[37]. It should be noted that this test has been fully incorporated into customary international law and has been invoked repeatedly in doctrine, as well as in legal cases, since the Nuremberg trials.

Therefore, it seems possible to assert that, under the circumstances highlighted above (necessity, proportionality, and imminence), a state can undertake offensive operations to pre-empt aggression when such aggression, if carried out, would amount to an armed attack due to the seriousness of its effects on people or property. It would appear permissible to pre-empt defence when faced with a necessity to react that is *irresistible, leaving no choice of means and no time for deliberation*.

---

[36] H. H. DINNISS, *Cyber Warfare (...)*, *op. cit.*,102-104; H. JONES, *To the Webster-Ashburton Treaty: A Study in Anglo-American Relations*, Chapel Hill, 1977, 1783 ff. The well-known episode is part of Canada's insurrection against Great Britain and refers to the attack that took place on the night of December 29, 1837 by some British soldiers who from Canada penetrated into US territory destroying the ship Caroline anchored on the banks of the Niagara from where it supplied an island occupied by Canadians and Americans with food and weapons. In the exchange of letters between the Ambassadors of the United States and Great Britain, the phrase of the US Secretary of State Daniel Webster remains famous, specifying the limits in which the use of force in self-defence was justified, for which it had to be demonstrated «a necessity of self-defence instant, overwhelming, leaving no choice on means and no moment for deliberation»; See British and Foreign State Papers, 1840-1841, XXIX, London, 1857, 1138.

[37] M. N. SCHIMTT, *Tallin Man.*, cit., Rule 73, point 4.

In this case, doctrine speaks of the «last available window», referring to the final moment when the defender can act to avoid the consequences of the opponent's offensive action.

Special attention must also be paid to intelligence acquired in the imminence of the attack: the more detailed the information about the nature, location, and timing of the attack, the more it can be invoked in support of the pre-emptive offensive operation[38].

In particular, Rule 73 of the Tallinn Manual, titled «Imminence and Immediacy», provides that the right to use force in self-defence arises if a cyber attack occurs or is imminent. It is also subject to the requirement of immediacy.

The position of the Experts of the Tallinn Manual appears reasonable. Their stance avoids a strictly time-bound view of self-defence (seconds or minute[39]) concerning a potential enemy attack.

This approach favours a perspective in which what matters for the legitimacy of the intervention is not the hypothetical temporal proximity of the attack, but rather the possibility of legitimately exploiting the «last available window»[40] for self-defence to prevent a lack of reaction from making it impossible to effectively counter the attack before it is physically launched.

Of particular significance is the position expressed by the Tallinn Experts in paragraph 7 of the aforementioned Rule 73, which is quoted here in full: «In assessing such cases, a distinction should be drawn between actions constituting the initial act of an armed attack and those that are merely preparatory. Consider the case of installing a logic bomb. Installation qualifies as an imminent armed attack if some specific conditions for activation could reasonably be expected to occur; the situation is akin to the placement of naval mines in shipping lanes passing through the territorial waters of the target state. Such situations should be distinguished from the remote installation of active malware. If the initiating party is merely acquiring the capability to launch an armed attack, the imminence criterion is not satisfied».

In this case, a logic bomb that, in addition to having sniffing purposes, *i.e.*, monitoring and data acquisition, also has a possible offensive function, even if potentially usable to launch a cyber or kinetic attack, represents a serious threat of an imminent attack.

---

[38] M. N. SCHIMTT, *Tallin Man.*, cit., Rule 73, point 6.

[39] In the cyber domain.

[40] Y. DINSTEIN, *War, Aggression and Self Defence*, Cambridge, 2011, 203-204.

Therefore, in the case of imminent enemy use of active malware that, for example, can disable a national missile system "at the click of a button", the author considers justifiable under international law to use force as a form of anticipatory self-defence, that is, in response (anticipated) to an imminent attack[41]. Therefore, the position of Dinstein, who invokes the concept of the «last available window» to act in self-defence, appears reasonable, thus directing the legitimacy criteria more towards the immediacy of the threat of anticipatory self-defence[42] than towards the enforcing criteria of pre-emptive self-defence[43].

In more detail, U.S. doctrine[44] defines pre-emptive self-defence as «the use of armed coercion by a state to prevent another state (or non-state actor) from pursuing a particular course of action that may not yet be directly threatening but, if left unchecked, could lead in the future to an act of armed coercion against the defender»[45].

This position, based on somewhat speculative assumptions, is closer to an emergency-based approach than to a more careful interpretation of applicable customary international law[46]. For these reasons, in the fifth domain, it should be prudent to strictly apply anticipatory self-defence and not pre-emptive self-defence based on only sufficiently reliable presumptions.

Concerning the concept of the imminence it seems relevant to mention the United Nations Secretary- General's report *In Larger*

---

[41] This case study is different from the one of a logic bomb (already sent) with an unknown moment of possible activation (which should not activate the pre-emptive self-defence).

[42] This institute is understood as «a using of force in anticipation of an imminent armed attack» (*See* G. S. DEWEES, *Anticipatory and Pre-emptive Self-defence in Cyberspace: The Challenge of Imminence*, 2015 NATO CCD COE Publications). *See also* S. D. MURPHY, *The Doctrine of Pre-emptive Self-defence*, 2005, p. 703, where the author defines anticipatory self-defence as «a situation in which a state has not yet been the victim of a coercive act, but perceives that such an act is about to occur in the immediate future (e.g. a foreign army is massing along the border in apparent preparation for invasion), and therefore in the state of potential victim he undertakes his own armed action to avoid, and therefore anticipate, the action of others».

[43] S. LA PISCOPÌA, S. SETTI, *op. cit.*, 127-128.

[44] S. D. MURPHY, *The Doctrine of Pre-emptive Self-defence*, in *Villanova Law Review, L.* 2005. This doctrine, developed after the well-known events of 11 September in the light of which the ability of non-state actors to project their own forces across the globe has become evident, with the consequent concern of states regarding the potential use of weapons of mass destruction.

[45] S. D. MURPHY, *The Doctrine of Pre-emptive Self-defence*, 2005, 704.

[46] A. CASSESE, *International Law*, Oxford, 2005, 361, according to which this doctrine has no basis in both conventional and customary law.

Freedom: Toward Security, Development and Human Rights for All, submitted to the United Nations General Assembly on 21 March 2005.

It has a Section on *Use of Force* in which he says: «In recent years, UN Member States have disagreed about whether States have the right to use military force pre-emptively, to defend themselves against imminent threats [that] are fully covered by Art. 51, which safeguards the inherent right of sovereign States to defend themselves against armed attack. Lawyers have long recognised that this covers an imminent attack as well as one that has already happened»[47].

What above mentioned shows, once more, the relevance of defining cyber weapons in order to have a fair approach to the legitimate use of force.

In this contest it is indeed appropriate to specify that the failure to carry out a destructive cyber offensive action cannot constitute the legitimate prerequisite for the implementation of countermeasures: «though customary international law contemplates the use of anticipatory actions, including cyber actions, in self-defence to repel an imminent armed attack, there is no such option for countermeasures under international law»[48].

In other words, the implementation of countermeasures always necessarily requires the execution of a cyber offensive operation.

4. As mentioned earlier, beyond doctrinal experiments on the definition of cyber weapons, it is difficult to find a clear taxonomic categorization of cyber weapons. For example, in the U.S. Department of Defence's Law of War Manual from June 2015, updated as of July 2023[49], Chapter VI - Weapons does not include them in its list, and Chapter XVI - Cyber Operations mentions them among those not necessarily illegal[50]. This seems to highlight the difficulty to define such emerging (and continually evolving) weapons.

On this topic, let's now briefly review some international pillars related to weapons and cyber threats for further considerations on counter-proliferation policies.

---

[47] *See* UN Doc.A/59/2005, para. 122.

[48] G. CORN and E. JENSEN, *The Use of Force and Cyber Countermeasures*, in *Temple International and Comparative Law Journal*, 2018, 127, 128.

[49] https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF.

[50] US Department of Defense Handbook on the Law of War, 2023, 1038.

The Arms Trade Treaty (ATT) is the first globally significant legal instrument that establishes criteria for the authorization (or prohibition) of conventional arms transfers. Adopted by a vote of the UN General Assembly on April 2, 2013, it is a pioneering instrument, with two main objectives: to regulate or improve the regulation of conventional arms trade and to prevent or eliminate their illicit trafficking, with the aim of contributing to international security, reducing human suffering and promoting responsible state action in this sector. However, the Treaty only applies to so-called conventional arms that fall within the categories of the United Nations Register of Conventional Arms[51] and their parts and ammunition, including small arms and light weapons.

Its core provisions are contained in Articles 6 and 7.

Art. 6, in particular, establishes cases in which arms transfers are prohibited, namely if they violate sanctions regimes, such as those imposed by the UN Security Council, or if there is a possibility that the transferred arms could be used to commit genocide, crimes against humanity, or violations of the 1949 Geneva Conventions.

Art. 7, on the other hand, sets out the criteria that state Parties must consider when deciding whether to grant authorization for exports.

In more detail, they must refuse authorizations if the export could lead to the commission or facilitation of serious violations of international humanitarian law, serious violations of international human rights regimes, illegal acts under international conventions related to terrorism, or illegal acts under international conventions related to transnational organized crime. When making export decisions, each state Party must also consider the possibility that the transferred arms could be used to commit acts of gender-based violence or violence against women and children. With much less detail, the ATT contains provisions concerning import controls, transit, and brokering activities. A robust article sets out measures to

[51] In particular, the eight categories are:
(a) Battle tanks;
(b) Armoured combat vehicles;
(c) Large-calibre artillery systems;
(d) Combat aircraft;
(e) Attack helicopters;
(f) Warships;
(g) Missiles and missile launchers; and
(h) Small arms and light weapons.

prevent, detect, and address the diversion of arms from legal to illegal circuits; international information exchange and cooperation play a significant role in this regard. It is worth noting that Italy was the first European Union country to ratify the ATT in September 2013, playing an active role throughout the diplomatic process leading to the Treaty's adoption. From the outset, Italy emphasized the need for a global and legally binding instrument that, while respecting the requirements of self-defence and the UN Charter more broadly, would create obligations to ensure the legality and responsibility of decisions regarding conventional arms exports.

Ultimately, as observed, cyber weapons are not currently included in the category of so-called conventional arms.

Staying within the United Nations framework, Resolution A/RES/70/237 adopted by the General Assembly on December 23, 2015, under the title *Developments in the field of information and telecommunications in the context of international security*, is also of particular interest[52]. In its preamble, it expresses clear concern about dual-use means and technologies[53], which are technologies that can be used for both civilian and military purposes: «Expressing concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields».

It is noteworthy that the United Nations uses the term *means*, which recalls the terminology of the Geneva Conventions of 1949 and their Additional Protocols of 1977. However, even in this case, although the concept of *technologies* that could potentially harm National Critical Infrastructures is introduced, there is no explicit reference to cyber weapons yet.

A subsequent United Nations General Assembly Resolution, A/RES/73/27 adopted on December 11, 2018, in point 1.7, takes a

[52] Available on https://undocs.org/A/RES/70/237.

[53] Interesting in this regard is the historical reference of the Resolution of the General Assembly of 1999 A/RES/53/70, entitled Developments in the field of information and telecommunications in the context of international security which, in its preamble, affirms. «Recalling its resolutions on the role of science and technology in the context of international security, in which, inter alia, it recognized that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needed to be maintained and encouraged». Available on https://undocs.org/en/A/RES/53/70.

step forward by suggesting that states should take measures to protect their Critical Infrastructures from ICT threats. At this point, it would be natural to ask whether such threats to international stability and security constitute means of cyber warfare, whether they can be considered an illegitimate use of force under the law of armed conflict, even in the absence of a (unlikely) declaration of war, and if so, what countermeasures could be adopted.

Additionally, there is a second equally significant issue.

Many experts recall the precept of compliance with international humanitarian law established concerning the adoption of new weapons by Art. 36 of the Additional Protocol I. However, are we sure that this treaty obligation is always respected by weapon manufacturers on one side and by states on the other? In the author's view, it is plausible to assume that illegitimate cyber combatants could utilize, wearing camouflage uniforms without distinctive signs, an illegal availability of non-conventional and seemingly non-illegal weapons from the dual-use software market, thus conveniently circumventing both, international arms control regulations (in peace time) and the aforementioned Article 36 (in war time).

This *status quo* is favoured both by the complexity of conducting [54] a *trial of intentions* regarding the use of such technological tools and by the objective technical and forensic difficulty of attributing a potential indiscriminate cyber attack to a state entity.

It should be noted that the High Contracting Parties to the Additional Protocol I displayed foresight in opening the door to new weapons that were not easily conceivable in 1977. However, the globalized world still struggles to recognize the invasiveness and offensiveness of cyber weapons with the regulatory force of international law.

Certainly, the *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, established in accordance with UN General Assembly Resolution No. 73/27 of December 5, 2018, represents an important step forward in structuring international dialogue on this sensitive challenge.

[54] Towards sellers and buyers.

In this regard, its Final Substantive Report of March 10, 2021, assumes a special significance[55], expressing the strong and widespread concern of the international community in point 16 «States recalled that a number of states are developing ICT capabilities[56] for military purposes. They also recalled that the use of ICTs in future conflicts between states is becoming more likely. The continued increase in incidents involving the harmful use of ICTs by state and non-state actors, including terrorists and criminal groups, is a disturbing trend. Some non-state actors have demonstrated ICT capabilities previously available only to states».

It would thus be natural to assume that a technological tool used in a conflict could qualify as a genuine cyber weapon.

It seems so. However, there is still no terminological evidence of this in the document under examination, which continues in point 17: «States also concluded that any use of ICTs by States in a manner inconsistent with their obligations under the framework, which includes voluntary standards, international law and the CBM[57]undermines international peace and security, trust and stability between States and can increase the likelihood of future conflicts between States».

These technological tools, therefore, if used outside the applicable legal framework (even) in the case of armed conflict[58], undermine international peace and security. And we know that even the mere threat to these core principles of the United Nations Charter is prohibited by the aforementioned Art. 2, para. 4.

Noteworthy are also the principal considerations expressed in point 18: «States have concluded that there are potentially devastating economic, social and humanitarian consequences resulting from malicious ICT activity against critical infrastructures and critical information infrastructures placed in support of essential services to the public».

On a regional level, the European Union has issued the Common Military List of the European Union adopted by the Council on February 17, 2020[59], which includes, among other things, electronic

[55] *See* https://ict4peace.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[56] Information and communications technologies.

[57] Confidence-building measures.

[58] Usually conducted by the military just mentioned.

[59] Equipment covered by Council Common Position 2008/944/CFSP defining common rules governing the control of exports of military technology and equipment.

countermeasure and electronic counter-countermeasure equipment[60], including jamming and anti-jamming equipment, as well as electronic systems or electronic equipment designed for surveillance and monitoring of the electromagnetic spectrum for intelligence or military security purposes, or for countering such surveillance and monitoring. In this document there is no explicit mention of cyber weapons that may exceed the threshold of offensiveness.

Very interesting is also, the Regulation (EU) 2021/821 of the European Parliament and of the Council of May 20, 2021[61], which established a Union regime for the control of exports, brokering, technical assistance, transit, and transfer of dual-use items.

In more detail, the preamble to this Regulation, at point (5) emphasizes the need for an effective common system for controlling exports of dual use items to ensure compliance with the international commitments and responsibilities of Member states and the Union, particularly in non-proliferation, peace, regional security and stability, and respect for human rights and international humanitarian law.

In this context, Art. 5.1 of this Regulation, concerning the export of computer network surveillance items not listed in Annex I, provides that such exports are subject to authorization if the exporter has been informed by the competent authority that these products are or may be intended, in whole or in part, for use related to internal repression and/or the commission of serious violations of human rights or international humanitarian law.

This is a fundamental point because, although it is not possible, yet, to find a clear definition of cyber weapons, there seems to be a clear imperative to subject exports – including potentially cyber weapons that could be used in violation of international humanitarian law – to special authorization.

In this regard, it should be noted that the list of dual use items contained in the aforementioned Annex I, implements international agreements on the control of dual-use items, including the Australia Group[62], the missile non-proliferation regime[63], the Nuclear Suppliers

[60] That is, equipment designed to introduce extraneous or erroneous signals into radar or radio communications receivers, or otherwise impair the reception, operation, or effectiveness of opposing electronic receivers, including their countermeasure equipment.

[61] *See* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02021R0821-20230526.

[62] Established in 1985 in light of international concerns over the use of chemical weapons in the 1980-1988 Iran-Iraq war.

[63] https://mtcr.info/.

Group[64], the Wassenaar Arrangement[65], and the Chemical Weapons Convention (CWC)[66].

In this context, with particular reference to the Wassenaar Arrangement, which aims to promote transparency and the exchange of information and opinions on the transfer of certain categories of goods, promoting greater responsibility in the transfer of conventional arms and related dual use goods and technologies, while seeking to prevent destabilizing accumulations.

It is significant to note that point 4.D.4 of the *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*[67] explicitly excludes *software upgrades* indicated in Note 2, namely «intrusion software», which incidentally invokes not only the terminology but also the concept of intrusive espionage coined by the author.

This form of espionage[68], potentially achievable with malware that can be activated «above the threshold of danger» even remotely, represents a concrete risk to national security (or that of an alliance).

From a national perspective, the cyber weapon used does not find a regulatory definition, even in the Italian law No. 185 of 1990 on the control of the export, import, and transit of armaments materials.

Article 2 (armament materials) of the aforementioned law, which dates back over thirty years, in paragraph 2, letter i), only «electronic, electro-optical and photographic systems or apparatus specially built for military use», without making any mention of possible exports or transits[69] of dual use software and without guaranteeing the forward-thinking openings for future weapons as allowed by the aforementioned Article 36.

---

[64] http://www.nuclearsuppliersgroup.org/.

[65] https://www.wassenaar.org/.

[66] https://www.opcw.org/chemical-weapons-convention.

[67] *Public Documents*, Volume II, List of Dual-Use Goods and Technologies and Munitions List Compiled by the Wassenaar Arrangement Secretariat, December 2020.

[68] Different from «transmitting military information for the immediate use of a belligerent» and from «gathering and transmitting military information» which represent, respectively, examples of direct and indirect participation to hostilities.

International Committee of the Red Cross, *Customary International Law*, Rule 6, Civilians' Loss Protection from Attack, *see* https://ihl-databases.icrc.org/en/customary-ihl/v1/rule6.

[69] Which obviously for these potentially offensive technological tools can now take place via the internet (and not by rail).

5. Even though the challenges of modernity seem to remind us that *omnia mutantur*[70], at the moment, international doctrine does not appear to have sufficiently highlighted with clarity and strength the enormous risks for the country and for NATO stemming from the spread of a pay-to-play system used without distinction between good and bad[71] to purchase interception and intrusion technologies from private companies[72].

This may be because the exclusive purposes of intelligence and surveillance are not clearly defined *a priori*; however, the potentially offensive dual use function of such tools, even in violation of the fundamental principles of international humanitarian law, seems to require a deep reflection non only by the scientific Community, but even by the states.

A recent study by international researchers from the Atlantic Council Research Centre[73] has found that offensive cyber capabilities are becoming increasingly privatized. In fact, governments no longer need to allocate significant resources to develop offensive computer capabilities using internal know-how.

This is because almost all governments can purchase capabilities to achieve a range of national security objectives, including the surveillance of domestic groups, cyber defence, foreign intelligence collection, and the enhancement of traditional military capabilities. What was once a *nobody but us* system, in which computer capabilities were difficult to develop and the prerogative of a limited number of states, has indeed evolved into a pay-to-play model in which any government, adversary or ally, can access offensive computer capabilities if it can buy from the company that suits it best.

Although offensive computer capabilities are useful for law enforcement and border protection, the dual use nature of many of these capabilities also offers opportunities for harmful and dangerous use, especially when these capabilities are sold to authoritarian actors.

---

[70] OVID, *The Metamorphoses*, Book XV.

[71] Because we remember that international espionage, although intrusive, is not expressly prohibited.

[72] Potentially by (also) other private companies involved in providing intelligence services to foreign states.

[73] W. DESOMBRE, L. GJESVIK, J. O. WILLERS, *Atlantic Council, Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets*, 2021, www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/.

The authors discovered that 75% of the companies that likely sell interception/intrusion technologies have marketed these capabilities to governments outside of their continent, marketing their capabilities beyond the perimeter of NATO countries.

This document classifies these companies as potentially irresponsible proliferators for various reasons. The issue, of course, is not only highly relevant at a time of serious international crisis, as the one we are experiencing from the East, but also it is highly topical given the posture that NATO has recently taken regarding the application of Article 5 of the Washington Treaty in the event of a cyber attack[74].

Cyber weapons must, therefore, emerge from the opacity guaranteed by the possible dual use of the related technologies and find a shared definition both in international organizations (from the United Nations to the European Union, from NATO to the OSCE), and in national legislation.

It is necessary to stress that the sale of such intrusive spying systems to a hostile (or enemy) Country could assign real cyber weapons (currently legally non-existent) with the simple sending of a subsequent system *patch*.

Regarding this, even in a context *other than war*, it does not seem irrelevant to recall that a cyber attack on hospitals that would inhibit life-saving surgical interventions for women and children, or a cyber sabotage of a radar control system, would be no less indiscriminate – and therefore illegitimate – than a conventional bombing of such critical infrastructure.

6. After examining the general framework that defines the areas of cyber aggression, which can obviously occur, as in the case of Albania analysed by the doctrine[75], even in the mentioned *other than war* contexts, we find it interesting to analyse the possible prerequisites for the categorization of offensive cyber operations in the crime of aggression as defined at the conclusion of the Kampala Conference in June 2010.

---

[74] «A serious cyberattack could trigger Article 5, where an attack against one ally is treated as an attack against all» Jens Stoltenberg, NATO Secretary General».
www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.

[75] A. L. SCIACOVELLI, *Taking Cyberattacks Seriously: the (likely) Albanian Cyber Aggression and the Iranian Responsibility*, 2023, www.osorin.it/uploads/model_4/.files/133_item_2.pdf?v=1680094363.

For this purpose, the text of the reference norm, which is known as Article 8-*bis*, is preliminarily referred to.

«1. For the purpose of this Statute, "crime of aggression" means the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a state, of an act of aggression which, by its character, gravity and scale, constitutes a manifest violation of the Charter of the United Nations.

2. For the purpose of paragraph 1, «act of aggression», means the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations. Any of the following acts, regardless of a declaration of war, shall, in accordance with United Nations General Assembly resolution 3314 (XXIX) of 14 December 1974, qualify as an act of aggression:

«(a) The invasion or attack by the armed forces of a State of the territory of another State, or any military occupation, however temporary, resulting from such invasion or attack, or any annexation by the use of force of the territory of another State or part thereof;

(b) Bombardment by the armed forces of a state against the territory of another state or the use of any weapons by a state against the territory of another state;

(c) The blockade of the ports or coasts of a state by the armed forces of another state;

(d) An attack by the armed forces of a state on the land, sea or air forces, or marine and air fleets of another state;

(e) The use of armed forces of one state which are within the territory of another state with the agreement of the receiving state, in contravention of the conditions provided for in the agreement or any extension of their presence in such territory beyond the termination of the agreement;

(f) The action of a state in allowing its territory, which it has placed at the disposal of another state, to be used by that other state for perpetrating an act of aggression against a third state;

(g) The sending by or on behalf of a state of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another state of such gravity as to amount to the acts listed above, or its substantial involvement therein».

Analysing the first paragraph of the article, it is noted that there is a necessary connection between the action of the state and the

commission of the crime on an individual level. It is therefore a matter of the responsibility of a state for a crime committed by its leader who is able to effectively control or direct the political or military action of the state itself.

In this regard, it is observed that in the case of offensive cyber operations, they are often subject to the direction and control, in different forms from state to state, of the political authority from which the military authority normally depends, and at appropriate levels, certain intelligence services may also be directed. However, it does not appear clear what the level of leadership adequate to identify the elements of the incriminating circumstance may be, considering that the military level, which as we will see is called to play a primary role, depends on the political level.

Further doubts arise after considering that, from a subjective point of view, the phases of planning, preparation, initiation, and execution of the act of aggression can only be entrusted to leaders of completely different levels. In other words, it does not appear clear whether the responsibility for an offensive cyber operation – if it could be configured as aggression – can also be attributed to a simple state operator (*e.g.*, launching malware) to whom it would be difficult to recognize a leadership purely in terms of decision-making.

In this case, even wanting to appreciate the nature and character of exclusive privilege in the relationship of organic identification existing between the cyber offender and the state, it seems reasonable to consider that the aforementioned relationship may be compromised by the specificity of the leadership crime in question.

Other necessary parameters for configuring the crime of aggression are the character, gravity, and scale of the aggression, which should all manifest together but, especially in terms of gravity, could also be appreciated with a certain time lag.

Regarding the latter parameter of gravity, in the case of offensive cyber operations through intrusion, it should be noted that the logic bomb could potentially manifest its destructive and lethal effects upon command, even after some time, representing a sort of «virtual sword of Damocles» over the heads of the leaders of the state victim of political ransom.

The definition provided by the subsequent paragraph 2 of Art. 8-*bis*, by establishing a correlation with the use of armed force, would seem to limit the action committed by the state to the use of armed force (against the sovereignty, territorial integrity, or political

independence of another state). It should be observed that the subsequent reference to any other way contrary to the Charter of the United Nations, seems to come to the aid of the evaluability of the offensive cyber operation under consideration, as an aggressive phenomenon that could potentially violate the *ius cogens* norm of non-intervention, directly related to the fundamental rule of sovereignty.

In this regard, it would seem plausible to argue that an offensive cyber operation that violates the rule of sovereignty of states, even in the absence of a declaration of war, could likely qualify as an act of aggression in the presence of an adequate threshold[76] of offensiveness identified by the aforementioned parameters of character, gravity, and scale of the operation.

Unfortunately, leaving aside the topic of objectifying the aforementioned threshold of offensiveness, the author just observes that the subsequent reference to compliance with General Assembly resolution 3314 (XXIX) of 14 December 1974, highlights a limited effectiveness[77].

The doctrinal position on this point seems decidedly shared: «Resolution 3314 was conceived not in the perspective of individual responsibility, but rather of the international responsibility of states and as a tool to guide the deliberations of the Security Council. Hence, the flexibility of its provisions[78], which finds a sure justification only in that perspective. But precisely this characteristic arises as the most immediately problematic datum when the Resolution is invoked for completely different purposes, in particular that of defining as many structural elements of an individual crime. This is an objectively unfortunate postponement, precisely because it seems to recall all the relevant provisions of the Resolution, with results that the prevailing doctrine however rejects because they are contrary to the principle of legality».

It is known that any modification or addition to an international treaty is the result of mediation, and it is therefore always much

[76] F. DELERUE, *op. cit.*, 291.

[77] F. DELERUE, *op. cit.*, 329.

[78] The reference is to the power of the Security Council (Art. 4 Res. 3314) to identify further acts of aggression than those expressly indicated in Res. 3314 (and reproduced, as we have seen, in Art. 8-*bis* of the International Criminal Court Statute), as well as that of excluding the illegality of an act apparently compliant with the typical ones (art. 2 Res. 3314). *See* A. DI MARTINO, *Il crimine ottativo*, for a criminal exegesis of the international crime of aggression, in *Criminalia - Yearbook of criminal sciences*, 2013, 575, note 35.

simpler to make observations on the text than to be assertive interpreters of complex norms in continuous evolution.

However, this attempt to highlight the rationale of the incriminating circumstance would perhaps have expressed greater clarity in a punctual and exhaustive systematic enumeration of acts of aggression, avoiding improper references by analogy.

Moving on to the exemplary examination proposed by the norm, paragraph 2(b) of the reviewed article makes reference to the use of any other weapon[79] by a state against the territory of another state.

Leaving aside, for the moment, the case of the logic bomb, it begs the question of whether the weapons of a cyber attack[80], such as those used in the famous Stuxnet Worm[81], fall among the aforementioned other types of weapons referred to generically by the norm[82].

Considering the destructive effects of the malware that severely compromised Iran's uranium enrichment program in the gas centrifuges of Natanz[83] by damaging PLC[84] programs interconnected with SCADA[85] computer control systems, the author is, in accordance with the doctrine, for a predominantly affirmative response[86].

This is assuming that on the technical-computer level, the traceability/responsibility of the attack[87] can be demonstrated to

---

[79] G. H. TODD, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, in *Air Force Review*, LXXVIII, 2009, 77, in which the author points out that the use of the term «any» obviously indicates that the use of cyber weapons resulting in severe consequences would be an act of aggression.

[80] Currently not defined as such by any international treaty act.

[81] N. FALLIERE, L. O. MURCHU, E. CHIEN, W32.Stuxnet Dossier, version 1.4, February 2001,archive.org/details/w32_stuxnet_dossier/mode/2upAndM. Clayton, Stuxnet: Ahmedinejad admits cyber weapon hit Iranian nuclear program, Christian Science Monitor, 2010.

[82] H. S. LIN, *Offensive, Cyber Operations and the Use of Force,* in *Journal of National Security Law & Policy*, IV/1, 2010, 75.

[83] M. ROSCINI, *op. cit.*, 6 and I. BARZASHKA, *Are Cyber Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Program*, in *RUSI Journal*, CLVIII/2, 2013, 50 ff.

[84] Programmable Logic Controllers.

[85] Supervisory Control and Data Acquisition.

[86] M. N. SCHMITT, *Computer network attack and the use of force in international law: thoughts on a normative framework*, in *Columbia Journal of Transnational Law*, XXXVII, 1999, 914 – 915; H. DINNISS, *op. cit.* 65 ff. and I. BARZASKA, *Are Cyber Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Program*, in *RUSI Journal*, CLVIII/2, 2013, 55. For more prudent reflections, J. RICHMOND, *Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?*, in *Fordham International Law Journal*, XXXV, 2011, 856.

[87] We recall that even in the absence of a declaration of war, as provided for by art. 8 bis of the Statute of the International Criminal Court, an international armed conflict could exist

belong to the armed forces of the attacking state or to state entities responsible for such purposes, based on the mission accomplishment resulting from authorization by the political leadership[88].

Continuing the examination of the article in question, it is interesting to recall the doctrinal perspective suggesting that since many Armed Forces have established specialized Commands, primarily joint forces aimed at managing cyberattacks, launching such an attack would be sufficient to create the conditions mentioned in letter d). This refers to an attack by the armed forces of a state on the land, sea or air forces, or marine and air fleets of another state[89].

While this perspective may initially seem somewhat simplistic, it must be acknowledged that it is quite effective from a purely academic standpoint.

This act of cyber-aggression could also originate from the territory of a third state, as indicated in paragraph 2 f) of Article 8 bis. It does not appear unlikely that this could occur in the context of a political or military alliance.

However, it is important to consider that, in this case, for shared responsibility to exist, merely using a common network would not suffice. The crime of aggression, in fact, as internationally defined, always requires clear leadership which, in this case, should be vested in an alliance decision-making board that assumes responsibility for ordering the cyberattack.

Lastly, it is worth noting that paragraph 2 g) of the article in question mentions the sending of groups, irregulars or mercenaries, which carry out acts of armed force, but it does not explicitly reference hackers or intelligence services consultants. Therefore, it would be challenging to hypothesize an interpretative framework that

---

even if a Party does not recognize the conflict as such, pursuant to the common article 2 of the I and IV Geneva Conventions.

[88] M. N. SCHMITT, *Tallin Man.,* cit., 384 that states: «the international group of experts was divided in deciding whether the damage was sufficient to determine the criterion of the armed attack. The categorization was further complicated by the fact that questions remained unresolved as to who conducted the Stuxnet operation if a state or individuals whose conduct is attributable to a state in order to determine the existence of an international armed conflict.

[89] J. ANDRESS, S. WINTERFELD, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, Waltham, 2011, 69 – 74, J. A. LEWIS, *Cybersecurity and Cyberwarfare: Assessment of National Doctrine and Organization*, in United Nations Institute for Disarmament Research, *The Cyber Index: International Security Trends and Realities*, New York, 2013, 9 *ff. See also* Y. RADZIWILL, *Cyber-Attacks and the Exploitable Imperfections of International Law*, Leiden 2015, 168.

would categorize these agents as possible responsible individuals[90] for individual criminal conduct aimed at committing an act of aggression[91].

Due to the aforementioned interpretative challenges, in an abstract sense, the crime of aggression would seem to be only conceivable if the international community reaches a consensus on the idea of *sending* military personnel or state agents into cyberspace.

7. In conclusion of our brief awareness assessment, perhaps the risks arising from the lack of a shared interpretative exegesis of crimes in the fifth dimension and the persistence of a shared definition of cyber weapons appear to be less opaque.

Unfortunately, in the absence of a common convergence of intent based on clear content-related assumptions regarding the categorization of cyber weapons and their thresholds of offensiveness, we will have to await suitable treaty instruments that can define the tools for such criminal acts, even before delineating their sanctioning prerequisites. This is a crucial and, in the author's opinion, urgent issue for the proper (and common) application of international humanitarian law, both in *ius ad bellum* and *ius in bello*.

The upstream issue, therefore, is not to be found in the likely inapplicability of the direct jurisdiction of the International Criminal Court in established cases (not only technically but also legally) of a state's responsibility regarding an offensive operation (compliant with potentially applicable soft law parameters). Instead, it is to establish that a hostile cyber operation can be carried out with destructive effects using cyber weapons.

This is because, as doctrinally reiterated, the International Court of Justice has clearly stated that the provisions of the United Nations Charter governing the use of force «apply to any use of force,

[90] Or it would be better to say co-responsible given that the constitutive elements and conditions for the punishability of the crime of aggression are aggregated both on the level of individual conduct and on that of state conduct integrating the act of aggression. See P. FOIS, *Sul rapporto tra i crimini internazionali dello Stato e i crimini internazionali dell'individuo*, in *Rivista di diritto internazionale*, 2004, 946-947.

[91] Although it does not seem possible to disagree in principle with those who in doctrine state: «while the "sending" of irregular gangs is normally foreseeable, a similar use of cracker groups belonging to military forces is not formally excluded in any part of the statute of Rome». Y. RADZIWILL, *op. cit*., 169.

regardless of the type of weapons used[92]». A sort of elevation of cyber weapons to the status of a genuine weapon, even from an international taxonomic perspective, would conform the use of this means of warfare to the regulatory content of Article 49 of the aforementioned Additional Protocol I, which expressly refers to armed force, substantiating the peripheral foresight of Article 36 of the Protocol itself.

It is a matter of fact that the evolving reality of the technological tools inherent to modern cyber operations is still not regulated by clear rules, and as we have outlined this creates further problems in the field of arms proliferation, as it appears exceedingly complex to curb the acquisition of cyber weapons by potentially hostile countries if there is no internationally shared definitional evidence of cyber weapons.

As known, a backdoor[93], similar to a logic bomb[94], can be used both for mere cyber gathering activities and for preparatory activities for a cyber attack[95], as well as for an actual attack that could be launched either with automated autonomous procedures or remotely at a specific time.

Indeed, as argued, if a dedicated malware or a suitable logic bomb were to succeed in its offensive intent remotely, we would no longer be dealing with a simple cyber gathering but with a genuine delayed destructive effect attack.

In conclusion, although there are some positions that tend to assume the sufficient regulatory value of *soft law* to comprehensively regulate hostile activities in cyberspace in the light of treaty-based international law, it has been noted that the direct application of norms born in different contexts is not immune to criticisms: it must be considered on a case-by-case basis[96].

While key actors in this decision-making process are already at work, the author's thought contribution merely aims to represent the

---

[92] International Court of Justice, *Military and paramilitary activities in and against Nicaragua* (Nicaragua v. United States of America), 26 November 1984, para. 176, www.icj-cij.org/en/case/70/judgments.

[93] Installed software or code (or compromised chip) that ensures constant and clandestine access to the computer system or server, thus bypassing the normal authentication method. D. DELIBASIS, *The Right to the National Self-Defence in Information Warfare Operations*, Bury St. Edmunds, 2007, 79.

[94] Which as we have said is a malicious program that can be activated at a certain time or when certain conditions are met.

[95] M. ROSCINI, *op. cit*., 13, 15, 17-18, 65, 179, 263.

[96] G. DELLA MORTE, *Limiti e prospettive del diritto internazionale nel cyberspazio*, in *Rivista di diritto internazionale*, fasc. 1, 2022, 5.

modest starting point for reflection by a scholar on the need to create the right conditions, including regulatory ones, for an even more vigilant attention and international cooperation in the sensitive area of cyber weapons typical of the fifth dimension.

To overcome this *status quo* – which we could currently define as metalegal – it appears necessary to continue down the path of defining norms and principles for responsible state behaviour, establishing a fruitful institutional dialogue aimed at defining not only the threats but also cyber weapons, because international law cannot find full application based solely on confidence-building measures, especially in a war context.

Responding to an attack in the cyberspace requires awareness of the nature of the weapons of hostile forces, without which there can be no legitimate and prompt defence.

Furthermore, alongside the serious need to define cyber weapons, there must also be a careful evaluation of the criterion of imminence of the attack because, even more so in the fifth dimension, swiftness is the essence of the cyber defence[97].

[97] S. TSU, *The Art of War, chap. II, para. 29*: The essence of war is speed. It allows you to gain an advantage over an unprepared enemy, arriving through unexpected routes and striking where defences are non-erected.

NON-WESTERN COUNTRIES PERSPECTIVE

UNVEILING INDIA'S CYBER STRATEGY: NAVIGATING INTERNATIONAL LAW AND INDIAN STATE PRACTICE ON SECURITY OPERATIONS

ARINDRAJIT BASU – BHARATH GURURAGAVENDRAN

As a leading digital economy, India's approach to international law and cyber operations matters deeply for the world. Yet, as this chapter demonstrates empirically, India has adopted a largely context-specific approach to international law aimed at justifying or asserting immediate interests, rather than holistic normative construction. This approach has applied to the cyber realm as well, where India has participated vigorously at international platforms but stayed clear of ideological fissures in discussions around the application of international law to cyberspace[1]. Therefore, an overarching assessment of India's approach to international law and cyberspace cannot be easily discerned by referring to a core strategic document or statement. Having said that, the lack of a central doctrine should not be misinterpreted as an absence of state practice or critical thinking writ large within the government machinery.

The trappings of India's approach to international law can therefore be discerned through an amalgamation of the vast instances of domestic and international practices of the several relevant institutions including the Executive, Armed Forces, Parliament and Judiciary. Here, it is worth pointing out that while parliamentary debates have immense clarificatory value in explaining positions on international law and foreign policy, they are not legally binding and as A.G. Noorani demonstrates in the context of parliamentary resolutions, "their moral role and political relevance have also been restricted"[2]. International law in cyberspace is not only determined by the prevailing conceptions of the use of force but also of the doctrinal

[1] "However, India's stance on specific aspects of international law and their interpretation remains unclear" See EU Cyber Direct, *Compare: International Law*, EU Cyber Direct- EU Cyber Diplomacy Initiative, available at: https://eucyberdirect.eu/atlas/country/united-states/compare/european-union/india (last visited May 06. 2024).

[2] A.G. NOORANI, *Constitutional Questions in India*, 26, The President, Parliament and the States, Oxford, 2006.

and international approach to operations below the threshold of the use of force. In particular, the cyberspace has often been characterised as an "intelligence contest"[3] which necessitates an evaluation of the regulation of intelligence agencies and constraints on their surveillance powers. To underscore our analysis we adopt a broad definition of cyber operations as "operations that employ capabilities aimed at achieving objectives in or through cyberspace"[4].

Our evaluation of the question of India's approach to international law and cyber operations hinges on four factors, which we analyse in the first four sections of this chapter; In the first section, we attempt to understand India's approach to the use of force and self-defence by examining several decades of state practice. Through this analysis, we aim to identify the core discernible features of India's military policy, as well as the specific pressures that motivate the decision-making processes of India's military command. In the second section, we analyse India's state practice on extraterritorial uses of force in the kinetic realm, to understand how the Indian state machinery validates such uses of force. In the third section, we explore the Indian legal framework within which intelligence agencies operate, specifically exploring the trajectory of the higher judiciary's cognizance of privacy, and its impact on the surveillance regime. In the fourth section, we explore India's domestic institutional architecture and domestic law on cybersecurity and highlight India's positioning on international law at international forums. Based on our findings, in the final section, we theorize the contours of an Indian approach to international law - specifically on the use force.

In this vein, the forthcoming analysis is inherently designed to weave together multiple strands, encompassing law, military practices, parliamentary processes, foreign policy stances, and archival evidence of India's historical conduct. This intricate approach is undertaken to construct a coherent understanding of how India's unique approach to international law intertwines with its evolving strategies in the cyber realm.

---

[3] J. ROVNER, *The Elements of an Intelligence Contest*, in R. CHESNEY AND M. SMEETS (eds.), *Deter, Disrupt or Deceive. Assessing Cyber Conflict as an Intelligence Contest*. Washington DC, 2023, 17-42.

[4] Y. DINSTEIN ET AL, *Section II: Cyber Operations,* in *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*, Cham, 2020, 19-29.

I. India's Legal, Policy and Doctrinal Framework – The Use of Force

As mentioned above, there is no single authoritative document or legal provision from which India's legal and procedural oversight mechanisms over the use of force can be discerned. As a result, we will analyse five different sources in this section to aid our analysis. First, we examine the constitutional framework enabling civilian control over the use of force. This is followed by an analysis of oversight mechanisms that may be exercised by the judiciary and the legislature and evaluate the extent to which (if any) oversight has been exercised in practice. Finally, we will look specifically at the role of the military in shaping India's doctrine on security operations and focus on the institutional structures underpinning civil-military cooperation and the reforms suggested over the years.

Constitutional Framework on the use of military force

The Constitution of India explicitly establishes civilian control over the military and the use of armed forces[5]. Anit Mukherjee argues that the enduring maintenance of civilian control represents one of the greatest successes of India's democratic history[6]. Article 53 of the Constitution of India clearly stipulates that the Supreme Command of the Defence Forces of the Union is vested in the President of India and that the exercise "thereof shall be regulated by law." However, neither the Constitution nor other legislations governing military and defence institutions expressly outline the criteria, procedures, or safeguards around the use of military force.

The sole explicit reference (albeit indirect) to the use of force is found in Article 352 of the Constitution[7]. Instead, Article 352 empowers the President to declare an emergency (in part, or across the whole of India) in certain scenarios including but not limited to: war, external aggression or the likelihood of war, or the probability of a foreign attack. While this provision ostensibly endows

---

[5] SUDHIR KRISHNASWAMY, MADHAV KHOSLA, *Military Power and the Constitution*, India Seminar, Available at: https://www.india-seminar.com/2010/611/611_sudhir_&_madhav.htm (last visited April 04, 2024).

[6] ANIT MUKHERJEE, *Towards control and effectiveness: The Ministry of Defence and civil-military relations in India*, in *Journal of Strategic Studies*, 45, 2022, 821.

[7] The Constitution of India, 1950, Art. 352.

the President with substantial authority, its scope was significantly curtailed by the 42nd constitutional amendment (1976) which stipulates that there shall be a Council of Ministers with the Prime Minister at the head to aid and advise the President, "*who shall act in accordance with such advices*"[8]. As India is a parliamentary democracy, the office of the President is largely a ceremonial position, and the real authority responsible for determining when to use force vests with the Prime Minister. No domestic legal provisions constrain the decision-making powers of the Prime Minister when authorising the use of force. However, there are parliamentary procedures enumerated (partly) in the Rules of Procedure for the Lok Sabha and Rajya Sabha that help enshrine some form of accountability (and they shall be discussed below).

It is also worthwhile noting that though federalism is an important organizing principle that is constitutionally recognized in India, there is a strong tendency towards a unitary system of government. Within this framework, there exist delineated lists – the Union (i.e., the federal), the state, and concurrent – that demarcate the jurisdictional ambit of the Federal and State governments respectively. Entry 14 of the Union List expressly stipulates that "entering into treaties and agreements with foreign countries, and implementing of treaties, agreements and conventions with foreign countries" falls within the purview of the Union Government. As a matter of practice, the Office of the Prime Minister decides when to use force, but in the case of an ongoing armed conflict, they delegate operational decisions to the military[9]. Nevertheless, the Constitution normatively signals that this must be done in conjunction with international law. The Directive Principles of State Policy (DPSP), though non-binding, function as overarching guidelines that encapsulate the aspirational framework envisioned by the constitution's drafters.

These principles delineate objectives for the Indian state, with Article 51 of the Indian Constitution in particular, expressly outlining a foundational pillar of India's approach to international law[10]. This includes, the promotion of international peace and security, the

[8] The Constitution (Forty Second Amendment) Act, 1976.

[9] SRINATH RAGHAVAN, *Soldiers, Statesmen and India's Security Policy*, in *India Review*, 11/2, 2012, 121–122.

[10] "The Directive Principles of State Policy may be considered as a commandment to the Union of India", see, P. CHANDRASEKHARA RAO, *The Indian Constitution and International Law*, New Delhi, 1993, 5.

maintenance of just and honourable relations between nations, the cultivation of respect for international law and treaty obligations in the interactions between organised peoples, and notably, the settlement of international disputes through pacific means (arbitration)[11]. Though the text of this provision seems to signal a normative alignment with international legal rules, the extent to which India's orientation has materialized in state practice is a more complex and multidimensional problem to resolve. The Constituent Assembly Debates offer significant interpretative insights, but their impact on shaping India's commitment to international law, particularly concerning its defense policy - both kinetic and cyber - has been minimal[12]. The following section which examines frameworks of judicial and legislative oversight will demonstrate this.

Judicial and Legislative Oversight

Judiciary - As a matter of judicial practice, the Courts have been somewhat inconsistent in their application of international law within a domestic context. Courts have generally subscribed to the transformation doctrine which requires explicit enforcement of international law through domestic legislation[13]. Notably, courts have referenced articles 51 and 73 – of the Indian Constitution detailing the Union's executive power over treaties – and Article 253, authorizing the Union to legislate the enforcement of international law (an implementation clause of sorts). Recent cases, however, reflect a shift from the doctrine of transformation to *incorporation* – which calls for recognizing international law as already a part of Indian law[14]. This

[11] Supra Note 7, see Art. 51.

[12] Shri H.V. Kamath contended that to establish an overarching international legal system – a "Super State", as he termed it – nations must first demonstrate adherence to international law. He viewed Art. 51 (formerly Art. 40) of the Constitution in this context, arguing that it symbolizes both India's longstanding cultural and historical tradition of non-aggression and the (then) contemporary need for a carefully designed and monitored international system (in a frenzied context of rising Cold War tensions). Shri K.T. Shah's support for the same provision stemmed from his belief that it significantly contributes to disarmament efforts. In both Shah and Kamath, one is able to sense a real commitment to engaging in the international arena (to move towards an international rules-based order), and a real sense that engaging proactively in the commitment to disarmament and international peace and security is at once both an instrumental endeavour and crucial to the postcolonial agenda.

[13] V.G. HEGDE, *International Law in the Courts of India*, in *Asian Yearbook of International Law*, 19, 2013, 72-75.

[14] APARNA CHANDRA, *India and international law: formal dualism, functional monism,* in *Indian Journal of International Law*, 57(1), 2017, 40-42.

progressive embrace of an international legal order is however restricted largely to contexts such as human rights, gender justice, and environmental law. In matters of defense, the Courts tend to be more reticent about the application of international law. For instance, in the interlocutory order in Mohammad Salimullah, the court refused to accept the principle of non-refoulment as part of CIL, despite its broad recognition[15].

Some scholars have attributed the subordinate treatment of customary international law (CIL) to judicial oversight which appears to be a systemic concern (given the lack of judicial engagement about both its validity and content in a series of cases). We argue however, that these cases are reflective of particular political choices. The case revolved around the deportation of Rohingya refugees and the Court's claim that non-refoulment is not a part of CIL, by virtue of India's non-ratification of the 1951 Refugee Convention, implies a deliberate prioritization of state sovereignty over international commitments. This has implications for understanding India's approach to recent international legal developments in regulating emerging technologies. Namely, that when CIL-recognition precedes India's treaty commitments (particularly in the context of 'instant-custom') – it remains unclear if Indian courts will consider such norms binding on the nation. And the court's turn to the doctrine of incorporation (recently in human rights contexts) seems unlikely to be repeated in the defence and national security context, where international law is often recognized only when articulated through stable treaty commitments.

Legislature – The Parliament was designed to function as a locus of accountability and oversight in India. To that effect, there are broadly, three formal mechanisms through which members of Parliament (MPs) can utilize the institution to hold the ruling party accountable. However, the effectiveness of these mechanisms, (briefly discussed in this section) has been restricted, largely due to the power disparities that permeate the legislative institution. Among these

[15] VAYUNA GUPTA, *Using International Law in Domestic Courts*, in *NYU Journal of International Law and Politics*, 54, 2022, 1084. See also, Unreported Judgments, Mohammad Salimullah v. Union of India, Interlocutory Application No. 38048 of 2021 in Writ Petition No. 793 of 2017, decided on Apr. 8, 2021 (SC), available at: https://main.sci.gov.in/supremecourt/2017/27338/27338_2017_31_1502_27493_Judgement_08-Apr-2021.pdf (last visited April 04, 2024).

mechanisms, the No-Confidence Motion stands out as a potent tool for holding the Government accountable, especially during periods of coalition rule[16]. That said, a government with a significant parliamentary majority is unlikely to be dissuaded by the introduction of no-confidence motions[17].

The second mechanism involves the Opposition's authority to question the Government and engage in Parliamentary debates, spotlighting critical national issues and revealing insights into government operations for the public. This occurs through two modes: the formal Question Hour, and the more informal Zero Hour[18]. Since public broadcasting of the Question Hour began in 1991, it has become one of the most prominently observable aspects of parliamentary proceedings. Parliamentary rules offer guidance on the kind of questions MPs could ask, such as keeping questions within a 150 word-limit, ensuring precision, and prohibitions on questions about confidential and sub-judice matters[19]. While MPs are required to specify whether they prefer oral or written responses (referred to as starred or unstarred questions, respectively), it is ultimately the presiding officers of the two Houses who determine whether an MP's question will be admitted. In contrast, Zero Hour although not formally mentioned in the rules of procedure stands as an innovative feature unique to the Indian Parliament. It serves as a valuable tool for raising important national issues[20].

Both the Zero Hour and Question Hour processes however, have been suspended during times of crisis, including but not limited to public emergencies, and war-time contexts[21]. Despite concerns being

---

[16] M. LAVER, K.A. SHEPSLE, *Government accountability in parliamentary democracy*, in A. PRZEWORSKI, S. STOKES, B. MARIN (Eds.), *Democracy, Accountability and Representation*, 1999, 279-296.

[17] Reuters, *India's Modi Survives No-Confidence Vote Over His Handling of Ethnic Violence*, NBC News, August 11, 2023, available at: https://www.nbcnews.com/news/world/india-narendra-modi-manipur-ethnic-violence-rcna99411 (last visited May 06, 2024).

[18] CHAKSHU ROY, *An Expert Explains: What are Question Hour and Zero Hour, and why they matter*, Indian Express, September 6, 2020, available at: https://indianexpress.com/article/explained/an-expert-explains-what-are-question-hour-zero-hour-parliament-session-6580747/ (last visited March 27, 2024).

[19] *Ibid.*

[20] *Ibid.*

[21] SMRITI KAK RAMACHANDRAN, *Not the first time Question Hour is being suspended*, Hindustan Times, September 03, 2020, available at: https://www.hindustantimes.com/india-news/not-the-first-time-question-hour-is-being-suspended-bjp/story-UQ20MwONW5kX8urWlYxsPP.html (last visited May 06, 2024).

flagged by Opposition MPs, (resulting in walkouts and protests) Zero Hour and Question hour were suspended recently during COVID (allowing only unstarred-written question). However, there is unfortunately, a richer bipartisan history of suspending these accountability-mechanisms in the past. During the Chinese Aggression in 1962, after agreement between the ruling and opposition parties, Question Hour was suspended. Further, during the Emergency era, special sessions of Parliament were held without a Question Hour[22].

The third mechanism, Parliamentary Committees, stands out as comparatively robust (though plagued by its own institutional shortcomings) in contrast to the previous two methods. There are various ways of categorizing Parliamentary Committees, for instance, into Departmentally Related Standing Committees (DRSC), Financial, Administrative, Accountability, and Ad-Hoc Committees[23]. For organizational ease, they can be grouped into Standing Committees & Ad-Hoc committees, which in turn can be either select or joint. Select committees consist solely of members from one house, whereas joint committees consist of members from both houses. While this may seem like a robust structure for scrutinizing government operations, it suffers from two institutional deficits, expertly highlighted by Devesh Kapur and Pratap Bhanu Mehta[24].

The first concern lies in the Parliament's tendency to overlook committee reports due to a mismatch of incentives. The Government is naturally disinclined to present reports for discussion if they diverge from its stance. Conversely, if reports largely align with the Government's position, the Opposition may perceive them as having limited value. And secondly, both the Government and the Opposition are invested in ensuring that the parliamentary agenda remains closely aligned with executive intentions, as the Opposition also conceives of

[22] ANJISHNU DAS, *Parliament special session: Very few instances of Question Hour being scrapped,* Indian Express, September 12, 2023, https://indianexpress.com/article/political-pulse/parliament-special-session-very-few-instances-of-question-hour-being-scrapped-8936588/ (last visited April 04, 2024).

[23] Parliamentary Committees Effectiveness, PRS Report. See also, Parliamentary Committees, Lok Sabha Secretariat, (2019), Available at: https://loksabha.nic.in/writereaddata/our%20parliament/Parliamentary%20Committees.pdf (last visited April 04, 2024).

[24] DEVESH KAPUR, PRATAP BHANU MEHTA, *The Indian Parliament as an Institution of Accountability*, in *Democracy, Governance and Human Rights*, Programme Paper Number 23, UNRISD, 2006, 11-14.

itself as a potential future government[25]. Though it is difficult to analyse the quality of deliberations when committees sit (outside of reviewing the reports they produce), the number of sittings by DRSCs can stand in as a quantitative-indicator. In that regard, the faults highlighted by Kapur and Mehta are reflected in the fact that the number of sittings has declined for most Committees and quite drastically in the Defense context[26].

To understand the role of Parliamentary Committees in overseeing and ensuring accountability, we propose a novel three-part classification to delineate their core functions. First, they act as pivotal tools for fact-finding, offering a means to document the historical record (i.e., of military operations) accurately. This is particularly critical in the absence of a transparent and legislated doctrine (the reports discussed in this section, shall offer a window into how this fact-finding function is realised in practice). Second, in cases where security lapses occur, such as inadequate responses to terror attacks, various committees contribute by identifying and highlighting the exact reasons for these failures and condemning those responsible. And finally, these committees play an active role in shaping national military policy. They are instrumental in helping construct efficient institutional frameworks that streamline military command inef-ficiencies and promote enhanced security measures.

Their fact-finding functions are well established, given the role DSRCs play in scrutinizing funds allocated to the ministries. Their recommendations help MPs understand the implications of financial allocations, facilitating more informed debates on the Demand for Grants in the Lok Sabha[27]. When these committees work effectively, they can significantly influence the way policies are received in the Parliament. With respect to the second function, i.e., critical security oversight and analysis, the committees' approach is generally reactive, prompted by Opposition members who actively seek briefings from the Ministry of Defence (MoD). This dynamic has manifested on

[25] *Ibid.*

[26] Study Material on Parliamentary Practices and Procedures, Lok Sabha Secretariat; PRS. See the following reports for recent source material: Departmentally Related Standing Committees - Summary of Work, Seventeenth Lok Sabha (2019-2020) (2021-2022), (2022-2023).

[27] MANISH KANADJE, ANYA BHARAT RAM, *Parliamentary Committees: Increasing their effectiveness*, PRS, December 2019 https://prsindia.org/files/parliament/discussion_papers/Parliamentary%20Committees%20Increasing%20their%20effectiveness.pdf (last visited May 06, 2024).

multiple occasions. For example, in the aftermath of the 26/11 terrorist attack, the Standing Committee on Defence highlighted the absence of a unified command structure, and intelligence integration[28]. In fact, this very concern was reiterated by the same committee during the 15th Lok Sabha session[29].

Additionally, following the Pathankot terror attack, a Parliamentary panel issued a scathing condemnation of the government, asserting that there were grave deficiencies in the country's counter-terrorism establishment.[30] In its 197th report, the Parliamentary Standing Committee on Home Affairs also expressed suspicion about the role of the Punjab Police forces in the Jan 2nd terror attack[31]. While Standing Committees are reactive, they do have some forward looking functions, and on occasion, offer key recommendations for policy formation and institutional improvements. For instance, the Standing Committee on Home Affairs presented a report titled "Border Security: Capacity Building and Institutions". Within this report, the committee highlighted that more than a year had passed since the Pathankot terror attack, yet the investigation by the NIA remained incomplete[32].

Moreover, the committee put forth constructive recommendations aimed at enhancing security. For instance, the committee proposed declaring the Pathankot airbase (located in close proximity to the border) as a high-security zone, and securing it through round-the-

[28] "The CDS in America, England, France and Germany are operational command and control authorities. We in India do not have such a set up and that is why the operational control during 26/11 was chaotic. No body really knew who was controlling the operation at Mumbai or whether it was being controlled from Delhi or Mumbai". See, Standing Committee on Defence, Fourteenth Lok Sabha, Status Of Implementation of Unified Command for Armed Forces, Thirty Sixth Report, 1.20, February 2009.

[29] Standing Committee on Defence, Fifteenth Lok Sabha, Action Taken Report on the recommendations/observations of the Committee contained in the Thirty-sixth Report (Fourteenth Lok Sabha) on 'Status of Implementation of Unified Command for Armed Forces, Second Report, ¶ 1.20 December 2009.

[30] Parliamentary Panel Raps Government For Terror Attack in Pathankot Airbase, The Economic Times, July 13, 2018, available at: https://economictimes.indiatimes.com/news/defence/parliamentary-panel-raps-government-for-terror-attack-in-pathankot-airbase/articleshow/52092160.cms (last visited April 04, 2024).

[31] *Ibid.*

[32] "The Committee also enquired as to why no post-facto analysis of intelligence failure was done after the Pathankot attack and why the Government failed to learn from the past failures as the terrorists perpetrated successive attacks during 2016". See Department-Related Parliamentary Standing Committee on Home Affairs, Rajya Sabha, Border Security: Capacity Building and Institutions, Two Hundred Third Report, 4.4.1, April 2017.

clock patrolling to restrict access to the surrounding population[33]. Similarly, the Standing Committee on External Affairs led by MP Dr. Tharoor, produced an insightful report shedding light on Indo-Pak relations, and reflects a nuanced and considered perspective, untainted by political exigencies. Regarding the surgical strikes, the committee observed that the Indian Army conducted a measured counterterrorism operation in September 2016, signifying a restrained response and continuity of India's policy of strategic restraint[34] in contrast to the largely bellicose political and media rhetoric[35]. Such Parliamentary reports consequently aid our analysis of India's strategic posture, including on international legal questions.

Role of the military in crafting India's doctrine on the use of force

An overarching governance doctrine outlining the decision-making process for the use of force is notably absent in India's military framework. Historically, India's military posture has been fundamentally "non-provocative", based on the philosophy of "defensive defence"[36]. The Sundarji doctrine, named after a former Chief of Staff, formed a crucial part of India's defence strategy, entailing the deployment of units along the border with geopolitical adversaries[37]. These units, categorized as "holding corps" were composed of infantry divisions primarily configured for static defence with limited offensive capabilities. Their wartime role encompassed halting enemy advances. Complementing this, the offensive "strike corps" were positioned in central India, far from the international

[33] *Ibid.* See 2.4.4 Additionally, the committee suggested the establishment of the National Centre for Counter Terrorism, as a central agency to address counter-terrorism efforts, See 3.4.5.

[34] SAI P. KODIDALA, Standing Committee Report Summary – Indo-Pak Relations, PRS Legislative Research, August 30, 2017, available at: https://prsindia.org/files/policy/policy_committee_reports/SCR%20Summary%20on%20Indo-Pak%20relations.pdf (last visited April 04, 2024). The committee recommended sustaining this policy while engaging in diplomatic efforts to highlight Pakistan's support for terrorism.

[35] S. PANDIT, S. CHATTOPADHYAY, *Coverage of the Surgical Strike on Television News in India: Nationalism, Journalistic discourse and India-Pakistan conflict*, in Journalism Practice, 12(2), 2018. 162-175.

[36] G. FERNANDES, *The Dynamics of Limited War,* in *Strategic Affairs*, 7, October 16, 2020, available at: http://www.stratmag.com/issueOct-15/page07.htm (last visited March 27, 2024).

[37] WALTER C. LADWIG III, *A Cold Start for Hot Wars?*, in *International Security*, 32(3), 2007.

border[38]. However, the persistent utilization of sub-conventional warfare tactics by Pakistan, including the terrorist attack on the Indian Parliament in Delhi, prompted a revaluation of India's approach around the turn of the century. This led to the emergence of the "Cold Start Doctrine" in 2004, characterized by operational readiness and swift mobilization[39].

The doctrine was introduced to address these shortcomings in India's military stance. Analysts characterize this limited war doctrine as aimed at establishing the capability to mount a retaliatory conventional strike against Pakistan or other geopolitical adversaries, causing substantial damage while maintaining a set of limited objectives narrow enough to prevent Islamabad from justifying an escalation to a nuclear conflict[40]. Military officials have stressed that India's doctrine is not a fig leaf for aggression and is primarily rooted in defending territory and furthering India's integrity[41].

After a rigorous review of India's military documents, Tarapore concludes that "the Indian Army—and by extension, Indian defense policy more generally—is dominated by an orthodox offensive doctrine. This is an approach to the use of force that centers on large army formations, operating relatively autonomously from political direction, seeking to impose a punitive cost on the enemy. The punitive cost often takes the form of capturing enemy territory as a bargaining chip, even though India usually pursues strategically defensive war aims to maintain the territorial status quo"[42]. Tarapore

---

[38] *Ibid.*, 160.

[39] Indian Army Doctrine 2004. ("Readiness of the Indian Armed Forces to meet national emergencies is a facet of national level endeavour. It calls for a synergised effort by all instruments of the Government to ensure that these forces are moved to their areas of operations, fully equipped and within an acceptable timeframe. The Government, on its part, would indicate and maintain a clear and strong resolve to go to war when it orders a general mobilisation. There may also be other methods of preparation for war even without ordering general mobilisation. On the part of the Armed Forces, they are responsible for ensuring that they are operationally ready, troops are in a high state of morale and units are appropriately trained to execute the missions assigned to them"); WALTER. C. LADWIG III, *A Cold Start for Hot Wars? The India's New Limited War Doctrine*, in *International Security*, 2007, 159.

[40] ALI AHMED, *India's limited war doctrine: The structural factor*, IDSA Monograph Series No. 10, December 2012, https://www.idsa.in/system/files/Monograph10.pdf (last visited May 06, 2024).

[41] Express Web Desk, *What is India's Cold Start doctrine?,* The Indian Express, September 21, 2017, available at: https://indianexpress.com/article/what-is/what-is-india-cold-start-doctrine-military-strategy-india-pakistan-indian-armed-forces-4854019/ (last visited April 04, 2024).

[42] ARZAN TARAPORE, *The Army in Indian Military Strategy: Rethink doctrine or Risk Irrelevance,* Carnegie India, August 10, 2020, available at:

acknowledges that this orthodox doctrine may be evolving as the Land Warfare Doctrine in 2018 recognizes grey zones and hybrid threats in today's security environment. Critically, Tarapore's work suggests that military operations by the army are run independently of the Executive. Therefore, for cyber operations not amounting to the use of force, we can expect that specific military institutions will be in charge rather than the Prime Minister.

Civil-military relations and reform measures

While recognizing the democratic and strategic value of civilian control over the military, scholars have also argued that a lack of cohesion and requisite cadres of expertise on military matters has plagued India's security posture[43]. The first major call for reform came in the Kargil Review Committee report which the Government commissioned in the wake of the Kargil War. Surprisingly, the report was published with limited redaction of information, and offers deeply illuminating insights into defence-related decision-making processes, and unveils numerous deficiencies with India's security management system, particularly in the realms of intelligence, border management, and defence-management[44]. The report distinctly emphasizes the need for a comprehensive reorganization of national security management and top-level decision-making protocols. It underscores the necessity to enhance coordination structures between the Ministry of Defence and the Armed Forces headquarters. Crucially, para 14.19 of the KRC Report asserts, "India is perhaps the only major democracy where the Armed Forces Headquarters are outside the apex governmental structure"[45].

The Group of Ministers (GoM) was established in April 2000, to review the national security system, and evaluate the recommendations made by the KRC. This initiative led to the

https://carnegieindia.org/2020/08/10/army-in-indian-military-strategy-rethink-doctrine-or-risk-irrelevance-pub-82426 (last visited April 04, 2024).

[43] *Supra* note 6.

[44] Kargil Review Committee, 29 Jul, 1999; see also, Kargil Review Committee Report: Executive Summary, reproduced in the U.S.I, Journal, January-March 2000,

[45] *Ibid.* See, ¶ 14.19 The report astutely notes that critical decisions on equipment, force levels, and strategy are not collegial but rather command oriented. This approach results in higher-level defence management decisions lacking in a consensus and broad based approach. To that effect, the report points out, "*The Prime Minister and Defence Minister do not have the benefit of the views and expertise of the Army Commanders and their equivalents in the Navy and Air Force*".

formation of four multidisciplinary task forces: Intelligence Apparatus, Internal Security, Border Management, and Management of Defence. The resulting recommendations from the GoM report, with the exception of one regarding the establishment of the Chief of Defence Staff, were accepted by the Cabinet Committee on Security[46]. These recommendations are useful in comprehending the foundations (and evolution) of India's institutional landscape for military intelligence operations. The newly integrated structures (namely, the Intelligence Coordination Group, and Technology Coordination Group) were introduced in anticipation of emerging security threats, which the GoM aptly identified as being integral to shaping India's military policy to this day. These threats range from nuclear-missile dynamics and cyber-information challenges to technological innovation and the persistence of international terrorism through means like low-intensity conflicts and proxy wars.

Following the tradition of the KRC and GOM Reports, The *Naresh Chandra Committee Report*, offers a range of recommendations aimed at reforming institutional structures[47]. A focal point of the report is its emphasis on synergizing the strengths of the armed forces through a unified command and control structure, notably through the establishment of the Special Operations Command[48]. The

[46] Report of the Group of Ministers on National Security, May 23, 2001, Government archives available at: https://archive.pib.gov.in/archive/releases98/lyr2001/rmay2001/23052001/r2305200110.html (last visited March 27, 2024). The establishment of the Intelligence Coordination Group (ICG), and the Technology Coordination Group (TCG) – working in conjunction with the National Technical Facility Organization. The ICG aimed to provide systematic intelligence oversight at the highest level. Its responsibilities encompassed overseeing the functioning of intelligence agencies and approving the annual tasking for intelligence operations.

[47] NITIN GOKHALE, *Naresh Chandra Task Force's Report on National Security: An Appraisal*, Vivekananda International Foundation, July 16, 2012, available at: https://www.vifindia.org/article/2012/july/16/naresh-chandra-task-force-s-report-on-national-security-an-appraisal (last visited April 04, 2024).

[48] Additionally, the report suggests the creation of a permanent position, the Chairman Chiefs of Staff Committee (COSC), albeit with a limited tenure of two years, filled by a four-star general. The eventual creation of the CDS, (further endorsed in subsequent reports), underscores the significance of an integrated approach – a notion echoed in various Standing Committee on Defence reports. See Brig. VINOD ANAND, *Defence Reforms and Naresh Chandra Task Force Review*, Vivekananda International Foundation, September 13, 2012, available at: https://www.vifindia.org/article/2012/september/13/defence-reforms-and-naresh-chandra-task-force-review (last visited May 06, 2024). This recommendation resonates with the suggestions outlined in the Arun Singh Committee on Defence Expenditure report and with the Standing Committee on Defence which strongly recommended a change in MoD staffing procedures to ensure that armed forces were "intrinsically involved in security management, and apex decision-making processes"[48]. See, Arun Singh Committee on

Naresh Chandra Report also advances the notion of synergy in civil-military functioning. This is proposed through the integration of armed services officers into the Ministry of Defence, progressing along the chain of command. Under the chairmanship of Lt. Gen (Retd) DB Shekatkar, the Ministry of Defence established a committee of experts known as the *Shekatkar Committee* entrusted with the mission of enhancing the armed forces' combat capabilities and rebalancing defence expenditure[49]. While the committee put forward a total of 99 recommendations in its report, the specific details remain classified due to security considerations.

The available information was facilitated through parliamentary inquiries, specifically through a written reply provided by Dr. Subhash Bhamre to Shri Amar Singh in the Rajya Sabha[50]. The committee's recommendations appear to be strategically aimed at cultivating a more streamlined and agile military force[51]. Strategic thinking by the military can be attributed in part to the Shekatkar Committee report (though the unification of the forces is a concept that has been referenced in earlier reports)[52]. This can also be gleaned from the speeches of political leaders. For example, the Prime Minister's address to military commanders aboard the INS Vikramaditya offers useful insights into the government's military policy stance. PM Modi urged them to reassess their beliefs, doctrines, objectives, and strategies. He underscored the importance of avoiding the simultaneous pursuit of divergent goals, such as modernization and force expansion. Instead, he stressed the significance of cultivating

---

Defence Expenditure (CDE), 1983, *and* Department-Related Parliamentary Standing Committee on Home Affairs, Rajya Sabha, Border Security: Capacity Building and Institutions, Two Hundred Third Report, ¶ No. 2.

[49] Press Information Bureau, Report of the Shekatkar Committee, Government of India, Ministry of Defence, 04-February, 2019.

[50] *Ibid.*

[51] These proposals encompass a range of measures, including the restructuring of forces involving approximately 57,000 posts of officers, JCOs and other ranks. The focal points of these recommendations involve harnessing technology-driven modernization initiatives for operational enhancement, optimizing infrastructure through the inclusion of radio monitoring companies, and rationalizing military operations by closing military farms and army postal establishments in non-conflict zones. See VINOD BHATIA, *Transformation: Military Force to Military Power*, in GURMEET KANWAL, NEHA KOHLI (eds.), *Defence Reforms – A National Imperative*, New Delhi, 2018, 99-106.

[52] SMRUTI DESHPANDE, *Theaterisation on the anvil, biggest change since independence says Chief of Defence Staff,* The Print, July 14, 2023, available at: https://theprint.in/defence/theaterisation-on-the-anvil-biggest-change-since-independence-says-chief-of-defence-staff/1670116/ (last visited April 04, 2024).

agile, technologically-driven forces that go beyond relying solely on human valour[53]. This indicates a proclivity to conduct cyber operations for which the institutional landscape is being readied, as we discuss later in the chapter.

However, one of the most significant reforms improving civil-military relations seemingly came out of nowhere as it was not deliberated upon or suggested by any previous reform committee. In 2019, while creating the post of the Chief of Defence Staff, the Indian government also designated General Bipin Rawat as the head of the newly minted Department of Military Affairs[54]. Staffed by military and civilian officers, the Department of Military Affairs handles matters pertaining to the armed forces, including the promotion of Jointness whereas the Department of Defense handles matters related to budget, Parliament and defence cooperation[55]. This development was pushed through to ensure better civil-military cooperation and to ensure that military officers have a say in the operational policies and doctrines applicable to the armed forces - consequently making them a relevant actor in the framing and implementation of international law.

Key takeaways

The Constitution of India, while vesting the Supreme Command of the Defence Forces in the President, delegates real authority to the Prime Minister, enabling civilian authority over decision-making. Judicial scrutiny (especially as it concerns the relevance and applicability of international law) to military operations (either cyber or kinetic) seems limited – given the reticence expressed by Courts to extend novel doctrines that recognize nascent international legal developments in the defence-national security context. The legislative framework, supplemented by various committees (such as DSRCs, and Government Committees, like the KRC, & GOM reports) plays a critical role in scrutinizing government actions, facilitating accountability, and suggesting key reforms to the institutional architecture for defence-decision-making. However, the effectiveness of these tools often wanes under the weight of parliamentary

[53] Press Information Bureau, PM chairs Combined Commanders Conference on board INS Vikramaditya at Sea, Government of India, Prime Minister's Office, 15-December 2015.

[54] Ministry of Defence, Government of India, Creation of New Department of Military Affairs, Press Information Bureau, February 03, 2020.

[55] *Supra* note 6.

majorities, or during crises, highlighting a periodic suspension of legislative oversight.

International law, while normatively significant, tends to be operationalized largely through treaties and formal agreements, with the Courts indicating a clear preference for treaty commitments over customary norms. This selective engagement with international law (in the defence context) underscores the strategic considerations that shape India's defence posture and reflect a cautious approach to integrating international legal norms directly into India's national defense policy. In summation, India's decision-making on the use of force is influenced by a centralized executive authority, legislatively moderated oversight, and a constrained but evolving judicial interpretation of international law. Traditional military doctrines, which emphasized defensive postures, are now pivoting towards operational readiness, synergy, and theaterization across the armed forces. This shift is reflected in the emerging emphasis on cyber operations, and the proactive reforms in civil-military relations, such as the establishment of the Chief of Defence Staff, and the Department of Military Affairs. This highlights a strategic realignment towards a more integrated and agile military.

II. Snapshots of India's State Practice on International Law and jus ad bellum.

India's overarching approach to international law has been context-specific and largely defensive, rooted in justifying specific actions after they have taken place or asserting specific interests, such as countering terrorism. Over the past few decades, there has been little attempt at normative construction or at proactively articulating India's position on the construction and implementation of key international law concepts such as the use of force and self-defence. As Sukumar poignantly suggests in an article aptly titled, 'How India lost its way in the study and use of international law': "There are two approaches to international law among pundits, politicos or practitioners in New Delhi: one that views it as 'rules for losers', i.e., weak and powerless states, to obey; and another, that argues states to

be in any case not bound by international law. To varying degrees, both claims are correct"[56].

He argues that this tainted perception of international law has led to the neglect of international legal scholarship and the institutions that promote it. Notably, this neglect contrasts sharply with the substantial investment made by India's first Prime Minister. A significant reason for this decline, is the segregation of international law from international relations (i.e., foreign policy). The use of international law in constructing a normative order that aligns with state interests, and in lending legitimacy either before or after the commissioning of geopolitically significant actions that potentially involve the use of force, has seen diminishing utility and declined in the eyes of the executive.

This approach has largely played out in the cyber domain as well. Ideological agnosticism on critical fissures in global debates allows India to partner with countries across the ideological divide on cyber and critical technology without getting boxed into an ideological corner. Consequently, India has not yet articulated a unified clear and coordinated position. Since Sukumar wrote his article in 2017, Indian Parliamentarians have also taken note. A report by the Parliamentary Standing Committee on External Affairs recognized the need to strengthen India's expertise and involvement in the framing and modification of international law in a report titled "India and International Law" published in 2021[57]. The Committee recommended that efforts to meet these objectives should involve both the recruitment of qualified personnel to the Ministry and also investments in research institutions through scholarships and funding of research undertaken by law students, professors, and academics. While it is too early to judge the uptake of this report and the specific recommendations contained therein, recent statements at the United Nations indicate some limited attempts at normative construction. Consequently, an Indian approach to international law can only be parsed together by a cumulative assessment of state practice and official statements made in the aftermath of major military incidents

[56] ARUN SUKUMAR, *How India lost its way in the Study and Use of International Law*, The Wire, April 02, 2018, https://thewire.in/diplomacy/india-is-lagging-behind-in-the-study-and-use-of-international-law (last visited May 06, 2024).

[57] Parliamentary Standing Committee on External Affairs, India and International Law (2021) Available at https://loksabhadocs.nic.in/lsscommittee/External%20Affairs/17_External_Affairs_9.pdf (last visited May 06, 2024).

with some more recent guidance from statements made at the United Nations Security Council.

Use of force in East Pakistan (1971). India's justification for the use of force in (then) East Pakistan(now Bangladesh) was justified with loose references to self-defence and humanitarian claims[58]. Ambassador Sen's justification for the use of force did not make an explicit reference to Article 51 of the UN Charter. However, he denied that India had violated the prohibition in Article 2(4) of the UN Charter as Pakistan had attacked first[59]. Therefore, Sen conjured up a new crime of 'refugee aggression' that stemmed from the victims of West Pakistan's atrocities in Bangladesh, who relocated to India. There was further reference to human rights as Sen argued that the "military repression" in East Pakistan was sufficient to "shock the conscience of mankind"[60]. India's justification for the use of force found few takers. Only the Soviet Union and Eastern bloc allies deftly argued that the use of force must be viewed in light of the significant military and political repression in East Pakistan but they also stopped short of justifying India's use of force. To that effect, on the 12th of December, 1971, India submitted communications to the UNSC, alleging that "India is a victim of yet another unprovoked Pakistani aggression and is engaged in defending its national sovereignty and territorial integrity in the exercise of its legitimate right of self-defence".

Surgical strikes in Pakistan (2016). On September 29, 2016 the Director General of Military Operations (DGMO) stated in a joint press release with the Ministry of External Affairs, that "surgical strikes" had been conducted by the Indian army against territory used as launching pads by terrorists in Pakistan. He stressed that "there had been continuing and increasing infiltration" and the strike was conducted "based on very credible and specific information which we received yesterday that some terrorist teams had positioned themselves at launch pads along the Line of Control". The DGMO also stressed that the matter of terrorists using Pakistani territory to

---

[58] N.J. WHEELER, *Saving Strangers: Humanitarian intervention in international society*, Oxford, 2002.

[59] Security Council Resolution (SCOR), 1606th Meeting, December 4, 1971, 17 cited in Wheeler.

[60] Transcript of Joint Briefing by MEA and MoD, Media Center, Ministry of External Affairs, September 29, 2016, available at: https://www.mea.gov.in/media-briefings.htm?dtl/27446/Transcript_of_Joint_Briefing_by_MEA_and_MoD_September_29_2016 (last visited May 06, 2024).

target India and inflict casualties was brought up with Pakistan at the highest military levels.

While the press release appears to use the framing of self-defence contained in the UN Charter and international law framework, the absence of explicit invocation of terms or legal provisions obstructs the extrapolation of a coherent Indian approach to the use of force and self-defence from this statement alone[61]. The 'surgical strike' was not reported to the United Nations Security Council, as the requirement in Article 51 of the United Nations Charter clearly stipulates. Further, the statement does not directly attribute the suspected terrorist activities to the Pakistani state although it suggests that the Pakistani government was unwilling to act. To be clear, Pakistan denied that these strikes took place and both countries did not explicitly state that these actions amounted to the 'use of force' under the United Nations Charter. In terms of understanding India's approach, therefore, we can discern that low intensity strikes against non-state actors in foreign territory is legally permissible.

The Balakot Air Strikes and Pulwama. Examining the Indian Government's position – that is, its officially articulated legal stance on the nation's adherence to international law – provides a valuable resource for understanding India's evolving approach to extraterritorial uses of force. However, before delving into an analysis of the Indian position regarding the air strikes carried out in Balakot, it is essential to review the series of encounters that precipitated this conflict. On February 14, 2019, a suicide bomber near Pulwama in Kashmir attacked a Central Reserve Policy Force (CRPF) convoy, killing 40 personnel[62]. Jaish-e-Mohammed (JEM), an organization proscribed by the UN, claimed responsibility for this attack. Notably, JEM has been implicated in a series of terrorist attacks, ranging from the Parliament bombing in 2001, and incidents in Pathankot and Uri[63]. Importantly, the historical record of these incidents was highlighted in

[61] SRINIVAS BURRA, *Use of Force as Self-Defence against Non-State Actors and TWAIL Considerations: A critical analysis of India's state practice,* in *Asian Yearbook of International Law*, Volume 24, 2018, 106-127.

[62] SAV editorial Staff, *Regional Roundtable: Reflections on Balakot*, SOUTH ASIAN VOICES (2022), https://southasianvoices.org/regional-roundtable-reflections-on-balakot/ (last visited Aug 30, 2023).

[63] ASAD HASHIM, *Profile: What Is Jaish-e-Muhammad?*, Al Jazeera https://www.aljazeera.com/news/2019/5/1/profile-what-is-jaish-e-muhammad (last visited Aug 30, 2023).

the Government's statement, as it contributes (in part) to India's defence justifying its use of force.

On February 26, 2019, the Foreign Secretary of the Ministry of External Affairs issued a statement in which - while characterizing the actions conducted by the Air Force - employed specific terminology that warrants scrutiny: "The Government of India is firmly and resolutely committed to taking all necessary measures to fight the menace of terrorism. Hence this non-military pre-emptive action was specifically targeted at the JeM camp. The selection of the target was also conditioned by our desire to avoid civilian casualties"[64].

The phrase used in the statement was that the air strikes in Balakot constituted a form of non-military pre-emptive self-defence. This declaration holds significant implications for understanding India's efforts to expand the potential for conventional military superiority and for offensive cyber operations (the latter shall be discussed at a later section of this paper). The use of the term "non-military" aligns with conventional usage, as it serves to communicate the operation's target - emphasizing their non-state-actor identity. This choice of language also aligns with the principles of the Geneva Convention[65], and serves the valuable purpose of clarifying the object of the operation in a manner that clearly limits its scope to a non-state actor (and not the Pakistani military or civilians). However, a closer examination of the term, "pre-emptive action" can be helpful given the ambiguity surrounding the exclusive use of these grounds as the Indian Government's sole recourse. An alternative legal basis could have been to assert that their actions were warranted by the traditional form of the right to self-defence, (when reinterpreted through the accumulation of events doctrine), thereby obviating the necessity to validate conceptions of pre-emptive action.

In his monograph, Tom Ruys elucidates that, according to the doctrine, "incidents that would in themselves merely constitute 'less grave uses of force', can when forming part of a chain of events, qualitatively transform into an 'armed attack' triggering the right of self-defence"[66]. Historically, this doctrine has had limited success in

[64] Media Center, Statement by Foreign Secretary on 26 February 2019 on the Strike on JeM training camp at Balakot, Ministry of External Affairs, Government of India, February 26, 2019.

[65] Additional Protocol I (1977), Articles 48, 51, and 52; ICRC, *Study on Customary International Humanitarian Law*, 2005, Rules 1 and 7

[66] TOM RUYS, *"Armed Attack" And Article 51 Of The Un Charter: Evolutions In Customary Law And Practice*, 2010, https://www.cambridge.org/core/books/armed-attack-

enabling states to undertake self-defensive military operations. Israel was the first to invoke this doctrine, contending that although individual terrorist attacks by the Palestine Liberation Organization lacked the status of an armed attack under international law, their cumulative effect elevated them to such a status[67]. Nonetheless, the UN Security Council did not endorse Israel's utilization of the doctrine[68]. Subsequently, the doctrine has garnered more recognition, receiving implicit endorsement in notable cases like *Nicaragua*[69]*, Oil Platforms*[70]*,* and *Democratic Republic of Congo v Uganda*[71].

Therefore, the government's decision to adopt a strategy that endorses the doctrine of pre-emptive self-defence - particularly when applied to non-state actors - certainly calls into question their broader motivations within the international legal landscape governing the use of force. This does not imply that the accumulation of events doctrine is devoid of shortcomings, given that it undermines the temporal requirements of the right to self-defence, and can broaden the notion of an armed attack[72]. Further, while referring to the unwillingness of Pakistan to deal with non-state actors operating on their territory, India stops short of explicitly underscoring the "unwilling or unable doctrine".

While potential for abuse exists, especially when wielded against non-state actors, the Government's approach on keeping this defence in reserve, while strongly advocating the right to engage in pre-emptive acts of self-defence against states accused of harbouring non-state actors such as Pakistan, provides significant insights into India's endeavours to enhance its capabilities for conventional military superiority. To gain a deeper understanding of the implications for India-Pakistan relations, Air Chief Marshal RSK Bhaduria, the Indian

---

and-article-51-of-the-uncharter/F31FCA4C7F6B1D561466CEEEDDF014FF (last visited Aug 30, 2023).

[67] DAVID KRETZMER, *The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum*, in *The European Journal of International Law*, 24(1), 2013, 243-244.

[68] J. FRANCISCO LOBO, *One Piece at a Time: The 'Accumulation of Events' Doctrine and the 'Bloody Nose' Debate on North Korea*, Default, https://www.lawfaremedia.org/article/one-piece-time-accumulation-events-doctrine-and-bloody-nose-debate-north-korea (last visited Aug 30, 2023).

[69] Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgement, 1986 I.C.J. Rep.

[70] Case Concerning Oil Platforms (Iran v USA), 2003 I.C.J. Rep. 246.

[71] Armed Activities on the Territory of the Congo (Democratic Republic of the Congo vs Uganda) 2005, I.C.J. Rep. 168.

[72] CH.J. TAMS, *The Use of Force against Terrorists*, in *The European Journal of International Law*, 20(2), 2009, 390.

Chief of Air Staff noted, "Balakot was a clear demonstration that there exists a space within the sub-conventional conflict boundary wherein the Air Force can be used for targeting and yet have escalation control"[73]. This presumably stands in contrast to India's approach of sending troops across the Line of Control carrying out missions (such as in 2016).

Normative articulation: The Arria Formula Meeting (2021). The clearest normative articulation came in India's statement at the Arria Formula meeting on the 24th of February, 2021. The statement embodies an expansionist interpretation, selectively incorporating dimensions of this right as rooted in both CIL and Art. 51 of the UN Charter[74]. The country's stance draws upon CIL, encompassing pre-emptive self-defence within the right of self-defence. Additionally, it leverages Art. 51 to assert the right to self-defence against non-state actors. Importantly, the statement offers insights into India's approach to dealing with Pakistan and terrorist outfits in its backyard. It establishes three criteria to aid in determining the permissibility of states employing force in the exercise of the right to self-defence against non-state actors operating from another state (typically referred to as the host state):

i. The non-state actor has repeatedly undertaken armed attacks against the State

ii. The host State is unwilling to address the threat posed by the non-state actor

iii. The host State is actively supporting and sponsoring the attack by the non-state actor[75].

Although there isn't express instruction regarding whether these conditions ought to be interpreted conjunctively or disjunctively, it is evident that (ii) and (iii) are inherently distinct. Condition (iii) applies to situations where the host State contributes positively to actions aiming to violate the sovereignty of the affected state, while condition

---

[73] Lt. Gen. DEEPENDRA SINGH HOODA (Retd.), *Three Years After Balakot: Reckoning with Two Claims of Victory*, Stimson Center (Feb. 28, 2022), https://www.stimson.org/2022/three-years-after-balakot-reckoning-with-two-claims-of-victory/ (last visited Aug 30, 2023).

[74] SRINIVAS BURRA, *India's Decisive Turn on the Right to Self-Defence,* Opinio Juris, March, 22nd, 2021, Available at: http://opiniojuris.org/2021/03/22/indias-decisive-turn-on-the-right-of-self-defence/ (last visited April 04, 2024).

[75] K. NAGARAJ NAIDU Statement by Ambassador, *Arria Formula Meeting Organized by Mexico: Upholding the Collective Security System of the UN Charter: The Use of Force in International Law, Non-State Actors and Legitimate Self-Defense*, https://www.pminewyork.gov.in/IndiaatUNSC?id=NDE3Nw (last visited Aug 30, 2023).

(ii) more closely approximates the widely recognized standard of "unwillingness to address the attack." However, as highlighted by Burra, the statement goes beyond the natural scope of the test, by referring to the unwillingness to address the 'threat' as opposed to the 'attack'[76]. A more appropriate interpretation of this statement is that (i) serves as a necessary condition, and either (ii) or (iii) must be present to justify the use of force by an affected state exercising its right to self-defence.

The contextual information presented in the Indian delegation's statement at the Arria Formula Meeting, is instrumental in clarifying the ramifications of this policy stance. In all but name, the statement unequivocally rebukes Pakistan for orchestrating a proxy war by providing support to terrorist groups and evading international censure. The statement further enumerates a series of terrorist acts that have affected India over the years, ranging from the 1993 Mumbai bombings, to the more recent incidents in Pathankot and Pulwama[77]. Additionally, the statement conveys the perspective that pre-emptive actions, even in the absence of consent from the state allegedly harbouring non-state actors, fulfil the above-stipulated criterion[78]. It posits that such actions do not amount to a reprisal, as the underlying intent is safeguarding the affected state's national integrity and sovereignty.

Overall observations. India's engagement with international law, particularly regarding the use of force and self-defence, reveals a pragmatic and evolving approach. Historically, the posturing has been defensive, with the Government often justifying actions post-facto rather than through proactive normative articulations. To understand how the Indian state has utilized international legal arguments within the UN system, it can be helpful to refer to the Harvard Law School's PILAC Catalogue of Communications to the Security Council[79]. This database outlines Member States' official responses in purported exercise of the right to self-defence from October 24, 1945, to December 31, 2018. Nearly all of India's state practice involving the invocation of international law and the UN system has occurred in the

[76] *Supra* note 74.
[77] *Supra* note 75.
[78] *Ibid.*
[79] Annex – HLS PILAC Catalogue of Communications to the Security Council of Measures Taken by United Nations Member States in Purported Exercise of the Right to Self-Defence: October 24, 1945 through December 31, 2018 (ed. D. A. LEWIS).

context of border skirmishes with Pakistan. The data reveals that Pakistan has more systematically used the UN system to assert compliance with international law and to accuse India of violating international legal commitments.

Over the 73 year period covered by the database, Pakistan has alleged on 12 separate occasions that India's actions were inconsistent with its international legal obligations, while India has submitted only four communications to the UNSC. In 1950, India did not respond to Pakistan's allegations, but it did in 1965, and 1971. In these instances, India's responses mirrored Pakistan's claims, with both sides accusing the other of territory encroachment, ceasefire violations, and acts of aggression, resulting in a tit-for-tat dynamic. However, recent developments such as the statements made at the UNSC, and the Arria Formula meeting, indicate a more assertive stance on the right to self-defence, specifically against non-state actors. This shift suggests an ongoing reassessment of traditional doctrines, moving towards a doctrine that accommodates preventive actions under certain conditions. Additionally, the military policy appears to be geared towards operational readiness and utilizing non-kinetic and sub-conventional modalities to deal with geostrategic threats on India's border. India's utilization of international legal rules, reflects strategic engagement, aimed at both legitimizing state actions against non-state actors (in the context of regional security threats that have been deemed significant), even in the absence of attribution to a sovereign state.

III. Institutional Architecture and Domestic Policy

India's cyber institutional architecture has already been covered in detail in existing literature, including by one of the authors[80]. Therefore, this section does not delve into a detailed overview of these institutions but highlights trends that might be relevant to assess and predict India's approach to international law. The newly minted

[80] ARINDRAJIT BASU, KARTHIK NACHIAPPAN, *Will India negotiate? The politics of multilateral engagement for fostering responsible state behaviour in cyberspace?*, in B. VAN DEN BERG, F. CRISTIANO (eds), *Hybridity, Conflict and the Global Politics of Cybersecurity*, Lanham, 2023, 189 ff.; see also ARINDRAJIT BASU, *India's cybersecurity operations: Tracing national doctrine and capabilities*, UNIDIR, 2023; GUNJAN CHAWLA, *The architecture of cybersecurity institutions in India*, Medianama, February 19, 2020, https://www.medianama.com/2020/02/223-architecture-cybersecurity-institutions-india-structure/ (last visited April 04, 2024).

Defense Cyber Agency that draws 1,000 personnel from all three branches of the armed forces falls under the administrative control of the Ministry of Defense (MOD)[81]. It was set up to "control and coordinate Joint cyber operations" according to the response to a Parliamentary question by the Minister of State for Defense[82]. Media reports suggest that the DCA has a wide array of offensive cyber capabilities and experts argue that the DCA may be developing a cyber doctrine in the future[83].

The Prime Minister's Office (PMO) oversees several entities with a cyber portfolio, of which the most significant is the Office of the National Cybersecurity Coordinator (NCSC). This Office advises on cybersecurity issues[84], and provides inputs in the formulation of India's stances at multilateral forums, in addition to advising national security officials within the PMO on cyber-focused issues[85]. The National Critical Information Infrastructure Protection Centre (NCIIPC),which was set up as a recommendation of the National Cybersecurity Policy, 2013 is tasked with protecting India's critical information infrastructure (CII). As per Section 70A of the IT Act, it has notified power, energy, banking, financial services, insurance, telecom, transport, government, and strategic and public enterprises as CIIs thus far[86]. Given its powers of notification, NCIIPC is important for shaping India's legal approach to the protection of CIIs.

The Ministry of Electronics and Information Technology (MeitY) is the nodal ministry for the formulation of technology related policy in India. MeitY officials are usually part of India's international delegations on forums negotiating cybersecurity related matters. India's Computer Emergency Response Team (CERT-In) also falls

---

[81] ET Bureau, *PM Narendra Modi attends combined Commanders conference in Jodhpur*, Economic Times, Sep 26, 2018, https://economictimes.indiatimes.com/news/defence/pm-narendra-modi-attends-combined-commanders-conference-in-jodhpur/articleshow/65996826.cms (last visited May 06, 2024).

[82] Ministry of Defence, Department of Government of India, Cyber Warfare Threats: Lok Sabha Starred Question No. 138, November 27, 2019.

[83] PRADIP R SAGAR, *Three-pronged plan*, The Week, June 01, 2019, available at: https://www.theweek.in/theweek/current/2019/05/31/three-pronged-plan.html (last visited May 03, 2024).

[84] E. HANNES ET AL, *Cyber resilience and diplomacy in India*, Digital Dialogue, EU Cyber Direct, July 2020, available at: https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/Rw8fdmZa/digitaldialogue-india-final.pdf (last visited May 4, 2024).

[85] *Ibid.*

[86] National Critical Information Infrastructure Protection Centre, Home Page, NCIIPC, https://nciipc.gov.in/ (last visited May 6, 2024).

within the ambit of the Ministry of Electronics and Information Technology.[87] CERT-In is critical for the implementation of international law as it ensures overall cyber hygiene within the country and also issues specific guidelines on cybersecurity practices by private sector entities. Another key international law implementing entity is the Ministry of Home Affairs (MHA) - responsible for tackling cybercrime and dealing with internal security threats. The Secretary of the Ministry of Home Affairs also has powers to authorise surveillance operations, which makes it critical to overseeing the implementation of international law (as we discuss below in the section on surveillance powers). Transparency and openness in the implementation of existing international law applied to cyberspace by both MeitY and MHA would go a long way towards bolstering India's image as a responsible cyber power.

Finally, the Ministry of External Affairs (MEA) leads India's cyber diplomacy efforts and is a key architect of India's stance on international law on various issues, including the cyberspace. It has two entities working specifically on cyber related issues. First the cyber diplomacy division usually coordinates India's positions at multilateral forums such as the United Nations First Committee. And second, the newly minted, New and Emerging Strategic Technologies (NEST) division, which was set up to "engage in technology diplomacy and deal with the foreign policy and international legal aspects of new and emerging technologies"[88]. As per a response by the Minister of State for External Affairs, NEST "will enable more active participation of India in global forums in the area of technology governance and promoting our national interests in that context"[89].

The panoply of institutions suggests that cyber operations capability may be distributed among relevant institutions in a given context. However, successful implementation will depend on whether and how the institutions are able to effectively coordinate responses and cooperate across various strategic dimensions. Given the expected frequency of cyber operations, it is unlikely that the Prime Minister's

---

[87] Ministry of Electronics and Information Technology, Indian Computer Emergency Response Team (CERT-in), MeitY, https://www.meity.gov.in/content/icert (last visited May 13, 2024).

[88] Lok Sabha, Question No.552 New and Emerging Strategic Technologies Division, Feb 05, 2020, available at: https://mea.gov.in/lok-sabha.htm?dtl/32359/question_no552_new_and_emerging_strategic_technologies_division (last visited May 6, 2024).

[89] *Ibid.*

Office will sign off on every single one. Existing practice suggests that operational autonomy has been given to the military during an ongoing armed conflict. Consequently, each institution takes on a critical role in conceptualising and overseeing both domestic and international cyber operations. The role of cyber institutions acquires even more salience due to the diluted powers of Parliament to undertake meaningful oversight. The recent establishment of institutions such as the DCA and NEST indicates that a clearer articulation or strategy in the cyber domain is likely to emerge from one of these institutions.

Domestic legislation governing cybersecurity. India's domestic legal framework on cyber operations is captured in the Information Technology Act (IT Act). It imposes monetary penalties on several actions related to computer infrastructure or resources[90]. This includes unauthorized access, downloads, introduction of computer contaminants, damage, and denial of access. The legislation covers acts by any person regardless of location or nationality insofar as the impacted computer system is located in India. This is an express legal prohibition on offensive cyber operations conducted on computer systems located in India. Further, there are several acts concerning computer infrastructure that are criminalised[91]. These include tampering with source code documents, impersonation via a computer resource or electronic device, and cyber terrorism including denial of access to computer resources or unauthorised access that threatens the unity, integrity, security or sovereignty of India. Law enforcement authorities have a clear role to play here. The Act stipulates that investigation of these said offences should be conducted by a police officer not below the rank of Inspector[92].

Legal and Policy Framework Governing the Activities of Intelligence Agencies

Law and Statutory Provisions. While the Army is in charge of intelligence connected to the military domain, a range of statutory provisions provide India's domestic intelligence agencies sweeping powers to conduct surveillance both on Indians and foreigners

[90] The Information Technology Act, 2000, S. 43.
[91] *Ibid.*, see. section 66.
[92] *Ibid.*, see section 78.

The Telegraph Act. The fulcrum of India's legal architecture enabling surveillance stems from Section 5(2) of the British era Telegraph Act. *Section* 5(2) requires a two-fold test that needs to be satisfied for the Central or State Government to authorise the interception of wired and wireless messages. First, there should be an occurrence of a public emergency or interest of public safety. Second, the interception must be 'necessary or expedient' in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence[93]. Rule 419A of the Indian Telegraph Rules states details regarding the process to be followed before, during, and subsequent to the interception. This includes the relevant sanctioning authority that can issue such an order, the review process, and the total duration of the interception order[94]. However, there is no provision for judicial oversight. The provisions of the Telegraph Act have been used to justify phone-tapping, as the case law discussed in the next section demonstrates.

The IT Act. The Information Technology Act, 2002 further extends the powers provided by The Telegraph Act. Through the IT Act, the government and intelligence agencies enjoy a wide range of powers when it comes to the interception, monitoring and decryption of data "generated transmitted, received or stored in any computer resource." Section 69A of the IT Act provides these powers if it is necessary for a gamut of purposes including protecting the sovereignty or integrity of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offence or for any investigation[95]. Section 69B empowers any agency notified by the Central Government to monitor or collect traffic data or information using any computer resource for the purpose of cybersecurity. The provisions do not differentiate between Indian citizens and foreigners. However, as the jurisdiction clause of the Information Technology Act suggests that the legislation applies to "the whole of India," section 69 can be interpreted to refer to any data being transmitted through computer systems located in India.

The procedural safeguards to these powers are provided for in the Information Technology Procedures and Safeguards for

[93] The Indian Telegraph Act, 1885, S. 5(2).
[94] Rule 419A of the Indian Telegraph Rules, 1951.
[95] *Supra* note 90, see, S. 69(A) and 69(B).

Intervention, Monitoring and Decryption of Information Rules read with section 69(2) of the Act. Rule 4 of the said rules stipulates that the competent authority has the power to authorize any agency of the Government to intercept, monitor or decrypt information generated, transmitted or stored in any computer resource. Through a statutory order dated 20.12.2018, the Ministry of Home Affairs codified existing legal provisions notifying that ten law enforcement agencies were empowered to generally conduct intelligence activities.[96] However, each case of interception, monitoring or decryption would require approval from a competent authority, that is the Union Home Secretary or the relevant state Home Secretary in certain cases. Further, as per rule 22, every case is placed before a review committee headed by the Cabinet Secretary that meets at least once in two months. However, these reviews are not made available for scrutiny by the judiciary or any non-governmental authority[97]. Moreover, the IT Act and rules are silent on the substantive grounds for restricting the powers of intelligence agencies. The recently passed Digital Personal Data Protection Act does not impose any restrictions either as it grants broad powers to the Central Government to exempt itself from data privacy requirements[98].

Case Law on Surveillance. The statutory provisions within the Information Technology Act and the Telegraph Act, respectively, confer considerable authority upon the State to surveil its citizens, often citing grounds such as public order and safety, which in practice tend to be nebulous and politically motivated. Nonetheless, the trajectory of the Judiciary can be characterized as progressively inching towards the realization of individual rights (though the path as it stands is asymptotic). Spanning from M.P. Sharma v Satish Chandra, to Manohar Lal Sharma, a series of pivotal decisions have

---

[96] PIYUSH JOSHI, PRITHVIRAJ CHAUHAN, *India's Leap Into Formalised Electronic Surveillance: The MHA Statutory 6227(E) Dated 20.12.2018*, Mondaq, December 27, 2018, available at: https://www.mondaq.com/india/it-and-internet/767906/indias-leap-into-formalised-electronic-survelliance-the-mha-statutory-order-6227e-dated-20122018 (last visited May 6, 2024).

[97] DEVDUTTA MUKHOPADHYAY, *IFF files rejoinder in PIL seeking surveillance reform*, Internet Freedom Foundation, April 23, 2019, available at: https://internetfreedom.in/iff-files-rejoinder-in-pil-seeking-surveillance-reform/ (last visited May 06, 2024).

[98] SARVESH MATHI, *Fifteen Major Concerns With India's Digital Personal Data Protection Bill, 2023*, Medianama, August 04, 2023, available at: https://www.medianama.com/2023/08/223-major-concerns-india-data-protection-bill-2023-2/ (last visited May 06, 2023).

been sequentially reinforcing one another. Through this process of accretion, these judgments have been gradually converging to establish a robust judicial framework that safeguards a citizen's right to privacy, including, crucially, informational privacy.

The judiciary's discussion of surveillance and its limits has understandably developed alongside the evolution of India's legal landscape around privacy. Before delving into these cases, it is important to underscore that privacy is absent from both the constitution, and the constituent assembly debates. The initial case addressing this matter, was M.P. Sharma v Satish Chandra, in which the Court rejected the right to privacy in the context of search and seizures of documents[99]. The subsequent significant case was Kharak Singh v. State of U.P. where the Police Regulations permitted the surveillance of history sheeters (i.e., individuals with extensive criminal records)[100]. An important feature of the Indian Judiciary's approach has been its engagement with international jurisprudence on this matter notably with US Courts. In that regard, the bench in Kharak deemed it pertinent to delineate its position on privacy from the largely propertarian jurisprudence of the United States (Wolf v Colorado)[101]. Instead, it anchored its concept of privacy in dignitarian principles. A pivotal part of the Court's analysis, wherein it echoed the State's argument that surveillance was warranted due to the targets being recognized threats to public order with a history of anti-social behaviour, has played a significant role in shaping the Court's trajectory in subsequent matters. The majority opinion held that unlawful intrusion into the home constitutes a violation of personal liberty, and the minority held that the right to privacy is an essential ingredient of personal liberty.

A decade later, in the case of R.M Malkani v State of Maharashtra, the Court following in line with its analysis in Kharak Singh, upheld the legality of phone tapping, while underscoring that it was permissible only when directed at a proven offender[102]. The Court explicitly stated that these laws were not intended for the surveillance of innocent civilians. By emphasizing the focused and specific nature of such interceptions, it offers valuable precedent in distinguishing between targeted actions, and the indiscriminate dragnet invasions of

[99] M.P Sharma v Satish Chandra, AIR 1954 SC 300.
[100] Kharak Singh v State of UP, AIR 1963 SC 1295 : (1964) 1 SCR 332.
[101] Wolf v Colorado, 93 L Ed 1782 : 338 US 25 (1949).
[102] R.M Malkani v State of Maharashtra, (1973) 1 SCC 471, 476.

privacy that are characteristic of the modern surveillance state[103]. In Gobind v State of MP, the Court's holding is altogether more significant, as the measure was backed by statutory authority. The judgment drew on influential American cases, such as Griswold v Connecticut, Roe v Wade, to contextualize privacy in the Indian setting. It positioned privacy as a right located in the penumbral zones of fundamental rights, e.g., the rights to freedom of expression, and movement[104]. Additionally, the Court clarified that intrusions into privacy, must be warranted by a compelling public interest – a noteworthy requirement, as fundamental rights are subject generally to the constraint of public interest, and the inclusion of the phrase "*compelling*", implies a more stringent requirement[105]. The Court also made decolonial arguments in this case, vehemently discouraging the use of surveillance methods by invoking India's history of freedom struggle against a police state. This argument draws a clear distinction between the general broad warrants issued by the British Empire, and the contemporary widespread, and non-targeted surveillance programs[106].

In Malak Singh, the Court advanced the jurisgenerative scope by asserting its authority to conduct judicial review, even in administrative decisions to assess the legitimacy of surveillance activities. These progressive steps culminated in a robust discourse on privacy's significance and the necessity for appropriate safeguards in surveillance activities, in the case of PUCL v Union of India. In this landmark case, the constitutionality of S. 5(2) of the Telegraph Act, was at issue, and the Court held that while privacy is not expressly enumerated in the Constitution, it constitutes an integral aspect of the right to life and personal liberty under Art. 21[107]. The Court held that this right can only be restricted through procedures established by law. Although the Court did not assert that judicial oversight alone was the exclusive safeguard for such surveillance measures, it did reprimand the Government for inadequately framing rules to prevent arbitrariness and ensure the protection of the right to privacy when

[103] GAUTAM BHATIA, *State Surveillance and the Right to Privacy in India: A Constitutional Biography*, in *National Law School of India Review*, 26(2), 2014, 127.
[104] Gobind v State of MP, (1975) 2 SCC 148.
[105] *Ibid.*
[106] *Ibid.*, see 134.
[107] PUCL v Union of India & Ors, AIR 1997 SC 568, (1997) 1 SCC 301.

issuing orders for telephone tapping under S. 5(2) of the Telegraph Act.

Ultimately, the right to privacy which had thus far been articulated in a patchwork (case-by-case) manner, resolved in K.S. Puttuswamy and Anr v UOI. In this case, the Court unanimously recognized that the right to privacy was constitutionally guaranteed (and fell under Art. 21), overruling M.P. Sharma and Kharak Singh[108]. The case drew on a range of relevant authorities in international law, including but not limited to the UDHR, ICCPR, and ICESCR. Justice D.Y. Chandrachud in his judgment discussed the bearing of international law in configuring the contours of the right to privacy – "In the view of this Court, international law has to be construed as a part of domestic law in the absence of legislation to the contrary, and perhaps more significantly, the meaning of constitutional guarantees must be illuminated by the content of international conventions to which India is a party. Consequently, as new cases brought new issues and problems before the Court, the content of the right to privacy has found elaboration in these diverse contexts"[109].

Despite the comprehensive constitutional affirmation of privacy in Puttuswamy, the practical feasibility of challenging the Government's surveillance endeavours, (e.g., Pegasus) remains bleak, and unlikely to yield success. In the instance of Manohar Lal Sharma v Union of India case (i.e., the Pegasus case), the Court mandated the formation of a committee of experts to recommend amendments to the existing law around surveillance, to secure the right to privacy, and to examine the existence, and validity of the Government's surveillance programs (ranging from Pegasus to the many Facial Recognition Technologies functioning in a legal grey zone in the absence of a specific framework)[110]. Regrettably, a year later, the committee was unable to conclusively determine whether there was evidence of the Government's engagement with NSO to use Pegasus, expressly outlining that they failed to cooperate with the Expert Committee[111].

---

[108] Justice K.S. Puttuswamy and Anr v Union of India And Ors, (2017) 10 SCC 1; AIR 2017 SC 4161.

[109] *Ibid.*

[110] Manohar Lal Sharma v Union of India, Writ Petition (Criminal) No. 314 of 2021.

[111] Ananthakrishnan G, *No evidence, Govt didn't cooperate: SC panel on Pegasus*, The Indian Express, August 26, 2022, available at: https://indianexpress.com/article/india/supreme-court-pegasus-spyware-case-8110566/, (last visited December 05, 2023).

While the Solicitor General's defence before the Court relies on national security considerations to shield Government actions, pertinent queries raised by Ministers in Parliament such as whether the Government has entered into a contract with Israeli cybersecurity firm NSO Group, are dismissed due to ongoing legal proceedings (i.e., assertions that the matter is sub-judice)[112]. The outsourcing of fact-finding from Parliamentary to judicial processes, only to have the Government cite national security reasons to withhold information in Court, creates a paradox. Notably however, J. Raveendran's committee proposed crucial recommendations, including the need for amendments to existing surveillance laws, a moratorium on spyware technology for non-state entities, and the establishment of an independent agency committed to cybersecurity-vulnerability investigations. Therefore, the current standard on surveillance and privacy can be pithily summarized by noting that while courts have played a role in fostering a legal culture of accountability, political and executive adherence remains notably lacking. This provides intelligence agencies a wide remit to conduct surveillance while being accountable only to the Ministry of Home Affairs.

V. India's Contributions to and Acknowledgment of International Law in Cyberspace

At global negotiations, India has largely adopted a non-committal approach to the fissures being debated globally. Despite being a member of five out of six Group of Governmental Experts on responsible state behaviour, India is yet to publish a consolidated statement on how specific points of international law apply to cyberspace[113]. However, India's understanding of the debates on the applicability of international law in cyberspace can be parsed together through an analysis of multiple documents and statements.

Notably, the Indian statement at the First Session of the 2021-2025 United Nations Open Ended clarified India's general approach to the applicability of international law in cyberspace[114]. Highlighting

[112] DHANANJAY MAHAPATRA, *Supreme Court picked panel finds no proof of Pegasus on 29 phones it got*, Times of India, August 26, 2022, available at: https://timesofindia.indiatimes.com/india/supreme-court-picked-panel-finds-no-proof-of-pegasus-on-29-phones-it-got/articleshow/93786248.cms, (last visited December 05, 2024).

[113] *Supra* note 79.

[114] ATUL M. GOTSURVE, Joint Secretary (EG & IT and CD), *Opening Statement on 13 December 2021*, Open Ended Working Group on Security of and in the Use of ICTs 2021-

the need to attain universal consensus, the statement stressed on the need for "Deepening our understanding of how international law applies is an iterative process, involving States forming national views and exchanging positions"[115]. The statement also acknowledged the challenges in obtaining consensus and highlighted the importance of forums like the OEWG to identify points of convergence and move towards greater legal certainty[116].

The statement also proclaimed that cyber-attacks on infrastructure located in another state's territory "might" constitute a breach of sovereignty. It reaffirmed that a State "enjoys the right to exercise sovereignty over objects and activities within its territory" and "has the corresponding responsibility to ensure that those objects and activities are not used to harm other States". Finally, the statement clarifies that if a state is aware of an internationally wrongful act originating from or being routed through its territory, it should take reasonable steps to end the said harmful activity.

In essence, by referring to the obligation of states to take action against wrongful action originating from its territory, India accepts the due diligence principle in cyberspace. Again, this affirmation is consistent with India's broader approach of vaguely referencing international law in diplomatic statements to further explain national interests or concerns. The wording of the statement enables India to call out non-state actors using the territory of adversaries like Pakistan or China while stopping short of making a principled normative articulation that would cement India's understanding of international law.

Indeed, given the threat India faces from non-state actors, calling out and combatting the role of non-state actors and "quasi state actors" has been an important pillar underpinning India's approach to international law. At the ongoing OEWG deliberations, India put out a clear statement on quasi-state actors which it defined as "entities that straddle the line between statehood and non-state existence, borrowing characteristics from both without fitting neatly into either

---

2025, UN General Assembly, available at: https://pminewyork.gov.in/IndiaatUNGA?id=NDQ1OA (last visited April 04, 2024).

[115] ATUL M. GOTSURVE, Joint Secretary (EG & IT and CD), *Opening Statement on 13 December 2021*, Open Ended Working Group on Security of and in the Use of ICTs 2021-2025, UN General Assembly, available at: https://pminewyork.gov.in/IndiaatUNGA?id=NDQ1OA (last visited April 04, 2024).

[116] *Ibid.*

designation"[117]. India cited cyber militias, cyber mercenaries and other state-sponsored groups that steal sensitive data or disrupt critical infrastructure. While identifying the challenges posed by these so called "quasi state actors", as they circumvent the regimes applicable to both states and non-state actors, India does not recommend any clear approaches or international law framework to tackle them[118].

Similarly, India has stressed, while arguing for the criminalization of cyberterrorism at UN that, "any legal instrument defining cyber terrorism needs to be specific taking into account the effects of terrorism that results in harm, damage to person or persons and societies as well as to include the ever evolving various methodologies / dimensions and layers of the use of ICTs for committing cyber terrorism"[119].

International law in cyberspace has also received some scrutiny by the Parliament. The Parliamentary Standing Committee on External Affairs (made up of legislators from both houses of Parliament and multiple parties) addressed this as one of the four issues in their 2021 report titled, "India and International Law"[120].The Standing Committee had heard oral depositions from representatives of the Ministry of External Affairs, Ministry of Electronics and Information Technology as well as external experts. Similar to the OEWG statement, the Committee concluded that "While International Law does apply to cyberspace, however, it is insufficient in its current

---

[117] Government of India,"India Statement on Quasi-State Actors (QSA". Open-Ended Working Group on the Security of and in the Use of ICTs 2021-2025.25 July,2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/India_QSA_25_July.pdf Quasi state actors have also been referred to as semi-state cyber actors in existing literature which generally includes state sponsored companies, cyber criminals and hacktivist groups F. EGLOFF, *Semi-State Actors in Cybersecurity*, Oxford, 2022.

[118] Government of India, "India Statement on Quasi-State Actors (QSA)."Open-Ended Working Group on the Security of and in the Use of ICTs 2021-2025.25 July, 2023. https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/India_QSA_25_July.pdf

[119] Government of India,"India's intervention on Criminalization:Group 4 Questions." UNODC. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/India_-_Agenda_item_4.pdf

[120] Parliamentary Standing Committee on External Affairs, India and International Law Including Extradition Treaties With Foreign Countries, Asylum Issues, International Cyber-Security And Issues of Financial Crimes, Ninth Report, September 2021, available at https://loksabhadocs.nic.in/lsscommittee/External%20Affairs/17_External_Affairs_9.pdf (last visited May 06, 2024).

form to address the issues of attribution in cyberspace, violation of sovereignty in cyberspace, and the threshold for reaction and proportionality of counter- measures when it comes to a cyber incident, and hence more deliberations would be necessary to define further modalities to deal with these issues. While the objectives and principles of these provisions of international law remains the same in cyberspace, their applicability, modality and usability would have to be customized for cyberspace"[121].

The Committee also affirmed the principle of sovereignty, sovereign equality, settlement of disputes by peaceful means and non-intervention in the internal affairs of other States and the need to comply with obligations under international law to respect and protect human rights and fundamental freedoms. The Committee did not spell out how these existing international law obligations apply to cyberspace. However, the Committee underscored the need for India to articulate these concepts more clearly and play a leadership role. They outlined that India ought to customize and clarify, "the modalities for application of International law in cyberspace and internet governance,.. build a global architecture for cyber security, formulate new legal regimes that will respect the sovereignty of countries and promote a peaceful order in cyberspace"[122].

VI. Summarising the Threads on India's Approach to International Law and Cyber Operations

Cyber conflict below the threshold of the use force has been a significant part of geopolitical rivalries in South Asia. In recent years both India and Pakistan have also stepped up their cyber warfare capabilities and while there is yet to be a large scale cyber-attack, small scale cyber-attacks continue with aplomb[123]. India-Pakistan relations are characterised by tit-for-tat attacks where both sides engage in low scale attacks responding to cyber or physical aggression from the other. This mirrors the regular tit-for-tat exchanges between both Indian and Pakistani soldiers on the Line of Control, and diplomats of both states at the UN. There are numerous actors in both

[121] *Ibid.*
[122] *Ibid.*, 25.
[123] MUHAMMAD ABDUL QADEER, *The Cyber Threat Facing Pakistan*, The Diplomat, June 06, 2020, available at: https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/ (last visited May 06, 2024).

the Indian and Pakistani spaces and they can be divided into two groups - hacktivists and patriotic hackers, and Advanced Persistent Threats (APTs)[124] - a majority of actors belong to the first category. Indian hacktivists and patriotic hackers have engaged in defacement and have also claimed responsibility for ransomware attacks on Pakistani airports and government websites[125]. Pakistani hacktivists and patriotic hackers have also targeted Indian government websites through defacement techniques and have been more active in retaliation to cyber or physical aggressions by India[126]. Both the Indian and Pakistani APTs have engaged in national security espionage against each other, along with other militaries in South Asia. Tools used by the various actors include website defacement, spearfishing, and the use of malware[127].

Despite both approaches being relatively piecemeal, there is some congruence between India's approach to international law in cyber-space and proclamations on the use of force in the kinetic domain. The articulated understanding of international law appears to be driven by the core geopolitical interest of proactively and pre-emptively countering threats emanating from non-state actors based in the territory of adversarial states. Meanwhile several retired officials and independent experts have urged Indian institutions to think offensively[128]. As discussed above, India is yet to articulate a single, written cyber strategy across domains. In this concluding section, we attempt to collate trends that outline the contours of India's approach to international law and cyber operations.

The overarching intent of India's approach to international law in cyberspace is to safeguard India's core interests, that is, protecting information infrastructure on Indian territory and countering cyber threats both from domestic and international adversaries, including non-state actors. This entails a balancing act that requires the

[124] M. BAEZNER, *Hotspot Analysis: Regional rivalry between India-Pakistan: tit-for-tat in cyberspace*, Center for Security Studies (CSS), ETH Zurich, August 2018, available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2018-04.pdf (last visited April 04, 2024).

[125] P. SHUKLA, *India-Pakistan Gear Up For Cyber Wars This I-Day [WWW Document]*, Businessworld, available at: http://businessworld.in/article/India-Pakistan-Gear-Up-For-Cyber-Wars-This-I-Day/14-08-2017-124037/.

[126] *Ibid.*, at 8.

[127] *Supra* note 120, at 8.

[128] The Cyber Task Force, *India's Preparedness in the Digital Milieu*, VIF, November 14, 2022, available at: https://www.vifindia.org/2022/november/14/indias-preparedness-in-the-digital-milieu (last visited May 06, 2024).

Government to not unduly upset potential allies while countering cyber threats. Domestic legal provisions and policy reflect *these* interests to a greater extent, than a normative commitment to international law. While the Constitution acknowledges the value of international law, we demonstrated that India's justifications for the use of force as well as legislative and executive approaches to surveillance do little to incorporate international legal rules and principles. India has seldom laid out its justifications for the use of force unambiguously, except when it comes to the right to self-defence against non-state actors.

India's declaratory approach on the application of international law to cyberspace is similar. Given the controversies around the application of international law and the points of departure between the United States and Russia - both of which are India's geopolitical partners - India has stayed clear of any risks that could end up disappointing either of them. Therefore, India's statements on international law have affirmed concepts already accepted by other countries such as sovereignty in cyberspace without weighing in on more nuanced debates such as whether sovereignty is a rule or principle. Further, it has stayed clear of endorsing Russia and China's 'information sovereignty' concept that envisages greater state control of the internet[129]. India encourages discussion and debate at the global level clarifying the application of international law concepts to cyberspace but is yet to weigh in on determining the content of these concepts. Of course, as the report of the Parliamentary Standing Committee on International Law urges, this posture could change given its recommendation that India ought to articulate its position.

What would be the pillars of this position? First, self-defence through offensive operations especially against non-state actors engaging in "cyber terrorism" could be cemented as legitimate. Second, India has already affirmed the sovereignty principle in cyberspace and the application of the due diligence concept, both of which may be further elaborated upon. Third, India would likely focus on the legal dimensions of protecting national critical infrastructure rooted in sectors critical to the national economy or security interests.Finally, India may, in reference to emerging scholarship on

[129] S. MCKUNE, SHAZEDA AHMED, *The contestation and shaping of cyber norms through China's internet sovereignty agenda*, in *International Journal of Communication*, 12, 2018, 3035-3855.

the topic,articulate a more robust framework to impose international legal obligations on quasi-state actors in cyberspace[130].

In terms of implementation of international law concepts, India has put in place domestic legislative provisions that criminalize offensive cyber operations including unauthorized access and cyber terrorism. At the same time, it adopts an expansive view of national security exceptions to the right to privacy, which means that intelligence agencies are provided significant operating space to conduct surveillance. Again, this points to India's approach of shoring up national interests such as strong cyber defences while not constraining the executive's policy options when it comes to the operating domain. Finally, India's views on the use of force and self-defence in the kinetic domain suggest that India's offensive cyber capabilities will be extensively deployed against non-state actors that continue to undertake 'pin-prick' cyber-attacks against India. The 'Cold Start' doctrine that has been used to enable high degrees of operational preparedness and retaliatory strikes at the conventional level can be applied to cyberspace as well. This could be done by keeping units tasked with both offensive and defensive functions such as CERT-In, NCIIPC, and DCA, coordinated and alert.

India has often been criticised for lacking a written grand strategy or cohesive vision for global governance[131]. However, several strategic thinkers have come to India's defense, stressing that strategic thought does not necessarily need to be written or articulated in one location to impact national decision-making in a rational manner[132]. Our examination of India's approach to and understanding of India's approach to international law in cyberspace certainly affirms this thinking. The lack of a single written document does not signal the absence of key institutions, legislation and statements that cast light on how India thinks. That said, clear and confident normative articulations aid any country's claims to being a key responsible cyber power. As India ascends in the international order, external observers will increasingly call for and scrutinize both doctrinal certainty and constitutionality. India will have to balance these pressures with its

[130] F. EGLOFF, *op. cit.*; J. COLLIER, *Proxy actors in the cyber domain: Implications for State Strategy*, in *St. Antony's International Review*, Vol 13 (1), 2017, 25-47.

[131] G. TANHAM, *Indian strategic thought: An interpretive essay*, RAND, 1992.

[132] A.J. TELLIS, *Between the Times: India's Predicaments and its Grand Strategy*, Carnegie Endowment for International Peace, December 03, 2012, available at: https://carnegieendowment.org/posts/2012/12/between-the-times-indias-predicaments-and-its-grand-strategy?lang=en (last visited May 06, 2024).

core strategic interests in an increasingly multi-polar and complex cyberspace.

JAPANESE REGULATORY FRAMEWORK ON CYBER OPERATIONS AND CYBERSECURITY: AMBITION TOWARD MORE ACTIVE POSTURE

KEIKO KONO[1]

Introduction

This article aims to give an overview of Japanese framework currently in place, an expected future posture set out by the government and pending issues relating to cyber operations and cybersecurity. The main parts of the article focus on the regulatory framework to respond to cyberattacks, specifically the legislation and procedures in both an armed attack situation (Chapter 1) and a cyberattack falling below the threshold of an armed attack (Chapter 2). The last chapter 3 of the article addresses a problem involving information sharing and its reporting to the agencies in the wake of peacetime cyberattacks, in which case an inter-ministerial coordination and cooperation is a key to minimizing damages done to critical infrastructure and get the entire society to be more resistant and robust to next chain of cyber incidents.

As described in the text below, the government is still in the middle of crafting details to materialize the goals set out in the latest National Security Strategy. Hence, the argument in the article may be proven to be mistaken about the government plan, although it strived to be as objective and neutral as possible, relying on credible media articles and episodes told at first hand by officials familiar with the subject.

To fully understand the entire legal landscape is difficult even for Japanese, as the implementation of cybersecurity measures, in particular, is being done in a dispersed manner. It will be even more so for non-Japanese audience, since the domestic legislation is only partially translated in English, like the Act on the Japan Self-Defense Forces (SDF Act), and the government website is less informative in English version than the native language in many cases. Hopefully the

[1] Views are my own and not the views of my former employer, Japan Ministry of Defence.

article might contribute to making the subject more visible to those who are interested.

1. *National Framework for Military Deployments and Intelligence.* 1.1. *Prohibition on Military Deployment Abroad.* The government of Japan has maintained since the creation of the Japan Self-Defense Forces (SDF) that the SDF units should not be deployed abroad with an aim of using force. So-called "the exclusively defense-oriented" policy would allow a use of force in self-defense only to the minimum extent necessary to repel an armed attack on Japan, which the government has defined as a systematic and deliberate use of force on Japan[2]. And it thus prohibits acquiring offensive weapons such as nuclear weapons, intercontinental ballistic missiles (ICBM), long-range strategic bombers, and aircraft carrier, as well as exercising the right of collective self-defense[3]. In relation to the term "abroad," the government has explained that the geographic scope of the self-defense does not necessarily confined to Japanese territory, territorial waters, and airspace[4] but the sending an armed SDF unit to the territory, territorial waters, or airspace of another nation for the purpose of use of force exceeds that limit and thus unconstitutional in general.

The Cabinet Decision in July 2014 and subsequent approval by the National Diet of the Legislation for Peace and Security[5] the following year enabled the exercise of collective self-defense by the SDF in an extremely limited circumstance, where another nation which is in a close relationship with Japan comes under an armed attack, leading to Japan's survival being threatened and a clear danger of fundamentally overturning people's right to life, liberty and pursuit

[2] The prime minister, at the House of Representatives, 154th session of the Diet, May 24, 2002, https://www.shugiin.go.jp/internet/itdb_shitsumon.nsf/html/shitsumon/b154066.htm (only in Japanese).

[3] The Cabinet Legislation Bureau, "The Relationship between Collective Self-Defense and the Constitution", October 14, 1972, in "The Government's view submitted to the Special committee of both Houses of the Diet on the Legislation for Peace and Security of Japan and International Society [衆議院及び参議院の「我が国及び国際社会の平和安全法制に関する特別委員会」に提出された政府統一見解等]", *The Journal of Law-making and Examination* [立法と調査], No. 372, December, 2015, 63, https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2015pdf/20151214059.pdf (only in Japanese).

[4] Japan MoD, "Overview and Fundamental Concepts of National Defense", https://www.mod.go.jp/en/d_act/d_policy/index.html.

[5] Japan MFA, "Japan's Security Policy", April 5, 2023, https://www.mofa.go.jp/fp/nsp/page1we_000084.html.

of happiness. However, the legislation of 2015 did not make any change regarding the prohibition of overseas deployment for using force.

The government's policy has come under the spotlight again for the past couple of years since counterstrike capabilities were put on the agenda in the ruling parties. Citing the past documents on the subject[6], a serious suspicion was raised by opposition parties as to whether the National Security Strategy of 2022 coincides with the long-standing defense policy in this regard, since it introduced stand-off defense capabilities as counterstrike capabilities. A senior MoD official explained at the Diet in 2023 that the launching counterstrike capabilities is not tantamount to the prohibited deployment of armed SDF units to a foreign nation, presumably on the basis of an understanding that striking enemy bases might be legitimate in case only when it is done as a last option of defensive measures and with minimum degree of force necessary to repel guided missiles, for example[7].

1.2. *National Procedures for Obtaining the Diet Approval.* The requirement of the Diet approval is imposed in most of the SDF operations, except for a few cases such as an overseas evacuation of citizens from a foreign state in crisis under article 84-3 and 4 of the SDF Act[8]. This section focuses on an armed attack and a "survival-threatening situation", as the SDF is permitted to use force in self-defense only in these two cases.

In the events of both an armed attack against Japan and a "survival-threatening situation" in which an armed attack on another state that is in a close relationship with Japan threats the survival of

[6] The resolution by the House of Councillors titled "Non-deployment Abroad of the SDF [自衛隊の海外出動を為さざることに関する決議]", June 2, 1954, the plenary meeting of the House of Councillors, the 19th session of the Diet, https://www.sangiin.go.jp/japanese/san60/s60_shiryou/ketsugi/019-57.html; A statement by then Defense Commissioner Nakasone Yasuhiro, The minutes of the plenary meeting of the House of Councillors, the 63th session of the Diet, May 8, 1970, https://kokkai.ndl.go.jp/txt/106315254X01519700508; A statement by then prime minister Kakuei Tanaka, "The minutes of the plenary meeting of the House of Representatives", the 76th session of the Diet, October 31, 1972, No. 4, p. 68, https://kokkai.ndl.go.jp/txt/107005254X00419721031 (only in Japanese).

[7] A statement by Mr. Masuda, Director General, Bureau of Defense Policy of Japan MoD, "The Minutes of the Committee of Diplomacy and Defense", House of Councillors, an ordinary session of the 211st Diet, No. 12, May 9, 2023, National Diet Library, p. 25, https://kokkai.ndl.go.jp/txt/121113950X01220230509 (only in Japanese).

[8] Act No. 165 of 1954.

Japan, the government must seek a prior approval from the Diet in principle, in order to issue a Defense Operations order to the SDF. Specifically, the prime minister must draft a basic responses plan that describes a factual basis and a reason for using force (article 9 (2) of the Act on the Peace and Independence of Japan and Maintenance of the Nation and the People's Security in Armed Attack Situations, etc., and a Survival-Threatening Situation (hereinafter referred to as the Armed Attack Situation Response Act))[9], and then send it to the National Security Council (NSC) for a counsel. After reflecting the recommendations from the NSC on the plan, it must be adopted by the Cabinet Decision (article 9 (6) of the Armed Attack Situation Response Act). Then, the plan must be submitted to the Diet for the approval (article 9 (7) of the same Act)[10]. In case of emergency where time does not allow, the approval can be sought afterwards (article 76 of the SDF Act)[11].

Although not written into the Acts, there are additional requirements to be met for the government. During the deliberation of the legislative bills of the Legislation of Peace and Security in the Diet, heads of five political parties including the two ruling parties reached an agreement on September 16th, 2015, in respect of ensuring the Diet's role regarding any SDF operations that would be undertaken thereafter under the new legislation.

First, with regard to the survival-threatening situation, they considered that it would almost always overlap an armed attack on Japan. In an exceptionally rare case where it does not, like a maritime blockade of the strait of Hormuz by sea mines, and only a survival-threatening situation exists, the prior approval of the Diet must be always sought without any exception for the Defense Operations of the SDF. Note that the mine-sweeping operations in the strait is not identical to the use of force in the light of the passive nature of the

[9] The Act on the Peace and Independence of Japan and Maintenance of the Nation and the People's Security in Armed Attack Situations, etc., and a Survival-Threatening Situation, the official web portal of Government of Japan, e-Gov, https://elaws.e-gov.go.jp/document?lawid=415AC0000000079 (only in Japanese).

[10] For a visualized image of a serios of processes for seeking the Diet approval, see T*he Defense of Japan (Annual White Paper) 2023*, 283, Figure II-6-1 Procedures for Responding to Armed Attacks, etc., and Survival-Threatening Situations, https://www.mod.go.jp/en/publ/w_paper/wp2023/DOJ2023_EN_Full.pdf.

[11] *Ibid.*, Reference 15, p. 109, https://www.mod.go.jp/en/publ/w_paper/wp2023/DOJ2023_EN_Reference.pdf.

operations, and as far as hostile acts are not taking place there, in the government's view[12].

Second, when the SDF is going to continue its operations beyond the originally fixed term, the Diet approval must be renewed for the extension. Moreover, the reporting to the Diet must be made thoroughly both after the completion of, and every 180 days of the operations. The reporting requirement after the completion is provided for in the Act (article 9 (15) of the Armed Attack Situation Response Act), but the Act does not regulate what to report.

Third, the operations must be terminated promptly if the Diet resolves to that effect, although the requirement is already provided for both situations in the Act (article 9 (14) of the Armed Attack Situation Response Act).

Fourth, both during and after the operations, the operations must be put under a constant monitoring and ex post scrutiny by a committee of the Diet in charge. After the agreement, the five parties held meetings named "the Five-Party Council on the Legislation for Peace and Security" at least twice in 2016[13] and are expected to arrange the details such as the procedure and how to organize this committee for monitoring and investigation[14], yet the progress is yet to be seen.

When cyber operations are carried out as part of the Defense Operations by the SDF in response to an armed attack and/or a survival-threatening situation, they are subject to the reporting obligation to the Diet, and also monitoring and scrutiny by the Diet committee.

1.3. *Japanese Intelligence Community.* Main actors in Japanese intelligence community are the National Policy Agency (NPA), the Public Security Intelligence Agency (PSIA) under the Ministry of

[12] The Cabinet Secretariat, "Q&A on the Legislation for Peace and Security", Q27, https://www.cas.go.jp/jp/gaiyou/jimu/anzenhoshouhousei.html (only in Japanese).

[13] Then Member of the House of Councillors, Kota Matsuda, "The Five-Party Council on the Legislation for Peace and Security", June 1, 2016, https://ameblo.jp/koutamatsuda/entry-12166220109.html (only in Japanese).

[14] YASUO NAKAUCHI, *Involvement of the Diet in SDF measures based on Legislation for Peace and Security: Consideration in view of controversy over the Diet approval* [平和安全法制に基づく自衛隊の活動に対する国会の関与― 国会承認の在り方をめぐる論議を中心に ―], in *The Journal of Law-making and Examination* [立法と調査], No. 416, October 2019, pp. 28-32, https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2019pdf/20191001020.pdf (only in Japanese).

Justice (MoJ)' s control, the MoD, the Ministry of Foreign Affairs (MFA), and the Cabinet Intelligence and Research Office (CIRO) including Cabinet Satellite Intelligence Center (CSICE), out of which the CIRO plays the central role[15]. They engage in respective intelligence missions, often in cooperation with each other, such as on the subject of counterterrorism. The MoD began its part soon after its creation, and its SIGINT capabilities are well known in relation to the downing Korean Air Line 007 by Soviet Air Force near Sakahlin Island in 1983, when the communications between Russian officers were recorded on Japanese Ground SDF radar site in the northern Japanese territory, Hokkaido[16], and were submitted to the UN Security Council through the US[17].

There was not a unified military intelligence division within the MoD until 1997, when the Defense Intelligence Headquarters (DIH) was established. The DIH mainly carries out SIGINT, Imagery intelligence (IMINT), and Geospatial intelligence (GEOINT). It is publicly unknown whether, and if so, and to what extent these intelligence organizations are engaging in cyber operations, as nothing is revealed officially from the government to date.

For some reasons, the ruling Liberal Democratic Party (LDP) seemingly had found their performances as insufficient, as they indicated their policy proposal toward the new National Security Strategy that was been under review at that time. In a section titled "intelligence including enhanced HUMINT" of the proposal, the proposal says there is a need for a new scheme to collect, share, and analyze intelligence in a more integrated manner, and the government should establish a new "state intelligence bureau," which seems to mean a cross-ministerial organization replacing the CIRO, and should

[15] The CIRO, "Intelligence Community of Japan and CIRO", https://www.cas.go.jp/jp/gaiyou/jimu/jyouhoutyousa/en/community.html See also R.J. SAMUELS, *Special Duty: A History of the Japanese Intelligence Community*, Cornell University Press, 2019.

[16] "Shooting Down Korean Air of 1983, Communications of Soviet Force Intercepted by Ground SDF [83 年の大韓航空機撃墜、旧ソ連軍交信を陸自が傍受]", *Nikkei Newspapers*, July 19, 2014, https://www.nikkei.com/article/DGXNZO74486160Z10C14A7PP8000/ (only in Japanese); D. BALL, R. TANTER, *Japan's Signals Intelligence (SIGINT) Ground Stations: A Visual Guide*, *NAPSNet Special Reports*, August 6, 2015, https://nautilus.org/napsnet/napsnet-special-reports/japans-signals-intelligence-sigint-ground-stations-a-visual-guide/. For details of the incident, TH. PATTERSON, *The Downing of Flight 007: 30 Years Later, a Cold War Tragedy Still Seems Surreal*, *CNN*, August 31, 2013, https://edition.cnn.com/2013/08/31/us/kal-fight-007-anniver sary/.

[17] KEISHI ONO, *Introduction to Defense Issues of Japan* [日本の防衛問題入門], Kawade Publishing, 2023, 55 (only in Japanese).

ensure the human resources and the budget for that purpose, and utilize artificial intelligence and other new technologies in OSINT term[18]. In a separate section on cyber, the proposal also referred to intelligence collection as part of active cyber defense that the LDP members were advocating to introduce[19].

The LDP's proposals above were favorably received in the Strategy. Main points of emphasis regarding intelligence capabilities in the Strategy are "close cooperation between the policy and intelligence departments," and "comprehensive analyses utilizing all means of collection and sources of information possessed by the Government"[20], which are paraphrased later in the Strategy. The cooperation within intelligence departments is also urged in relation to imagery intelligence via information gathering satellites, that is assumed by both the CIRO, especially the CSICE and the MoD/SDF[21]. The Strategy also suggests "a mechanism will be established to aggregate information in an integrated manner"[22], whilst an exact plan is yet to be drawn up later. Lastly, with respect to cybersecurity, the Strategy is significantly in line with the LDP's proposal and sets out to "develop information gathering and analysis capabilities in the field of cybersecurity and establish systems to implement active cyber defense"[23].

On the other hand, there are existing organizations that assume cyber-related missions, but not intelligence in strict sense. First, the National center of Incident readiness and Strategy for Cybersecurity (NISC), Japanese Government's point of contact as a cyber security organization at international level, is seemingly not a member of

---

[18] The LDP, "A Policy Proposal towards the Drawing up of a New National Security Strategy [新たな国家安全保障戦略等の策定に向けた提言]," April 26, 2022, chapter on changes in the modality of warfare, section 6 on intelligence including enhanced HUMINT, 8, https://storage2.jimin.jp/pdf/news/policy/203401_1.pdf (only in Japanese).

[19] *Ibid.*, the same chapter, section 4 on cyber, 7-8.

[20] The government of Japan, "National Security Strategy of Japan," December 22, 2022, Part VI: Strategic Approaches Prioritized by Japan, Chapter1: Main Elements of Comprehensive National Power for Japan's National Security, section 5 on intelligence capabilities, p. 12, https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

[21] *Ibid.*, same Part, chapter 2: Strategic Approaches and Major Ways and Means, section (4): Strengthening Efforts to Seamlessly Protect Japan in All Directions, (v) Strengthening Intelligence Capacities for Japan's National Security, 26-27.

[22] *Ibid.*

[23] *Ibid.*, Part VI: Strategic Approaches Prioritized by Japan, chapter 2: Strategic Approaches and Major Ways and Means, section (4): Strengthening Efforts to Seamlessly Protect Japan in All Directions, (i) Improving Response Capabilities in the Field of Cybersecurity, 23.

Japanese intelligence community. For example, the Government Security Operation Coordination Team (GSOC) under the NISC has been monitoring central government networks with their sensors set up at the entry points of their networks. Thus, the GSOC team is supposed to detect both inward communications containing malicious files sent to the government ministries and agencies, and outward irregular communications, like sensitive information flowing out to overseas destinations controlled by criminal groups. Then the GSOC team notifies the affected agency of the incident. The NISC also takes on cyber security audits and investigation into incidents. Due to the shortage of human resources at the NISC, however, part of the monitoring functions is currently delegated to an external technical institute, the Information-Technology Promotion Agency (IPA) since 2017. Thereafter, the GSOC of the NISC focuses its monitoring effort on government ministries and agencies, while the IPA is taking care of the networks of independent administrative agencies and other government-affiliated organizations, which often engage in administrative services by delegation, just as the IPA does. Whether the GSOC under the NISC or the IPA, scope of monitoring is limited to public or quasi-public entities, and the purely private companies are not under their supervision[24]. The MoD Cyber Defense Group does not belong to the intelligence community either, as its responsibilities are to monitor 24 hours a day, and audit the MoD-run unique information system: the Defense Information Infrastructure (DII) and the MoD/SDF common network as well as virus analyses in response to cyberattacks on their networks.

2. *Response to Cyberattacks below the Threshold of an Armed Attack.* 2.1. *Shift toward active cyber defense.* The Government's Cybersecurity Strategy of 2018 recalls G7 Declaration on Responsible States Behavior in Cyberspace (2017) that affirmed that the victim of an internationally wrongful act may, in certain circumstances, resort to proportionate countermeasures against the State responsible for the wrongful act, and the strategy notes that "based on the recognition,[…] Japan will take resolute responses against cyber

[24] KEIKO KONO, *In Search of a Targeted Approach: Japan-Estonia Cybersecurity Cooperation*, in The International Centre for Defence and Security (ICDS), (ed.), *Europe's Indo-Pacific Tilt: Estonian and Japanese Interests*, January 2023, 48-49, https://icds.ee/en/europes-indo-pacific-tilt-estonian-and-japanese-interests/.

threats that undermine our national security, including those possibly state-sponsored" [25]. For the government to engage in cyber countermeasures under international law, an amendment of domestic legislation is needed. No matter which unit is assigned to the task, it requires a specific legal authorization to launch such a measure of the circumstances precluding wrongfulness. Despite this endorsement in the Strategy, however, there were not any legislative measures taken for that purpose after the Strategy.

When the ruling LDP released its policy proposals in April 2020, it recommended that the government should 1) ramp up its cyber capabilities including attribution to respond to a potential attack below an armed attack threshold; 2) revisit and update the relevant domestic legislation for the implementation of active cyber defense; 3) recruit talented cyber experts and scale up the research and education in the MoD to nurture cyber force, among other things[26]. Taken into careful consideration, the proposal was well reflected in the new strategic documents in regards to cyber defense too.

On December 16th, 2022, the long awaited three documents, namely the National Security Strategy, the National Defense Program Guidelines, and the Medium-term Defense Capability Development Plan were adopted by the cabinet decision and released. The National Security Strategy upheld the LDP's proposals and described the concept as follows.

Japan will introduce active cyber defense for eliminating in advance the possibility of serious cyberattacks that may cause national security concerns to the Government and critical infrastructures and for preventing the spread of damage in case of such attacks, even if they do not amount to an armed attack[27].

Along with the introduction of active cyber defense, the Strategy set out that a new organization replacing the NISC will be established to "comprehensively coordinate policies in the field of cybersecurity, in a centralized manner." To proceed with the policy, the government was due to work on legislation necessary to realize the new policy[28].

There is not any definition of the concept in the Strategy, neither has the government made any follow-up announcement to public so

[25] The Government of Japan, *Cybersecurity Strategy*, July 2018, 45-46, https://www.nisc.go.jp/eng/pdf/cs-strategy2018-en-booklet.pdf.

[26] The LDP, *A Policy Proposal towards the Drawing up of a New National Security Strategy*, 7-8, https://storage2.jimin.jp/pdf/news/policy/203401_1.pdf (only in Japanese).

[27] Government of Japan, *National Security Strategy of Japan*, 23.

[28] *Ibid.*, 24.

far, whilst a NISC official presented its view at an international event that it is the Japanese version of the US's Defense Forward concept[29]. Such a silence by the government in public has led to a range of speculation among experts as to possible measures to be taken in the name of active cyber defense.

On January 31st, 2023, the government set up a new division within the cabinet secretariat, named the office for policy coordination and development on national cybersecurity to prepare the legislative work necessary to realize the active cyber defense. The office consists of forty-five government officials transferred from the ministries and agencies concerned, such as the MoD and the MFA[30]. The office is expected to convene a group of subject matter experts that can give counsel to the government in due course, as is always the case with the government businesses.

Over one year passed since the release of the Strategy, but the legislative bills have not been submitted to the Diet for deliberation to date, and reportedly it is not likely to happen at least during an ordinary session of the Diet in 2024 due to the argument within the coalition parties (the LDP and the Komeito Party) being still underway. They seem to be struggling to build an agreement, in particular, with regard to how to reconcile the active cyber defense with a set of legal and policy issues under the current legal scheme. Among those are, both article 21(2) of the Constitution[31] and Telecommunications Business Act (articles 4 and 179)[32] in relation to the secrecy of communication; second, Act on Prohibition of Unauthorized Computer Access[33] that is an implementing legislation of Budapest Convention of Cybercrime of the Council of Europe (2001)[34], and Penal Code[35], involving criminal acts that would be

[29] The International Institute for Strategic Studies (IISS), Europe Workshop, *Russia's War Against Ukraine: Lessons learned for Cyber Military Strategy and Operations*, held in Berlin on October 25, 2023.

[30] "'Active Cyber Defense': Preparation in the Cabinet Secretariat, Drafting Legislative Bills by the Government Underway [「能動的サイバー防御」、内閣官房に準備組織　政府、法整備進める],"　*Nikkei Newspapers*, February 1, 2023, https://www.nikkei.com/article/DGKKZO68069650R30C23A1PD0000/ (only in Japanese).

[31] The Constitution of Japan, November 3, 1946, Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/ja/laws/view/174/je#je_ch3at12.

[32] Act No. 86 of December 25, 1984, Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/ja/laws/view/3648.

[33] Act No. 128 of August 13, 1999, Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/ja/laws/view/3933.

[34] ETS No. 185, Japan ratified the Convention on July 3, 2012.

[35] Act No. 45 of April 24, 1907, Japan MoJ, Japanese Law Translation website,

committed by the active cyber defense unless amended; and even the government's "the exclusively defense-oriented" policy in relation to article 9 of the Constitution[36]. Not to mention, there needs to be the amendment of the SDF Act[37] to give it a new legal authorization for carrying out the active cyber defense when the government decides to assign the mission to it, because any provisions under the existing SDF Act on measures taken by the SDF unit in a situation below the threshold of an armed attack is not possibly sufficient to allow the exercise of the active cyber defense. Currently, moreover, the SDF is tasked only to protect its own systems and networks, but not critical infrastructure run by the private sector, in the first place.

2.1. (i) *Does ACD Violate the Secrecy of Communication?* Apparently, the most controversial topic among lawmakers is the secrecy of communication. Opponents are reportedly arguing that the active cyber defense is unconstitutional as it fringes on the constitutional rights by mass surveillance of communications, as the scope of application under article 21(2) includes not just the content of communications, but also information on senders/receivers' address, name, time and location of the communication, as well as the fact of the communication. This objection posits the right of secrecy of communication as absolute one, dominating all other considerations including the public welfare recognized by both articles 12 and 13 of the constitution. Take an example of communication interception for criminal investigation for the sake of the comparison. The interception by a public prosecutor and a judicial police officer are permitted for a limited category of serious crimes, and to the minimum extent necessary, in the light of the public welfare and thus does not violate the secrecy of communication[38].

A new sign of support is seemingly emerging around the

https://www.japaneselawtranslation.go.jp/ja/laws/view/3581.

[36] "'Active Cyber Defense': Preparation in the Cabinet Secretariat, Drafting Legislative bills by the Government Underway"; "Dire Prospect for Submission of Cyber Legislative Bills to the Diet. Delay about Controversy over 'Secrecy of Communication' [サイバー法整備、通常国会見通せず 「通信の秘密」議論に遅れ」", *Tsusin*, January 4, 2024, https://www.jiji.com/jc/article?k=2024010300274&g=pol (only in Japanese).

[37] Act No. 165 of 1954.

[38] Articles 1 and 14 of the Act on Communications Interception for Criminal Investigation (Act No. 137 of August 18, 1999), Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/ja/laws/view/3857/en; Japan MoJ, "Q&A on the Legislative Bill on the Act Communications Interception for Criminal Investigation," https://www.moj.go.jp/houan1/houan_soshikiho_qanda_qanda.html#qa02

government. The head of the Cabinet Legislation Bureau[39], that is also known as "a guardian of law", gave its view at the budget committee of the House of Representatives of the Diet on February 5th, 2024, in response to a question from a LDP lawmaker, by noting that the constitutional right of the secret of communication might be constrained by the public welfare concern in the event of cyberattacks causing enormous harm to citizens residing in Japanese territory. For the same question, the prime minister also replied that the bills are under review at an accelerated pace so that they will be submitted to the Diet as promptly as possible, although some challenges are to be sorted out[40].

2.1. (ii) *Is ACD Criminal Act?* Regardless of national interests to be served or an urgent need to respond on the spot, the ACD might constitute a criminal act under Penal code in force. The procurement and use of a software for the purpose of ACD might be regarded as a crime of "making of electronic or magnetic records containing unauthorized commands" under article 168-2, and as a crime of "acquisition of electronic or magnetic records containing unauthorized commands' under article 168-3 of Penal Code[41]. It also constitutes a crime of an unauthorized access to a closed network under Act on Prohibition of Unauthorized Computer Access[42]. Under the current legislation in force, the same actions are presumably treated differently depending on which situation defensive measures are taken against, either an armed attack or the below the threshold of that. For the former, the use of software (malware) and the unauthorized access can be regarded as part of the exercise of the self-defense and thus legal under article 76(1) of the SDF Act. For the latter, however, the

[39] One of the responsibilities of the Bureau is to give opinions on legal issues to the prime minister and to individual ministers as well as to the Cabinet as a whole. Article 3(3) of the Act for Establishment of Cabinet Legislation Bureau (Act No. 252 of 1952), https://www.clb.go.jp/english/about/. There is not an available translation of the Act on the MoJ's database.

[40] "'Certain Limitations' on the Guarantee of Secrecy of Communication. A View Presented by Cabinet Legislation Bureau [通信の秘密の保障に「一定の制約」 内閣法制局が見解]," *Nikkei Newspapers*, February 6, 2024, https://www.nikkei.com/article/DGXZQOUA062CQ0W4A200C2000000/ (only in Japanese). The minutes of Diet deliberation is not available at the time of writing.

[41] Act No. 45 of April 24, 1907, Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/ja/laws/view/3581#je_pt2ch21at1.

[42] Act No. 128 of August 13, 1999, Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/ja/laws/view/3933.

same actions might not be legal due to the lack of legal authorization to the SDF to that effect.

2.1. (iii) *Is ACD Compatible with "the Exclusively Defense-Oriented" Policy?* It is sometimes heard in media that ACD must be compatible with the "the exclusively defense-oriented" policy. On the other hand, the compatibility problem has barely been heard in the context of the exercise of the self-defense.

As noted earlier in this article, "the exclusively defense-oriented" policy means that "defensive force is used only in the event of an armed attack, that the extent of the use of defensive force is kept to the minimum necessary for self-defense, and that the defense capabilities to be possessed and maintained by Japan are limited to the minimum necessary for self-defense"[43]. As far as ACD is exercised in a situation below the threshold of an armed attack, and thus the right of self-defense is not invoked, the issue of the compatibility seems irrelevant. Even assuming the relevance, cyber operations that are presumed to be launched from Japanese territory in the below-threshold-situation might not be the same as sending the SDF unit to another nation, thus not triggering the controversy over the prohibited military deployment overseas, like striking capabilities do not. At any rate, the argument comes down to a denial of such cyber operations amounting to a use of force.

2.1. (iv) *Who Will Be Tasked with ACD?* It remains to be clarified what is meant by, and how to organize the active cyber defense, but as described above, a new organization in the cabinet secretariat is thought to oversee the measures as the highest command center. Both the SDF and the Police units are thought to assume it on the ground, along with private hackers that the cabinet secretariat might hire directly[44]. As proposed by a former SDF cyber expert, however, it might encompass much milder measures rather than hacking back, taking down and making command & control server and other misused network inoperable. As he cites, the Cybersecurity

[43] Japan MoD, "Other Basic Policies", https://www.mod.go.jp/en/d_policy/basis/others/index.html.

[44] "Toward a New 'Control Tower' of Active Cyber Defense. Overseeing the SDF and the Police Units and Recruiting Hackers Are also Under Review [積極的サイバー防御の「司令塔」新設へ…自衛隊や警察庁の指揮・民間ハッカー登用も検討]", *Yomiuri Newspapers*, November 1, 2022, https://www.yomiuri.co.jp/politics/20221031-OYT1T50257/ (only in Japanese).

and Infrastructure Security Agency (CISA) of the US government recommends that the Federal Civilian Executive Branch (FCEB) should undertake preparation activities. If these new measures are also introduced as part of Japanese active cyber defense, there might be opportunities for cyber experts other than the SDF or the Police to take on these tasks[45].

2.2 *Transition from NISC to a New Cybersecurity Organization.* Currently, both the Cybersecurity Strategy Headquarters (CSSH) and the NISC stand as the control tower of the government in terms of taking cybersecurity measures in peacetime[46]. The CSSH is a decision-making body established under the Basic Act on Cybersecurity of 2014[47], with its roles of drafting the cybersecurity strategy, setting the cybersecurity standards for government ministries and agencies and other associated organizations, investigating into cyber incidents, and coordinating with stakeholders, including domestic and foreign, on the incidents, and so on (article 26, section 1 of the Act). It is headed up by the chief cabinet secretary and consists of state ministers and subject matter experts (articles 28-30 of the Act) (see Figure 1 below).

The NISC is a division in the cabinet secretariat and serves as a secretariat of the CSSH (see Figure 1 below). The head of the NISC, also as both the assistant chief cabinet secretary and the deputy director general of the National Security Secretariat (NSS) assumes responsibilities other than the NISC's. Among these are emergency

[45] YASUSHI UCHIDA, *Underdevelopped Nation in Cyber Defense Terms. Crisis for Japan. Even Signs of Attacks Are Not Detected* [サイバー防衛後進国・日本の危機、攻撃の兆候すら検知できない実態]", *Nikkei Xtech*, January 19, 2024, https://xtech.nikkei.com/atcl/nxt/mag/ne/18/00108/00004/ (only in Japanese). An interviewee in this article refers to the Active Defense as one of preparation activities recommended by CISA. It is described as follows: Federal Civilian Executive Branch (FCEB), agencies with advanced defensive capabilities and staff might establish active defense capabilities—such as the ability to redirect an adversary to a sandbox or honeynet system for additional study, or "dark nets"—to delay the ability of an adversary to discover the agency's legitimate infrastructure. Network defenders can implement honeytokens (fictitious data objects) and fake accounts to act as canaries for malicious activity. These capabilities enable defenders to study the adversary's behavior and TTPs and thereby build a full picture of adversary capabilities. CISA, "Federal Government Cybersecurity Incident & Vulnerability Response Playbooks", November 2021, p. 8, https://www.cisa.gov/sites/default/files/2023-02/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.

[46] Japan MoD, *The Defense of Japan (Annual White Paper) 2023*, 330.

[47] Act No. 104 of November 12, 2014, Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/ja/laws/view/3677/je#je_ch2at1.

response and crisis management, where he/she is supposed to assist the chief cabinet secretary, the deputy chief cabinet secretary, and the deputy chief cabinet secretary for crisis management, all together, with responses to, or prevention of a national emergency that has caused, or is likely to cause, material damage to the lives, bodies, or property of citizens[48], thereby assist the prime minister directly as a member of a subsidiary organ of the Cabinet (see Figure 2 below)[49].

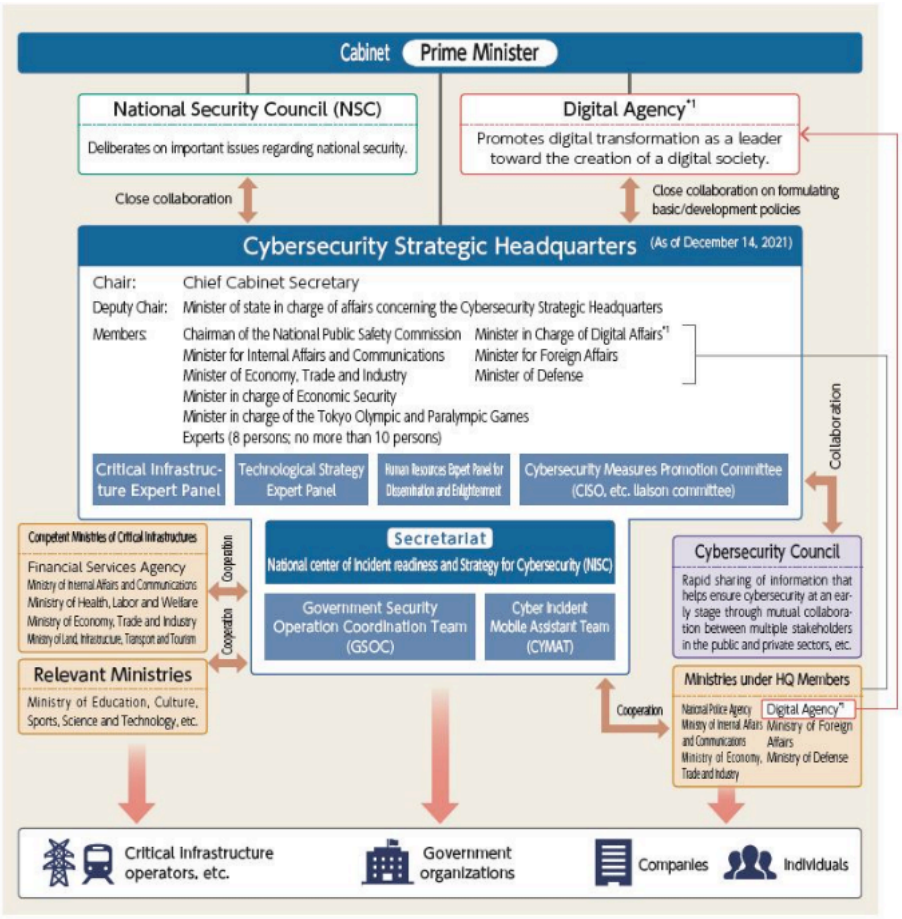

Figure 1: NISC, "CSSH and NISC: Organizational Chart," https://www.nisc.go.jp/eng/index.html

[48] Article 15 and 17 of the Cabinet Act (Act No. 5 of 1947), Government of Japan, e-Gov, https://elaws.e-gov.go.jp/document?lawid=322AC0000000005 (only in Japanese); KONO, *In Search of a Targeted Approach: Japan-Estonia Cybersecurity Cooperation*, 50-51.

[49] The Cabinet Secretariat, *Overview*, https://www.cas.go.jp/jp/gaiyou/index.html (only in Japanese).

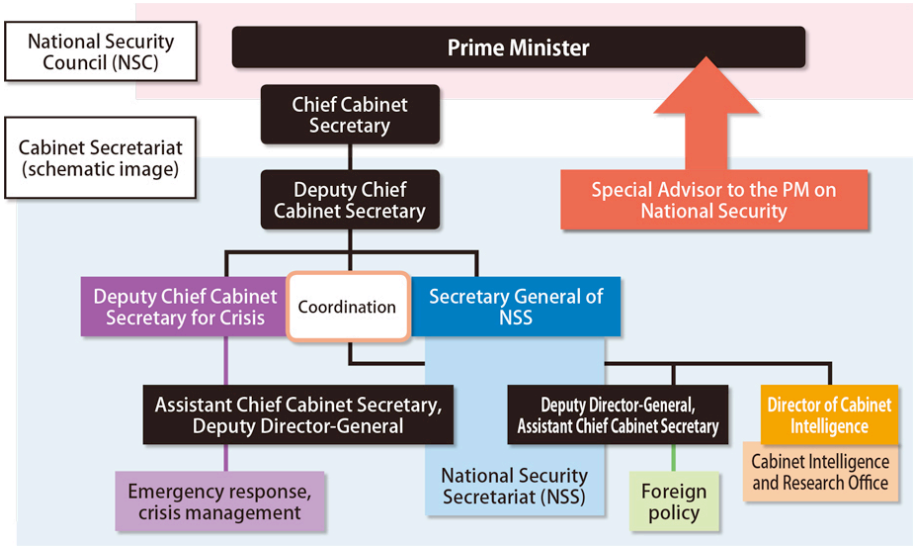

Figure 2: Japan MFA, "Organizational Chart of the Cabinet Secretariat," *Diplomatic Bluebook 2014*, https://www.mofa.go.jp/policy/other/bluebook/2014/html/chapter3/efforts.html

As noted earlier in the article, the NISC, specifically the GSOC sensors, are monitoring the entry points of government networks around the clock, and in case an incident occurs, it makes an analysis and assists a victim organization through the Cyber Incident Mobile Assistant Team (CYMAT) in response to a call for help[50]. The supervision has been extended to cover organizations other than central government ministries and agencies. In the wake of the leak of personal data on over one million citizens in 2015, the affected entity came under the GSOC supervision. The Japan Pension Service (JPS) had succeeded the Social Insurance Agency's service to manage public pension, and still had been operating under the Ministry of Health, Labour and Welfare (MHLW)'s jurisdiction. On the other hand, it had been reorganized as a non-governmental special corporation in Japanese legal term, and thus its information systems had been placed outside the GSOC monitoring scheme. In October 2016, the CSSH decided to designate the JPS along with other eight corporations to be covered by its supervision in the light of "the impact on the people's living conditions and economic activities

[50] The CYMAT was set up in 2012 and consists of cyber technical experts across ministries and agencies. The NISC, "The CYMAT," https://www.nisc.go.jp/pdf/council/cs/taisaku/ciso/dai05/05shiryou04.pdf (only in Japanese).

accrued in the case in which cybersecurity in the corporations is not ensured", based on article 13 of the Basic Act on Cybersecurity[51]. Not just GSOC monitoring, but other measures taken by the CSSH for improving cybersecurity in central government ministries are also applied to these corporations, such as common cybersecurity standards, cyber exercises and training opportunities, information sharing and so on.

As opposed to a growing demand for cybersecurity management, the NISC resources does not live up enough to the expectations. Due to the shortage of in-house technical experts, some of the NISC missions are being delegated to external technical institutes like the IPA or the JPCERT/CC, as the NISC officials seconded from ministries are often busy with tasks arising from the NISC responsibilities as a policy department. The CYMAT scheme also relies on voluntary cooperation from ministries and agencies. Even after registering themselves as the CYMAT personnel, they are expected to come for assistance just on a convenience basis in case of cyber emergency.

More fundamentally, the NISC is not in a vertical position to supervise each ministry and agency, in the first place. The latter still retains the power to manage cyber security over their own information systems and networks. It means that IT specialists in each ministry and agency might be always tied up with handling cyber incidents in their home ministry. It was clearly shown in regard to the JPS leak incident, where the MHLW arranged its own process of investigation into it and published its reports, independently of the NISC efforts.

In the case of the control over the private sector, the NISC plays little to no role. No sensor is not attached to information systems and networks operated by the private sector. Hence, the detection of cyber incident is not in the NISC, but completely in their hands. When WannaCry ransomware attacks were detected in the private entity in 2017, what the NISC did was posting a security alert for raising awareness on social media, according to the former senior NISC official's account. Other government actions relating to the incident were a security alert issued by the IPA, setting up an information and liaison office in the Cabinet's Crisis Management Center[52], and a

[51] The CSSH, "Designation of Entities Based on Article 13 of the Basic Act on Cybersecurity", October 21, 2016, https://www.nisc.go.jp/pdf/council/cs/shiteihojin.pdf (only in Japanese).

[52] IKUO MISUMI, *The Implications of Responses to Major IT Security Incidents on*

press release by both the chief cabinet secretary and the MFA denouncing North Korea about its involvement in the attacks[53].

Right after releasing the NSS in 2022, the government announced its plan to revamp the NISC for fiscal year 2024, as a tentative measure until the planned new organization takes it over. First, the number of full-time staffs working at the NISC will be raised from 95 to 175 presumably through the secondment from the ministries and agencies concerned, and part-time experts will be recruited from the private sector. Second, several new positions at the management level will be created, namely one vice-minister level position, two director-level positions, and three deputy director-general level positions just below the head of the NISC, which will be filled up by the transfer from externally[54].

2.3. *Buildup of More Cyber Capabilities in MoD. The MoD's Annual White Paper 2023* published after the release of the National Security Strategy does not describe clearly whether the MoD/SDF will take on the active cyber defense[55]. Notwithstanding, a statement that in approximately ten years from now, the MoD/SDF will have strengthened its posture *for supporting the cybersecurity of entities other than the SDF*, seems to indicate that the MoD/SDF might get involved in it one way or another, departing from the past posture[56]. The MoD's defense plan for the next five years to reinforce cyber capabilities can be understood from that perspective.

2.3 (i) *Defense Spending Increase.* More than two weeks before the National Security Strategy was released, the prime minister announced a new defense budget plan in late November 2022 to increase up to around 2% of the current gross domestic product (GDP).

Cybersecurity Policies, in *The Journal of Japan Society of Security Management*, Vol. 34, No. 2, 2020, 26, https://www.jstage.jst.go.jp/article/jssmjournal/34/2/34_22/_pdf/-char/ja (only in Japanese).

[53] Japan MFA, "The U.S. Statement on North Korea's Cyberattacks (Statement by Press Secretary Norio Maruyama)", December 20, 2017, https://www.mofa.go.jp/press/release/press4e_001850.html

[54] "The Government Increases NISC Staffs, as well as Adding Vice Minister-Level Official. Reinforcing a Chain of Command [政府、内閣サイバー職員倍増へ　次官級配置、指揮系統を強化]", *Kyodo Tsushin*, December 30, 2023, https://news.yahoo.co.jp/articles/026fd253c474592de3e8f652d111cce698c664a1

[55] Japan MoD, *The Defense of Japan (Annual White Paper) 2023*, 239.

[56] An emphasis by the author. *Ibid.*, 330.

The total defense spending over the next five years from FY2023 - 2027 will exceed 43 trillion yen ($315.46 billion)[57].

Then-Defense Minister Kishi noted at the press conference on April 1st, 2022 that the Japanese defense spending in 2021 would reach approximately 1.24% of GDP, based on the calculation using the NATO criteria, including pensions paid to military veterans, monetary contributions to the UN peace keeping operations, and the budget for the Coast Guard[58]. Still a target 2% of GDP is a dramatic hike and far from easy to achieve considering ever deteriorating fiscal conditions[59].

According to data on the MoD website, cyber-associated expenditure for next 5 years in FY 2023- 2027 is set at around 1 trillion yen ($6.6 billion) in contract-based amount[60]. Breaking down to annual basis, the cyber budget accounts for 236.3 billion yen (around $ 1.57 billion) out of a total budget of FY2023 at around 8.9 trillion yen (over $ 59 billion), and 202.6 billion yen (around $ 1.35 billion) out of around 9.3 trillion yen (around $ 62 billion) in FY 2024, respectively, in contract-based amount[61].

2.3 (ii) *Reinforcing Cyber Technical Experts in MoD.* To begin with, the MoD/SDF has been suffering a personnel shortage issue for a long time. Only about 90% of the staffing level has been filled[62]. Without the conscription in place, the SDF must count on young

[57] The amount in US Dollar is based on the exchange rate around the time of the announcement in late 2022.

[58] ONO, *Introduction to Defense Issues of Japan* [日本の防衛問題入門], 70-71.

[59] TETSUSHI KAJIMOTO, TAKAYA YAMAGUCHI, *Japan Vows to Balance Budget While Boosting Military Spending*, *Reuters*, December 9, 2022, https://www.reuters.com/markets/asia/japan-vows-stick-budget-balancing-goal-despite-defence-boost-2022-12-09/; "Japan's Total Debt Swells to Record 1,286.45 Tril. Yen in 2023," *Mainichi Newspapers*, February 9, 2024, https://mainichi.jp/english/articles/20240209/p2g/00m/0bu/061000c#:~:text=As%20of%20Dec.%2031%2C%20the%20total%20debt%20consisted,in%20financing%20bills%2C%20the%20Finance%20Ministry%20data%20showed.

[60] Japan MoD, "Overview of the Defense Spending Plan for FY2024: Summary", December 22, 2023, p. 5, https://www.mod.go.jp/j/budget/yosan_gaiyo/2024/yosan_20231222_summary.pdf (only in Japanese).

[61] Japan MoD, *Overview of the Defense Spending Plan for FY2024*, December 22, 2023, 6, https://www.mod.go.jp/j/budget/yosan_gaiyo/2024/yosan_20231222.pdf (only in Japanese).

[62] NOBUHIKO TAJIMA, *Panel Urges SDF Pay Increases amid Recruitment Shortage Issues*, *Asahi Newspapers*, July 13, 2023, https://www.asahi.com/ajw/articles/14955804.

volunteers. But the recruiting campaign has been struggling more and more in the face of shrinking working force.

The MoD's plan for reinforcing cyber force indicates that Cyber Defense Units should have core members of up to around 2,230 at the end of fiscal 2023 (in March 2024), more than doubling FY2022 number (about 890). Thereafter, it is set to raise to about 2,410 at the end of 2024, and eventually to 4,000 by fiscal 2027. Besides, additional officers of around 16,000 are expected to assume other cyber-associated tasks such as procurement, maintenance of the MoD/SDF systems. With a total number of the SDF personnel unchanged (247,154)[63], there needs to be an adjustment across the MoD/SDF.

Other initiatives in MoD include recruiting a part-time chief cybersecurity advisor since 2021, candidates for SDF reserve specialized in cybersecurity since 2022[64], and high-skilled personnel for a fixed term up to 5 years with salary equivalent of that of the head of Joint Staff or the vice minister (top of civilian officials in MoD) expected to start in 2024[65].

As internal organizations responsible for education and training, the Ground SDF High Technical School, the Ground SDF System and Signal/Cyber School (tentative name) that was reorganized from GSDF Sigint School, and the National Defense Academy teach cyber related subjects with improved curricula.

2.3 (iii) *Research and Development.* The MoD is also looking to further step up the collaborations with the private sector in respect of research and development (R&D) of defense equipment and technologies. Compared to defense industry, however, the collaboration with academia is slower at progressing due to the long tradition of rejecting scientific research "for war purposes"[66] as has

[63] *Ibid.*, 49.

[64] Japan MoD, *The Defense of Japan (Annual White Paper) 2023*, 333.

[65] "Cyber Expert into the SDF from the Private Sector, Recruiting FY2024 for the First Time [自衛隊に民間サイバー人材　政府、24 年にも初採用]", *Nikkei Newspapers*, May 12, 2023, https://www.nikkei.com/article/DGXZQOUA2098R0Q3A420C2000000/. Defense Minister Kihara told on November 10, 2023, at the Committee on National Security of the House of Representatives of the Diet to introduce it as soon as possible. "Introducing 'High-Skilled SDF Personnel' with a Fixed Term and Salary Equivalent to That of the Head of Joint Staff. Defense Minister's Comment [「高度人材自衛官」を早期導入　任期付きで統幕長並み給与―木原防衛相]," *Jiji Tsuhin*, November 10, 2023, https://www.jiji.com/jc/article?k=2023111000428&g=pol (only in Japanese).

[66] "1 Year on, Japan Science Council's Rejection of Military Research Has Little

been promoted by the Science Council of Japan (SCJ) since 1950[67]. One illustrating example is the number of applications by academia for a competitive research funding program named "the Innovative Science & Technology Initiative for Security (MoD Funding)" that MoD's Acquisition, Technology & Logistics Agency (ATLA) has been running to promote advanced basic research in defense area[68]. In March 2017, the SCJ reiterated its concerns because of what they call "government intervention" that might force researchers to be diverted in an unintended direction[69]. Some major universities in Japan followed suit[70]. Since an inception of MoD Funding in 2015, the applications from university researchers were downward until around 2022 (see Table 1 below), when the SCJ submitted a new document to the Minister of State for Science and Technology Policy, stating that it is no longer possible to split research between dual-use and purely non-military, and reportedly gave a de-facto endorsement of the program for them to apply under certain conditions[71]. A tide might be turning in favor of the program in the wake of the SCJ's submission, as their applications doubled for FY2023.

FY / Applications	2015	2016	2017	2018	2019	2020	2021	2022	2023
The number	58	23	22	12	9	9	12	11	23
Ratio (%)	53	52	21	16	9	8	13	11	19

Table 1: The Applications by Academia for ATLA's Innovative Science & Technology Initiative for Security.

Note: The number is not limited to cyber-related proposals, but all-inclusive in subject wise.
Source: ATLA of Japan MoD, "The Innovative Science & Technology Initiative for Security in FY2015-FY2023," https://www.mod.go.jp/atla/funding/kadai.html (only in Japanese).

Traction", *Mainichi Newspapers*, March 30, 2018, https://mainichi.jp/english/articles/20180330/p2a/00m/0na/010000c.

[67] The SCJ is equivalent to the National Academy of Sciences (NAS) in the US.

[68] Japan MoD, *The Defense of Japan (Annual White Paper) 2023*, pp. 473-474.

[69] The Science Council of Japan (SCJ), "Statement on Research for Military Security", March 24, 2017, https://www.scj.go.jp/ja/info/kohyo/pdf/kohyo-23-s243-en.pdf.

[70] E.g. "Kyoto University's Basic Policy on Military Research," reads as follows: The University's research activities are undertaken with the aims of increasing the safety of society and contributing to human well-being and peace. No one at the University is permitted to be involved in military research that threatens those aims. March 28, 2018, https://www.kyoto-u.ac.jp/en/research/research-compliance-ethics/military-research.

[71] "Japan Science Council Says Drawing Line between Military, Civil Use Technology Difficult", *Mainichi Newspapers*, July 28, 2022, https://mainichi.jp/english/articles/20220728/p2a/00m/0na/023000c.

3. *National Framework on Cybersecurity.* 3.1. *Reporting of Cyber Leak.* With respect to a reporting and/or information sharing of cyber incidents, there are a couple of frameworks in place, some of which are mandatory, others are not. Regardless of whether it is voluntary reporting, however, a victim organization may be pressured to do so to multiple agencies depending on the situation and the purpose to be served, leading to heavy burdens to bear for them. Below is an overview of some of major frameworks in place in the event of unauthorized access to network/system.

3.1 (i) *Reporting to the Personal Information Protection Commission.* First, when any entity handling personal data, causes a leak as a result of cyber incidents, and the leak is "likely to harm individual rights and interests," it must report it to the Personal Information Protection Commission (PPC) of the government promptly[72]. It must also notify affected individuals about a brief summary, a list of data leaked or possibly leaked, the cause, and a secondary (or possibly secondary) harm, to the extent necessary to ensure the protection of the rights and interests of the affected persons, promptly in accordance with the circumstance concerned[73]. The reporting to the PPC is mandatory in the following four cases including likely ones: "sensitive personal information" is involved[74], the leak might risk property degradation through the misuse of personal data, illegitimate purposes are behind the leaks, or the leaks surpassed one-thousand cases[75].

[72] Article 26 of Act on the Protection of Personal Information (Act No. 57 of May 30, 2003), amended in 2020 and came into effect in April 2022. Japan MoJ, Japanese Law Translation website, https://www.japaneselawtranslation.go.jp/en/laws/view/4241; Article 8 (1) of Enforcement Rules for the Act on the Protection of Personal Information (Rules of the PPC No. 3 of October 5, 2016), Government of Japan, e-Gov, https://elaws.e-gov.go.jp/document?lawid=428M60020000003 (only in Japanese). The term "promptly" means within 3-5 days after the leak is found (sec. 3-5-3-3 of the guideline on a preliminary report, https://www.ppc.go.jp/personalinfo/legal/guidelines_tsusoku/#a3-5 (only in Japanese)). The preliminary report is to be followed by detailed report to be made no later than 30 days after the finding of the leak (article 8 (2) of the Rules of the PPC and sec. 3-5-3-4 of the guideline on a detailed report.)

[73] Article 10 of the Rules of the PPC.

[74] Sensitive personal information means "personal information as to an identifiable person's race, creed, social status, medical history, criminal record, the fact of having suffered damage by a crime, or other identifiers or their equivalent prescribed by Cabinet Order as those of requiring special care so as not to cause unjust discrimination, prejudice or other disadvantages to that person" under article 2 (3) of the Act on the Protection of Personal Information.

[75] Article 7 of the Rules of the PPC.

3.1 (ii) *Reporting to IPA.* The IPA is tasked by the Ministry of Economy, Trade and Industry (METI)'s two public notices to collect and analyze data on computer viruses (including ransomware) and unauthorized access through notification from victim entities[76]. Affected entities are not legally mandated, but immensely urged to submit data to the IPA as the METI-designated entity.

When it comes to scope of application, more cases will fall under the IPA-run framework than crimes covered by both Penal Code (Chapter XiX-2 on Crimes related to Electronic or Magnetic Records Containing Unauthorized Commands)[77] and the Act on Prohibition of Unauthorized Computer Access (article 3 on Unauthorized Computer Access)[78] as the IPA receives a case in which no access restrictions is put in place in the affected network, that is the cause of an unwanted access to it[79].

3.1 (iii) *Closer Coordination Among Ministries/Agencies.* There was a consensus view growing up across ministries and agencies that their roles might be overlapping in certain cyber incidents where unauthorized access to a network/system occurs, personal data is leaked, electronic services are disrupted, and thus a victim entity's rights and/or interest protected under penal law are infringed on[80].

With a view to preventing the leak beforehand, keeping the situation from worsening, and thereby reducing the level of infringement of rights and interests of affected individuals amid cyberattacks, relevant government agencies have signed a Memorandum of Understanding (MoU) with each other, aiming to

---

[76] Japan METI, "Responses Criteria for Computer Viruses [コンピュータウイルス対策基準]", https://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm and "Responses Criteria for Unauthorized Access to Computers [コンピュータ不正アクセス対策基準]", https://www.meti.go.jp/policy/netsecurity/UAaccessCMG.htm (only in Japanese).

[77] Act No. 45 of April 24, 1907, Japan MoJ, Japanese Law Translation, https://www.japaneselawtranslation.go.jp/ja/laws/view/3581#je_pt2ch21.

[78] Act No. 128 of August 13, 1999, Japan MoJ, Japanese Law Translation, https://www.japaneselawtranslation.go.jp/ja/laws/view/3933/en#je_at3.

[79] The IPA, "Reported Cases of Computer Viruses and Unauthorized Access in the Former Half of 2023," September 2023, n. 4, 1, https://www.ipa.go.jp/security/todokede/crack-virus/ug65p9000000nnpa-att/2023-h1-jirei.pdf (only in Japanese).

[80] The PPC, "Boosting of the Coordination between the PPC and the Government Ministries and Agencies in Charge of Cybersecurity: Sorting Out the Schemes and Signing Memorandum of Understanding [情報保護委員会とサイバーセキュリティ関係省庁・機関との連携の強化－連携の仕組み整理と覚書締結－]", March 15, 2023, p. 4, https://www.ppc.go.jp/files/pdf/230315_renkei.pdf (only in Japanese).

promote a closer coordination between them when addressing the same viruses or incidents[81]. More specifically, various joint actions are intended, such as to remind victim organizations of the reporting obligation it owes to other agencies concerned, to conduct a joint hearing to victim entities and share hearing results when held individually, to share expertise and technical counsel produced through investigations by each agency, to issue a joint notice, and to confirm mutual supervisory measures in advance to enable a consistent exercise of the authorities[82]. All these measures are expected to streamline the flow of incident responses measures.

3.1 (iv) *Remaining Challenges to Coordination.*

Despite an improved efficiency of the procedures, there remains a serious concern regarding the reporting burden for the affected organizations to shoulder. The reporting, whether it be mandatory or voluntary, must be made to the various government agencies in accordance with the modalities set by each regulator, such as filling out the different form depending on which agencies to report. A unified form for the reporting is suggested to be one solution for easing the burden[83].

The way of coordination across stakeholders is subject to a constant update. "The Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks" released in March 2023 is the most recent attempt in this regard. The guidance was produced by a Study Group consisting of eleven external experts, while multiple government entities were involved in the process[84]. The chief cabinet secretary-chaired steering committee of the Cybersecurity Council

[81] *Ibid*. As for MoUs signed between the PPC with other agencies, https://www.ppc.go.jp/personalinfo/legal/supervision/; The IPA with the National Police Agency, https://www.ipa.go.jp/news/2023/announce/ex20231222.html (all only in Japanese).

[82] The PPC, "Enhancing Coordination between the PPC and Government Agencies in Charge of Cybersecurity [個人情報保護委員会とサイバーセキュリティ関係省庁・機関との連携の強化]", March 15, 2023, https://www.ppc.go.jp/files/pdf/230315_renkei.pdf (only in Japanese).

[83] "The PPC Coordinates Responses to Leak Incidents with the NISC, the Police, and the IPA. Burdens Remain for Service Providers [個情委が NISC・警察・IPA と情報漏洩事故対応で連携、なおも残る事業者の負担]", *Nikkei Xtech*, March 31, 2023, https://xtech.nikkei.com/atcl/nxt/column/18/00001/07875/?ST=simpleview (only in Japanese).

[84] The NISC, "Study Group of the Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks", https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html (only in Japanese).

convened the study group, and the METI, the Ministry of Internal Affairs and Communications (MIC), the NPA, the NISC and the JPCERT/CC attended rounds of meeting as its secretariat[85]. The NISC as an umbrella organization of the Cybersecurity Council, not just took the lead in its implementation, but also disseminated the guidance both within the Council members and beyond.

However, a couple of months after the release, the efficacy of the guidance was tested in a severe manner. The NISC issued a press release in the beginning of August 2023 regarding the leak of personal data due to irregular access to their email system[86]. According to some media articles, up to 5,000 persons fell victim by having electronic correspondence through that system[87]. The NISC reported it to the PPC and notified affected persons as required by the Act on the Protection of Personal Information. The NISC explained that the cause was found to be vulnerabilities in an equipment used for their email system, resulting in irregular communications that had continued for about eight and a half months until the finding. Overall, their way of both disclosing and sharing the information was received with disappointment and dissatisfaction by a couple of organizations and cyber security experts. The JPCERT/CC[88], for example, claimed that

[85] Japan MIC, press release, "Results of Solicitation of Opinions on Draft Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks and Publication of Guidance for Sharing and Disclosure of Information on Damage from Cyberattacks", March 8, 2023, https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pressrelease/2023/3/08_02.html; For the guidance and the background documents that are released only in Japanese, Japan METI, press release on the same subject, https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html (only in Japanese).

[86] The NISC, press release, "Possible Leak of Email Data from the NISC Systems [内閣サイバーセキュリティセンターの電子メール関連システムからのメールデータの漏えいの可能性について]", August 4, 2023, https://www.nisc.go.jp/news/20230804.html (only in Japanese).

[87] "Unauthorized Access to the Cabinet Intelligence Division. Possible Leak of Email Data [内閣情報機関に不正アクセス　メールデータ漏洩可能性]", *Nikkei Newspapers*, August 4, 2023, https://www.nikkei.com/article/DGXZQOUA047RI0U3A800C2000000/; "Cyberattacks on the NISC Leaking Email Data of 5,000 people. The Japan Meteorological Agency Were Affected Too. [NISC にサイバー攻撃、メールデータ 5 千人分流出か　気象庁も被害]", *Asahi Newspapers*, August 5, 2023, https://www.asahi.com/articles/ASR8545P7R84ULZU009.html (both only in Japanese).

[88] As for a suspected equipment that caused the leak and the attacker, Ko Nonomura, " The JPCERT/CC Points Out the NISC Didn't Value Information Sharing in the Case of Cyberattacks despite its Norm-Setting Role [規範示すべき NISC がサイバー攻撃時の情報共有を軽視、JPCERT/CC が指摘]", *Nikkei Xtech*, September 4, 2023, https://xtech.nikkei.com/atcl/nxt/column/18/00001/08341/?P=2; *Idem*., "A Public Institute Speaks Bitterly against the Government Cyber Organization. Information Sharing was

they did not receive any sharing from the NISC, apparently contrary to their expectations based on a partnership agreement signed with the NISC in 2015 on the matter. A press release by the JPCERT/CC on the incident announced their wish that any potential victim of the leak should adhere to the procedure drawn up by the guidance and disclose or share detailed technical information including vulnerabilities and suspectedly leaked email-related information[89]. Another expert noted a suspicion that the NISC disregarded the guidance despite their active involvement in the drafting process and the guidance turned out to be lacking utility to prospective users[90].

3.2. *Critical Infrastructure Providers with Special Protection and Duty*. A "critical social infrastructure provider" is a legally defined term in Japan. The Basic Act on Cybersecurity defines it in its article 3 (1) as "those engaged in business that provides infrastructure which is the foundation of the lives of the people and economic activities, and whose functional failure or deterioration would cause an enormous impact on them." To date, fourteen sectors are listed as such whose operations are regulated by the respective Ministries or Agencies, as shown in Table 2 below.

Government organization with supervisory authorities	Category of CI sector
Finance Services Agency (FSA)	financial services
Ministry of Internal Affairs and Communications (MIC)	information and communication services, government and administrative services
Ministry of Health, Labour and Welfare (MHLW)	medical services, water services
Ministry of Economy, Trade and Industry (METI)	electric power supply services, gas supply services, chemical industries, credit card services, petroleum industries

Disregarded [政府サイバー組織に民間組織が苦言　情報共有を軽視", *Nikkei Newspapers*, September 14 2023, https://www.nikkei.com/article/DGXZQOUC056FS0V00C23A9000000/ (only in Japanese).

[89] The JPCERT/CC, press release, "Regarding the Press Release on Email Data Leak from Email-Associated Systems [電子メール関連システムからのメールデータ漏えい被害が公表されている件について]", August 7, 2023, https://www.jpcert.or.jp/press/2023/PR20230807_notice1.html (only in Japanese).

[90] TOSHIO NAWA, "Too Bad 'Cybersecurity Measures' Ingrained in Japanese Companies. What is Inhibiting Cybersecurity Division? [日本企業に染みついた残念すぎる「サイバー対策」 セキュリティ部門にブレーキかけているのは？]", *Toyokeizai Online*, January 16, 2024, https://toyokeizai.net/articles/-/726917?page=3 (only in Japanese).

Ministry of Land, Infrastructure, Transport and Tourism (MLIT)	aviation services, airport, railway services, logistics services

Table 2: List of Critical Infrastructure and responsible Ministries/Agencies

3.2 (i) *Obligatory Reporting.* In the event of cyber incidents occurring to service providers causing a certain level of harm, they have a legal duty to report the incidents to the Ministry/Agency with supervisory authority[91]. For example, telecommunication service providers must report it to the MIC under Article 28 of the telecommunications Business Act, when the incident disrupts services over an hour and affects more than 30,000 customers. Then, the MIC forwards information to the NISC to be later shared within the entire Cabinet Secretariat. All collected information on incidents are also circulated to the CSSH once year where some members, particularly, non-governmental experts might know of them for the first time.

With regard to responsibility of critical social infrastructure providers, the Basic Act on Cybersecurity provides that the provider "is […] to endeavor independently and actively to ensure cybersecurity, as well as endeavoring to cooperate in the implementation of the cybersecurity policy that the national or local government implements" (Article 6). But this provision does not obligate service providers directly to carry cyber incident information to the NISC. The obligatory reporting frameworks are applied primarily to the relation between each ministry/agency with relevant business sector, and are designed to cover all kinds of accidents, out of which cyber is just one of the causes. Afterwards, cyber-related incident information is supposed to be assembled to the NISC. In that sense it is fair to say that information reporting/sharing is implemented in a de-centralized manner across the government bodies and relies on the inter-ministerial cooperation.

3.2 (ii) *Cybersecurity Council.* The Cybersecurity Council is a virtual platform for information sharing among stakeholders in both

[91] The CSSH, "The Cybersecurity Policy for Critical Infrastructure Protection," ANNEX 2 Explanation of CI Services and Service Maintenance Levels, June 17, 2022, 57, https://www.nisc.go.jp/eng/pdf/cip_policy_2022_eng.pdf ; *Idem.*, "The Cybersecurity Policy for Critical Infrastructure Protection (4th Edition)", ANNEX 2. Explanation of CI Services and CI Service Outage Examples, April 18, 2017, 55, https://www.nisc.go.jp/pdf/policy/infra/infra_rt4_r1.pdf.

the public and private sectors. The WannaCry ransomware attacks of 2017 were known as a triggering event, making the government more aware of the importance of information sharing with diverse stakeholders, information on cyber threats and incidents that affect the entire society. The CSSH suggested creating a new scheme[92] and eventually it resulted in the setting up the Council by amending the Basic Act on Cybersecurity in December 2018[93].

Of particular note is that not only central government ministries and agencies, local municipalities, and critical infrastructure providers, but also ICT service providers including cyber security vendors, academic institutions are eligible for the membership. Both the NISC and the JPCERT/CC serve it as its secretariat, while the latter plays a more substantial role in processing cyber incident information in the Council. For example, the first contact point from a victim entity is the JPCERT/CC.

The Council aims to share cyber threat information, including early signs of system malfunctions, develop solutions (counter-measures), and encourage mutual feedback, thereby prevent similar incidents from happening. Critical infrastructure providers are under a legal duty to cooperate with the Council once they choose to join it as members (Article 17, para. 3). As long as service providers belong to the Council, they are exempt from a mandatory reporting of the same cyber incident to the supervising ministry so that duplication of reporting obligation can be avoided. It started with ninety-one members for the first term and for FY2023 three hundred and fifteen entities registered for it[94], although the NISC does not officially

[92] The CSSH, "Cybersecurity from 2020 Onwards: Cybersecurity Strategy Mid-Term Review [2020 年及びその後を見据えたサイバーセキュリティの在り方について －サイバーセキュリティ戦略中間レビュー－]", July 13, 2017, https://www.nisc.go.jp/pdf/council/cs/jinzai/dai07/07sankoushiryou0102.pdf (only in Japanese).

[93] The Cabinet Secretariat, "Bills on the amendment of the Basic Act on Cybersecurity submitted to the 196th session of the Diet", 2018, https://www.cas.go.jp/jp/houan/196.html; IKUO MISUMI, The Background of Enactment and Amendment of the Basic Act on Cybersecurity [サイバーセキュリティ基本法制定・改正の経緯], in *The Journal of Japan Society of Security Management*, Vol. 34, No. 1, 2020, 32, https://www.jstage.jst.go.jp/article/jssmjournal/34/1/34_28/_pdf/-char/ja (only in Japanese); *Idem.*, The Implications of Responses to Major IT Security Incidents on Cybersecurity Policies, 26.

[94] The NISC, "The Summary of the Cybersecurity Council [サイバーセキュリティ協議会について（簡略版）]", https://www.nisc.go.jp/pdf/council/cs/kyogikai/kyogikai_gaiyou_kanryaku.pdf (only in Japanese).

disclose information on the number and what companies belong to it. The Council is the latest development in the Japanese government regarding information sharing of cyber threats and incidents, but as it is a voluntary decision by each service provider whether to join or not the Council, many still seem to hesitate out of concerns about the reporting burdens.

3.2 (iii) *Other Frameworks of Voluntary Information Sharing.*

(a) *Incidents Response and Coordination by JPCERT/CC.* The JPCERT/CC, which itself is a non-governmental non-profit entity called "a general incorporated association" in Japanese legal terms, is delegated with some governmental functions in relation to cyber-security, as is the case with the Cybersecurity Council. Moreover, the JPCERT/CC has been outsourced from the METI with certain cyber incidents and coordination activities[95]. Any entity, including both the public and private sector, whether the defined critical infrastructure sectors or not, can inform the JPCERT/CC of cyber incidents for technical advice. This reporting is done completely based on their voluntary decision. Then the JPCERT/CC contacts controllers of networks and websites affected or involved in incidents concerned. According to the webpage of the JPCERT/CC, about 10,000 cases have been handled annually[96]. It shows that the JPCERT/CC has the double functions, both delegated by the government with regard to handling of cyber incidents.

(b) *J-CSIP by IPA*. The J-CSIP stands for Initiative for Cyber Security Information sharing Partnership of Japan. Unlike the JPCERT/CC, the IPA is a public organization called as "independent administrative agency" under Japanese legal terms and operates under the METI's jurisdiction and implements IT policies and strategies that the METI set out[97].

Launched on October 25th, 2011, J-CSIP has been up and

[95] The project is named as a project on building up cybersecurity economic bases (a project on international coordination and responses on cyberattacks) [サイバーセキュリティ経済基盤構築事業（サイバー攻撃等国際連携対応調整事業）] in Japanese. An official English translation is not found on the METI website.

[96] The JPCERT/CC, "What Is Incident Response? [インシデント対応とは？]", March 20, 2018, https://www.jpcert.or.jp/ir/index.html#handling (only in Japanese).

[97] The IPA, "Overview of IPA", 22, https://www.ipa.go.jp/en/about/gg62ps00000012si-att/gg62ps00000014hh.pdf.

running between the IPA and participating member organizations. Under this framework, member organizations inform the IPA of detected cases of cyberattacks on them, in accordance with a Non-Disclosure Agreements (NDA) signed with the IPA, and then the IPA, as an information hub, disseminate data and its analysis on the incident in an anonymous form to other member organizations after obtaining a consent from the informers for that purpose. It started with thirty-nine entities in five sectors and by the end of 2023, two-hundred-seventeen-nine entities in thirteen sectors have joined it: electricity, gas, chemical, credit card, petroleum, aviation, airport, railway, logistic services, steel, automobile, natural resource exploration, and producer of critical infrastructure equipment. Besides, the IPA assists other sectors with internal information sharing outside of J-CSIP without signing NDA. Currently, thirteen entities in two sectors are in cooperation with the IPA: medical and water. However the number of informed cyber incident cases and circulated cases from FY2012[98] to the former half of FY2023[99] are declining from 246 down to 50 cases in 13 sectors, and from 160 down to 45 cased in external 2 sectors, respectively.

The distinctive feature of J-CSIP is, in addition to being a voluntary character, a wide range of industry sectors participating in it, including five critical infrastructure sectors falling under the METI supervision: electricity, gas, chemical, credit card, petroleum, and four other critical infrastructure sectors under the MLIT: aviation, airport, railway, logistic service. It implies that an incident reporting may take place to both the MLIT and the IPA in the case of these sectors. The last four sectors are not defined as critical infrastructure in the government: steel, automobile, natural resource exploration, producer of critical infrastructure equipment. Lastly, the two sectors in cooperation from the outside of the framework are both the "critical infrastructure" under jurisdiction of the Ministry of Health, Labour and Welfare (MHLW): medical and water services. Therefore, the redundant sharing occurs here too like the MLIT sectors.

[98] The IPA, "Initiative for Cyber Security Information Sharing Partnership of Japan (J-CSIP) Annual Activity Report FY2012", 2012, https://www.ipa.go.jp/security/j-csip/ug65p9000000nkvm-att/000032417.pdf

[99] The IPA, "J-CSIP [サイバー情報共有イニシアティブ J-CSIP（ジェイシップ）について]", November 9, 2023, https://wwkeiOnw.ipa.go.jp/security/j-csip/about.html (only in Japanese).

Conclusion

As discussed above in this article, some cyber incidents have contributed to improving the existing regulatory framework, as in the cyber leak involving the Japan Pension Service in 2015 and the WannaCry ransomware attacks in 2017, and possibly the leak on the NISC in 2023, yet with no positive feedback yielded at the time of this writing. All these incidents made stakeholders more aware of the challenges that emerged on the surface. The term coordination or cooperation between government bodies is all too familiar on paper, although apparently it did not go as smoothly as expected in the past. There is no doubt that other causes also stand in the way of advancing cyber capabilities in Japan, such as no consensus being formed in lawmakers and policymakers, human resource shortages problems, and let alone slow-moving public and private partnership, especially in respect of academia. All these elements can be said to be contributing factors for delaying detailed planning after a grand design was presented in the National Security Strategy.

A future cyber posture might appear in the different form than this article projected, as the preparation is still underway. Having said that, the new Strategy is undeniably a breakthrough in that it acknowledged the need for change in cyber and intelligence posture toward more active one**,** and to that end, it showed its aspiration to overhaul both the Cabinet Intelligence and Research Office (CIRO) as for intelligence, and the NISC as for cybersecurity, in the hope that they play a vital role in pursuing the government policy set out in the Strategy. We will find out more exact plan on how to proceed with the ambitious goals soon.

THE NEED FOR OVERSIGHT ON SURVEILLANCE TECHNOLOGIES: A (PAINFUL) PERSPECTIVE FROM ISRAEL

TAL MIMRAN – LIOR WEINSTEIN

1. *Introduction.* The State of Israel is a leading actor in the international cyber arena, with a strong industry that includes expertise both on the defensive and offensive levels. Israel harnesses its capabilities as part of its diplomatic toolbox, that helps it in reaching out to other States and to gain international legitimacy[1], out of a desire to establish itself as a leader in the design of international cyber governance[2]. As part of that effort, Israel has also joined recently the international discourse on the application of international law to cyberspace, and articulated its perspective on timely international law legal dilemmas[3].

A strong sense of partnership between the government, the security bodies, and the private sector, leads Israel to impressive advancements and success. But, at the same time, it is also a source to challenges in the ability to properly supervise technological developments, and their deployment, in military, police, or intelligence operations.[4] One of the main fields in which this triangle –

---

[1] F. CRISTIANO, *Israel: 'Cyber Warfare and Security as National Trademarks of International Legitimacy'*, in SCOTT N. ROMANIUK S. & MARY MANJIKIAN (eds.), *Routledge Companion to Global Cyber-Security Strategy 13*, 2020.

[2] Government Resolution No. 2443 (Advancing National Regulation and Governmental Leadership in Cyber Security, 15 February 2015). Israel is also a signatory to the European Convention on Cybercrime. *See*: Council of Europe, Convention on Cybercrime, Explanatory Report, C.E.T.S. No. 185, P 38 (8 November 2001), <https://rm.coe.int/16800cce5b>, visited on 26 January 2022. For regional instruments, *see*: Arab Convention on Combating Information Technology Offences (adopted 21 December 2010); African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014).

[3] R. SCHONDORF, *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, in EJIL Talk! (9 December 2020). For discussion, see: TAL MIMRAN, *Between Israel and Iran: Middle-East Attitudes to the Role of International Law in the Cyber-Sphere*, in *Baltic Yearbook of International Law*, 2022, 209, 221-224.

[4] For illuminating discussion on the question of the proper path, for the consideration of new legal instruments in the context of intelligence operations, with a focus on espionage, see D. GIOVANNELLI, *Extraterritorial Jurisdiction Over Cyber Espionage: A New Trend in*

government, security and private sector – converge and at times collide, is in the area of cyber spywares. In this field, the company NSO Group (NSO) has become a household name, for better and worse, alongside its infamous spyware – Pegasus[5].

NSO was once an Israeli success story, and a prime example of the unique Israeli cyber eco-system that fueled the myth of the "Start-Up Nation". But, just like every honeymoon comes to an end, this success story was recently abrupted. It began with reports about the way in which Pegasus was misused around the world, even against high-profile figures, including ten prime ministers, three presidents and a King[6]. Soon after, the controversy spilled-over into Israel, after revelations about the use of a spyware purchased from NSO by the Israeli Police, named Saifan, against Israeli citizens. This led to the establishment of an inquiry team, appointed by the Israeli Attorney General, and to parliamentary discussions over the crisis[7].

The scandals surrounding NSO reveal the good and bad about the Israeli offensive cyber story, and illustrates the unique relationship between the Israeli government, security forces and private sector. It also highlights strengths and weaknesses in law – notably the difficulty in the ability to harmonize between international and domestic legal norms, both of which are challenged by new technologies and the unique, and over-reaching, abilities they introduce. As such, we chose to focus on the test case of NSO and Pegasus in this article.

The article is constructed as follows. The first chapter is this introduction. Then, the second chapter will set the stage, by laying down the Israel cyber eco-system, and the legal infrastructure underlying it, particularly its domestic military export rules (which apply to spywares) and its perspective on the application of international law to cyberspace. Then, the third chapter will delve into the case study – the Pegasus scandal around the world, and the Saifan

---

International Law or Just an Example of Lawfare, in *Contemporary Military Challenges*, 2022, 24(2), 49.

[5] T. MIMRAN, L. WEINSTEIN, *A Path Forward for Israel Following the NSO Scandal*, in *Lawfare*, June 12, 2023, at https://www.lawfaremedia.org/article/a-path-forward-for-israel-following-the-nso-scandal.

[6] C. TIMBERG, M. BIRNBAUM, D. HARWELL, D. SABBAGH, *On the list: Ten Prime Ministers, Three Presidents and a King*, in *The Washington Post*, July 20, 2021, available at: https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.

[7] A. OBEL, *Israel Police use of NSO Spyware Set to be Probed by Knesset Subcommittee*, in *The Times of Israel*, Apr. 23, 2023, available at: https://www.timesofisrael.com/israel-police-use-of-nso-spyware-set-to-be-probed-by-knesset-subcommittee/.

scandal in Israel – and the responses to it (the Merari Report, alongside parliamentary discussions). Following that, the fourth chapter will evaluate the ability of international law, and domestic norms, to deal with spywares, and suggest a possible step moving forward: technological oversight mechanisms, that will integrate privacy and freedom of expression concerns in legality reviews of technology. The fifth chapter will conclude the article.

2. *Setting the Stage.* 2.1. *Israel's Cyber Eco-System – Who Regulates Israeli Cyberspace?* Israel is an advanced cybersecurity actor[8], with proved cyber robustness and resilience[9]. The main regulator in this field is the Israel National Cyber Directorate (INCD)[10]. The INCD's mandate was first assigned by governmental decisions, but starting from 2018 we witnessed the attempt to promote a draft bill, the so-called 'cyber-law', via the Israeli Parliament, with a view to concretize and clarify different aspects of the INCD's operation. According to the suggested bill, the INCD is designed as a security agency[11], that operates and manages the national critical infrastructure and operative cyber defense, and promotes Israel's ability to handle cyber-attacks, alongside shaping wider cyber policy and international cooperation[12]. The INCD works in concert with the Israeli military, police, and other governmental agencies, and of course – it has strong ties with the private sector.

The need to safeguard Israel from cyberattacks is not a theoretical one. For example, in April 2020 Iran targeted Israel's water infrastructure facilities, to which Israel responded with a cyber-operation against Iranian ports[13]. Shortly afterwards, three cyber-

---

[8] J. FREI, *Israel's National Cybersecurity and Cyberdefense Posture: Policy and Organizations*, in *ETH Zurich* 2020, 5, available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2020-09-Israel.pdf.

[9]: L. TABANSKY, I. BEN-ISRAEL, *Cyber Security in Israel*, 2015, 49-54.

[10] Government Resolution 2444, 15 February 2015, article 3, available at: https://ccdcoe.org/uploads/2019/06/Government-Resolution-No-2444-Advancing-the-National-Preparedness-for-Cyber-Security.pdf.

[11] Draft bill cyber security and national cyber Directorate (2018) (hereinafter: "the cyber law"). See criticism on the matter in T. SHWARTZ ALTSHULER, *Cyber law or government spying law*? in *Israel Today*, 25.6.2018, http://www.israelhayom.co.il/article/566437 (Hebrew).

[12] §3, the cyber law.

[13] TOI Staff, Israel behind cyberattack that caused 'total disarray' at Iran port – report, Times of Israel (19 May 2020), <https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/>, visited on 26 January 2022.

attacks hit Israeli companies: Shirbit (an insurance company)[14], Amital Data (an Israeli technology company that provides software solutions in the field of importation and logistics)[15], and Habana Labs (an artificial intelligence company)[16]. Israeli experts have tied these operations also to Iran[17]. According to the Israeli National Cyber Directorate, 18% of businesses in Israel have experienced a cyber-attack, and in the hi-tech sector as much as one-third of them[18]. As such, these incidents represent the tip of the iceberg of a longstanding campaign carried out against Israeli companies.

Returning to the INCD, the suggested bill is still in the legislative pipe, and it is unclear when it will finally be adopted[19]. The premise of the bill reflects value-based interests that demonstrate the pillars of the Israeli eco-system: enhancing technological capabilities, promoting innovation, advancing crisis-management tools and retaliation abilities[20], while maintaining cyber resilience, robustness and defense capabilities[21]. As we will show in the coming parts, enhancing

[14] Israel National Cyber Directorate, Data Breach event at Shirbit (01 December 2020), <https://www.gov.il/en/departments/news/news_shirbit>, visited on 26 January 2022.

[15] M. ORBACH, G. HAZANI, *Israel's supply chain targeted in massive cyberattack*, in *Ctech*, 13 December 20, <https://www.calcalistech.com/ctech/articles/0,7340,L-3881337,00.html>, visited on 26 January 2022.

[16] L. ABRAMS, *Intel's Habana Labs hacked by Pay2Key ransomware, data stolen*, in *Bleeping Computer*, 13 December 2020, <https://www.bleepingcomputer.com/news/security/intels-habana-labs-hacked-by-pay2key-ransomware-data-stolen/>, visited on 26 January 2022.

[17] U. BERKOVITZ, *Iranian hackers aim to sow panic in Israel – report*,in *Globes*, 17 December, 2020, <https://en.globes.co.il/en/article-iranian-hackers-aim-to-sow-panic-in-israel-report-1001353603>, visited on 26 January 2022.

[18] HUAXIA, *18 Pct of Israeli Businesses Suffer Cyberattack: Survey*, News, July 21, 2021, <http://www.xinhuanet.com/english/2021-07/21/c_1310075937.htm>, visited on 26 January 2022.

[19] Some have criticized the broad authorities proposed by the bill, for example regarding data collection, and the lack of oversight mechanisms over the exercise of governmental authority in cyberspace. See E. CHACKO, *Persistent Aggrandizement? Israel's Cyber Defense Architecture*, Aegis Series Paper no.2002, 5-7; A. CAHANE, *The New Israeli Cyber Draft Bill – A Preliminary Overview*, *The Federmann Cyber Security Research Center blog* https://csrcl.huji.ac.il/news/new-israeli-cyber-law-draft-bill#_ftn5; D. HOUSEN-COURIEL, T. MIMRAN, Y. SHANY, *Israel's Version of Moving Fast and Breaking Things: The New Cybersecurity Bill*, in *Lawfare*, May 7, 2021, available at: https://www.lawfareblog.com/israels-version-moving-fast-and-breaking-things-new-cybersecurity-bill.

[20] D. HOUSEN-COURIEL, *National Cyber Security Organisation: Israel*, NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE, 2017, available at: https://ccdcoe.org/uploads/2018/10/IL_NCSO_final.pdf.

[21] National Cyber Directorate, *Israel National Cyber Security Strategy In Brief*, 2017, 9, https://cyber.haifa.ac.il/images/pdf/cyber_english_A5_final.pdf.cc.

technological and innovation, and also equipping ones industry and security forces with advanced technological tools, might come at a price.

2.2. *Israel's Weapon Export Regime.* The Israeli military export industry is a predominant one, amounting to around 10 billion dollars annually[22]. Israeli export laws restrict every marketing and exporting of military products, and conditions them to a license for sale and marketing abroad by The Israeli Defense Export Controls Agency (DECA), an administrative body within the ministry of defense[23]. This is the only body allowed to grant a market and export license for military goods[24], and in fact it is the main body that regulates technology with military or security use in Israel.

The considerations underlying the work of DECA are: to safeguard national security interests, maintain Israel's international relations, and uphold international obligations alongside other vital interests[25]. At times, DECA consults with other departments in the governments – be that the ministry of justice or the ministry of foreign affairs[26].

The inspiration to the Israeli Defense Export Control Law is the Wassenaar Arrangement on Export Controls (WA), notwithstanding that Israel did not join it[27]. Through national legislation the WA is

---

[22] O. YARON, *Israeli Arms Exports Skyrocket Amid Ukraine War, Iran and Abraham Accords*, in *Haaretz*, 22.11.2022, https://www.haaretz.com/israel-news/security-aviation/2022-11-22/ty-article/.premium/israels-arms-exports-flourish-amid-ukraine-war-iran-and-abraham-accords/00000184-81eb-dfe4-adff-b9fbbb840000.

[23] DECA, *About DECA*, DESA SITE https://exportctrl.mod.gov.il/English/Pages/default.aspx.

[24] § 10-11 Defense Export Control Order (Licenses)-2008.

[25] §1 Defense Export Control Law, 5766-2007.(hereinafter: Defense Export Control Law) See (unofficial) translation: https://exportctrl.mod.gov.il/Documents/%D7%97%D7%95%D7%A7%20%D7%94%D7%A4%D7%99%D7%A7%D7%95%D7%97%20+%20%D7%A6%D7%95%D7%95%D7%99%D7%9D%20+%20%D7%AA%D7%A7%D7%A0%D7%95%D7%AA/Defense_Export_Contro_Law.pdf.

[26] A report by the state comptroller on export noted several cases when the Ministry of Defense didn't consult with the Ministry of foreign affairs. See T. INBAR, *State Comptroller Report: Flawed Ministry of Defense Decision-Making*, in *Israel Defense*, 1.05.2012, https://www.israeldefense.co.il/en/content/state-comptroller-report-flawed-ministry-defense-decision-making.

[27] For the relationship see for example press release, Israeli statement at the conclusion of the Wassenaar Arrangement Outreach Delegation visit https://www.gov.il/en/departments/news/israeli-statement-at-the-conclusion-of-the-wassenaar-arrangement-outreach-delegation-visit-20-november-2019. "Israel, which has long ago adopted a policy of adherence to the export control regimes, including the WA,

incorporated into Israeli arms export regime. For example, in Israeli legislation all Wassenaar controls automatically are adopted automatically, without any form of domestic implementation[28]. The WA is a non-binding multilateral agreement between 42 states, promoting transparency and accountability in the exportation of conventional arms and dual use goods and including technologies. The arrangement invites States to legislate their export protocols and licensing rules in order to promote transparency and international regulation[29]. It also provides tools for States to exchange international knowledge and promote international cooperation that can serve States both on the domestic level, and also in their joint international efforts against threats such as terrorism[30].

The WA is of importance, but it has some inherent limitations. *First*, a main issue is the impartiality of the regulating body, as States are at times the client and at other times the regulator. *Second*, Wassenaar is an arrangement and not an obligating treaty, and it allows for significant consideration of domestic interests (notably security and economic needs). *Third*, even if we would have been referring to a more coercive mechanism, it is usually very limited in terms of membership (less than a quarter of the States of the world are a member of it). for example, WA doesn't prohibit the purchase of surveillance technologies from a non-participating state, and therefore eased the importation to states in the European Union[31]. Hence, the arrangements have 'loopholes' that significantly weakens its ability to limit arms export efficiently. As such, it is subject to, and impacted by, geo-political considerations which might supersede it. *Fourth*, there is the matter of broad definitions which inhibit on the private market, or the flip side, under-encompassing ones. In this regard,

---

incorporates through national legislation and regulation the control lists of the export control regimes. Israel administers export controls through a foundation of collaborative interagency process and vast industry outreach."

[28] §1 The Export Control Order (Dual-Use Goods), 2008. For discussion on the implications on export of technologies see D. HINDIN, *Can Export Controls Tame Cyber Technology?: An Israeli Approach*, in *Lawfare*, February 12, 2016, https://www.lawfaremedia.org/article/can-export-controls-tame-cyber-technology-israeli-approach.

[29] The Wassenaar Arrangement on Export Controls of Conventional Arms and Dual Use Goods and Technologies, Participating States.

[30] K.A. DURSHT, *From Containment to Cooperation: Collective Action and the Wassenaar Arrangement*, in *Cardozo Law Review*, 19, 1997, 1079, 1107-1109.

[31] See A. LUBIN, *Selling Surveillance*, in *Indiana University Legal Studies Research Paper Series 495*, 2023, 10-11 (hereinafter: Lubin, 2023).

international law aspires for proximity to reality, as can be seen from principles like *ex factis jus oritor*, namely that effective power cannot be ignored, at the risk of rendering redundant legal rules in the face of new reality[32]. This principle, *ex factis jus oritur*, is fundamental, as the international legal order, absent of a centralized structure, demands strong and concrete impact on reality in order to solidify its foundations[33].

Indeed, to this day, the Wassenaar Arrangement does not cover properly all issues regarding software due to wide and general definitions, leaving many offensive-cyber technologies to be regulated only on the domestic level[34]. To be honest, one must admit that supervising a technological tool or weapon is uniquely complex – given the intangible nature of the products, and the ability to easily transfer them across borders. Also, unlike a physical weapon that can only be located in one place at the same time, a software can be located in numerous locations simultaneously, making containment especially complicated. Codes can also lead to derivative malwares, as we saw after the use of Stuxnet (Duqo, Flame, Havex against US and Canada, Industroyer in Ukraine, Triton in the Middle East)[35].

As a result of these challenges, offensive cyber companies can and do settle where the regulation is relatively weak[36], and provides them with a wide leeway to operate in, as NSOs' former CEO, Shalev Hulio, testified[37]. Indeed, it is a challenge to supervise NSO by a

---

[32] N. BHUTA, *The Role International Actors other than States can Play in the New World Order*, in A. CASSESE (ed.), *Realizing Utopia: The Future of International Law*, 2012, 70.

[33] S. ZAPPALÀ, *Can Legality Trump Effectiveness in Today's International Law*?, in A. CASSESE (ed.), *Realizing Utopia: The Future of International Law*, 2012, 106.

[34] E. MULBRY, *Arms Control 2.0: Updating the Cyberweapon Arms Control Framework*, Michigan Technology Law Review, 28, 2021, 175, 183-186; to a specific reference to Pegasus see R. KLEIN, *Trimming Pegasus' Wings International Export Control Law and 'Cyberweapons'*, in *Voelkerrechtsblog*, October 27, 2021.

[35] FREI, *supra* note 8, 7. "Duqu" is a cyber espionage malware, and "Flame" is another information collecting platform, that enables espionage via saving screen shots, browsing through storage devices or switching on the microphone and the camera. For discussion see B. BENCSÁTH, G. PÉK, L. BUTTYÁN, M. FÉLEGYHÁZI, *The Cousins of Stuxnet: Duqu, Flame, and Gauss*, in *Future Internet*, 4(4), 2012, 971, 980.

[36] S. D. KASTER, P. C. ENSIGN, *Privatized espionage: NSO Group Technologies and its Pegasus spyware*, in *Thunderbird International Business Review*, 1, 2022, 3-4 (hereinafter: Kaster, Ensign)

[37] P. H. O'NEILL, *The Man who Built a Spyware Empire Says it's Time to Come out of the Shadows*, *MIT Technology Review*, 19.8.2020, https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/.

domestic regime, since the company is subject to different export regimes in Bulgaria, Cyprus and Israel.

To delve into Israeli regulatory practices, we will delineate the licensing procedure. To obtain marking license applicants must specify the purpose of the license (e.g., future sale, presentation, knowledge exchange, or cooperative development), the end-user's country of origin, and furnish relevant details about the end-user[38]. These are followed with a cover letter explaining the circumstances and facts of the deal and the personnel involved in trade.

Later, a vetting process will proceed, which includes a questionnaire that encompasses information on the cooperate governance/ownership of the user, any sanctions imposed by the United States or Israel, that nature of business activities, and its past doings with to enemy states[39]. The level of accuracy required in an exportation license is greater than that required at the marketing stage. For example, it necessitating precise identification of end-user (to the level of different military units)[40], a more comprehensive cover letter, and an extended vetting process[41]. We advocate for maintaining a high threshold early in the process, to set a clear standard to the industry and also to safeguard investors from sunk costs (in the design of the technology, and also in the marketing efforts).

Returning to the licensing process, DECA will then evaluate several stipulations as past behavior of the applicant, technical rules, type of equipment provided, defense know-how and considerations regarding the end-user or the end-use[42]. These do not explicitly include human rights considerations and international law obligations[43]. This legal situation has led to many cases when DECA

---

[38] Application to gain marketing license 2.01 (16.10.2018) https://exportctrl.mod.gov.il/Documents/%D7%98%D7%A4%D7%A1%D7%99%D7%9D/%D7%A8%D7%99%D7%A9%D7%99%D7%95%D7%A0%D7%95%D7%AA%20%D7%A9%D7%99%D7%95%D7%95%D7%A7/api_2.01.pdf.

[39] Basic Questionnaire for Foreign Company Vetting 2.06 (21.06.21) can be found in https://exportctrl.mod.gov.il/About/Pages/Froms.aspx.

[40] Explanation to form 3.01 a request to military export license p.2 (25.7.2018) https://exportctrl.mod.gov.il/Documents/%D7%98%D7%A4%D7%A1%D7%99%D7%9D/%D7%A8%D7%99%D7%A9%D7%99%D7%95%D7%A0%D7%95%D7%AA%20%D7%99%D7%A6%D7%95%D7%90/api_3.01a.pdf.

[41] Extended Questionnaire for Foreign Company Vetting 21.06.21 can be found in https://exportctrl.mod.gov.il/About/Pages/Froms.aspx.

[42] §8 Defense Export Control Law.

[43] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression *Surveillance and human rights* A/HRC/41/35, ¶34 (28.5.2019). (hereinafter: Surveillance and human rights)

approved export to authoritarian regimes, such as Myanmar[44] and Russia[45].

Due to the *need* for approval and the detailed information granted to the State, the question of responsibility arises – whether direct or indirect, when an approved technology for sale, like Pegasus, infringes upon human rights. Article 16 of the Draft Articles on Responsibility of States for Internationally Wrongful Acts allows to attribute responsibility on a wrongful act, based on assistance and knowledge of the circumstances[46]. The threshold of knowledge is relatively high, and requires practical certainty regarding the commission of a wrongdoing[47]. It is not clear if Israel can become jointly responsible to human rights violations simply due to authorizing the marketing and sale of the surveillance[48].

The Israeli High Court of Justice (HCJ) has the authority to perform judicial review on the actions of DECA, as an administrative entity. To this day, the HCJ has consistently rejected petitions challenging the legality of licensing due to the wide discretion (or, margin of appreciation) conferred to DECA[49]. Since the HCJ immediately dismisses such petitions, there is little transparency on the different considerations DECA take in to account *de facto*, when making a decision. In one dismissal of a petition regarding NSO, the

---

[44] The economic interests of the Myanmar military: Independent International Fact-Finding Mission on Myanmar A/HRC/42/CRP,¶154-174, September 12, 2019; N. LANDAU, *Israel Denies Arming Myanmar. But Its Officials Are Still Visiting a Tel Aviv Arms Expo*, in *Haaretz*, 4.6.2019, https://www.haaretz.com/israel-news/2019-06-04/ty-article/.premium/israel-denies-selling-weapons-to-myanmar-but-reps-are-still-at-tel-aviv-arms-expo/0000017f-f56b-d5bd-a17f-f77b735c0000;

[45] H. RAVET, *Rights activists petition court to block export of Cellebrite spy tools to Putin's investigative committee*, in *Calcalistech,* 14.9.2020, https://www.calcalistech.com/ctech/articles/0,7340,L-3851242,00.html; O. YARON, *Russia Still Using Israeli Tech to Hack Detainees' Cellphones*, in *Haaretz*, 21.10.2022, https://www.haaretz.com/israel-news/security-aviation/2022-10-21/ty-article/.premium/russia-still-using-israeli-tech-to-hack-detainees-cellphones/00000183-eb6c-d15c-a5eb-ff6cf86e0000.

[46] § 16 Draft Articles on Responsibility of States for Internationally Wrongful Acts, ILC, 56 U.N. GAOR Supp. No. 10, U.N. Doc. A/56/10 (2001).

[47] M. MILANOVIC, *Intelligence Sharing in Multinational Military Operations and Complicity under International Law*, in *International Law Studies*, 97, 2021, 1269, 1322, 1349-1350.

[48] See Lubin, 2023, supra note 31, 17-19.

[49] See HCJ 1942/21 *Agmon v. CEO of Ministry of defense* para.7 (2021); O. YARON, *The State's Right': Top Court Refuses to Rule on Israeli Sale of Spy Tech to Russia*, in *Haaretz*, https://www.haaretz.com/israel-news/tech-news/2021-06-28/ty-article/.premium/top-court-refuses-to-rule-on-israeli-sale-of-spy-tech-to-russia/0000017f-e568-d97e-a37f-f76dc4350000.

administrative court has (exceptionally) noted that DECA discovers "high sensitivity to human rights", but this is quite a rare statement[50].

The Israeli Parliament Security and Foreign Affairs committee has oversight powers on DECA[51]. Traditionally, the discourse in the committee is rather very general and procedural[52], and many inquiries by members of the committee are not addressed by DECA, due to confidentiality. Recently, though, the tide seems to turn and the need for a greater monitoring power was expressed by the committee[53]. Following many incidents where exports were approved by DECA in the past[54], several parliament members drafted suggested bills to include compliance with international law, and violations of human rights by the end-user, in order to prevent cooperation with violations of international law[55]. And still, these bills were not yet adopted by the Parliament.

2.3. *Israel's Perspective on the Application of International Law in Cyberspace.* Israel has expressed its positions as a member of the fifth United Nations (UN) Group of Government Experts (GGE)[56]. In

[50] AdminC (TA) 28312-05-19 *Malkar v. head of DECA* (12.7.2020).

[51] See articles for oversighting powers regarding regulations under the law§ 45-47 Defense Export Control Law.

[52] Protocol num.161 of the security and foreign affairs committee of the 20th Knesset (10.5.2017); Knesset news, *Foreign Affairs and Defense Committee Chair MK Ben Barak: There has to be closer supervision of defense exports*, KNESSET (14.6.2022) https://main.knesset.gov.il/en/news/pressreleases/pages/press14622v.aspx.

[53] Protocol num.116 of the security and foreign affairs committee of the 24th Knesset, p.32 (13.5.2022).

[54] For historical overview on military export and authoritarian regimes See B. BAHBAH, *Israel's Military Relationship with Ecuador and Argentina*, in *Journal of Palestine Studies*, Vol. 15 (2), 1986, 76; for a more contemporary look, see E. KONRAD, *The story behind Israel's shady military exports*, +972 *Magazine*, 22.11.2015. https://www.972mag.com/who-will-stop-the-flow-of-israeli-arms-to-dictatorships/. It should be mentioned that the discourse in the Knesset revolves between the two, though DECA in relatively new, founded in 2007.

[55] B. RAVID, *Israeli Foreign Ministry Opposes Restrictions on Arms Sales to Human Rights Violators*, in *Haaretz*, 22.11.2015 https://www.haaretz.com/israel-news/2015-11-22/ty-article/.premium/bid-to-restrict-arms-sales-to-rights-violators-meets-opposition/0000017f-e3df-d568-ad7f-f3ff513f0000`; J. LIS, *Israeli Lawmakers Unite to Fight Arms Exports to Countries That Violate Human Rights*, in *Haaretz*, 10.7.2016 https://www.haaretz.com/israel-news/2016-07-10/ty-article/.premium/ministers-to-discuss-bill-limiting-israeli-arms-export/0000017f-db2f-df9c-a17f-ff3f7ece0000.

[56] Israel National Cyber Directorate, *Israel International Cyber Strategy International Engagement for Global Resilience*, 2021, 26. See UN General Assembly Res. 73/266, 22.12.2018, available at: https://undocs.org/en/A/RES/73/266; Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report, 10.3.2021, available at https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

addition, it has further detailed its perspective regarding the application of international law to cyberspace in a declaration delivered by its former Israel Deputy Attorney General, Roy Schöndorf[57].

As noted above, one of Israel's goals is to position itself as a leader in the international discourse[58]. Israel approach on the application of international law in cyberspace was viewed as cautious and conservative in its approach[59]. As noted by Schöndorf, this approach was chosen due to the rapid changes in the technological field, and the need for international law to react in appropriate and prudent manner[60]. Generally speaking, the notion presented is that though international law generally applies to cyberspace, the cyber domain is unique and it requires as such tailored-made rules. As noted by Akande, this assertion, *de facto*, narrows international laws' scope of application[61].

2.3.1. *The New Battlefield - Use of Force and International Humanitarian Law.* Article 2(4) of the UN Charter articulates the prohibition against the use of force[62]. Schöndorf presented the notion that the prohibition applies in the cyber domain only when the operations is expected to cause physical damage, including injury or death[63]. Hence, this is yet another reaffirmation of the effects-based approach[64]. According to this approach, use of force must include a

---

[57] R. SCHONDORF, *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, in EJIL TALK!, December 9, 2020, available at https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

[58] Government Resolution No. 2443 (Advancing National Regulation and Governmental Leadership in Cyber Security, 15.2.2015).

[59] M. SCHMITT, *Israel's Cautious Perspective on International Law in Cyberspace: Part I (Methodology and General International Law)*, in EJIL TALK!, December 17, 2020, available at https://www.ejiltalk.org/israels-cautious-perspective-on-international-law-in-cyberspace-part-i-methodology-and-general-international-law/ (hereinafter: Schmitt); D. AKANDE, A. COCO, T. DE SOUZA DIAS, *Old Habits Die Hard: Applying Existing International Law in Cyberspace and Beyond*, in EJIL TALK!, January 5, 2021) available at https://www.ejiltalk.org/old-habits-die-hard-applying-existing-international-law-in-cyberspace-and-beyond/ (hereinafter: Akande).

[60] Israeli Perspective, *supra* note 3.

[61] Akande see *supra* note 59.

[62] United Nations Charter, 24 October 1945, 1 UNTS XVI (hereinafter: UN charter); CH. GRAY, *The use of force and the international legal order*, in International Law, 2010, 617.

[63] Israeli Perspective, *supra* note 3.

[64] See D. E. GRAHAM, *Cyber Threats and the Law of War*, in *Journal of National Security Law and Policy*, 4, 2010, 87, 91. There are two more approaches: The instrument-based

significant physical damage[65], which can be assed using criteria as the degree of the physical destruction, invasiveness and measurability of the harm[66].

Schöndorf reiterated that states have the right to self-defense, under Article 51 of the UN Charter[67], against the use of force that amounts to an armed attack, against both a state or non-State actor, both in the kinetic or cybernetic spheres. In addition, Schöndorf clarified that International Humanitarian Law (IHL) applies to cyber operations during armed conflicts[68]. For example, a cyber-operation can constitute an attack when it is expected to cause physical damage[69]. By this interpretation, the loss of functionality to infrastructure is insufficient, while emphasizing that data cannot constitute objects, and as a result to possess a military or civilian nature. While these issues are not completely settled in international law[70], Schmitt noted that the interpretation is reasonable and mirrored by the views of other States[71].

2.3.2. *Sovereignty and the Rule of Non-Intervention.* Schöndorf differentiates between the political concept of sovereignty, associated

---

approach categorizes an act as an armed attack only if it will bare characteristics traditionally associated with military force. It was perceived as outmoded. See: D. B. HOLLIS, *Why States Need an International Law for Information Operations*, in *Lewis & Clark Law Review*, 11, 2007, 1023, 1041. The target-based approach classifies a cyber-attack against critical computer system as an armed attack regardless physical destruction or casualties. The problem with this approach is that it might increase the risk of a conventional military operation following a cyber-attack, even without physical damage. See SH. LI, *When Does Internet Denial Trigger the Right of Armed Self-Defense?*, in *Yale Journal of International Law*, 38, 2013, 179, 186.

[65] M. ROSCINI, *Cyber Operations and the Use of Force in International Law*, 2014, 54.

[66] See *Tallinn Manual on The International Law Applicable to Cyber Warfare*, M. N. SCHMITT ed., 2013, 46.

[67] § 51, UN Charter, see *supra* note 62.

[68] For discussion concerning IHL in the cyber-sphere, see N. LUBELL, *Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply?*, in *International Law Studies*, 89, 2013, 252.

[69] Israeli Perspective, *supra* note 3.

[70] *See*: SC Res. 1368 (12 September 2001); SC Res. 1373 (28 September 2001); SC Res. 1530 (11 March 2004); Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, 2004 ICJ 136, 139; CH. GRAY, *International Law and The Use of Force*, Oxford, 2008, 135–138.

[71] Schmitt, *supra* note 59. *See*, e.g.: J. WRIGHT, Attorney General, United Kingdom, *Cyber and International Law in the 21st Century*, Gov.UK, May 23, 2018), <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>, visited on January 26, 2022.

with autonomy, and the legal rule of territorial sovereignty[72]. The declaration relates to the debate surrounding the question whether sovereignty is a principle or a primary rule of international law, while not taking an unequivocal stance[73]. This is since Schöndorf clarified that it is unclear if transit through networks located in other States amounts to violations of their sovereignty. In other words, the primary rule is territorial sovereignty, and the principle of sovereignty merely functions as the protected interest violated, as a result of the primary rule[74].

As for the customary rule of non-intervention, it derives from the rule of sovereignty and is found in Article 2(7) of the UN Charter[75]. The Israeli declaration recognizes the high threshold needed[76], since intervention entails coercive interference by a State in the internal affairs of other States[77]. An intervention would be illegal if two criteria are required: 1) Intervention with matters which a State is free to decide on its own[78]; 2) Intervention that involves coercion[79]. Whilst cyber operations can meet the first condition[80], they could rarely the second one[81]. It should be noted, though, that the position that intervention with national elections can meet this threshold[82]. Spywares, however, can be a game changer in this regard in the future.

---

[72] Israeli Perspective, *supra* note 3.

[73] Currently, only the United Kingdom asserts that sovereignty is merely a principle and not a primary rule of international law.

[74] H. LAHMANN, *On the politics and ideologies of the sovereignty discourse in cyberspace*, in *Duke Journal of Comparative and International Law*, 32, 2022, 61, 89-97.

[75] United Nations Charter, 24 October 1945, 1 UNTS XVI, Art 2, ¶7; M. N. SCHMITT, A. E. WALL, *The International Law of Unconventional Statecraft*, in *Harvard National Security Journal*, 2014, 5, 349, 355.

[76] Israeli Perspective, *supra* note X.

[77] PH. KUNIG, *Intervention, Prohibition of*, in *The Max Planck Encyclopedia of Public International Law*, 1, ¶4, *at* https://opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e1434?prd=EPIL.

[78] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. U.S.), Merits, 1986 ICJ Rep. 14 (June 27), at ¶205.

[79] Other parallel terms to coercive are forcible or dictatorial. *See*: *Oppenheim's International Law*, R. JENNINGS, A. WATTS (eds.), 9th ed., 1992, 43.

[80] TH. MOULIN, *Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward*, in *Journal of Conflict and Security Law*, 25, 2020, 423, 430.

[81] R. CROOTOF, *International Cybertorts: Expanding State Accountability in Cyberspace*, in *Cornell Law Review*, 103, 2018, 565, 623.

[82] Israeli Perspective, *supra* note 3.

2.3.3. *The Principle of Due-Diligence.* Due-diligence (DD) is a well-grounded rule under international law, as well as its application to a wide variety of international law branches[83]. DD requires a State to take possible measures to safeguard against misusing its territory to commit violations of international law[84]. Its application is wide, and its status is longstanding[85]. A failure to meet the principle might give rise to a violation of international law.

Schöndorf asserted that principle of DD is "voluntary, non-binding norm of responsible State behavior"[86] in the cyber context. This assertion is rooted in the 2015 GGE report[87]. This position was criticized as demoting to the status of DD, though a well-established rule of international law[88]. Therefore, some States suggested this notion is complementary, and not an alternative to existing norms[89].

The view of Israel is, to say the least, surprising. Since new technologies are subject to already existing norms of international law, DD obligations are applicable not only on a voluntary basis[90]. This principle has been recognized as applicable in cyberspace by Brazil[91], Finland[92] and France[93], and also Iran[94]. In the Tallinn Manual, DD was interpreted as not allowing the exercise of cyber operations

---

[83] Human Rights Committee, General Comment No. 31, U.N. Doc. CCPR/C/21/Rev.1/Add.13, 8 (May 26, 2004) (hereinafter: GC 31).

[84] Corfu Channel (*U.K.* v. *Alb.*), Judgment, 1949 ICJ Rep. 4, 18, 22 (9 April).

[85] For early discussion of this principle, *see* The Alabama Claims of the United States of America against Great Britain (*US* v. *UK*), 29 R.I.A.A. 125, 131 (1871). For a more recent application of the principle, see Human Rights Committee, General Comment No. 31, U.N. Doc. CCPR/C/21/Rev.1/Add.13, ¶ 8 (26 May 2004).

[86] Israeli Perspective, *supra* note 3.

[87] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/70/174 §13(c) (22 July 2015) (hereinafter: GGE 2015).

[88] Akande see *supra* note 59.

[89] For example, the UKs' position towards this section that DD is an obligation. See *Non-Paper on Efforts to Implement Norms of Responsible State Behaviour in Cyberspace, as Agreed in UN Group of Government Expert Reports of 2010, 2013 and 2015* (foreign and commonwealth office), 2019, 11.

[90] *Tallinn Manual 2.0*, *supra* note 66.

[91] Schmitt, *supra* note 59.

[92] Finland's Position, *supra* note 51.

[93] Ministre des Armées, *supra* note 42, 6 ("Conformément à l'obligation de diligence requise13, elle veille à ce que son territoire ne soit pas utilisé pour commettre des faits internationalement illicites à l'aide des TIC").

[94] Open-ended working group on developments in the field of information and telecommunications in the context of international security, Final Substantive Report (10 March 2021), <https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf>, visited on January 26, 2022.

addressed against another State's rights, and producing serious adverse consequences to it from their territory[95].

In the following parts, we will delve into the case study – the Pegasus and Saifan scandals. Then, we will evaluate the role and capacity of international law to cope with the development, marketing, sale and deployment of spywares, while returning to the Israeli perspective on these legal issues.

3. *Offensive Cyber Technologies (Spywares): NSO as a Case Study.* 3.1. *The NSO Scandal and International Responses.* NSO is a cyber-offensive intelligence company, founded by Niv Karmi, Omri Lavie, and Shalev Hulio in 2010[96], that is best known for its Pegasus spyware. The story of NSO, in fact, exemplifies two of the main reasons for Israel's technological state of mind, which helped it to become a tech power house: *first*, Israel insists on exposing children from an early age to the opportunities and possibilities enabled by technology; and, *second*, the Israel Defense Forces absorbs tech-driven youth to strong cyber units, and provides with the opportunity to learn cutting edge skills. These two factors, in turn, incentivize young people in Israel to seek a future in the luxurious hi-tech industry.

How then should one frame the discussion, when discussing spyware and international law? In the view of Frank La Rue, the Special Rapporteur on the right to freedom of expression, spywares form part of the world of "communications surveillance" – which encapsulates a wide range of actions, such as monitoring, collecting, obtaining, analyzing, using, preserving, and retaining information about a person's communications[97]. Pegasus is one of the first known spywares, and it allows its operator to place surveillance of smartphones remotely, by zero-click technology[98], enabling a

[95] *Tallinn Manual 2.0*, *supra* note 66, 31.

[96] G. COPPOLA, *Israeli Entrepreneurs Play Both Sides of the Cyber Wars*, in *Bloomberg News*, September 29, 2014 https://www.bloomberg.com/news/articles/2014-09-29/israeli-entrepreneurs-play-both-sides-of-the-cyber-wars.

[97] F. LA RUE, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/23/40, (17.4.2013), ¶6. (hereinafter: La Rue)

[98] See for additional technical explanations on the system, AMNESTY INT'L, *Forensic Methodology Report: How to Catch NSO Group's Pegasus*, 2021. https://www.amnesty.org/en/documents/doc10/4487/2021/en/.

complete access to the targeted device[99]. This, no doubt, amounts to "communication surveillance". The same can be said about Saifan, as we will show below.

In technical terms, Pegasus monitors all the applications in the phone, collects passwords, contact and files in the phone, and it also provides the option to turn on microphone and listen to the surrounding sounds of the target (hence, real-time data collection)[100]. NSO asserts that the operator of Pegasus can surveil while switching virtual identities[101]. In order to assure anonymity and prevent tracing back, Pegasus also uses anonymizing transmission network[102].

These features make the product much more effective than the traditional surveillance methods, like wiretapping[103], positioning Pegasus as an attractive tool to many security and intelligence agencies. Per the last transparency report of the company, it has 60 customers from 40 countries, varying from intelligence agencies to law enforcement agencies to militaries[104].

Pegasus was successful in locating weaknesses and flaws in Apple's iOS system, Whatsapp, and other apps. These abilities did not go unnoticed by big-tech companies, and Whatsapp alleged that NSO, in more than 1,400 cases, have hacked the platform by sending malicious code, designed to exploit a flaw[105], that could be delivered even as a missed phone call[106]. Then, NSO allegedly reverse engineered, and used the apps contrary to the terms of use, in order to trespass it[107]. Given that, Whatsapp sued NSO before the United States courts, in a claim of a fraud and illegal access to computers

---

[99] O. MARZOCCHI, M. MAZZINI, *Pegasus and surveillance spyware*, 2022, 22 (hereinafter: Marzocchi, Mazzini).

[100] NSO Pegasus, "Pegasus – Product Description", 19-20. https://www.documentcloud.org/documents/4599753-NSO-Pegasus.html.

[101] *Ibid.*, 9, 26-27.

[102] *Ibid.*, 23.

[103] G. SARTOR, A. LORGGIA, *The impact of Pegasus on fundamental rights and democratic processes*, 2023, 21 (hereinafter: Sartor, Lorggia).

[104] *Transparency and Responsibility Report 2021 (NSO group)*, 2021, 6 (hereinafter: NSO transparency).

[105] For a technical explanation see PAWAN KUMAR PATIDAR ET AL. *A Threat modeling approach to analyze and mitigate WhatsApp attacks: A Review*, IEEE INTERNATIONAL STUDENTS' CONFERENCE ON ELECTRICAL, ELECTRONICS AND COMPUTER SCIENCE, 2023.

[106] *The NSO WhatsApp Vulnerability -This is How It Happened*, CHECK POINT RES. (13.5. 2019) https://research.checkpoint.com/2019/the-nso-whatsappvulnerability-this-is-how-it-happened/.

[107] *WhatsApp v. NSO Group, et. al*, No. 4:19-cv-7123 ¶1-78 (N.D. Cal. Oct. 29, 2019) https://files.lbr.cloud/316009/whatsapp-fb-v-NSO-group.pdf

without authorization[108]. Similarly, Apple sued NSO and emphasized the breach of contract and terms of service in numerous Apple products, in addition to claims over the loss of business revenues caused by the hacks[109].

While the mission statement of NSO is to "help governments protect innocents from terror and crime by providing them with the best intelligence technology of its kind"[110], many reports and evidence were shown that the system is used in order to persecute human rights activists and journalists around the world[111]. One of the most notorious examples is the assassination of the Saudi journalist Jamal Khashoggi, which entered the embassy of the Kingdom of Saudi Arabia in Turkey, where he was cruelly assassinated[112].

According to the report of the Special Rapporteur on the extrajudicial, summary, or arbitrary executions[113], and the American Office of the Director of national intelligence[114], Pegasus spyware was used against Khashoggi and his closest circle[115], and that he was targeted for political reasons and criticisms he made against the Saudi regime. In the report, some of the technical abilities of Pegasus were reaffirmed, such as the ability to use the phone's microphone and camera.

---

[108] For a fuller analysis see J. W. PENNEY, B. SCHNEIER, *Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group*, in *Berkeley Technology Law Journal*, 36, 2021, 469. NSO claimed it had immunity since it was hired by foreign governments, an argument that has been rejected twice. See: W. S. DODGE, *NSO v. WhatsApp: Should the Solicitor General Recommend Allowing Foreign Corporations to Claim Immunity?* In *Just Security*, 9.6.2022 https://www.justsecurity.org/81843/nso-v-whatsapp-should-the-solicitor-general-recommend-allowing-foreign-corporations-to-claim-immunity/.

[109] *Apple Inc. v. NSO Group Technologies Limited* No. 3:21-cv-09078 (N.D. Cal. 23.11.2021) https://www.courtlistener.com/docket/61570971/apple-inc-v-nso-group-technologies-limited.

[110] NSO transparency, see supra note 104, 5.

[111] B. MARCZAK ET AL., *Hide and Seek Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries*, 2018.

[112] *Investigation of accountability for and prevention of intentional State killings of human rights defenders, journalists and prominent dissidents* (Special Rapporteur on extrajudicial, summary or arbitrary executions), A/HRC/41/36, 2019, 7.

[113] And see Annex to the Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions: Investigation into the unlawful death of Mr. Jamal Khashoggi A/HRC/41/CRP.1 para. 68-97(2019).

[114] ASSESSING THE SAUDI GOVERNMENT'S ROLE IN THE KILLING OF JAMAL KHASHOGGI (office of the director of national intelligence), 2021.

[115] B. MARCZAK ET AL., *The Kingdom Came to Canada How Saudi-Linked Digital Espionage Reached Canadian Soil*, 2018.

The Khashoggi controversy led to the filing of a lawsuit against the NSO Group in Israel[116], but as of today the company denies any connection to it[117]. Additional cases arise on daily basis regarding the usage of the system, joining the numerous already documented[118], including the many high-profile figures in countries such as France, Spain, and Germany, the United Kingdom and the United States[119]. The revelations led to numerous reactions internationally as well. In the United States, NSO group was included in to the "blacklist" of the American Ministry of Commerce[120], and a new executive order was adopted by President Biden on the Prohibition on Use by the United States Government of Commercial Spyware[121].

In the European Union, a special commission of inquiry, PEGA, was founded writing several critical reports to the European Parliament[122], in addition to reports to the European Council[123], as well as other domestic procedures[124]. According to those reports

[116] D. D. KIRKPATRICK, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, in *New York Times*, December 2, 2018, https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html.

[117] TOI staff, *NSO founder denies its phone hacking software was used to track Khashoggi*, in *The Times of Israel*, 12.1.2019, https://www.timesofisrael.com/nso-founder-denies-its-cellphone-hacking-software-used-to-track-khashoggi/.

[118] O. BENJAKOB ,*The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware*, in *Haaretz*, 5.4.2022 https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000.

[119] Marzocchi, Mazzini, see *supra* note 99, 7-13.

[120] RIN 0694-AI64 Docket No. 211019-0210 (4.1.2021), https://www.federalregister.gov/documents/2021/11/04/2021-24123/addition-of-certain-entities-to-the-entity-list

[121] Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security (march 27, 2023) https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/. §2(a)(ii)(A)(1) The Executive Order prohibits the uses of Commercial Spyware by departments and agencies when it is "to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb dissent or political opposition; otherwise limit freedoms of expression, peaceful assembly, or association; or enable other forms of human rights abuses or suppression of civil liberties"

[122] SOPHIE IN 'T VELD, *Draft Report Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance* spyware, 2022, 8-26 (hereinafter:Veld) https://media.euobserver.com/281e6fa170b4673bc87da11181f30041.pdf; Sartor, Lorggia, see *supra* note 103, 31.

[123] T. KALADANI, Z. PROKOPETS, *Pegasus Spyware and Its Impact on Human Rights*, 2022. 9-19.

[124] See Reporting team, *Demonstrations and inquiries: the global impact of the Pegasus project*, in *The Guardian*, 23.7.2021.

Pegasus interfered with many fundamental international human rights, such as the right to due process, the right to privacy, and freedom of speech[125], and undermined democratic values[126].

The ability of a private company to impact the relations of Israel with so many States, many of them considered allies, demonstrates the difficulty in regulating the production, sale and deployment of advanced technologies with over-reaching intelligence and security applications. As we will show in the next part, the spill-over of such technologies to the domestic level exacerbates the challenge and complicates it even more.

3.2. *NSO Scandal Inside Israel.* In a set of exposé articles published in Calcalist, a leading financial newspaper in Israel, it was revealed that Israeli Police is among the various users and operators of NSOs' products[127]. The discoveries presented a troubling use of surveillance and remote searches of cellphones, at times without any judicial warrant (or in excess to warrants that were granted)[128]. In later publications, it was argued that the Israeli police has used spywares in order to surveille against political activists[129], heads of local municipalities[130], officials in government ministries, and journalists. The system was even deployed against Israel's Prime Minister relatives[131], and witness at his criminal legal proceeding[132]. Not surprisingly, a public outcry soon came, surrounding highly sensitive issues in the political and public discourse in the Israeli society[133].

---

https://www.theguardian.com/news/2021/jul/23/demonstrations-and-inquiries-the-global-impact-of-the-pegasus-project.

[125] Veld, see supra note 122, 115-120.

[126] *Ibid.*, 7.

[127] T. GANON, *Israel police uses NSO's Pegasus to spy on citizens*, *Calcalist*, 18.1.2022, https://www.calcalistech.com/ctech/articles/0,7340,L-3927410,00.html.

[128] T. GANON, *Step-by-step: How Israel Police used NSO's Pegasus to spy on citizens*, *Calcalist*, 20.1.2022 https://www.calcalistech.com/ctech/articles/0,7340,L-3927615,00.html.

[129] T. GANON, *Israel Police used Pegasus to track activist's secret use of gay dating app, Calcalist*, 20.1.2022 https://www.calcalistech.com/ctech/articles/0,7340,L-3927606,00.html.

[130] T. GANON, *Israeli police used NSO's Pegasus to spy on local mayors, their relatives*, *Calcalist*, 23.1.2022 https://www.calcalistech.com/ctech/articles/0,7340,L-3927704,00.html.

[131] T. GANON, *No one was immune: Israel Police Pegasus surveillance list revealed*, *Calcalist*, 7.2.2022 https://www.calcalistech.com/ctech/articles/0,7340,L-3928830,00.html.

[132] P. BEAUMONT, *Israeli police 'may have hacked phone' of key witness in Netanyahu trial*, *The Guardian*, 3.2.2022 https://www.theguardian.com/world/2022/feb/03/israeli-police-may-have-hacked-phone-of-key-witness-in-netanyahu-trial-spyware.

[133] A. ATTALI, Y. KARNI, *Netanyahu compares alleged police use of NSO spyware to IDF bombing Israeli civilians*, *Ynet*, 7.2.2022 https://www.ynetnews.com/article/bj5dfk1jc.

Later, NSO admitted that it has sold the Israeli police a *specially tailored* version of Pegasus – Saifan. According to interviews with NSO officials, the system differs from Pegasus, as it can be used against Israeli devices (a capability which Pegasus cannot, allegedly)[134], and by lacking the ability to receive full access to past correspondence on the cellphone[135]. Up until today, many features of Saifan are still unknown.

The revealed Surveillance of Israeli citizens was severely criticized[136]. Commentators sparked a discussion on common practices by the Israeli police, the need for regulation of private spyware[137], the implication of cooperation between private tech sector and state[138], and the role of the judicial system for approving many of those practices at first place[139]. Following the political implications of the scandal, announcements on investigations were delivered shortly after[140], and the public pressure compelled the Israeli Police admit *some* misuses[141].

---

[134] A. ATTALI, Y. KARNI, *Netanyahu compares alleged police use of NSO spyware to IDF bombing Israeli civilians*, *Ynet*, 7.2.2022 https://www.ynetnews.com/article/bj5dfk1jc.

ttps://www.timesofisrael.com/nso-group-confirms-police-have-watered-down-version-of-pegasus-spyware/.

[135] D. WILLIAMS, *NSO says Israeli police got 'weaker' variant of Pegasus phone hacking tool*, Reuters, 29.3.2022 https://www.reuters.com/technology/nso-says-israeli-police-got-weaker-variant-pegasus-phone-hacking-tool-2022-03-29/.

[136] See for example, ACRI, *Stop the Use of Pegasus Spyware Against Civilians*, *Acri*, 19.1.2022 https://www.english.acri.org.il/post/__378; T. SHWARTZ ALTSHULER, *The NSO scandal should be an earthquake for the Israel Police*, *The Times of Israel*, 21.1.2022, https://blogs.timesofisrael.com/the-nso-scandal-should-be-an-earthquake-for-the-israel-police/.

[137] A. CAHANE, *Israeli Police: From Warrantless Cellphone Searches to Controversial Misuse of Spyware*, in *Lawfare*, 27.1.2022, https://www.lawfareblog.com/israeli-police-warrantless-cellphone-searches-controversial-misuse-spyware.

[138] For a proposed solution to found a commission to oversee online surveillance powers see T. SHWARTZ ALTSHULER, A. CAHANE, *NSO in Israel: Would You Let the Police Handle Uranium?* in Haaretz, 24.1.2022 https://www.haaretz.com/israel-news/tech-news/2022-01-24/ty-article/.premium/nso-in-israel-would-you-let-the-police-handle-uranium/0000017f-dc3b-df62-a9ff-dcff028d0000.

[139] N. LANDAU, *NSO Scandal Shows Israelis Are Fine With Human Rights Violations as Long as Judges Approve*, in *Haaretz*, 19.1.2022, https://www.haaretz.com/israel-news/2022-01-19/ty-article/.premium/nso-scandal-shows-israelis-are-fine-with-human-rights-violations-when-judges-okay-it/0000017f-ed51-d0f7-a9ff-efd5b7b60000.

[140] P. KINGSLEY, R. BERGMAN, *Israel to Investigate Domestic Use of Pegasus Spyware as Scrutiny Hits Home*, in *New York Times*, 7.2.2022 https://www.nytimes.com/2022/02/07/world/middleeast/israel-pegasus-spyware.html.

[141] Z. ZERAHIA, *Police confirm for the first time: There have been irregularities in the use of NSO software*, in *Calcalist*, 2.2.2022, https://www.calcalistech.com/ctech/articles/0,7340,L-3928468,00.html.

3.3. *The Merari Report.* As a result of public pressure, an official inquiry team was appointed by the Israel Attorney General to investigate the affair[142]. The inquiry team included three members, all of whom with an institutional background in the Israeli government – the serving Deputy Attorney General for Criminal Matters, Amit Merari, alongside two former officials in the Israel Security Agency (ISA) – Tsafrir Kats and Eyal Dagan.

The composition of the team was criticized since it was seen as biased, as all its members enjoyed the benefits of wiretapping in the past and are not impartial in their views on the matter[143]. The team's first action was to investigate whether the serious allegations presented in the "Pegasus surveillance list" are true. An interim report by the Merari team has contradicted those allegations, stating that there was no indication of surveillance without a judicial warrant, and added that some of the hacking attempts failed[144].

In its concluding and final Merari Report, the team used audit logs, with the assistance of NSO[145], in order to understand if the police used Saifan to conduct surveillance without a warrant. The scope of the investigation was from the purchase of the system spanned from 2015 to 2022, with a main focus to 2020-2021 (the time-frame mentioned in the exposé). The report concluded that all the records of the usages of Saifan were authorized (excluding four cases where the Israeli Police exceeded the permission granted in the warrant)[146].

Contrary to the publication stating that Saifan is limited to real-time surveillance only, the report showed that Saifan is capable of

---

[142] Y. VERTER, *The Curious Case of the Pegasus Commission of Inquiry*, in *Haaretz*, 11.2.2022, https://www.haaretz.com/israel-news/2022-02-11/ty-article/.highlight/the-curious-case-of-the-pegasus-commission-of-inquiry/0000017f-e715-df2c-a1ff-ff55ce140000.

[143] R. PELED, *Two Comments and Arguments After Reading the Merari Report*, ICON-S-IL BLOG (9.10.2022) (Hebrew) https://israeliconstitutionalism.wordpress.com/2022/10/09/%D7%A9%D7%AA%D7%99-%D7%94%D7%A2%D7%A8%D7%95%D7%AA-%D7%95%D7%A9%D7%AA%D7%99-%D7%98%D7%A2%D7%A0%D7%95%D7%AA-%D7%91%D7%A2%D7%A7%D7%91%D7%95%D7%AA-%D7%A7%D7%A8%D7%99%D7%90%D7%94-%D7%91%D7%93%D7%95%D7%97/.

[144] B. MCKERNAN, *Police use of Pegasus malware not illegal, Israeli inquiry finds*, *The Guardian*, 22.2.2022, https://www.theguardian.com/world/2022/feb/22/police-use-of-pegasus-malware-not-israeli-inquiry-finds.

[145] The Inquiry Team to Wiretapping Communications Between Computers, Final Report, 2022, 1 (Hebrew) (hereinafter: Merari Report).

[146] *Ibid.*, 4-5. See A. SHAPIRO, *Probe finds Israel Police did not unlawfully hack phones of politicians activists*, in *The Times of Israel*, 1.8.2022, https://www.timesofisrael.com/probe-finds-israel-police-did-not-unlawfully-hack-phones-of-politicians-activists/.

collecting data prior to the warrant, noting that the police indeed misused these functions[147]. Additionally, Saifan allows the aggregation of data other than communications (the subject of the warrant), such as calendar, contacts, and notes[148]. This data can be extremely valuable, and sensitive, since it can teach many features of a person: *e.g.* sexual orientation[149], religious beliefs, medical status (mental treatment or private doctors), and social circles[150]. This gap between the legal authorization and the technological capacities of Saifan was known to the police, that knowingly overlooked it[151].

As can be seen, even if Saifan is meant to a more modest version Pegasus, it is nevertheless a very competent tool with far-reaching capabilities, and as such a challenge for regulators and legislators – domestically and internationally. In fact, the Merari report alluded that the police may be using more privately developed offensive cyber technologies, but left the public without any concrete and clear understanding on the topic[152]. The report recommended the adaptation of legal rules, in order to gain closer oversight on surveillance. On the practical level, the team stressed the need for closer cooperation between legal advisers, specifically between the police and the Attorney general office[153].

This report seems to be very forgiving towards misuse of police powers[154], and some claimed that it might even provide the legal basis for deepening surveillance by law enforcement authorities[155].

---

[147] *Ibid.*, 5.

[148] *Ibid.*, p.6. Those were later criticized since they were lacking the needed specificity and were indicating the knowledge of the police of their overreaching powers, see 56.

[149] As argued by Calalist, Saifan was used the use sexual orientation as a leverage. For general discussion see A. E. WALDMAN, *Navigating Privacy on Gay-Oriented Mobile Dating Applications,* in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, J. BAILEY, A. FLYNN, N. HENRY (eds.), 2021, 369.

[150] This argument was raised to the Attorney General in a letter sent by ACRI regarding the usage of Saifan by the police that could be find here (in Hebrew) https://z.calcalist.co.il/assets/pickerul/4851e43d-fd2a-4547-b83b-d188c42efc16.pdf. For general discussion of the matter see K. DEGIRMENCI ET AL., *Mobile Applications and Access to Personal Information: A discussion of users' privacy concerns*, *Proceedings of the 34th International Conference on Information Systems*, 2013, 1, 5.

[151] Merari Report, see *supra* note 154, 55.

[152] *Ibid.*, 57.

[153] *Ibid.*, 67-68.

[154] O. KABIR, *The Marari report shows a severe violation of the privacy and rights of suspects*, *Calcalist*, 4.8.2022 https://www.calcalistech.com/ctechnews/article/b169fbyac,

[155] E. HABER, *The Law of the Trojan Horse*, *UC Davis Law Review*, 18 (*forthcoming*, 2024), available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4400283. Haber argues that is police hacking is prescribed by law, other security features will nullify.

Nevertheless, the recognition in the report that the police's used Saifan against Israelis, without legal authorization[156], contributed to further investigation of the matter – this time by the Israeli Parliament.

3.4. *Parliamentary Oversight.* The Saifan scandal reached the corridors of the Israeli Parliament, at the request of concerned Parliament members, and given the requirement of the police to report to parliament on the extent of wiretaps performed every year[157]. This requirement derives from the alarming number of wiretapping in Israel[158], and given the high rate of approval of this measure by the Israeli courts (more than 97% of the warrant requests are approved)[159]. All and all, we witnessed three rounds of discussions: 1) discussion prior to the establishment of the Merari team, soon after the breakout of the scandal; 2) discussion during the Merari team operated, and based on its interim reports; 3) discussion after the release of the Merari report.

Only a few days after *Calcalist's* exposé, regarding the police's usage of a spyware, a first discussion was held, in the Homeland Security Committee[160]. Senior police officers provided justifications and explanations on the wiretapping procedure, denying the allegations on over-reaching their powers[161]. This assertion was later debunked by the Merari report.

During the discussion in the Homeland Security Committee, various members of Parliament, in a cross-party consensus, raised concerns regarding the usage of law enforcement authorities with offensive cyber tools[162], and suggested the establishment of a commission of inquiry[163]. Others drew the connection between the

---

[156] Y. SHANY, *Stay Calm and Proceed With Caution: The Merari Report on Israeli Police's Pegasus Scandal*, in *Lawfare*, 25.8.2022, https://www.lawfareblog.com/stay-calm-and-proceed-caution-merari-report-israeli-polices-pegasus-scandal.

[157] § 4(e), 6(g) Wiretap Act – 1979.

[158] J. BREINER, *Amount of Israel Police Wiretaps More Than Doubled Over Last Decade*, in *Haaretz*, 3.6.2018, https://www.haaretz.com/israel-news/2018-06-03/ty-article/.premium/amount-of-israel-police-wiretaps-more-than-doubled-over-last-decade/0000017f-e816-dc7e-adff-f8bf85c40000.

[159] Z. HENNESSEY, *Israel's law enforcement uses spyware, AI to access private data – report*, in *The Jerusalem Post*, 17.1.2023, https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-728790.

[160] Protocol num.55 of the internal security committee of the 24th Knesset (24.1.2022)

[161] *Ibid.*, 35-42.

[162] *Ibid.*, 4-5, 16.

[163] Many have raised the criticism of the members of the Merari's team, in similar fashion as present, 17-18.

Israel Security Agency practices in the West Bank and the police, alongside the problems discussed above relating to Israel's arms export regime[164]. In the next chapter, we will discuss some of the technologies used in the West Bank, that indeed spill-over at times to domestic law enforcement operations.

A few months later, after the submission of the interim report, a session of the Constitutional Committee of the Israeli Parliament was devoted to the matter[165]. Again, cross-party consensus sounded criticisms, and doubt were raised relating to the capacity of the Merari team to investigate impartially, and regarding alleged warrantless uses of *other* spywares[166].

Another issue raised was the concern over the erosion of democratic values, given the infringement of privacy, and the misuse of public powers by the authorities[167]. The police senior officers repeatedly stated that: "The Israeli police do not spy on Israelis", only to be contradicted later down the road[168]. The Israeli Commissioner for Privacy noted, that the uses of spyware in Israel are under-regulated, and he suggested to appoint a Data Protection Officer to the Israeli police, that will integrate privacy concerns in the use of spyware[169].

The next step of parliamentary oversight, came after the conclusion of the Merari Report, and this time the Constitution Committee set to discuss the conclusions of the report[170]. In this round, the legal adviser of the police finally admitted to the use of spywares, and revealed the police used it in over than 1,000 incidents[171]. The legal adviser of the police also approved that they knew about the over-reaching uses of the system[172]. The author of the Merari Report, Amit Merari, was also present – and she argued that the widespread use of the spyware does not amount to infringement of

[164] *Ibid.*, 5, 8-9, 14.
[165] Protocol num.224 of the constitutional committee of the 24th Knesset (1.3.2022).
[166] *Ibid.*, 3-8.
[167] *Ibid.*, 16-17.
[168] *Ibid.*, 21-23.
[169] *Ibid.*, 38-40.
[170] Protocol num.47 of the constitutional committee of the 25th Knesset (13.3.2023). It should be noted that the authors were invited to present their opinion on the matter in this session.
[171] *Ibid.*, 16-17.
[172] *Ibid.*, 59-60.

the right to privacy (an assertion that was not accepted with great support, neither by the general public nor by experts in the field)[173].

After this session, it was evident that more investigation, and supervision, is due. Pursuantly, the Constitution committee decided to establish a sub-committee to supervise and promote the implementation of the conclusions of the Merari Report[174]. It was decided that the sub-committee will operate behind closed doors, in order to enjoy more significant access to confidential information regarding the use of spyware by the Israeli police. While the establishment of a sub-committee is a positive step forward, it is far from being enough.

First, transparency is crucial in order to improve the effectiveness of the process, to reconstruct the public's trust by clearing the cloud of uncertainty hovering around the scandal, and to debunk any conspiracies that can stem from a lack of understanding of the full facts of the incident. The need for public oversight was expressed by the former Special Rapporteur on the Right to Privacy, Joseph A. Cannataci, that stressed the need for safeguards such as public oversight, pre-Authorization authority, and inter-institutional whistle-blower mechanisms[175]. Similarly, the High Commissioner for Human Rights emphasized the importance of public oversight on surveillance as a preventive measure against the misuse of cyber offensive technologies[176], notions addressed in the General Assembly Resolution on the matter as well[177].

---

[173] *Ibid.*, 26.

[174] A. OBEL, *Israel Police use of NSO Spyware Set to be Probed by Knesset Subcommittee*, in *The Times of Israel*, April 23, 2023, available at https://www.timesofisrael.com/israel-police-use-of-nso-spyware-set-to-be-probed-by-knesset-subcommittee/. In addition, calls were made to form another commission of inquiry, one that is detached from the actual police work and utilization of Seifan (unlike the Merari team which was composed of persons with institutional affiliation to the Israeli police and government). See: Toi Staff, Knesset Passes Motion Urging Government to Probe Police Use of Spyware, TIMES OF ISRAEL (June 12, 2023), available at: https://www.timesofisrael.com/knesset-passes-motion-urging-government-to-probe-police-use-of-spyware/.

[175] J. A. CANNATACI, *Draft Legal Instrument on Government-led Surveillance and Privacy* §3(3) (10.1.2018) https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/DraftLegalInstrumentGovernmentLed.pdf (hereinafter: Draft Legal Instrument).

[176] The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37 (June 30, 2014).

[177] United Nations General Assembly, The right to privacy in the digital age, A/RES/73/179 (January 21, 2019).

Second, we believe that more institutional monitoring is due, especially in earlier stages of the development. Today, technologies with military application are only reviewed in Israel at the licensing for use, marketing and sale stage. The fact that the evaluation of risks occurs so late in the process, makes it harder to demand changes in the technology without economically crippling the project. As such, a preliminary and complementary stage of monitoring is required, at an earlier stage of the product's development. In the next part of this article, we will suggest such a monitoring body.

4. *Lessons Learned from the Use of Pegasus in the West Bank & Saifan in Israel, and a Look Ahead.* 4.1. *International Humanitarian Law* (*IHL) and International Human Rights Law (IHRL) – Pegasus in the West Bank.* The Israeli declaration on the application of international law to cyberspace did not touch upon the issue of applicability of International Human Right Law (IHRL) to cyberspace[178]. The Tallinn Manuel, by comparison, is of the position that IHRL applies in cyberspace and raises duties to respect and protect recognized human rights in the same fashion as in the kinetic world[179]. In addition, human rights bodies accepted the notion that existing human rights deserve equal protection online, in parallel to the effort of promoting newly tailored human rights specifically for cyberspace[180].

More broadly, there is a growing consensus within the international community on the issue of the co-application of IHL and IHRL[181]. One of the objectors of this trend is Israel, the discussion in this part will clarify some of the reasonings for that.

As for the way in which the two branches of law should be harmonized, the International Court of Justice considered IHL to be the *lex specialis* and as such enjoy interpretive precedence over

[178] Israeli Perspective, *supra* note 3.

[179] Tallinn Manual 2.0, *supra* note 66, rules 34-37.

[180] See D. DROR-SHPOLIANSKY, Y. SHANY, *It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights – A Proposed Typology*, European Journal of International Law, 32(4), 2021, 1249. UN GA Res. 71/199, 19 December 2016, para. 3; UN GA Res. 73/179, 17 December 2018, para. 3; HRC Res. 32/13, A/HRC/RES/32/13, 1 July 2016, at 3, para. 1; HRC Res. 38/7, A/HRC/RES/38/7, 5 July 2018, at 3, para. 1.

[181] for the roots and recent developments on the matter see Y. SHANY, *Co-application and harmonization of IHL and IHRL: are Rumors about the death of lex specialis premature?* in R. KOLB, G. GAGGIOLI, P. KILIBARDA (eds.), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, 2022, 9.

IHRL[182], this is not the case with respect to legal areas where IHRL contains more detailed norms or where IHL contains *lacunae*[183]. For example, the prohibition against torture, which constitutes a grave breach of the Geneva Conventions[184], should be interpreted during an armed conflict in light of the Convention against Torture[185], and the right to privacy, which is missing from IHL treaties[186], can be applied from IHRL, as long as it does not contradict applicable IHL norms.

In the latter context, it has also been claimed in the literature, though state practice does not appear to support this, that international law should adopt a *pro humanitas* presumption, favoring the most international standard protective most protective of human welfare[187].

---

[182] *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion,* [1996] I.C.J. 226, 25 ("…In principle, the right not arbitrarily to be deprived of one's life applies also in hostilities"). Other international institutions have supported the view that both regimes apply simultaneously, and enriched the discussion on this issue. The Human Rights Committee grants priority to the norm which benefits most the individual in the relevant context, differently from the *lex specialis* suggested by the ICJ. The European Court of Human Rights (ECHR) and the Inter-American Commission of Human Rights (IACHR) are also of a similar view to the one prescribed by the Human Rights Committee. See: Human Rights Committee, *General Comment No. 29: Article 4: Derogations during a State of Emergency*, CCPR/C/21/Rev.1/Add.11 (August 31, 2001); Human Rights Committee, *General comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life*, CCPR/C/GC/36 (October 30, 2018), 64 ("… both spheres of law are complementary, not mutually exclusive… practices inconsistent with international humanitarian law, entailing a risk to the lives of civilians and other persons protected by international humanitarian law… would also violate article 6 of the Covenant"); *Hassan v. the United Kingdom* [GC], no. 29750/09, (16 September 2014); *Isayeva v. Russia*, App. No. 57950/00 (February 24 2005), ¶176; IACmHR, Juan Carlos Abella (Tablada case), Case No. 11.137, 18 November 1997, Annual Report of the IACmHR 1997 (OEA/Ser.L/V/II.95 Doc. 7 rev) 271. For discussion by the African Commission of Human Rights, see: *Sudan Human Rights Organisation & Centre on Housing Rights and Evictions (COHRE) v. Sudan*, 27/5/09 (45th Ordinary Session).

[183] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion*,* [2004] I.C.J. 136, 106; M. KOSKENNIEMI (Chairman of ILC), *Fragmentation of International Law: Difficulties Arising from the Diversification and Expansion of International Law*, A/CN.4/L.682, April 13, 2006.

[184] Convention (III) relative to the Treatment of Prisoners of War, Geneva, 12 August 1949, 75 UNTS 135, art. 130; Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, Aug. 12, 1949, 75 U.N.T.S 287, art. 147.

[185] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 1984, A/39/51; N. S. RODLEY, *The Prohibition of Torture: Absolute Means Absolute*, *Denver Journal of International Law and Policy*, 34, 2006, 145.

[186] For discussion, see A. LUBIN, *The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, in R. KOLB, G. GAGGIOLI, P. KILIBARDA (eds.), *Research Handbook on Human Rights and Humanitarian Law: Further Reflections and Perspectives*, 2022, 462 ff.

[187] W. SCHABAS, *Lex Specialis? Belt and Suspenders? The Parallel Operation of Human Rights Law and the Law of Armed Conflict, and the Conundrum of Jus ad Bellum*, in Israel Law Review, 40, 2007, 592, 593.

Accepting such a presumption might have led to the application of the right to privacy even with respect to matters directly regulated by IHL.

In any case, the rights to privacy and freedom of expression are largely absent in IHL treaties[188], hence there is a need to resort to IHRL as a complementing tool[189], so long as it does not contradict relevant IHL norms[190]. The International Committee of the Red Cross (ICRC) is of the stance that though IHL does not prohibit surveillance, it exacerbates the vulnerabilities of individuals during armed conflicts and in cases of occupation (like the West Bank), recalling the prohibition on threats to violence aim to spread fear among the civilian population[191].

Another relevant source to the protection of privacy and freedom of expression can be found in Art.27 of the Fourth Geneva Convention, which is a core document when dealing with occupation[192]. This article prescribes respect for honor and family rights, and recognizes that they are well-enshrined in the notion of human dignity[193]. Per this day, this part of "conventional IHL" is general and lacks practical tools to handle privacy dilemmas[194]. Therefore, we refer in this article to obligations under the two

---

[188] A little attention is devoted to those manners, for example, article 76 of the Third Geneva Convention and Article 5 of the Fourth Geneva Convention regulated censorship and communication rights. For discussion, see A. LUBIN,cit. *supra* note 186, 463, 479-485.

[189] Another possible path derives from article 43 of the hauge regulations, stating that the occupier has to respect the laws prior to the occupation and thus privacy regimes can be sources in Jordanian law of the time see B. WATERS, *An International Right to Privacy: Israeli Intelligence Collection in the Occupied Palestinian Territories*, Georgetown Journal of International Law, 50, 2019, 573, 592–594.

[190] In the context if privacy see T. MIMRAN, Y. SHANY, *Integrating Privacy Concerns in the Development and Introduction of New Military or Dual-Use Technologies*, in *The Rights to Privacy and Data Protection in Times of Armed Conflict*, R. BUCHAN, A LUBIN (Eds.), 2022, 29 (hereinafter: Mimran and Shany).

[191] ICRC, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, 2019, 21 https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges report_EN.pdf?fbclid=IwAR3ksX7qBnQd61yJFgKqYlAhRKF3VPh9sFFhIZaQB2hNzxqAh ksEjJJ83HM.

[192] Lubin, see supra note 31, 485-486; §27Geneva Convention relative to the Protection of Civilian Persons in Time of War. Geneva, (1949).

[193] Human Rights Committee, General Comment 16, (Twenty-third session, 1988), Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies,§1 HRC/GEN/1/Rev.1 at 21 (1994) (hereinafter GC 16). See J. Q. WHITMAN, *Two Western Cultures of Privacy: Dignity Versus Liberty*, Yale Law Journal, 113, 2004, 1153, 1161.

[194] Omar Y. SHEHABI, *Emerging Technologies, Digital Privacy, and Data Protection in Military Occupation*, in *The Rights to Privacy and Data Protection in Times of Armed Conflict*, cit. supra note 190, 87.

branches of IHL and IHRL, in the context of the West Bank, but we will rely more significantly on IHRL due to its high level of detail.

Mass surveillance technologies are widely used by Israel in the West Bank, and two predominant examples of them are the AnyVision and Wolf systems[195]. The AnyVision system is a facial recognition technology used in checkpoints[196] that expedites the crossing process of Palestinians, used by more than 450,000 Palestinians[197]. As for the Wolf systems, it is a group of platforms operating in concert[198]: *Wolf Pack*, a database managed by the Civil Administration and shared with the Shin Bet; *Blue Wolf*, a network that allows for the gathering and sharing of information; *White Wolf,* which allows Security Coordinators in the settlements access to information relating to Palestinian workers; and *Red Wolf*, a system of cameras deployed at checkpoints which pulls data from and sends data back to the other systems.

These systems attracted international attention and criticism, and are regarded as digital, or automated, discriminating systems of control[199]. The challenge is, to balance between the legitimate need to safeguard human lives, and between Palestinians human rights. These systems differ, of course, from Pegasus in several aspects: the level of invasiveness, the 'voluntary' nature of AnyVision, and the knowledge regarding the monitoring process[200].

And yet, in order to deprive any remedy of IHL it has to be based that data has an object quality, and only then do the principles of distinction, proportionality, and precautions in attack come into

---

[195] Lubin, see supra note 31, 486-487.

[196] A. ZIV, *This Israeli Face-recognition Startup Is Secretly Tracking Palestinians*, in *Haaretz*, July 15, 2019, https://www.haaretz.com/israel-news/business/.premium-this-israeli-face-recognition-startup-is-secretly-tracking-palestinians-1.7500359.

[197] D. ESTRIN, *Face Recognition Lets Palestinians Cross Israeli Checkposts Fast, But Raises Concerns*, NPR, 29.8.2019, https://www.npr.org/2019/08/22/752765606/face-recognition-lets-palestinians-cross-israeli-checkposts-fast-but-raises-conc.

[198] E. DWOSKIN, *Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank*, Washington Post, 8.11.2021, https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html.

[199] AMNESTY INTERNATIONAL, *Israel and Occupied Palestinian Territories: Automated Apartheid: How facial recognition fragments, segregates and controls Palestinians in the OPT*, May 2, 2023.

[200] For the importance of knowledge of surveillance see Human Rights Committee, *Concluding observations on the sixth periodic report of Italy* CCPR/C/ITA/CO/6, ¶37 (1.5.2017) (hereinafter: periodic report of Italy).

play[201]. As presented above, the formal Israeli approach is that data is not an object, and cannot have a military or civilian nature. Therefore, under its paradigm IHL has little to contribute. While Israel opts for a stance which similar to the view presented in the Tallinn Manual[202], it contradicts States such as France, which accepts that civilian data constitutes a protected object[203]. From the IHRL perspective, General Comment 16 stresses that "Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant"[204].

AnyVision's former CEO has told in an interview that though most of the company's clientele are not from Israel, the West Bank was the "first territory where we validated our technology"[205]. This statement that echoes what many have already imagined: the West Bank is a "test-lab" to mass surveillance technologies, particularly ones developed in Israel[206].

In November 2021, a joint technical report of Citizen Lab, Amnesty International and Front Line Defenders was published - revealing that devices of six Palestinian human rights activists, some of them lawyers, were hacked with Pegasus. The time of interception of data varies from months to a year before the publication of the report[207], which was not able to attribute the hacking to a specific operator[208].

---

[201] Pomson, see *supra* note X, 5-7.

[202] Tallinn Manual 2.0, cit. *supra* note 66, 373. See also M. N. SCHMITT, *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive and Applicative Precision*, *Israel Law Review*, 48, 2015, 81, 93.

[203] Ministre des Armées, *supra* note 42, 16 ("la France considère que des données civiles de contenu peuvent être considérées comme des biens protégés" [France considers that civil content data can be considered as protected property]).

[204] GC 16 see *supra* note 193, 10.

[205] O. SOLON, *Why did Microsoft Fund an Israeli Firm that Surveils West Bank Palestinians?*, *NBC News*, 28.10.2019, available at https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116.

[206] C. DEMETROVICH, *The Oslo Accords: A Modern-Day Story of Occupation Told Through Violations of the Right to Freedom of Privacy*, in *Indiana Law Journal*, Vol. 98(1), 2022, 308, 325; M. FAFTA, D. SAMARO, *Exposed and Exploited: Data Protection in the Middle East and North Africa*, 2021, 28 (hereinafter: Fafta, Samaro).

[207] *OPT/Israel: Six Palestinian human rights defenders hacked with NSO Group's Pegasus Spyware,* Front Line Defenders, 2021 https://www.frontlinedefenders.org/sites/default/files/fld_pal_statement_-_final_-_5_nov_2021.pdf; Citizen Lab, *Devices of Palestinian Human Rights Defenders Hacked with*

Shortly after, the Palestinian Authority blamed Israel for the hack, linking it to the work these persons do with the International Criminal Court, in the context of the ongoing investigation against Israel and the Palestinian occupied Territories[209]. This link was made after the Israeli Defense Ministry announced Palestinian NGOs as terrorist organizations[210]. These occurrences ultimately led to the submission of a criminal complaint against NSO in France[211].

Various Israeli and Palestinian civil society organizations have responded to the revelation. In a letter to the Attorney General, The Association for civil rights in Israel ("ACRI") argued that the surveillance is illegal both from IHL and IHRL perspectives[212]. Concerning IHL, the authority to maintain security and public order is limited to proportionality and the upholding of human rights, which were breached if the usage of Pegasus provides its operator with private data without a military justification, which is particularly concerning when dealing with professions which enjoy confidentiality (like lawyers)[213].

A similar notion can be found in article 3 of the Draft Legal Instrument on Government-led Surveillance and Privacy made by the former Special Rapporteur on the right to privacy, stating that "The surveillance itself must be necessary and proportionate and the least intrusive means shall be used"[214]. Additional safeguards are needed, requiring oversight, a pre-authorization authority, inter-institutional whistle-blower mechanisms, and more. The document also stressed

---

NSO Group's Pegasus Spyware (8.11.2021) https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasusspyware/.

[208] S. KIRCHGAESSNER, M. SAFI, *Palestinian activists' mobile phones hacked using NSO spyware, says report* ,THE GUARDIAN, 8.11.2021 https://www.theguardian.com/world/2021/nov/08/palestinian-activists-mobile-phones-hacked-by-nso-says-report.

[209] P. KINGSLEY, R. SHEIKH AHMAD, *Palestinian Diplomats Targeted by Israeli Spyware, Official Says*, N.Y. TIMES, 11.11.2021, https://www.nytimes.com/2021/11/11/world/middleeast/israel-palestinian-nso-hacking.html.

[210] Kaster, Ensign see supra note 36, 360. For more critical approach see E. FAKHRO, T. BACONI, *A Shared Vision: Security Convergence between the Gulf and Israel* in Journal of Palestine Studies, Vol.51(3), 2022, 50.

[211] AFP, *Detained Palestinian lawyer sues Pegasus spyware maker NSO in France*, in *The Times of Israel*, 5.4.2022, https://www.timesofisrael.com/palestinian-lawyer-sues-pegasus-spyware-maker-nso-in-france/. The activist was later deported to France.

[212] R. PELLI, G. GAN-MOR, *Use of the NSO's Spyware Program Pegasus by the GSS*, ACRI, 14.11.2021, https://www.english.acri.org.il/post/__353 (hereinafter: Pelli and Gan-Mor).

[213] *Ibid.*, ¶5-10.

[214] Draft Legal Instrument.

the need for a strictly "defined specific and legitimate purposes and in response to a concrete and legitimate need"[215]. From this perspective, the use of Pegasus has to be limited to the least intrusive mechanism possible with a relatively narrow function, but this incident does not seem to meet this standard.

As per IHRL, ACRI argued that the use of Pegasus constitutes a breach of basic human rights, including the right to privacy and the freedom of expression, creating a chilling effect to human rights defenders[216]. The invasiveness[217] of Pegasus contains irrelevant information and lack of justification to interfere with the rights of third parties, including ones with special protections like journalists and diplomats[218]. An emphasis on this political chilling effect was also expressed in the latest Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967[219].

Similarly, the NGO Al-Haq sent an appeal to the United Nations Special Procedures branch of the Human Rights Council[220], emphasizing the obligation to ensure and respect the right to privacy[221] and the freedom of opinion[222]. The appeal also included

---

[215] *Ibid.*, §3(5)-3(9).

[216] Interestingly, the recognition of a right to activism is growing, for example under Article 7(c) to CEDAW. see *Rosanna Flamer-Caldera v Sri Lanka* [2022] United Nations Committee on the Elimination of Discrimination against Women (UN CEDAW Committee), Communication No. 134/2018 [Rosanna Flamer-Caldera v Sri Lanka]. See R. VIJEYARASA, *Flamer-Caldera v Sri Lanka: Asia-Wide Implications of an Essential Evolution in CEDAW's Jurisprudence*, in Asian Journal of International Law, 2022, 2.; Ch. Chinkin, K. Yoshida, *CEDAW's Landmark Decision on the Criminalisation of Same Sex Conduct Between Women*, in *EJIL: TALK!*, 4.5.2022, https://www.ejiltalk.org/cedaws-landmark-decision-on-the-criminalisation-of-same-sex-conduct-between-women/.

[217] La Rue, see *supra* note 97, 81.

[218] Pelli and Gan-Mor, see *supra* note 212; see also Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on his mission to Mexico, A/HRC/38/35/Add.2, 53 (13.11.2018).

[219] F. ALBANESE, *Report of the Special Rapporteur on the situation of human rights in the Palestinian territories occupied since 1967*, A/77/356, 5 (21.9.2022).

[220] Al-Haq, *Urgent Appeal to the United Nations Special Procedures Israel-Orchestrated Mass Surveillance Campaign Against Palestinian Human Rights Defenders* (16.11.2021) https://www.alhaq.org/cached_uploads/download/2021/12/07/urgent-appeal-spyware-pegasus-1638860090.pdf.

[221] The Pegasus bagging was the only matter mentioned in the Working Group on the Universal Periodic Review regarding the right to privacy, see, *Israel: Compilation of information prepared by the Office of the United Nations High Commissioner for Human Rights*, 36, A/HRC/WG.6/43/ISR/2 (15.2.23).

[222] It is important to note that the two rights are highly interconnected, especially in this context, see La Rue, see supra note 97, 79.

testimonies on the implications on the victims were attached, as per feelings of anxiety and fear of monitoring[223]. These testimonies strengthened the assertion of the ICRC of exacerbation of vulnerabilities.

As presented above, according to the Israeli approach, IHL obligations can barely arise regarding the collection of data. The position does not entail the position towards the application of IHRL in the cyber domain, this position raises an issue with the general right to remedy in IHRL[224]. The legal climate where private companies test their products in the West Bank before being exported worldwide (or sold in Israel, as occurred with Saifan) exists due to an intersection of financial interests, lack of oversight, and legal ambiguity[225].

This legal ambiguity is a result of the Israeli interpretation of the co-applicability between IHL and IHRL, and it seems that Schöndorf followed suit in his articulation of the Israeli perspective on the application of international law in cyberspace (specifically in the discussion over data as an object of an attack). This seems like one of the junctures in which the unique relation between the government, the security forces and the private sector infringes on the rights of volatile individuals, in the West Bank and in Israel – as we will show in the next part.

4.2. *International Human Rights and the Saifan Scandal in Israel.* According to the Tallinn Manuel, IHRL applies in cyberspace and includes, just like in the physical world, both the duties to ensure respect and to protect. In the context of communication surveillance, the Manuel states that "a State that instructs, or directs or controls, third parties, like private companies, to collect, retain, or disclose personal data will be responsible for human rights violations that occur in the course of that conduct"[226].

In pursuant to the ICCPR, the right to privacy and the freedom of expression[227] can only be limited if the state is to demonstrate necessity, proportionality and with a legitimate aim[228]. Additionally, permitting or failing to take appropriate measures or to exercise DD to

[223] *Ibid*., pp.9-10.

[224] Draft Legal Instrument, see supra note 214, §10(4).

[225] See E. ZUREIK, *Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel*, in *Middle East Critique*, vol.29(2), 2020, 219.

[226] TALLINN MANUAL 2.0, *supra* note 66, rule 36.

[227] § 17, 19 International Covenant on Civil and Political Rights, 999 U.N.T.S. 171 (1966).

[228] GC 31, see supra note 83, 6.

prevent, punish or investigate actions done by private entities will constitute a violation as well[229].

In the path to impose DD obligation, the challenge of extra-territoriality arises, since that obligation lies within the territory of the state. While the majority of cases of misuse of Pegasus took place outside Israel[230], this is not the case in the context of Saifan. Also, while we are not aware of Israel instructing, directing or controlling actions by NSO abroad, with Saifan it was the Israeli police which was the main actor – and as an organ of the State, its actions are attributed to Israel[231], even if the conduct exceeds the authority of that person (*ultra-vires*) or contravenes instructions[232].

As noted above, DD obligations are relative, and dependent on the state's capabilities[233], technological knowledge, and risk related to the obligation[234]. The more the state possesses wider knowledge and resources in the field, the obligation is stronger[235]. Israel is an international leader in cyber technology, being at the top of the world in the amount of cybersecurity and cyber offensive companies in its territory[236]. Indeed, Israeli companies raise hundreds of millions of dollars each year[237] and benefit the States' reputation and economy.

---

[229] *Ibid.*, 8.

[230] Lubin, see supra note 31, 21-22.

[231] International Law Commission, *Draft articles on Responsibility of States for Internationally Wrongful Acts with Commentaries*, [2001] 2 Y.B. Int'l L. Comm'n 31, 40, A/CN.4/SER.A/2001/Add.1.

[232] Certain expenses of the United Nations (Article 17, paragraph 2, of the Charter), Advisory Opinion, 1962 ICJ Rep. 151, 168 (July 20); Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, Advisory Opinion, 1999 ICJ Rep. 62, 88–89 (Apr. 29); International Law Commission, *Draft Articles on the Responsibility of International Organizations*, [2011] 2 Y.B. Int'l L. Comm'n 88, 56-60 A/66/10.

[233] ILA report, 15; M. N. SCHMITT, *In Defense of Due Diligence in Cyberspace*, in *Yale Law Journal Forum*, 125, 2015, 68, 75 (2015) (hereinafter: Schmitt, DD).

[234] *Responsibilities and obligations of States with respect to activities in the Area, Advisory Opinion*, (1.2.2011), ITLOS Reports 2011, ¶117. Though the Israeli position, following the 'domain' approach aims to differentiate the different branches of law, as widely accepted, they are closely related and do not need a need *opinio juris* to include them as binding, see Schmitt DD, and ILA report above.

[235] N. TSAGOURIAS, *Self-Defence against Non-state Actors: The Interaction between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule*, in *Leiden Journal of International Law*, 29, 2016, 801, 817.

[236] T. HATUKA, E. CARMEL, *The Dynamics of the Largest Cybersecurity Industrial Clusters: San Francisco Bay Area, Washington D.C. and Israel*, 2021, 4.

[237] *Israeli Tech Review* Q1/2022 (IVC) (2022).

Naturally, a significant number of senior officers at Israeli cyber offensive companies come with rich previous military experience[238].

Given all of that, and regardless of Israel's position in relation to the status of DD in the context of the cyber realm, we nevertheless believe that this principle obligates Israel, and that it sets a high threshold to meet. Israel has strong capabilities, knowledge, and even an ability to impact the adherence to the law (in the context of the sale, marketing and deploying of spywares), the Saifan scandal illustrated that much more could have been done.

This Scandal has revealed an over-reaching technological tool used by the police, and the problems in its introduction to the police and in its deployment. And still, no accountability was imposed on the police. The parliamentary oversight is of importance, but not sufficient as well, as it limited at this stage *ex-post* oversight only.

In order to fill the gap, we believe that IHL and IHRL can be of use. In particular, we will suggest in the next part a complementary toolbox to monitor surveillance practices, ensuring fulfillment of DD obligations, and better adherence to IHRL and other international obligations. The first step we suggest, is to anchor parliamentary oversight over the introduction, and use, of advanced technologies by security forces. The second step, is to establish an early mechanism of legality review of new technologies with military application (including spywares – which for dual-use technology)[239].

4.2.1. *Parliamentary Oversight Mechanisms.* Throughout the years, the Special Rapporteur on the freedom of expression pointed to the need for greater public transparency[240], and for action against the misuse of communication surveillance technologies[241]. We believe that an important step to better meet Israel's DD obligations, is to establish oversight mechanisms that are founded in domestic law[242], but are inspired by international law and designed to implement it[243].

---

[238] Fafta, Samaro, see supra note 206, 28-29.

[239] V. BOULANIN, M VERBRUGGEN, *Article 36 Reviews Dealing with The Challenges Posed by Emerging Technologies*, 2017, 3, available at https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf.

[240] The position was supported *Ibid*., 49.

[241] La Rue, see *supra* note 97, 91-97.

[242] Report of the Special Rapporteur on the right to privacy, A/HRC/37/62, 25.10.2018, 16; periodic report of Italy, see *supra* note 200, ¶36.

[243] Same notion was shared in United Nations High Commissioner for Human Rights, *The right to privacy in the digital age* A/HRC/27/37 30.6.2014, ¶37 (hereinafter: Commissioner for Human Rights, The right to privacy in the digital age).

It is important to differentiate between the public-political and professional oversight mechanisms[244]. This part will discuss such a political mechanism, and the next part will present a professional one.

As recently understood, surveillance technologies invite public discourse, that should be led by elected parliament members, who have an obligation to supervise governmental agencies, including the security forces and law enforcement agencies. This is another layer of supervision, additional to judicial review on particular instances. Though the public discussions might reveal information that will inflict on investigative methods, we believe that monitoring the implementation of them is crucial to prevent infringements of human rights such as privacy and freedom of expression. In that sense, discussing surveillance under the public scrutiny, can incentivize better compliance with legal obligations, and re-build public trust.

The parliamentary oversight should be of a permanent nature, rather than sporadic discussions in different committees. The shadow of such an oversight mechanism can impact positively the approach of the security forces to human rights considerations, and to foster better understanding between all involved actors. In addition, those who exercise oversight should gain expertise that will help that to better preform their role, especially since we are dealing with a complex and dynamic field of knowledge.

4.2.2. *Integration of Privacy and Freedom of Expression Concerns in Legality Reviews.* The second step we suggest, is inspired both by IHL and IHRL. We believe the Israel should establish a professional mechanism for legality review, as prescribed by Article 36 of the First Additional Protocol to the Geneva Conventions (API)[245], that will evaluate new technologies with a military application. While Israel is not a member of API, General Comment 36 of the Human Rights Committee took the approach that ensuring protection of the right to life invites prophylactic impact assessment measures, including

[244] See General Assembly Resolution, *The right to privacy in the digital age*, A/RES/73/179, 21.1.2019, ¶6(d); Commissioner for Human Rights, The right to privacy in the digital age, see *supra* note 243, 38.

[245] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, article 36 (hereinafter API). For the broad argument and more detailed analysis see Mimran and Shany, see supra note X.

legality review for new weapons[246], and, in practice, some States have resorted to review procedures without being members of API (the United States is a prominent example for such a State)[247].

The legality review is particularly important and challenging when dealing with weapons or means or methods of warfare based on new technologies (such as computing, nanotechnology and synthetic biotechnology)[248], given the lack of scientific certainty as to their impact on humanitarian interests[249]. In such cases, questions relating to the application of the precautionary principle, or some version thereof, might arise[250]. Given the recent experience Israel had both with Pegasus and Saifan, there is no better time than the present to construct a mechanism that will be able to cope with the need to supervise this dynamic and complex field.

Article 36 limits States' ability to develop weapons, means or methods of warfare by imposing a procedural obligation to conduct legality reviews. The obligation arises in the "development, acquisition or adoption" of the weapons, or the means of warfare[251]. The terms are understood broadly, when "Means of warfare" – of relevance to spywares – includes military equipment, systems, platforms, as well as other instruments used in the facilitation of military operations[252]. Communication surveillance systems indeed fall under this category, when they can collect information about potential military targets[253]. Specifically, Pegasus, and Saifan as well, definitely meet this threshold. This also includes intelligence surveillance as well, naturally[254].

---

[246] Human Rights Committee, *General comment No. 36 on article 6 of the International Covenant on Civil and Political Rights, on the right to life*, CCPR/C/GC/36 (October 30, 2018), at para. 65.

[247] I. DAOUST, R. COUPLAND, R. ISHOEY, *New wars, new weapons? The obligation of States to assess the legality of means and methods of warfare*, in International Review of the Red Cross, 84, 2022, 345, 348.

[248] ICRC, *A Guide to The Legal Review of New Weapons, Means and Methods of Warfare Measures to Implement Article 36 of Additional Protocol I of 1977*, 2006, 5, available at https://shop.icrc.org/a-guide-to-the-legal-review-of-new-weapons-means-and-methods-of-warfare-pdf-en.

[249] V. BOULANIN, M. VERBRUGGEN, *Article 36 Reviews Dealing with The Challenges Posed by Emerging Technologies*, 2017, 6, available at: https://www.sipri.org/sites/default/files/2017-12/article_36_report_1712.pdf.

[250] See e.g., B. RAPPERT, R. MOYES, *Enhancing the Protection of Civilians from Armed Conflict: Precautionary Lessons*, in Medicine, Conflict and Survival, 26, 2010, 24.

[251] ICRC, *op. cit. supra* note 248, 23.

[252] W. H. BOOTHBY, *Weapons and The Law of Armed Conflict*, 2009, 4.

[253] V. BOULANIN, M. VERBRUGGEN, *op. cit. supra* note 249, 3.

[254] For further discussion, see D. GIOVANNELLI, *op. cit. supra* note 4, 49.

According to the ICRC, the review should follow whenever possible, a multidisciplinary approach, with particular scrutiny given to weapons, means or methods of warfare that generate novel health effects[255]. This is of particular relevance to the violations of the right to privacy, which may have physical and mental health repercussions[256]. States should consider during the review all the international rules that prohibit or limit the use of specific weapons and means of warfare, regardless of whether they derive from a treaty, a custom or a general principle of law[257]. In our context, the legality review process should evaluate the possible harm to IHRL, and especially to the right to privacy and the freedom of expression.

This mechanism will complement the existing arms export regime in place in Israel, and it will allow to better impact the design of the technology. When a technology is brought to approval in the later stages of its development, when it is basically ready for exportation, it is costlier to perform changes in it. An earlier stage of review, will create a stronger sense of partnership between the government and the private sector – with a view to better protect human rights – and also safeguard investors from sunk costs (in the design of the technology, and in the marketing efforts).

5. *Conclusion.* Offensive cyber technology, particularly in the context of surveillance, is a game changer in the world of intelligence operations, and it impacts States on the different levels. As such, neither a domestic tool, nor an international one, suffice on their own. It is through a combined approach that we can deal with a dynamic challenge such as this one.

Israel, as an international leader in the technological field, enjoys its many benefits. Its approach to international law in cyberspace serves its interests, as per the high threshold to the definition of an attack and use of force and its perception of the voluntary nature of DD obligation to prevent human right abuses.

---

[255] ICRC, *op. cit. supra* note 248, 6.

[256] Bensaid v. the United Kingdom, Application no. 44599/98, ECHR (6 May 2001), ¶47

[257] I. DAOUST, R. COUPLAND, R. ISHOEY, *op. cit. supra* note 247, 345, 350. Examples for customary prohibitions include poison or poisoned weapons, biological weapons, chemical weapons, herbicides and more. See J-M. HENCKAERTS, L. DOSWALD-BECK, *Customary International Humanitarian Law*, 2006; P. Lin, *Could Human Enhancement Turn Soldiers into Weapons That Violate International Law? Yes*, in *The Atlantic*, January 4, 2013, available at https://www.theatlantic.com/technology/archive/2013/01/could-human-enhancement-turn-soldiers-into-weapons-that-violate-international-law-yes/266732/.

And still, technological tools present a serious threat to human rights, especially to the right to privacy and the freedom of expression. Against the backdrop of the Pegasus and Saifan scandals, which raised questions on the ability of a democratic State to deploy such over-reaching technologies to surveil individuals, the need for additional oversight mechanisms is obvious. This mechanism is needed in order to fine-tune the relationships in the triangle of the government, security and private sector, which went astray in the context of spywares.

In order to balance between the real need to equip security forces with spywares, in order to safeguard human lives and to deal with threats such as terror and organized crime, and between human rights considerations and other obligations of the State, we suggest to introduce additional oversight mechanisms over dual-use technologies with a military application. These mechanisms derive from the two main international law branches of relevance to spywares – IHL and IHRL.

Concerning IHL, we find Article 36 of the first additional protocol is a useful mechanism to ensure that offensive cyber technologies will not infringe on fundamental human rights. The need to establish prophylactic impact is also derived from General Comment 36 of the Human Rights Committee. Economically-wise, this mechanism is useful since it is more effective to integrate privacy by design rather than impose the limitation in later stages. The monitoring body should include various perspectives and disciplines, including but not only ethics, technology, regulation, security and law. this body can find inspiration in models that already function well, like that of privacy by design.

Relating to IHRL, we offer to strengthen the role of the Israeli Parliament in the oversight of the introduction and deployment new technologies in the service of security forces. This oversight should be held on a permanent basis, and publicly. Those who exercise oversight should gain expertise that will help that to better preform their role, in this complex and dynamic field.

Finally, our suggestions should not be construed as limited to Israel alone. Advanced technologies, and spywares particularly, become relevant to more and more States with every day that passes. The experience of Israel should serve other States in putting place mechanisms to facilitate responsible introduction and deployment of technologies in the service of their security forces, in a way that will

maximize the potentials of technology, but not at the expanse of individual rights and other interests.

NORMATIVE FRAMEWORK, DECISION-MAKING AND RESPONSES TO CYBER OPERATIONS: A VIEW FROM MEXICO

ISAAC MORALES TENORIO – MARIANA SALAZAR ALBORNOZ

1. *Introduction.*- In today's global reality, there is no doubt about the increasing importance of international discussions related to cyberspace. As all regions of the world face more and more sophisticated cybersecurity concerns, a number of states have adopted new rules, legislation and standards aimed at improving their response to malicious cyberoperations and promoting common understandings and procedures through multi-stakeholder collaboration and international cooperation.

Despite the general recognition from the field that some operations in cyberspace could threaten national security or other state interests, the existing international norms leave much leeway for states on the specific criteria for determining such a threat and the procedures to respond thereto.

The United Nations' Group of Governmental Experts' (GGE) Norms of Responsible state Behaviour in Cyberspace, followed by the recommendations made by the Open-Ended Working Group (OEWG), provide some general clues inviting states to adopt or strengthen national policies, legislation, mechanisms, structures and procedures to assess and respond to cyberthreats. In turn, the International Committee of the Red Cross (ICRC) has also provided some guidance on the particularities and implications of cyber operations in contexts of armed conflict, while the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations also provides detailed references on these operations both in the context of armed conflicts and during peacetime.

The interpretation and appropriation of these international non-binding rules, guidelines and references has differed from region to region. Contrary to other regions, Latin American states are not part of any joint military alliance, and therefore they are not subject to a commonly- applicable rule, doctrine or strategy to declare the existence of a cyberthreat, nor do they have a joint understanding or a

visible margin of action to collectively respond thereto. Each state has adopted its own approach and domestic framework in this regard.

This paper seeks to ascertain Mexico's vision of cyberoperations. It starts by reviewing the domestic legal and policy framework applicable to cyberoperations and its evolution. Next, it provides a snapshot of reported cyberoperations in Mexico and proceeds to identify, from both the strategic and the practical level, the authorities and procedures involved in the response thereto. Finally, it examines the significance of international cooperation in this response, to conclude identifying the main characteristics, challenges and opportunities of Mexico's current vision on cyberoperations.

2. *Mexico's legal and policy framework on cyberoperations*.- Contrary to countries of other regions, Mexico –like most countries in Latin America and the Caribbean– does not have a single, central authority responsible for determining the policy, strategy and implementation of actions in the field of cybersecurity. Instead, Mexico's institutional framework for this field is rather fragmented: it provides a patchwork of specific responsibilities to various federal and local authorities, throughout a complex chain of decisions around cybersecurity.

This collage of differentiated responsibilities on cybersecurity in Mexico is distributed between the armed forces, public security and law enforcement authorities, and intelligence organs. It was not the result of a specific analysis of the evolution of threats and challenges in cyberspace. Rather, it emerged from makeshift adjustments of existing mandates on national security and public safety issues. As stated by Piña, "from a comparative politics point of view, Mexico inserted itself many years late into the maelstrom of understanding, developing and establishing a public policy aimed at the computerization of society and, above all, on cybersecurity"[1].

2.1 The evolution of Mexico's public policies on cybersecurity.- Some initial steps on digital regulation in Mexico started in the year

[1] H. R. PIÑA LIBIÉN, *Cibercriminalidad y ciberseguridad en México* [*Cibercriminality and cibersecurity in Mexico*], in *Ius Comitiãlis*, vol. 2, no. 4, 2019, July-December, 47-69. Universidad Autónoma del Estado de México, México. DOI: https://doi.org/10.36677/iuscomitialis.v2i4.13203. "Vale decir que, desde un punto de vista de política comparada, México se insertó con muchos años de retraso en la vorágine que conlleva el entendimiento, desarrollo y establecimiento de una política pública orientada a la informatización de la sociedad y sobre todo de ciberseguridad". Translation is ours.

2000, with the project titled "e-Mexico" which sought to reduce the digital divide in the country. In 2012, the "*Agenda Digital*" public policy was launched by the government to coordinate actions by the public and private sectors to benefit from digital technologies in promoting development, productivity and competition.

Important steps forward were taken in 2013 and 2014. Upon the issuance of Mexico's 2013-2018 National Digital Strategy[2] (NDS), various articles of the Constitution were amended[3] in 2013 to recognize the fundamental right to access information and communications technologies (ICTs) and regulate their services. Consequently, in 2014, the Federal Law on Telecommunications and Broadcasting and the Law of the Public Broadcasting System of Mexico were adopted[4]. These include, among others, the obligation for concessionaires and service providers to collaborate with security and justice authorities.

In 2017 Mexico issued its first National Cybersecurity Strategy[5] (NCS), which was the result of roundtables with the public, private, civil and academic sectors, with the collaboration of the Organization of American States (OAS). It was the eighth Latin American country to issue a NCS of this nature[6]. Mexico's NCS seeks to establish and strengthen cybersecurity actions in the social, economic and political spheres, in order to allow for a responsible use of ICTs for the state's sustainable development, including harmonizing the national legal framework.

---

[2] Estrategia Digital Nacional [National Digital Strategy] 2013-2018, available at https://www.gob.mx/cms/uploads/attachment/file/17083/Estrategia_Digital_Nacional.pdf.

[3] Amendments were made to articles 6, 7, 27, 28, 73, 78, 94 and 104 of the Mexican Constitution, published in the Official Gazette of the Federation on June 11, 2013.

[4] Ley Federal de Telecomunicaciones y Radiodifusión [Federal Law on Telecommunications and Broadcasting], and Ley del Sistema Público de Radiodifusión del Estado Mexicano [Law of the Public Broadcasting System of the Mexican state], both published in the Official Gazette of the Federation on July 14, 2014.

[5] https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf.

[6] After: Panama (2013); Trinidad and Tobago (2013); Jamaica (2015); Colombia (2011 and 2016); Paraguay, Chile and Costa Rica (2017). See J. M. AGUILAR ANTONIO, *Panorama de nacional de ciberdelitos: ¿qué sabemos al respecto en México?* [National panorama on cybercrime: what do we know about it in Mexico?], *Academia Mexicana de Ciberseguridad y Derecho Digital*, Praxis Legal No. 67, 11 March 2022, footnote 7. Available at https://cdnusers3ros.s3.amazonaws.com/public/9e3213120ef1ec5246ed316117908803/cbaebf2678a85366359c341eaabaa7eb1690768418_1690768418.pdf; and L. PARRAGUEZ-KOBEK, *Quo Vadis? Mexico's National Cybersecurity Strategy,* Mexico, Wilson Center, 2018. Available at https://www.wilsoncenter.org/publication/quo-vadis-mexicos-national-cybersecurity-strategy.

The NCS includes national security as one of its strategic objectives, in the sense of "developing capacities to prevent risks and threats in cyberspace that may alter national independence, integrity and sovereignty, affecting national development and interests"[7], including regarding critical infrastructure. However, as stated by Aguilar, the NCS "is more focused on increasing Internet penetration and consolidating its use as a universal right, more than on creating resilience capabilities towards cyberthreats", therefore "neglecting to understand cybersecurity under a national security and defense of the nation-state perspective"[8].

Up until 2018, the NCS was implemented by all Federal authorities and led by the office of the Mexican Presidency. These included the National Security Commission, the Ministry of Interior, the Federal Police and its Division of Scientific Police, the Ministry of Defense and the Ministry of Navy. Nevertheless, the expected coordination subcommittee was never formalized and, upon the entry into office of a new government in 2018, the NCS was left forgotten.

In 2019, under Mexico's current government, the National Strategy on Public Safety[9] was issued, to align security efforts in coordination with state and municipal authorities considering the violence and exponential growth of crime in its different modalities faced by Mexico. It led to the creation of the National Guard in 2019. Additionally, in 2020 the 2020-2024 Sectorial Program on Citizen Safety and Protection[10] was issued. In its Strategic Priority 4.2, it foresees to implement infrastructure and information-security protocols to prevent cyberattacks, as well as to promote agreements on this matter with the security institutions of all three levels of government and with the private sector. It also provides that it will conduct training on the use, maintenance and updating of the

[7] Estrategia Nacional de Ciberseguridad [National Cybersecurity Strategy], *supra* note 5, Objective V., 18.

[8] J. M. AGUILAR ANTONIO, *op. cit. supra* note 6, 3. "[…]está más centrado en incrementar la penetración del internet y consolidar su uso como un derecho universal más que en crear capacidades de resiliencia ante ciberamenazas […], descuidando la comprensión de la ciberseguridad con un enfoque de seguridad nacional y la defensa de la soberanía del Estado-nación". Translation is ours.

[9] Estrategia Nacional de Seguridad Pública [National Strategy on Public Safety], available at https://comisiones.senado.gob.mx/seguridad_publica/docs/SP/ESPR.pdf.

[10] Programa Sectorial de Seguridad y Protección Ciudadana [Sectorial Program on Citizen Safety and Protection] 2020-2024, published in the Official Gazette of the Federation on July 2, 2020, available at https://www.dof.gob.mx/nota_detalle.php?codigo=5596028&fecha=02/07/2020#gsc.tab=0.

technological tools available for cybersecurity in order to prevent and respond to cyberattacks, and that it will establish coordination mechanisms at the national and international levels to prevent, investigate and prosecute cybercrimes, among others.

Although there is no universal and single definition of the term `critical infrastructure`, Mexican practice denotes a prioritization of preventing attacks against infrastructure and essential public services which, if impacted, could affect National Security.

The current administration also issued a new National Digital Strategy for 2021-2024[11], focused on increasing the coverage of Internet in the country and making better use of ICTs for government services, although it has produced little advancements on cybersecurity and cyberoperations to this date. Under its objective of digital policy in the federal administration, it established a *National Homologated Protocol to Manage Cyber Incidents among Government Institutions*[12]. The purpose of this Protocol is to coordinate security evaluations in such institutions to detect risks and improve information-security risk management, and to strengthen coordination among authorities to improve the processes on prevention and response to cyber incidents in collaboration with the National Center for Response to Cyber Incidents (CERT-Mx)[13].

In 2022, the National Program for Public Safety[14] for 2022-2024 was issued. Among its priority strategies, it includes strengthening investigation mechanisms to prevent cybercrimes, implementing mechanisms to detect cyberthreats and safeguard information on technological platforms, implement operation protocols for the prevention of cybercrimes and the protection of users in cyberspace, adopt agreements with national and international actors for prevention, investigation and prosecution of cybercrimes, as well as to implement

[11] Estrategia Digital Nacional [National Digital Strategy] 2021-2024, published in the Official Gazette of the Federation on September 6, 2021. Available at https://dof.gob.mx/nota_detalle.php?codigo=5628886&fecha=06/09/2021#gsc.tab=0.

[12] Protocolo Nacional Homologado en Gestión de Delitos Cibernéticos (National Homologated Protocol to Manage Cyber Incidents], *Presidency- Coordination of the National Digital Strategy; Ministry of Safety and Citizen Protection- National Guard,* October 2021, available at https://www.gob.mx/gncertmx/documentos/9408.1

[13] *Idem,* objective I, specific objective 5, lines of action.

[14] Programa Nacional de Seguridad Pública [National Program for Public Safety] 2022-2024, available at https://www.dof.gob.mx/nota_detalle.php?codigo=5673252&fecha=05/12/2022#gsc.tab=0.

response mechanisms to cybersecurity incidents and follow-up their mitigation and prevention[15].

2.2 Mexico's legal framework on cybersecurity.- Despite the above-mentioned national policies, Mexico's legal framework has not changed much in recent years regarding decision-making and response to cyberoperations that affect the state. Mexico does not have a law specifically dedicated to cybersecurity. In the past four years, five draft laws on cybersecurity[16] and a dozen reform proposals to address cybercrime have been presented in the Mexican Congress, some of which propose the creation of a national cybersecurity agency. Nevertheless, none of these drafts have passed to this date. Therefore, the current legal framework in Mexico on cybersecurity activities is distributed throughout the Mexican Constitution, the Federal Criminal Code, the General Law of the National System of Public Safety and the National Security Law.

The Mexican Constitution distinguishes between public safety functions and national security functions, as follows:

- As per article 21 of the Constitution, public safety functions include prevention, investigation and prosecution of crimes, as well as administrative sanctions. These functions correspond to the state, through the Federation, the 32 federal entities, and the municipalities. They are carried out through the public safety institutions which include the police –at the federal, state and municipal levels–, public prosecutors (*Ministerio Público*) and the National Guard, all of which are of a civilian nature.
- On the other hand, article 89-VI of the Constitution provides that one of the functions of the Mexican President is to preserve national security and dispose of the Armed Forces – which include the Army, the Navy and the Airforce– for interior security and external defense of the Federation.

[15] *Ídem,* Strategic Priority 3.4 and concrete actions 3.4.1 to 3.4.5.

[16] 1. Senator Miguel Ángel Mancera Espinosa, '*Iniciativa de la Ley General de Ciberseguridad',* September 1st, 2020; 2. Deputy Javier Salinas Narváez, '*Iniciativa que expide la Ley Nacional de Seguridad en el Ciberespacio',* October 19, 2020; 3. Deputy Juanita Guerra Mena, '*Iniciativa de Ley General de Ciberseguridad',* October 6, 2022; 4. Senator Jesús Lucía Trasviña Waldenrath, *'Proyecto de decreto por el que se expide la Ley General de Ciberseguridad'*, March 23, 2021; 5. Deputy Javier Joaquín López Casarín, '*Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Ciberseguridad',* April 25, 2023.

The latter aspect is further regulated in the National Security Law, issued in 2005. It defines national security as actions destined to immediately and directly maintain the integrity, stability and permanence of the Mexican state, aimed to (i) protect the nation from the threats and risks that it may face; (ii) preserve national sovereignty and independence, and defend the territory; (iii) maintain the constitutional order and strengthen the government's democratic institutions; (iv) maintain the Federation's unity; (v) exercise Mexico's right of self-defense against other states or subjects of International Law; and (vi) preserve democracy, founded in Mexico's economic, social and political development[17].

Article 5 of the National Security Law includes a list of the following twelve acts that threaten national security. While none of these refer specifically to the cyber sphere, all of these acts could, in fact, be the result of a malicious cyberoperation:

I. Acts tending to commit espionage, sabotage, terrorism, rebellion, treason, genocide, against the United Mexican states within the national territory;

II. Acts of foreign interference in national affairs that may affect the Mexican state;

III. Acts that prevent the authorities from acting against organized crime;

IV. Acts tending to break the unity of the constituent parts of the Federation;

V. Acts tending to hinder or block military or naval operations against organized crime;

VI. Acts against aviation security;

VII. Acts that threaten diplomatic personnel;

VIII. Any act intended to consummate the illegal trafficking of nuclear materials, chemical, biological and conventional weapons of mass destruction;

IX. Illegal acts against maritime navigation;

X. Any act of financing terrorist actions and organizations;

XI. Acts tending to hinder or block intelligence or counterintelligence activities;

[17] *Ley de Seguridad Nacional* [National Security Law], published in the Official Gazette of the Federation on January 31, 2005, article 3. Available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LSN.pdf.

XII. Acts intended to destroy or disable infrastructure of a strategic or essential nature for the provision of public goods or services.

To coordinate actions to preserve national security, the National Security Law created the National Security Council, chaired by the President and composed of the Ministers of Interior, Defense, Navy, Public Safety, Treasury, Public Administration, Foreign Affairs, Communications, Infrastructure and Transportation, the Attorney-General and the Director of the National Center for Intelligence[18]. As per articles 56 to 60 of the Law, all policies and actions related to national security are subject to the control and evaluation of the Federal Legislative Power, through a Bicameral Commission of 3 Senators and 3 Deputies, to which the Council reports each semester on the activities it carried out. Reports from the Council to the Legislative power must omit any information which, if revealed, may threaten national security or the fulfillment of the Center's functions or the privacy of individuals.

In turn, the General Law for the National Public Safety System[19], issued in 2009, defines public safety as the functions to preserve integrity and rights of persons, public liberties, order and peace, and includes special and general crime prevention, administrative sanctions, and investigation and prosecution of crime, as well as social reinsertion of sentenced persons[20]. Even though this law does not include a specific reference to cybersecurity, it allocates public safety functions to police forces, law enforcement institutions, penitentiary system institutions, and public safety authorities at the federal, state and municipal levels.

In the Federal Criminal Code, a specific chapter was added in 1999, as articles 211 bis 1 through 7, on crimes regarding illicit access to computer systems and equipment. These encompass unauthorized amendment, destruction or loss of information contained in computer systems or equipment, both private and state-owned, as well as illicit intercepting and other crimes against data integrity and against system integrity. These are also included in most local criminal codes of the federal entities of Mexico. However, as stated by Boyer, "[a]t the

[18] *Ídem,* article 12.

[19] Ley General del Sistema Nacional de Seguridad Pública [General Law for the National Public Safety System], published in the Official Gazette of the Federation on January 2, 2009. Available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNSP.pdf.

[20] *Ídem*, article 2.

federal and state levels, there is a lack of consistency in the definition of criminal behavior connected to security issues, as well as the consequences and sanctions that go along with it"[21]. In the same sense, the OAS and the InterAmerican Development Bank's Observatory on Cybersecurity in Latin America and the Caribbean identified in 2020 that the provisions on computer crimes contained in Mexico's Federal Criminal Code "are limited and leave may gaps, hindering the fight against cybercrime"[22].

This composite Mexican legal framework is applicable to address cybersecurity concerns and all sort of activities in cyberspace. It is complemented by a robust legal framework on privacy and personal data protection in Mexico. The right to privacy and data protection is recognized as a human right in article 16 of the Mexican Constitution since 2009. It is regulated through two specific and comprehensive laws: the Federal Law for Protection of Personal Data Held by Private Parties, of 2010, and the General Law for Protection of Personal Data Held by Public Authorities, of 2017[23]. Data protection laws provide for security and personal data protection measures to avoid attempts to steal, alter, disable or destroy information through access to computer systems, including cyberoperations.

As may be seen from the above-described legal framework, under Mexican laws there is no precise definition on cyberoperations that attack the state's interests, nor is there a national agency in Mexico leading all state responses to cyberoperations. Therefore, cyberoperations fall under the existing legal frameworks of criminal law, public safety and national security concerns, and, consequently, the response

[21] J. BOYER, *Mexico's National Defence Data Breach: A Wake-Up Call for the Country's Cybersecurity Landscape*, *EMILDAI Blog Post,* June 11, 2023. Available at https://emildai.eu/mexicos-national-defence-data-breach-a-wake-up-call-for-the-countrys-cybersecurity-landscape/.

[22] Observatorio de la Ciberseguridad en América Latina y el Caribe, update on Mexico, 2020. "México no cuenta con una ley dedicada de delito cibernético, pero el artículo N° 211 del Código Penal prevé el delito informático. Sin embargo, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen". Translation is ours. Available at https://observatoriociberseguridad.org/#/home.

[23] Ley Federal de Protección de Datos Personales en Posesión de los Particulares [Federal Law for Protection of Personal Data Held by Private Parties], published in the Official Gazette of the Federation on July 5, 2010, available at https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf; and Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados [General Law for Protection of Personal Data Held by Public Authorities], published in the Official Gazette of the Federation on January 26, 2017, available at: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf.

to them is coordinated among the relevant instances. In sum, as stated by Athié, "[c]yberattacks are considered crimes under federal criminal law, and, depending on the characteristics of the attack, it may also be considered a menace to national security"[24].

3. *A snapshot of reported cyberoperations in Mexico*.- In recent years, renowned cyber forensic studies have reported that Mexico is among the most targeted countries in Latin America in terms of cyberattacks. For example, according to Fortinet, during the first half of 2022 the region of Latin America and the Caribbean was the target of 137 billion attempts of cyberattacks, of which Mexico was the most attacked country in the region with 85 billion cyberattacks, followed by Brazil with 31.5 billion and Colombia with 6.3 billion[25]. Mexico had the region's highest ransomware distribution activity in the period, with more than 18,000 detections, followed by Colombia (17,000), Costa Rica (14,000), Peru, Argentina and Brazil[26].

A few of these cyberoperations against Mexico have been attributed to states, while the vast majority of them have come from cybercriminals, private hackers and other private groups.

Unpacking evidence of the main state-sponsored cyber operations, the Council on Foreign Relations' Cyber Operations Tracker[27] reports that Mexico has been targeted with the following:

(i) In 2013, Mexico was affected by *The Dukes,* also known as Advanced Persistent Threat (APT) 29, Cozy Bear, Dark Halo, Nobelium and Cloaked Ursa. According to such Tracker, Estonian intelligence services associate this group with the Russian Federal Security Service and Foreign Intelligence Service.

(ii) In 2014, Mexico was one of the countries targeted by *Operation Cleaver,* also known as Cutting Kitten and Group 41, affecting Mexico's government and private sector entities for

[24] A. ATHIÉ, *Cybersecurity and data protection in Mexico*, *Basham, Ringe y Correa Legal Briefing,* Spring 2023, available at https://www.inhouselawyer.co.uk/legal-briefing/cybersecurity-and-data-protection-in-mexico/.

[25] 'Fortinet registró 137 mil millones de intentos de ciberataques en América Latina en la primera mitad del año' [Fortinet registered 137 billion attempts of cyberattacks in Latin America during the first half of the year], Fortinet, Press Release, 18 August 2022. Available at https://www.fortinet.com/lat/corporate/about-us/newsroom/press-releases/2022/fortinet-registro-137-mil-millones-de-intentos-de-ciberataques-e.

[26] Mexico is one of the top victims of cyberattacks in Latin America, *Mexico News Daily,* December 27, 2022. Avialable at https://mexiconewsdaily.com/news/mexico-top-victim-of-cyberattacks/.

[27] Available at https://www.cfr.org/cyber-operations.

espionage and sabotage purposes. According to such source, the suspected state sponsor of this attack was the Islamic Republic of Iran.

(iii) In 2018, Mexico was one of the countries targeted by the global bank attacks, when a supposed North Korean group, the Lazarus Group, sponsored by the Democratic People's Republic of North Korea, is believed to have stolen hundreds of millions of dollars by infiltrating the computer systems of banking system in the region.

(iv) For 2020, the same tracker reports Mexico as a victim of hackers affiliated with the Lazarus Group, who targeted automated teller machines (ATMs) by manipulating transaction-processing software to initiate fraudulent cash-outs.

(v) Also in 2020, Mexico is reported to have been one of the countries targeted by Chinese threat actor APT 41, suspected to be sponsored by China, who attempted to exploit three vulnerabilities at over seventy-five organizations across sectors and countries.

Taking the above-mentioned state-sponsored cyberoperations together with the other billions of cyberattacks that Mexico has received from cybercriminals and other private actors, the cost of cybercrime and cyber fraud to the Mexican economy has been estimated to be as high as $7.7 billion U.S. dollars a year[28].

Many experts have attested to the connection between cyber-security and national security concerns in Mexico. As stated by the Center for Strategic & international Studies (CSIS), "[t]he connection between cybersecurity and more conventional national-security issues has sharpened in recent years as criminal groups in Mexico have expanded into the digital sphere"[29]. Among others, CSIS cites as an example throughout 2018 the Bandidos Revolution Team, whose members were found to have ties to criminal enterprises "stretching from Venezuela to Romania", targeted Mexican banks and ATMs, stealing between $2.5 and $5 million a month. Moreover, the same source also indicates that «[c]artels have also integrated dark-web communications networks and cryptocurrencies into their trafficking operations as nearly untraceable methods for acquiring synthetic drug precursors and selling them in the United States»[30].

---

[28] https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment.

[29] R. C. BERG, H. ZIEMER, *The Development of the ICT Landscape in Mexico: Cybersecurity and Opportunities for Investment*, *Center for Strategic & International Studies,* November 19, 2021. Available at https://www.csis.org/analysis/development-ict-landscape-mexico-cybersecurity-and-opportunities-investment.

[30] *Ibid.*

Some of the cyberattacks that have affected Mexico have targeted critical infrastructure. This was the case, for example, of the nearly three million cyberattacks that targeted the National Electoral Institute in 2018, as well as of the 2019 serious ransomware attack against Mexico's state-owned oil company Pemex[31].

Additional concerns have arisen due to recent cyberattacks that have leaked confidential government information and stolen government credentials, which have been presumably developed by politically motivated actors. This was the case of the massive cyberattacks against the Mexican Congress in 2021 and 2022, and the 2022 operation by *Guacamaya*, an international hacktivist group, which leaked more than six thousand gigabytes of confidential documents and sensitive military information from the Ministry of Defense[32].

4. *Authorities and procedures involved in response to cyber-operations.*- As mentioned above, the expansion of criminal groups' activities in Mexico to the digital sphere has led to a common understanding, by Mexican authorities, that there is a somehow natural convergence between national security, homeland security and public safety issues. One of the main reasons for this has been the evolution of the special mandates and responsibilities that have been conferred to Mexican military forces, since 2006 and still to this date, to act in support of police forces in countering organized crime. As was described in section 3 *supra,* any acts that hinder or prevent the authorities from acting against organized crime are now considered a threat to national security.

In light of the above, despite the lack of a specific normative framework for cyberoperations, and the absence of a national cybersecurity agency to centralize and lead all of Mexico's responses to cyberoperations, there has been a history of common understandings, collaboration and coordination at the operative level among public safety and national security institutions. Inter-agency coordination mechanisms have played a key role in identifying cyber threats and emerging risks, and in assessing national capabilities to launch prevention and response measures. In addition to this

[31] *Ibid.*

[32] *Confidential Mexican Military Documents Leaked by Hacktivist Group*, *Justice in Mexico,* 29 November 2022. Available at https://justiceinmexico.org/sedena-document-leak/

collaboration, each sector has strengthened its institutional capabilities to respond to cyberoperations that fall within its mandate.

4.1 The military and Intelligence operative framework.- The Mexican Armed Forces, under the Ministry of Defense (Army and Air Force) and the Ministry of the Navy (Navy), are responsible for responding, in practice to any cyberoperation that is determined in the framework of the National Security Council to be a potential threat to national security (as per the definition contained in the National Security Law described in section 2 above), and any issue of state cyber defense. These institutions have rapidly and silently strengthened their defense capabilities, expertise and actions, both institutionally and in military doctrine, procedures and practice, to deal with major cyber threats and cyberoperations, in a much quicker pace than the normative advancements.

In 2016, the Ministry of Defense created a specialized Center for Cyberspace Operations, and the Ministry of Navy created its own Cybersecurity Unit, which it transformed in 2022 into a General Coordination, in order to update and improve the Ministry's work in this area[33].

In the realm of military doctrine, in 2021 the Navy adopted its 2021-2024 Institutional Strategy for Cyberspace, to strengthen its capabilities to identify and respond to cyberthreats[34]. Moreover, a very relevant advancement was produced in 2021, with the adoption of the *Joint Ministry of Defense- Ministry of Navy Glossary of Terminology in the Sphere of Cyberspace Security*. This document updates the prior one adopted in 2013 and includes, among others, a common definition of cyberoperations from an operative perspective, as follows: «Operations in Cyberspace (Cyberoperations): Activities launched by the nation-state in or through cyberspace to provide security to the

[33] J. M. AGUILAR ANTONIO, *La constitución de la Coordinadora General del Ciberespacio (EMCOGCIBER) y la semana de la ciberseguridad en SEMAR*, [The creation of the General Coordination of Cyberspace and the week of cybersecurity in the Ministry of Navy], *El Independiente,* December 1, 2022. Available at https://elindependiente.mx/opinion/dia-cero/2022/12/01/la-constitucion-de-la-coordinadora-general-del-ciberespacio-emcogciber-y-la-semana-de-la-ciberseguridad-en-la-semar/.

[34] Secretaría de Marina, Estrategia Institucional para el Ciberespacio 2021-2024. Available at https://www.gob.mx/cms/uploads/attachment/file/661788/Estrategia_Institucional_Ciberespacio_SM.pdf.

society. For Armed Forces, cyberoperations are considered military operations in cyberspace, in fulfillment of their mandated missions»[35].

4.2 The police and law enforcement operative network.- The response to all cybercrimes other than those that threaten national security is carried out by public safety institutions which, as mentioned, includes the police – at the federal, state and municipal levels- and the National Guard. As mentioned, the National Guard was proposed in 2019 by the National Strategy on Public Safety; it was thus established in 2019 through an amendment to the constitution and the adoption of a specific Law of the National Guard[36]. It has a civilian mandate and head, but it is of a dual nature where its members have military training, hierarchy and structure.

The National Guard's attributions include, in relation to cyber-space, «to carry out actions of surveillance, identification, monitoring and tracking on websites in the public network of the Internet, in order to prevent criminal conducts»[37].

In order to implement this mandate, the Center for Response to Cyber Incidents ("CERT-Mx")[38] was created within the National Guard (previously operating under the Federal Police), to support the response to cyber incidents against institutions with critical infrastructure, as well as to identify threats and the *modus operandi* of criminal networks in order to provide early warning to the relevant sectors and raise awareness in the population. The CERT-Mx mainly works with five categories of cybercrimes:

I. Offenses against people: crimes of harassment, threats, defamation and identity fraud;

II. Fraud and extortion: extortion crimes, electronic banking user fraud, e-commerce fraud, various frauds, e-mail scams;

---

[35] *Glosario de Términos SEDENA-MARINA en Materia de Seguridad en el Cibersepacio,* 11. "Operaciones en el Ciberespacio (Ciberoperaciones): actividades que realiza el Estado-Nación en o a través del ciberespacio, para proporcionar Seguridad a la sociedad. Para las Fuerzas Armadas son consideradas como operaciones militares en el CIberespacio en cumplimiento de las misiones encomendadas". Translation is ours. Available at https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-_SM_compressed.pdf.

[36] Ley de la Guardia Nacional.

[37] Ley de la Guardia Nacional, art. 9, fr. XXXVIII: "Realizar acciones de vigilancia, identificación, monitoreo y rastreo en la red pública de Internet sobre sitios web, con el fin de prevenir conductas delictivas". (Translation is ours).

[38] https://www.gob.mx/gncertmx.

III. Computer security events: crimes such as system intrusion, hacking (deface), *malware* (police virus), *cryptolocker, phishing*, password theft on social networks.

IV. Reports of various crimes through the web: only citizen reporting of web pages.

V. Crimes against minors: crimes such as harassment, threats, cyberbullying, corruption, disappearance, defamation, grooming, other preventive information, pedophilia, child pornography, theft of passwords on social networks, sexting, identity theft and trafficking minors[39].

4.3 Inter-agency coordination and response procedure.- Regarding cyberoperations and cyber risks that affect national security and critical infrastructures, upon the establishment of the National Security Council, in 2007 a Specialized Committee on Information Security was, *de facto,* created[40]. It was composed of cyber experts from the armed forces and from the law enforcement, public safety, intelligence, foreign affairs, central bank and energy sector authorities, consolidating itself as specialized and action-oriented body to advance collaborations and operate alerts. Even though this Committee continued being the operative coordination entity until the current government, it was never formalized by law, and therefore its work, operations and products remained discrete.

As for other types of cybercrimes, law enforcement agencies have also been characterized by an operative inter-agency collaboration lead by the National Guard and CERT-Mx to respond to malicious cyber activities. Since 2016, as an agreement issued by National Council of Public Security, the former federal police -now National Guard-promoted the adoption of an homologated model for cyber police at the state and local levels[41]. Today, almost all federal states in Mexico, including Mexico City, have created cyber police units[42].

---

[39] J. M. AGUILAR ANTONIO, *Panorama de nacional de ciberdelitos: ¿qué sabemos al respecto en México?*, Academia Mexicana de Ciberseguridad y Derecho Digital, Praxis Legal No. 67, 11 March 2022, 4.

[40] J. L. GARCÍA CANCINO, *Hacia un modelo de protección al ciberespacio en México para las instituciones del Consejo de Seguridad Nacional*, México, Instituto de Investigaciones Estratégicas de la Armada de México, 2018, 9-10 https://cesnav.uninav.edu.mx/cesnav/ININVESTAM/docs/docs_analisis/da_35-18.pdf.

[41] https://www.gob.mx/cms/uploads/attachment/file/189189/Modelo_homologado_unidades_policia_cibernetica.pdf.

[42] See, in this sense A. L. GUTIÉRREZ, *En México solo hay cuatro policías cibernéticos por cada millón de habitantes*, in *Expansión,* 24 october 2023, available at

One of the tangible results of these inter-agency coordination efforts was the adoption, in October 2021, of the *National Homologated Protocol of Cyber Incidents Management,* mentioned in section 2 above. Under the leadership of the National Guard, it represents a significant starting point for both public and private organizations' readiness, and for incorporating international standards, cyber crisis management models and guidelines to mitigate and even respond to cyber-attacks[43].

In light of the above, and depending on which elements are reported when a cyber risk or emergency is detected, the cyber incident response process in Mexico has at least four stages, involving different authorities and requiring relevant coordination:

1) Permanent monitoring activities are a priority responsibility of CERT-Mx, the Army, Navy and other relevant incident response centers.

2) Once a cyber risk or threat is identified, it is communicated to other agencies and authorities, particularly those participating in the Specialized Committee of the National Security Council. Different alert categories are used to communicate the threat:

a. Situations to keep in monitoring are communicated directly to potential affected entities (such a specific government institution), on a preventive basis.

b. Serious situations considered to require multiple contention and mitigation actions are elevated to the Specialized Committee.

c. Critical malicious cyberoperations are communicated to the National Security Council or National Security Cabinet.

3) In case of critical incidents, the National Security Council or National Security Cabinet, at the highest level, defines the principal authority that will lead the state's investigation or responses, or when international cooperation is required.

4) The recovery efforts, and normalization of the situation or new scenarios faced, are again communicated to the inter-agency mechanism.

These four stages are identifiable and can be deducted from the response that national authorities have provided to cyberoperations

https://expansion.mx/empresas/2023/10/24/mexico-4-policias-digitales-por-cada-millon-de-habitantes.

[43] https://www.gob.mx/cms/uploads/attachment/file/735044/Protocolo_Nacional_Homologado_de_Gestion_de_Incidentes_Ciberneticos.pdf.

and cybercrimes that have targeted Mexico. However, to this date there has been no evidence of an international cyberoperation launched by Mexico against another state or private group. This may be due to Mexico's historically defensive, and not offensive, military tradition. In fact, and as mentioned by the CFR's tracker, the government of Mexico appears as an alleged perpetrator only of local cyberoperations related to the controversial surveillance software *Pegasus* used against journalists and human rights activists, and political opposition parties[44]. As Hurel has identified: «While the incipient discussion (or lack of one) on cyber operations at the regional level is partly tied to a lack of capacities or a mismatch of focal points at the national and regional levels, it can also serve as a smoke screen for Latin American countries to continue developing their cyber capabilities with little to no oversight. The blurriness between police forces and other public security bodies can (and has) posed challenges to accountability over software acquisitions. This is particularly worrying as it raises important questions over states' purchasing power of cyber weapons with a risk of little public oversight»[45].

5. *The significance of International Cooperation*.- Military alliances, such as NATO or other military joint operations, bring to participating states common doctrinal definitions and ground-level understandings of what cyberoperations *are* and what they are *not*, how to respond to them and how to launch them. However, Mexico is not a part of any military alliance, and it has not participated in security coalitions. In this scenario, Mexico's involvement and participation in multilateral processes on cybersecurity plays a key role in influencing Mexico's views and national decision-making regarding cyberoperations, as well as its possible next steps in the normative sphere.

In recent years, the Government of Mexico, through diplomatic, law enforcement and military authorities, has participated actively in the main multilateral discussions on cybersecurity, and has advanced important capacity-building programs with regional and international counterparts. International cooperation is a key element in the way

[44] https://www.cfr.org/cyber-operations.

[45] L. M. HUREL, *Beyond the Great Powers: Challenges for Understanding Cyber Operations in Latin America*, in *Global Security Review*, Volume 2, January 2022, 28 https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=1014&context=gsr.

Mexico addresses and responds to malicious cyberoperations. Article 89 of the Mexican Constitution includes international cooperation, non-intervention, the prohibition of the use of force and the pursuit of international peace and security, among the fundamental principles of Mexico's foreign policy. Moreover, the National Security Law also provides for international cooperation, indicating that diplomatic embassies and missions in Mexico should inform Mexican authorities of possible risks according to bilateral cooperation agreements on security matters. In addition, it provides that foreign servants such as police, inspection or law or technical supervision agents may be authorized to enter Mexico temporarily to exchange information under such agreements[46].

In the UN's GGE and OEWG processes, Mexico has openly embraced the reaffirmation of the applicability of international law in cyberspace, despite the fact that, like most states of the region, it has still not presented a comprehensive national position on the matter. Mexico has also called for the universal implementation of the voluntary norms of responsible state behaviour in cyberspace, and in particular the one calling states to consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats.

At the regional level, Mexico has led efforts to build confidence by promoting the creation of the OAS Working Group on Cooperation and Confidence Building Measures in Cyberspace and the operationalization of the measures adopted within. It has also embraced the guidance provided by the reports and seminars organized by the InterAmerican Juridical Committee to assist states in advancing in the comprehension of this topic.

Mexico's international cooperation efforts were one of the five criteria considered, thanks to which Mexico was ranked 52nd out of 182 nations in the fourth edition of the International Telecommunication Union (ITU) Global Cybersecurity Index corresponding to 2020. These efforts have resulted in the implementation of concrete agreements and mechanisms within Mexico's national security and public safety institutions, as follows:

- The National Guard's CERT-Mx has international cooperation agreements and mechanisms with other security institutions for

[46] Ley de Seguridad Nacional, articles 68-74.

preventive actions, digital forensic investigations, and technical police analysis in support of public prosecutors to bring perpetrators to justice. As of June 2020, it had more than 4,000 international collaboration mechanisms, 80% of which are with the United States, to issue cybersecurity alerts and newsletters[47].

• Mexico's CERT-Mx fully contributes in the "CSIRT Americas" initiative, which promotes regional early-warning and exchange of experiences. CERT-Mx also participates in the very operative FIRST forum, in addition to its involvement in INTERPOL's programs. Even when Mexico has not ratified the Council of Europe's Budapest Convention, it operatively participates in the corresponding 24/7 network.

• The Army and the Navy's respective cyber units hold continuous exchanges and trainings with counterparts in the Americas, and actively participate in the cooperation programs of the Inter-American Committee against Terrorism (CICTE) and within the Inter-American Defense Board (JID). In fact, the Mexican Navy recently chaired the Ibero-American Cyber Defense Forum.[48]

• Finally, since 2021, trilateral cyber experts dialogues were consolidated between Mexico, the US and Canada, and Mexico has been involved the White House's Ransomware Initiative. These are perhaps the most influential factors over Mexico's operative and doctrinal conception of cyberoperations.

6. *Conclusions*.- The current landscape of emerging cyber risks, challenges, and threat actors is increasingly complex. Regardless of a country's level of development or the degree of maturity of its critical infrastructures, malicious cyberoperations are targeting all regions of the world. Although countries are accelerating the adoption of specific norms, standards and legislation on cybersecurity and cyberspace governance, the definition of tools, processes, and practices around the conception of cyberoperations is not homogeneous for all. It continues to have components that are defined on the ground and on a case-by-case basis.

---

[47] J. R. ARTEAGA, *Así es como la Guardia Nacional lucha contra la delincuencia en Internet*, *Forbes Mexico,* 23 June 2020, https://www.forbes.com.mx/noticias-asi-es-como-la-guardia-nacional-lucha-contra-la-delincuencia-en-internet/.

[48] https://www.gob.mx/semar/prensa/marina-se-fortalece-en-materia-de-seguridad-en-el-ciberespacio-al-recibir-la-secretaria-pro-tempore-del-foro-iberoamericano-de-ciberdefensa.

As we have depicted in this article, the Mexican case is characterized by having a disperse and non-cyber specific normative framework, in addition to policy developments that are still incipient, and which have been overly marked by changes in government. In contrast, at the operational level, common understandings, collaboration and coordination between authorities are very evident and stand out. Nonetheless, inter-agency coordination mechanisms are not permanent and have not been formalized by law.

In comparison to other international experiences, it is important to recognize that Mexico faces:

- A lack of a cybersecurity law
- A lack of national central cybersecurity agency
- A lack of formal cyber accountability mechanisms

At the procedural level, and as occurs in many other Latin American countries, actionable mandates to respond to cyberoperations may be identified in Mexico in terms of differentiated threats to national security and to public safety. Nevertheless, as organized crime is considered both a threat to national security and to public safety, similar monitoring responsibilities are assumed by police, law enforcement, intelligence and military authorities when facing cybercrime.

In light of the above, the advancement of multilateral discussions and international cooperation is strongly influential and complementary for Mexico's comprehensive vision on cyberoperations. The Mexican government's commitment to international law and to the norms of responsible state behaviour in cyberspace, as well as to confidence-building measures and ethical standards for the use of ICTs, the basis and the limits that frame Mexico's views and practices with regards to cyberoperations.

INTERNATIONAL ORGANIZATIONS PERSPECTIVE

THE UNITED NATIONS AND CYBERSECURITY

PIETRO GARGIULO

1. Just over two years ago, Russia invaded Ukraine, employing a strategy characterized by military actions preceded or accompanied by cyberattacks. Russia's "hybrid war" against Ukraine was thoroughly described by Microsoft in a report published in June 2022, which stated that various Russian military and civilian intelligence services had conducted destructive cyberattacks while military forces attacked the country[1]. It is also known that Ukraine's response involved cyber operations conducted not only with the help of "western cyber military teams and private cyber-security companies", but also with the support of various hacker groups[2].

It is equally known that these events led some analysts to consider the Russia-Ukraine War as the first true cyber war[3]. In reality, this was not the case[4]. However, this does not mean that cyber operations, alongside kinetic ones, did not play a particularly significant military role in the ongoing conflict between Russia and Ukraine, underscoring the importance of cybersecurity in international conflicts. In such contexts, it is easy to verify the widespread use by states of information and communication technologies (ICT) to carry out malicious actions against other states, often through the use of non-state actors.

---

[1] V. MICROSOFT, *An overview of Russia's cyberattacks activity in Ukraine*, Digital Security Unity, April 27, 2022. See also M. ORENSTEIN, *Russia's Use of Cyberattacks: Lessons from the Second Ukraine War*, Foreign Policy Research Institute, June 7, 2022, www.fpri.org.

[2] J. TIDY, *Meet the hacker armies on Ukraine's cyber front line*, in BBC News, April 15, 2022, www.bbc.com.

[3] Y. SHCHYHOL, *Vladimir Putin's Ukraine invasion is the world's first full-scale cyber war*, June 15, 2022, www.atlanticcouncil.org/blog.

[4] A. PYTLAK, *False Alarms: Reflecting on the Role of Cyber Operations in the Russia-Ukraine War*, February 22, 2024, www.stimson.org.

The war between Russia and Ukraine is just one of many episodes of cyber operations that have taken place in recent years, creating various situations of international tension. Hence, the need to identify a legal framework applicable to the conduct of states in cyberspace. It is easy to understand, however, that this is not a simple objective to achieve, not only due to the complexity of the matter[5] but also because of the diverse interests of the states, which, even concerning the use of cyberspace, seek to gain hegemonic roles politically and militarily, both internationally and regionally.

Several key international organizations, both universal and regional, have long played a crucial role in shaping the international legal framework applicable to cyber operations. In this work, we will focus on the role and activities of the UN as it is the main universal organization that has been addressing cybersecurity issues over an extended period. Moreover, within the UN context, it is possible to assess the diversity of interests and positions of the member states, particularly the great powers like United States, Russia, and China, whose contrasts in cybersecurity matters are often exacerbated by evolving international relations and emerging crises that promote competition and conflict.

At the UN, cybersecurity issues are primarily examined within the framework of developments in information and communication technologies concerning international security. This clearly shows the link between the use of ICT and the UN's primary pillar: maintaining international peace and security[6]. A positive trend in the development of ICT is crucial for maintaining international stability and security. However, it is also easy to see that these technologies are often used for malicious purposes.

It is no coincidence that in its first intervention on the issue, the UN General Assembly, on the one hand, emphasized the benefits for the international community as a whole, while, on the other, it expressed concern about ICT use for purposes contrary to the objectives of maintaining international stability and security[7]. This

[5] See in this volume the work by A. SCIACOVELLI, *Malicious Cyber Operations Committed by States and Non-State Actors: The International Legal Landscape*.

[6] It is important to emphasize that developments in the field of ICT also impact the other two pillars of the UN's activities: sustainable development and the promotion and protection of human rights. This is because ICT is at the heart of a transformation process in the international arena that has political, economic, social, and cultural implications, in addition to being a catalyst for international cooperation.

[7] See par. 2.

initiated a dialogue among member states aimed, among other things, at identifying the rules of international law applicable to ICT use. On these points, it is important to note that divergent positions among member states continue to obstruct the creation of a universal legal framework for cyberspace[8].

This work focuses on the following aspects: the initiation of the UN's efforts through the analysis of relevant initiatives of the General Assembly; the assessment of the activities of the Group of Governmental Experts on the impact of ICT developments on international security, especially concerning the development of the applicable international legal framework; the analysis of the activities of the open-ended working group open to the participation of all UN member states established following the re-emergence of divergent opinions on the matter; next we shall analyze the initiatives of the Security Council, which since 2021 has been closely focused on cybersecurity issues; finally, we shall try to provide some indications on possible future developments.

2. The issue of ICT in the context of international security was first addressed by the UN General Assembly in the 1990s, based on a resolution proposal presented by the Russian Federation within the work of the First Committee (Disarmament and International Security). The Russian proposal was approved by consensus on December 4, 1998, as Resolution 53/70[9]. The reasons behind the widespread support that the Russian initiative received are essentially threefold: the indication that the dissemination and use of ICT could constitute an opportunity for the international community as a whole, and that the need existed to establish broad international cooperation

[8] On the issues forming the subject of this work, we shall limit ourselves for the moment to recalling a number of works of Italian scholarship: A. STIANO, *Il cyberspazio nel diritto internazionale contemporaneo: tra frammentazione e patrimonio comune dell'umanità*, in *La Comunità Internazionale*, 2018, 673 ff.; G.M. FARNELLI, *Il contributo delle Nazioni Unite allo sviluppo dell'*International Cybersecurity Law, in Osorin Working Paper 1-2020 (www.osorin.it); A. SARDU, *L'*international cybersecurity law*: lo stato dell'arte*, in *La Comunità Internazionale*, 2020, 5 ff.; M.C. VITUCCI, *Le ciberoperazioni e il diritto internazionale, con alcune considerazioni sul conflitto ibrido russo-ucraino*, in ivi, 2023, 7 ff.; A.L. SCIACOVELLI, *International Law Aspects of Information Warfare in Digital Age*, ivi, 2023, 197 ff.

[9] See UN Doc. A/RES/53/70 adopted by consensus on December 4, 1998. V. I BRUNNER, *1998: UNGA Resolution 53/70 'Developments in the Field of Information and Telecommunications in the Context of International Security' and Its Influence on the International Rule of Law in Cyberspace*, April 20, 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3856900.

for this purpose; the concern expressed about the potential use of ICT against the security of states and international stability; and the affirmation of the need to prevent the abuse and exploitation of ICT for criminal or terrorist purposes.

In the brief operative part of the resolution, the General Assembly first asked Member states to commit to promoting the assessment of existing potential threats in the field of information security at a multilateral level. Secondly, Member states were invited to submit to the Secretary-General their views and assessments on a series of issues, including the opportunity to develop international principles aimed at strengthening the security of global information and telecommunications systems and assisting in combating terrorism and crime.

The resolution concluded by recommending that the issue remain on the First Committee's agenda in subsequent sessions of the General Assembly. Based on this resolution, a Group of Governmental Experts (GGE) was established to study the impact of ICT on international security.

3. The concrete result of Resolution 53/70 was the General Assembly's continuous attention to the issue[10] and the establishment in 2004 of the "United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security" (UNGGE or simply GGE) through Resolution 58/32. The resolution characterized the GGE as a working group of government experts in cybersecurity appointed by the Secretary-General based on equitable geographical distribution. Its task was to examine international concepts relevant to strengthening the security of global information and telecommunications systems, thereby contributing to identifying appropriate measures to address the growing use of ICT by states for political, military, and intelligence purposes.

From 2004 onwards, several GGEs with biennial mandates and varying compositions of 15 and 25 members were established by the General Assembly. These have focused on a comprehensive examination of current and potential threats from cyberspace and on various forms of international cooperation to address them. However,

[10] See UN Docs A/RES/54/49 dated December 1, 1999, A/RES/55/28 dated November 20, 2000, A/RES/56/19 dated November 29, 2001, A/RES/57/53 dated November 22, 2002.

the work of different GGEs has not always yielded positive results, especially as regards defining the international regulatory framework applicable to state activities in cyberspace[11].

To obtain a precise indication of the outcomes of this activity, attention will focus on the 2012-2013, 2014-2015, and 2016-2017 GGEs, as they well illustrate the trend of the debate that has developed among government experts regarding the application of existing international law in cyberspace.

The 2012-2013 GGE was established by the General Assembly in 2011 and concluded its work by adopting a report by consensus[12]. This report highlighted the importance that Member states attribute to strengthening cooperation against the threats posed by the malicious use of ICT and the need to adopt measures to reinforce international peace, stability, and security. A common vision of the norms, rules, and principles of international law applicable to state behavior in cyberspace was considered an essential part of such cooperative measures[13].

Regarding this specific aspect, the report mentioned that international law, particularly the UN Charter, is applicable in cyberspace and that this is essential for maintaining peace and stability and promoting an open, secure, peaceful, and accessible ICT environment[14]. The responsible behaviour of states in cyberspace is also linked to the principle of sovereignty and the international rules deriving from it, as well as respect for the rights and fundamental freedoms as established in the Universal Declaration of Human Rights and other international instruments, which must be applied in ICT-related activities[15].

Moreover, the report recommended that states intensify cooperation against the criminal and terrorist use of ICT, including through harmonizing measures and practical collaboration between police forces and judicial structures[16]; that they respect international

[11] For an overview of the activities of the GGEs, see UNODA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, July 2019, available online at www.disarmament.unoda.org/ict-security/.

[12] The 2012/2013 GGE was established by the General Assembly with Resolution 66/24, adopted by consensus on December 2, 2011, UN Doc. A/RES/66/24. For the final report, see UN Doc. A/68/98 of June 7, 2013.

[13] See the final report cited in the previous note, para. 11.

[14] *Ibid.*, para 19.

[15] *Ibid.*, paras 20-21.

[16] *Ibid.*, para 22.

obligations regarding responsibility for wrongful acts and not delegate the commission of such acts; and that they ensure their territory is not used by non-state actors for malicious activities in cyberspace.

The recommendations of the 2012/2013 GGE are highly significant, as it was the first time a group of government experts at the UN level from major powers or states with particular interests in ICT reached a consensus on the applicability of existing international law to cyberspace[17], thus marking a significant step towards a universally accepted normative framework to make ICT use an element of international peace and stability. This explains the enthusiasm with which the report was received both diplomatically and academically[18].

However, without diminishing the importance of the achieved result, the same report contained at least two elements that called for caution. The first was the reference to the need for further examination to reach a common understanding of the conditions for applying international law to state behaviour in ICT use. Furthermore, given the peculiar characteristics of ICT, it did not exclude the need to develop new rules over time. The second concerned the reference to the "International Code of Conduct for Information Security" project presented to the General Assembly by representatives of China, Russia, Tajikistan, Uzbekistan, later joined by Kazakhstan and Kyrgyzstan, whose scrutiny raises legitimate doubts about the willingness of these states to consider the existing international law applicable to ICT despite references to the UN Charter and its principles[19].

The 2014-2015 GGE[20] saw a positive and constructive dialogue among the twenty participating government experts regarding the international legal rules applicable in cyberspace. Indeed, in the final report[21], approved by consensus, the obligations of states were articulated with greater clarity than in previous documents. The report

[17] *Ibid.*, paras 22-23.

[18] For the first aspect, see U.S. Department of State, Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues, Press Release, June 7, 2013, https://2009-2017.state.gov/r/pa/prs/ps/2013/06/210418.htm. For the second, see W. DETLEV, *The UN Takes a Big Step Forward on Cybersecurity*, in Arms Control Today, 43, September 2013, www.armscontrol.org.

[19] For the code of conduct project, see UN Doc. A/66/359 of September 12, 2011.

[20] The 2014-2015 GGE was created with Resolution 68/243 adopted by the General Assembly on December 27, 2013, by consensus, UN Doc. A/RES/68/243.

[21] See UN Doc. A/70/174 transmitted to the Secretary-General on June 26, 2015.

emphasized key principles such as sovereign equality, the peaceful settlement of disputes, the prohibition of the threat or use of force in international relations against the territorial integrity or political independence of any state and the requirement to act consistently with the purposes of the United Nations. It also highlighted the importance of respecting human rights and fundamental freedoms, as well as the principle of non-intervention in the internal affairs of other states.

A particularly notable point in the report is its discussion on the application of international law to the state use of ICT[22], marking progress compared to previous work. Among the noteworthy aspects is the report's assertion of state jurisdiction over all ICT infrastructures within their territory, thereby likely underscoring the particular responsibility of states to prevent malicious use of these technologies.

Also of particular interest is the emphasis the report places on "the inherent right of states to take measures consistent with international law and as recognized in the Charter"[23]. This language closely mirrors the Charter, particularly Article 51 which references "the inherent right of individual and collective self-defense". However, the report's general indications do not clarify whether the GGE ventured into the possibility of considering cyber-attacks as equivalent to "armed attack", which would justify the use of force in self-defense. The explicit call for further examination on this issue does however suggest a cautious approach[24].

The report's caution is also evident in its reference to international legal principles such as humanity, necessity, proportionality, and distinction, which are fundamental principles of international humanitarian law. Their mention is not accidental, given the increasing frequency of cyber operations in armed conflict contexts, often resulting in destructive effects on civilian infrastructure and significant human costs.

Regarding the application of international law to state use of ICT, two key aspects of the report stand out. The first concerns the obligation of states not to delegate the commission of wrongful acts in

[22] *Ibid.*, para. 28.

[23] *Ibid.*

[24] It is almost needless to emphasize how extremely problematic the application of the rules regarding the prohibition of the use of force and self-defense to cyberspace is, especially since the scope and content of these norms are subject to divergent opinions. For a general overview on these aspects, see P. GARGIULO, *Uso della forza (Diritto internazionale)*, in *Enciclopedia del Diritto*, *Annali*, V, Milano, 2012, 1376 ff.

cyberspace and to ensure that their territory is not used by non-state actors for such purposes. Second, the report addresses states' compliance with international obligations regarding responsibility for wrongful acts. However, it clarifies that activities launched or originating from a state's territory are insufficient to attribute these acts to that state. In other words, accusations of a state organizing or carrying out wrongful acts in cyberspace must be substantiated[25].

The positive trend in evaluating applicable international law in cyberspace was interrupted by the 2016-2017 GGE, established by the UN General Assembly in 2015[26]. Indeed, divergent opinions prevented consensus on the final report. The United States, through its expert Michele Markoff, stressed the need to establish an international legal framework addressing issues such as international humanitarian law, self-defense, state responsibility, and countermeasures to mitigate risk of conflicts arising from cyber incidents[27]. The U.S. expert also criticized the GGE's work noting that some state's reluctance to define this normative framework represented a step backward and could potentially hinder the peaceful settlement of disputes and conflict prevention in cyberspace.

The Cuban representative Miguel Rodríguez expressed concerns about some states' intention to transform cyberspace into a theater of military operations and legitimize unilateral use of force and sanctions in response to illicit ICT activities. He particularly cautioned against equating malicious ICT use with the concept of an armed attack under Article 51 of the UN Charter, as this could be used to justify self-defense in the event of cyber attacks[28].

It is reasonable to assume that the Cuban position was shared by Russia and China, as both states had explicitly taken similar positions

[25] The issue of state responsibility for cyber attacks is analyzed by D. MANDRIOLI, *Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati*, in *La Comunità Internazionale*, 2018, 473 ff. and more extensively by A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023.

[26] UN Doc. A/RES/70/237 adopted by the General Assembly by consensus on December 23, 2015.

[27] See Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Expert (GGE) on Developments in the Field of Information and Telecommunications in the context of International Security, in 2017-2021.state.gov/, June 23, 2017, available online.

[28] See Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, in justsecurity.org, June 23, 2017, available online.

in previous GGE exercises. Despite the progress made in various areas for defining the international regulatory framework applicable in cyberspace, the various GGE exercises show overall difficulties largely due to the opposition between proponents of concluding an international agreement on the matter—Russia, China, and Cuba—and opponents of such a proposal, namely Western countries led by the United States.

4. The emergence and crystallization of divergences among UN member states within the GGE also led to an "institutional" opposition. This refers to the fact that in 2018, two working groups were set up: the 2019-2021 GGE, composed of 25 experts appointed on the basis of equitable geographical distribution, and a new Open-Ended Working Group (OEWG). The former was established through a resolution proposed by the United States[29], while the latter was based on a resolution proposed by the Russian Federation[30]. Both groups had the same mandate: to study the application of international law to state use of ICT. However, the groups differed in composition: the former continued to be a restricted expert group, while the latter was open to all UN member states, aiming for a more democratic, inclusive, and transparent negotiation process. Nevertheless, support for the Russian initiative was rather limited as evidenced by the numerous votes against and abstentions which accompanied the resolution establishing the OEWG.

Developments in GGE negotiations did not introduce significant novelties compared to previous work. Nonetheless, to provide a comprehensive examination of the topics addressed here, it is useful to consider the work of the OEWG, especially on specific issues relating to the application of international law in the use of ICT as outlined in the 2022 report[31]. On this point, the document is rather disappointing as it primarily presents a non-exhaustive list of topics and proposals that received varying levels of support from states during the negotiations and requiring further examination. These topics and

[29] See UN Doc. A/RES/73/266 adopted on December 22, 2018, with 138 votes in favor, 12 against, and 16 abstentions. Those who voted against include China, Cuba, North Korea, Nicaragua, Russia, and Syria.

[30] See UN Doc. A/RES/73/27 adopted on December 5, 2018, with 119 votes in favour, 46 against, and 14 abstentions.

[31] UN Doc. A/77/275 distributed on August 8, 2022. This is the report prepared by the OEWG established by the General Assembly with Resolution 75/240, whose mandate covers the period 2021-2025.

proposals are essentially identical to those highlighted in the GGE's work. Notably, the report omits any reference to international humanitarian law, which, as noted, had been a highly contentious issue among GGE experts. Additionally, the report contains an invitation for member states to continue exchanging their views on how international law applies to ICT use.

The OEWG report's scant indications on applicable international law in cyberspace clearly testify the significant divergences characterizing the negotiation process, as evidenced by the explanatory statements made by states upon adopting the report[32]. These statements confirm the ongoing general disagreement among member states, divided between those who believe the entire current body of international law can address the threats posed by malicious cyber activities conducted or sponsored by states and those who argue that some areas of international law, particularly concerning international humanitarian law, do not apply to ICT use.

5. The Security Council has also explored the impact of cybersecurity on the maintenance of international peace and security[33]. It has addressed the role of ICT in informal meetings and broader discussions such as the ministerial-level debate, organized at the proposal of Poland in August 2019. Such debate focused on challenges to peace and security in the Middle East, in the context of which one of the questions put to the Member states was "How to counteract cyber threats, including threats to energy infrastructure, in terms of promoting cooperative mechanisms for deterring and responding to significant cyber incidents in the Middle East?"[34]. This allowed several member states to highlight the enormous challenge posed by cybersecurity, especially since the malicious use of cyber capabilities is a factor in destabilizing international relations and security.

A succession of serious cyberattacks has made evident the absence of international legislation governing this domain and

[32] See UN Doc. A/AC.292/2022/INF/4, September 7, 2022.

[33] In general on the topic see UNIDIR, *The United Nations, Cyberspace and International Peace and Security. Responding to Complexity in the 21st Century*, UNIDIR, 2017; E. TIKKA, N.N. SCHIA, *The Role of he Security Council in Cybersecurity. International Peace and Security in the Digital Age*, in *Routledge Handbook of International Cybersecurity*, edited by E. TIKKA, M. KERTTUNEN, Abingdon/New York, 2020, 354 ff.

[34] See the concept note prepared by the Permanent Representative of Poland, UN Doc. S/2019/643, August 6, 2019.

highlighted the urgent need for measures to hold perpetrators of cybercrime accountable, including by subjecting them to sanctions, in addition to making them fully responsible legally for such crimes[35]. Moreover, several speeches also pointed out the danger of cyberattacks against infrastructures as an obstacle to any attempt to establish a dialogue among key Middle Eastern actors[36].

The subsequent discussions among Council members regarding cyber threats took place according to the Arria-formula meetings.

As is known, the Arria-formula is a practice, initiated in 1992 by the then-President of the Security Council, the Venezuelan Ambassador Diego Arria, consisting of informal meetings of the Security Council convened by one or more member States in order to hear the views of individuals, organizations or institutions on issues within the Council's purview[37].

November 28, 2016, Spain and Senegal organized an Arria-formula meeting to discuss the challenges to international peace and security resulting from ICT use. The meeting highlighted the dangers of cyberattacks and the difficulties in countering them and identifying perpetrators for accountability.

In this context, member states were encouraged to develop national strategies to prevent cyberattacks and to strengthen international cooperation, including through partnerships with governments, businesses, regional and sub-regional organizations, and representative civil society organizations[38].

Another Arria-formula meeting took place in March 2017, this time focusing on "hybrid wars as a threat to international peace and security". Two aspects of this meeting, chaired by Ukraine, deserve to be highlighted. The first concerns the wide range of factors that were identified as characteristic of hybrid warfare: "advanced weapons system, cyberattacks, interference with political processes, quasi-military activities, systematic dissemination of propaganda domestically and internationally, secret intelligence operations and abuse and manipulation of available international instruments…used

[35] See the position expressed by the Representative of Qatar in UN Doc. S/PV.8600, August 20, 2019, pp. 43-44.

[36] See the speech of the Representative of Saudi Arabia, UN Doc. S/PV.8600, cit., p. 31.

[37] *UN Security Council Working Methods: Arria-formula meetings*, securitycouncilreport.org, posted December 16, 2020.

[38] *Open Arria-formula Meeting on Cybersecurity*, What's in Blue, securitycouncilreport.org, posted November 25, 2016.

to achieve political objectives"[39]. The second concerns the idea that hybrid warfare involves "actions designed to fall below military response thresholds to deny or de-legitimate a military response from the target"[40].

Between 2020 and 2021, the Security Council intensified its work on the peace and security aspects of cybersecurity.

On May 22, 2020, Estonia organized an Arria-formula meeting on "Cyber Stability, Conflict Prevention and Capacity Building". In line with the concept note prepared by Estonia, the meeting aimed "at raising awareness of cyber challenges in terms of international peace and security, and to allow for discussions on the global, regional and national policy mechanisms in place to mitigate cyberthreats and advance responsible state behaviour"[41]. The analysis of the indicated issues was conditioned by the fact that at the meeting Ukraina accused Russia of conducting "hybrid aggression" against it and called for the adoption of appropriate enforcement mechanisms to prosecute the organizers and perpetrators of cyberattacks. Russia, by contrast, did not participate in the debate and denounced in a statement that "an elite minority" of states was actively pursuing the goal of militarizing cyberspace and of exploiting any pretext to justify the adoption of unilateral measures, including the use of force[42].

On August 26, 2020, Indonesia organized an Arria-formula meeting on "Cyber-Attacks Against Critical Infrastructures". The concept note prepared by Indonesia underlined the importance assumed by ICT for the public and private sectors and the potential risks of its malicious use. According to the Indonesian document, the meeting was intended to highlight the vulnerability of critical infrastructures and the need to protect them from cyberattacks. In addition, it stressed the need to for improved international and national regulatory frameworks to ensure responsible state behaviour as regards the use of ICT[43]. At the meeting, several states recognized the applicability of international law to cyberspace in peacetime.

---

[39] *In Hindsight: the Security Council and Cyber Threats*, Securitycouncilreport.org, January 2020 Monthly Forecast, posted December 23, 2019.

[40] *Ibid.*

[41] For the Estonia's concept note see UN Doc. S/2020/389, May 12, 2020.

[42] *In Hindsight: The Security Council and Cyber Threats, an Update*, Securitycouncilreport.org, February 2022 Monthly Forecast, posted January 31, 2022.

[43] *Arria-formula Meeting on Cyber-Attacks Against Critical Infrastructures*, What's in Blue, securitycouncilreport.org, posted August 25, 2020.

However, significant disagreements emerged over the application of international norms of armed conflict[44].

The most recent Arria-formula meeting on cybersecurity issues took place on April 4, 2024. Organized by the Republic of Korea, with the support of Japan and the United States, the meeting addressed the "Evolving Cyber Threat Landscape and Its Implications for the Maintenance of International Peace and Security".

The concept note[45] prepared by the Republic of Korea, made reference to the evolution of the cyber threat landscape (the proliferation of ransomware, the misuse of cryptocurrency by malicious cyber actors, the rise of malicious non-State actors) and their implications for international peace and security.

The same document indicated the objectives of the meeting: to raise awareness among the Security Council members and other Member states on the current cyber threat landscape and their potential impact on global public and private sectors alike; to promote better understanding of the impact of various malicious cyber activities on international peace and security; to discuss and provide possible recommendations on enhancing the UN Security Council's pivotal role and comprehensive engagement in addressing the multifaceted nature of cyber threats.

During the meeting, several speakers highlighted the dangers arising from the emergence of new cyber threats and the evolution of existing ones. Furthermore, representatives of several states expressed concern about the use of cyber tools by criminals and terrorists.

Divergent views were expressed on the strengthening of the role of the Security Council in addressing cyber threats. In general, most of the representatives of the member states wanted the role of the Security Council to be strengthened, partly because of the relationship between cyber security and the Council's responsibility for maintaining international peace and security. However, Russia's dissent should be noted as it considered the discussion of cyber security issues in the Security Council to be a useless duplication of efforts conducted in other UN bodies.

---

[44] *In Hindsight: The Security Council and Cyber Threats, an Update*, cit.

[45] See *Arria-formula Meeting on Cyber Security*, *Evolving Cyber Threat Landscape and Its Implications for the Maintenance of International Peace and Security*, www.securitycouncilreport.org.

6. In recent years, the UN has significantly increased its activity in the field of cybersecurity. However, as has already been noted in the past[46], the Organization's activities are very fragmented considering that the matter is addressed in the context of different bodies, agencies and programs due to the specificity of the topics covered (terrorism, disarmament, crime, human rights, etc.).

In this paper we have been mainly concerned with the activities of the General Assembly and the Security Council regarding cybersecurity due to their close link with the maintenance of international peace and security.

The analysis carried out above allows us to make some concluding remarks.

The first concerns the division that still exists between member states on the international regulatory framework applicable in cyberspace. The deepest divergences, especially between the leading states of the international system, concern the application of the rules relating to the use of force, self-defense and international humanitarian law. In addition, several Member states would like to see more detailed application of state responsibility regime, especially with regard to malicious activities by non-state actors in cyberspace.

Second, these global divergences contribute to the fragmentation of the cybersecurity regulatory framework considering the development of increasingly concrete forms of cooperation between States on a regional level. On the other hand, the hoped-for integration of universal and regional efforts, as mentioned in General Assembly resolutions and especially in the working group documents reviewed above, does not seem to us to be occurring.

The fact that UN member states consistently recognize the need to establish an international regulatory framework as a fundamental element of their cooperation in the matter, in our opinion, is not sufficient to give the negotiation process the necessary impetus to achieve concrete results within a reasonable period of time. Especially in the current international context in which confrontation and hegemonic aims prevail over dialogue.

[46] T. MAURER, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?*, Discussion Paper 2011-11, Cambridge, Mass., Belfer Center for Science and International Affairs, Harvard Kennedy School, 47.

THE COUNCIL OF EUROPE'S ACTIONS IN THE FIELD OF CYBERSECURITY*

IVAN INGRAVALLO**, ELENA DRAGO***

SUMMARY: 1. Introduction. – 2. The Budapest Convention on Cybercrime and its Second Protocol of 2022, concerning enhanced cooperation and the disclosure of electronic evidence. – 3. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its 2018 Updating Protocol. – 4. Other cybersecurity initiatives within the Council of Europe.

1. The Council of Europe is the oldest regional organization in Europe, established by the Treaty of London on May 5, 1949 (in force since August 3 of the same year). Its main objective is the protection of human rights and democracy[1], which has given it a significant role not only during the Cold War, but especially in facilitating the transition of many European states, during the Cold War (i.e. Portugal and Spain), but especially at its end. Since the late 1980s, all Central and Eastern European states (except for Belarus) have joined the organization, bringing the Council of Europe's membership to 47 member states, which decreased to 46 after Russia's withdrawal following the military intervention in Ukraine that began on February 24, 2022[2].

The structure of the organization in Strasbourg follows a peculiar model of international organization, where the Secretariat and the collegial body composed of States (the Committee of Ministers) are accompanied by the Parliamentary Assembly (originally called the Consultative Assembly), which includes delegations of national

* The chapter was prepared together by the two authors. Ivan Ingravallo is responsible for paragraphs 1 and 3, and Elena Drago for paragraphs 2 and 4.

[1] According to Article 3 of its Statute: «Every member of the Council of Europe must accept the principles of the rule of law and of the enjoyment by all persons within its jurisdiction of human rights and fundamental freedoms».

[2] There is a debate whether this occurred following Russia's withdrawal (Article 7 of the Statute) or its expulsion from the organization decided by the Committee of Ministers (Article 8 of the Statute) following the Russian military intervention in Ukraine. On this topic, see the contributions of G. RAIMONDI, *Il Consiglio d'Europa e gli effetti giuridico-istituzionali della guerra in Ucraina sul sistema convenzionale*, in *Freedom, security & justice*, 2022, n. 2, 124 et seq.; A. SACCUCCI, *Le conseguenze dell'espulsione della Russia dal Consiglio d'Europa sui trattati stipulati nell'ambito dell'organizzazione*, in *Diritti umani e diritto internazionale*, 2022, 211 et seq.; C. ZANGHÌ, *La Federazione Russa al Consiglio d'Europa: dall'ammissione alla perdita dello status di membro*, in *I diritti dell'uomo, cronache e battaglie*, 2022, 311 et seq.

parliamentarians. This choice is in line with the organization's objectives, but particularly significant considering the time it was established[3]. It is also worth noting the presence of the so-called Venice Commission (European Commission for Democracy through Law), an independent advisory body established in 1990 by the Committee of Ministers[4].

Over its more than seventy years of activity, the Council of Europe has successfully pursued its objectives, establishing itself as one of the main actors in the gradual expansion of international human rights protection, which – as widely known – represents one of the defining features of contemporary international law. Through various legal instruments of different types and value (acts of secondary law, international conventions and protocols, jurisprudence of the control bodies provided for in some of them, etc.), it has contributed to the emergence and regulation of new human rights, favoring the evolution of this distinctive branch of international law[5].

The most well-known and important treaties (also for the control mechanisms associated with them) concluded within this organization are the European Convention on Human Rights and the European Social Charter. However, the role it has played in advancing the protection of human rights should not be underestimated, for it was a forerunner. Without any claim of completeness, in order to highlight the diversity and versatility of the Council of Europe's actions, we point out, among the over two hundred treaties concluded within the organization, those on medical and social assistance (1953), adoption of children (1967, revised in 2008), legal status of children born out of wedlock (1975), protection of archaeological heritage (1969, revised in 1992), protection of animals in farming (1976), legal status of migrant workers (1977), compensation for victims of violent crimes (1983), anti-doping (1989), human rights and biomedicine (1997), landscape (2000), prevention and combating violence against women

[3] See M. UDINA, *Lineamenti del Consiglio d'Europa*, in *Rivista di studi politici internazionali*, 1956, 549 et seq.

[4] The Statute of the Venice Commission, originally approved by the Committee of Ministers with Resolution Res(90)6 of 10 May 1990, concerning a Partial Agreement, was replaced by Resolution Res(2002)3 of 21 February 2002, concerning an Enlarged Agreement, which currently involves 61 members, extending well beyond the membership of the Council of Europe. See V. VOLPE, *Commissione Europea per la Democrazia attraverso il Diritto*, in *Digesto delle discipline pubblicistiche*, Aggiornamento, 2017, 182 et seq.

[5] See A. SACCUCCI, *Profili di tutela dei diritti umani. Tra Nazioni Unite e Consiglio d'Europa*, Padua, 2002; F. BENOIT-ROHMER, H. KLEBES, *Council of Europe Law: Towards a pan-European Legal Area*, Strasbourg, 2005.

and domestic violence (2011), trafficking in human organs (2015), as well as the Charter of Local Self-Government (1985) and the Charter for Regional or Minority Languages (1992) and the Framework Convention for the Protection of National Minorities (1995).

As mentioned, in addition to numerous treaties, the Council of Europe has adopted many acts, which have the character of soft law but are nevertheless relevant to express the will of the organization and its member states, as a first step towards the subsequent negotiation and conclusion of international agreements and contributing to the formation of international customs (and European regional customs).

2. This is the context in which the Council of Europe's actions in the field of cybersecurity are inserted, which have two main profiles: combating cybercrime and protecting individuals regarding the automated processing of personal data.

Under the first profile, the organization in Strasbourg began to deal with cybercrime as a criminal law issue as early as the 1980s, starting with the promulgation of two recommendations, relating to cybercrime and criminal procedural law related to information technology[6]. In the mid-1990s, with the consolidation of new technologies, which also led to their malicious use, the Committee of Ministers decided to establish the Committee of Experts on Cybercrime (PC-CY), responsible for drafting an agreement on cybercrime. The resulting Convention, concluded in Budapest on November 23, 2001, and entered into force on July 1, 2004, is supported by a specific Committee (T-CY), which represents the 69 contracting parties[7] and ensures its implementation through assessments, guidelines, and other means, and by the capacity-building programs managed and coordinated since 2014 by the

[6] Recommendation R(89)9 on cybercrime and related criminal law was adopted by the Committee of Ministers of the Council of Europe on September 13, 1989, while the second recommendation, R(95)13, concerning issues of criminal procedural law related to information technology, was adopted on September 11, 1995. Both are based on Article 15(b), of the Statute of the Strasbourg organization, which states: 'In appropriate cases, the conclusions of the Committee may take the form of recommendations to the governments of members, and the Committee may request the governments of members to inform it of the action taken by them with regard to such recommendations'.

[7] The Convention has been ratified by 45 member states of the Council of Europe (with the exception of Ireland) and is also open to third states. Among these, which have joined in significant numbers, we recall Argentina, Australia, Brazil, Canada, Japan, Nigeria, and the USA.

Council of Europe's Cybercrime Program Office (C-PROC), based in Bucharest, which are fundamental to assist the different countries involved[8].

The adoption of this Convention has constituted a fundamental step in addressing cybercrime, facilitating international cooperation among member states in investigations and criminal actions against cybercrimes. In summary, it aims to harmonize elements of criminal law in the context of cybercrime, making punishable behaviors such as unauthorized access, attacks on the integrity of a system, computer fraud, and child pornography, creating necessary criminal procedures to investigate and punish attacks on information systems and other cybercrimes, while implementing procedural law tools to conduct investigations and acquire reliable electronic evidence regarding various types of crimes, and to promote a regime of rapid and effective international cooperation[9].

The role of the Committee on the Convention (T-CY), composed of representatives of the contracting Parties, is to carry out assessments regarding its implementation. These aim to improve the practical application of the Convention by identifying good practices and resolving any issues encountered. Furthermore, it commits to promoting the Budapest Convention by encouraging the accession of states that are not members of the Council of Europe and promotes training and capacity building in the field of cybercrime and electronic evidence[10].

The Council of Europe's strategy to promote cybersecurity and combat cybercrime is divided into three main pillars: the definition of common norms and standards, constant monitoring of the implementation of these norms, and investment in capacity building programs.

Under the first aspect, the contracting states of the Budapest Convention commit to adopting common rules and protocols in the

[8] On this subject, see R. MAZZA, *Recenti sviluppi nella repressione internazionale dei crimini informatici: la Convenzione di Budapest del 2001*, in *La Comunità Internazionale*, 2004, 91 et seq.; C. SCHULMAN, A. SEGER, *Convention on Cybercrime, Special edition dedicated to the drafters of the Convention (1997-2001)*, Council of Europe, March 2022, available online; and the special issue of *Diritto penale e processo*, 2022, No. 8, devoted to the *20° anniversario della Convenzione di Budapest*.

[9] European Commission, Questions and Answers: Mandate for the Second Additional Protocol to the Budapest Convention, February 5, 2019, https://ec.europa.eu/commission/presscorner/detail/it/MEMO_19_865.

[10] Cybercrime Convention Committee (T-CY), T-CY Rules of Procedure as revised by T-CY on October 16, 2020: https://rm.coe.int/t-cy-rules-of-procedure/1680a00f34.

field of cybersecurity, to establish a uniform basis for addressing challenges related to data protection and the prevention of cybercrime, and to facilitate international cooperation. As for monitoring and evaluation, the role of the aforementioned T-CY Committee is relevant, as it closely monitors the implementation of the agreed measures in the Convention. It is a follow-up mechanism that plays an essential role in ensuring that the participating states maintain the agreed standards over time and constantly commit to enhancing cybersecurity. Finally, the third pillar focuses on capacity building through programs and initiatives aimed at improving skills and resources available to strengthen cybersecurity in the involved states. The C-PROC ensures that all contracting parties have the necessary knowledge and resources to address cyber threats effectively and promptly[11].

In 2024, the 20th anniversary of the entry into force of the Budapest Convention will be celebrated, marking a significant advance in international cooperation. However, it should be noted that not all member states have signed the Convention. Russia, for example, has argued that it threatens fundamental principles such as state sovereignty and non-interference[12]. At the same time, it passed a resolution on cybercrime in the United Nations Legal Affairs Committee: the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communication Technologies for Criminal Purposes[13]. It is tasked with drafting a draft Convention by February 2024, so that it can be examined by the United Nations General Assembly during its 78th session in September 2024.

Concern has been expressed by multiple parties that the new proposed tool on cybercrime could pave the way for a potential replacement of the Budapest Convention[14]. Furthermore, as noted in the negotiations on cybersecurity in the United Nations' Open-ended Working Group on Information and Communications Technology (OEWG), when there are divergent interpretations on the definition of

[11] *Why and how is the Council of Europe working against cybercrime?*; https://www.coe.int/en/web/cybercrime.

[12] I. WILKINSON, *What is the UN cybercrime treaty and why does it matter?*, Chatham House, The Royal Institute of International Affairs, 2023, https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.

[13] V. https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

[14] D. BROWN, *Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights*, Human Rights Watch, August 2021.

cybercrime and preferences regarding the most appropriate rules, the proposal of new legislative instruments offers the possibility to implement the proposed vision more effectively and targeted[15].

Similarly, the central role of the Council of Europe regarding cyber capacity building projects could be overshadowed by the activities of the International Telecommunication Union (ITU), which seems to be the preferred organization by Russia and China to promote their vision of centralized internet governance and security[16].

The described framework make it clear the context that led to the elaboration of the Second Additional Protocol to the Budapest Convention [17], on strengthening the sharing of electronic evidence, concluded in 2022 and not yet in force[18]. It aims to extend judicial cooperation to direct relations with digital service providers (see Articles 6 and 7 of the Protocol)[19], increasing the tools available to national judicial authorities. Consider the new provisions on videoconferencing and joint investigative teams, for which Articles 11 and 12 of the Protocol establish the regulatory framework, applicable in the absence of other specific provisions between the operating authorities[20].

In order to reconstruct relevant behaviors from a criminal point of view, judicial and police authorities must acquire information and

---

[15] E. DRAGO, *Cybersecurity Governance. Comment on the 2021 Final Document of the OEWG*, in *Osservatorio sulle attività delle organizzazioni internazionali e sovranazionali, universali e regionali, sui temi di interesse della politica estera italiana*, May 2021, https://www.osorin.it/uploads/model_4/.files/75_item_2.pdf?v=1622104401.

[16] These countries have indeed managed to place national experts in leadership positions within the ITU. L. BERTUZZI, *China, Russia prepare new push for state-controlled internet*, EURACTIVE, February 2022.

[17] The First Additional Protocol to the Budapest Convention, concerning the criminalization of racist and xenophobic acts committed through information systems, concluded in Strasbourg on January 28, 2003, entered into force on March 1, 2006. As of June 18, 2024, it has been ratified by 35 states, including non-members of the Council of Europe. Italy has signed it in 2011, but not ratified it.

[18] The Second Additional Protocol, like the Budapest Convention, is also open to non-member states of the Council of Europe; it was concluded in Strasbourg on May 12, 2022, and as of June 18, 2024, it has been signed by 44 states (including Italy) but ratified only by Serbia and Japan. At least five ratifications are required for it to enter into force. See G.M. RUOTOLO, *Il Secondo Protocollo alla Convenzione "cybercrime" sulle prove elettroniche tra diritto internazionale e relazioni esterne dell'Unione europea*, in *Diritto penale e processo*, 2022, 1022 et seq.

[19] Article 6 is titled 'Request for domain name registration information', Article 7 'Disclosure of subscriber information'.

[20] F. SPIEZIA, *International cooperation and protection of victims in cyberspace: Welcoming Protocol II to the Budapest Convention on Cybercrime*, in *ERA Forum*, 2022, 101 et seq.

digital data often stored on servers or computers located in different states from those of belonging. Indeed, due to the extraterritorial nature of the internet, electronic data usable as evidence is often of a transnational nature, as they are not tied to the territory where the crime was committed, or the investigation is ongoing. Therefore, law enforcement authorities must obtain digital evidence from private entities bound by a set of rules different from those of the country in which they are established[21]. Since the powers of law enforcement are limited by the boundaries of territorial sovereignty, only a small percentage of reported cybercrime cases result in criminal proceedings or court decisions.

The Second Protocol has also facilitated the strengthening of the ongoing regulatory process in the European Union regarding access to digital evidence, which for a prolonged period had not been adequately addressed at the EU level[22].

One of the main criticisms of the Second Protocol to the Budapest Convention concerns the lack of adequate privacy protection standards (and other human rights such as freedom of expression), proportionate to the increase in procedural powers for the search and seizure of computer data, the possibility of investigating cybercrimes outside one's own State, and receiving mutual assistance in cross-border investigations.

Indeed, Article 14 of the Protocol includes provisions for the protection of personal data, particularly regarding their processing and security[23]. However, it has been noted that such safeguards can be eliminated through mutual agreement between two States parties. Furthermore, Article 14 does not require independent supervision of

[21] *Ibidem*.

[22] On July 12, 2023, a regulation, and a directive on cross-border access to electronic evidence (e-evidence) were approved. The first is Regulation (EU) 2023/1543 of the European Parliament and of the Council, regarding European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. The second is Directive (EU) 2023/1544 of the European Parliament and of the Council, which establishes harmonized rules on the designation of designated facilities and the appointment of legal representatives for the purpose of collecting electronic evidence in criminal proceedings. More information can be found here: https://commission.europa.eu/law/cross-border-cases/judicial-cooperation/types-judicial-cooperation/e-evidence-cross-border-access-electronic-evidence_en.

[23] In particular: purpose and use, quality and integrity, sensitive data, retention periods, automated decisions, data security and security incidents, record keeping, internal sharing within a Party, subsequent transfer to another State or international organization, transparency and notification, access and rectification, and judicial and non-judicial remedies.

law enforcement activities and prohibits additional safeguards in the use of biometric information. The result is to expand the powers of law enforcement without simultaneously providing sufficient protection of human rights[24].

In the absence of adequate security standards, digital evidence could be vulnerable to security breaches, compromising the privacy of the data involved. On the other hand, expecting such data to be removed from a system after being entered would create a cumbersome and difficult process[25]. It is important to emphasize that even the most secure system is limited when digital evidence is shared among states with different regulations on privacy protection. Greater alignment of internal regulations in this matter is essential to ensure the effective implementation of such systems[26].

3. As mentioned, another significant action of the Council of Europe in the field of cybersecurity concerns the 1981 Convention on the Protection of Individuals regarding Automatic Processing of Personal Data[27], amended in 2018. The Amendment Protocol, concluded on October 10, 2018, has not yet entered into force, but it is reasonable to expect that it will do so during 2024[28].

---

[24] Article 19's briefing, *The Council of Europe Convention on Cybercrime and the First and Second Additional Protocol*, https://www.article19.org/wp-content/uploads/2022/06/Budapest-Convention-analysis-May-2022.pdf.

[25] M. ARENA, *La Convenzione di Budapest del Consiglio d' Europa sulla repressione della criminalità informatica*, CRIO Papers A Student-Led Interdisciplinary Paper Series. The School of Laws University of Catania, 2021: https://www.lex.unict.it/sites/default/files/crio/papers/CRIO_Papers_n59_Arena.pdf.

[26] In this regard, it is worth mentioning that within the Council of Europe, the "Octopus Conference" on cybercrime took place from November 17th to 19th, 2021, and was proposed in an expanded version for the Western Balkans in the context of the Lightning Talks of the Octopus Conference in 2023. One of the main objectives of this innovative project is to facilitate the sharing of digital evidence through a blockchain mechanism to ensure efficiency and respect for privacy. See LOCARD – Lawful evidence collecting and continuity platform development. More information can be found here: https://rm.coe.int/lt-1-10-pablo-lopez-aguilar-locard-lightning-talks/1680a4968d.

[27] The Convention, concluded in Strasbourg on January 28, 1981, entered into force on October 1, 1985. As of June 18, 2024, it binds all 46 member states of the Council of Europe and 9 non-member states, including Argentina, Mexico, Russia, and Senegal. With an amendment approved by the Committee of Ministers of the Council of Europe on June 15, 1999, under Article 21 of the Convention, was also provided the possibility of accession to the same by the European Communities (now the European Union).

[28] The Protocol, in accordance with its Article 37, will enter into force once ratified by the 55 contracting States of the 1981 Convention or, after October 11, 2023, when at least 38 of them have ratified it. As of June 18, 2024, it received 31 ratifications (including Italy's).

The 1981 Convention was a precursor in extending the right to privacy in the face of the intensification of automated data flows, as well as in reconciling this right with freedom of information[29]. The 2018 Protocol pays specific attention to the protection of personal data, considering the diversification, intensification, and globalization of the processing and flows of this data[30].

According to Article 2(a) of the Convention personal data is defined as 'any information relating to an identified or identifiable natural person', while the 2018 Protocol adds a definition of data processing, referring to 'any operation or set of operations performed on personal data, such as collection, recording, storage, alteration, extraction, communication, provision, erasure or destruction of data, or the carrying out of logical and/or arithmetic operations on such data'.

In the original version of the Convention, Article 5 clarifies that personal data subject to automated processing must be obtained and processed fairly and lawfully, recorded for specified and legitimate purposes, and not used in a manner incompatible with those purposes, adequate, relevant and not excessive in relation to the same purposes, and kept in a form that allows the identification of the individuals concerned for a period not exceeding that necessary for the purposes for which they are recorded.

The updated version of the 2018 Protocol includes a clear reference to the fact that data processing must be proportionate to the legitimate purpose pursued and reflect a fair balance between all the interests involved, both public and private, and the rights and freedoms at stake (para. 1) and commits the Contracting Parties to provide that data processing may be carried out 'only on the basis of the data subject's free, specific, informed and unambiguous consent or on the basis of other legitimate grounds provided for by law' (para. 2). The requirements for collection, processing and use are better specified and articulated compared to the 1981 Convention. Taking

[29] See V. FROSINI, *La Convenzione europea sulla protezione dei dati*, in *Rivista di diritto europeo*, 1984, 3 et seq. On November 8, 2001, an Additional Protocol to the Convention was concluded, concerning the establishment of national authorities responsible for supervising its implementation, as well as the regulation of cross-border data flows to third countries, which entered into force on July 1, 2004, and was ratified by 44 States (Italy not included).

[30] Also noteworthy is the Explanatory Report on the Protocol, which clarifies its context and content and – as recognized in it (par. 6) – 'forms part of the context in which the meaning of certain terms used in the Convention is to be ascertained' in accordance with Article 31 of the 1969 Vienna Convention on the Law of Treaties.

into account the enormous technological developments that have occurred, it is indeed stated that personal data subject to processing must be 'processed fairly and transparently; collected for explicit, specified and legitimate purposes, and processed in a manner compatible with those purposes; further processing of personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or for statistical purposes is compatible with those purposes provided that additional safeguards are applied; adequate, relevant and not excessive in relation to the purposes for which they are processed' (para. 4)[31].

The need to update conventional discipline in the sense of increased protection for individuals clearly emerges in the comparison between Article 8 of the 1981 Convention, dedicated to 'additional guarantees for the data subject', which, following the 2018 Protocol, becomes Article 9, much more articulated and appropriately titled 'Rights of the data subjects', complemented by the inclusion of a new Article 10, which obliges the Contracting Parties to impose additional obligations on the data controller and, if necessary, on the data processor (para. 1), as well as, before any processing begins, 'the data controller and, if necessary, the data processor shall assess the potential impact on the rights and fundamental freedoms of the data subjects'. Article 18 of the Convention, as resulting from the 2018 Protocol, is also relevant, as it requires each Contracting Party to aid any data subject, regardless of their nationality or residence, for the exercise of their rights provided for in the aforementioned Article 9.

A very recent development is the adoption of the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, which will be open for signature in Vilnius on November 5, 2024.

4. The Conventions and Protocols we have focused on have not remained isolated within the context of the Strasbourg organization. In fact, they have been accompanied by numerous soft law documents (recommendations and declarations of the Committee of Ministers and the Parliamentary Assembly, guidelines of ad hoc committees, etc.) concerning specific issues of personal data protection. These are more flexible instruments compared to an international treaty and, also

[31] Transparency in data processing is also dedicated to the new Article 8 of the Convention, inserted by the 2018 Protocol.

because of that, they can address in real time the issues and risks posed by the rapid advancement of technological development in the field of information technology, including the recent emergence of Artificial Intelligence.

Among the most recent and relevant documents, we highlight the declaration of the Committee of Ministers adopted on February 13, 2019, on the manipulative capabilities of algorithmic processes, followed by the recommendation to the member states approved on April 8, 2020, on the impact of algorithmic systems on human rights, which includes specific guidelines[32]. The Committee of Ministers refers, inter alia, to the 1981 Convention, as updated by the 2018 Protocol. However, considering the continuous processes of technological advancement and digital transformation that European societies are experiencing, as well as the unprecedented rise in the use of digital applications as essential tools of everyday life, it states that the human rights impact of algorithmic systems are broader and call for additional protections compared to those governed by these two treaties.

Having regards to cybersecurity, the Council of Europe has progressively added an operational dimension to the legal tools that we have focused on. Among the numerous activities carried out, relevance is given to the strategy on Internet governance (2016-2019)[33] , as well as the various projects implemented by the Strasbourg organization since 2014 to enhance the cybercrime capabilities of its member states[34], for example by facilitating awareness programs, training, and support for the development of legal and technical skills in cybersecurity.

The Office of the Cybercrime Programme of the Council of Europe (C-PROC) is in Bucharest and is responsible for implementing and coordinating the various projects[35]. The currently active projects are: GLACY, CYBERSOUTH, IPROCEEDE, CyberEAST. These are joint projects between the European Union and the Council of Europe.

The countries involved in the GLACY (Global Action on Cybercrime) project are those in Africa, the Asia-Pacific region, and

[32] See Decl(13/02/2019)1 and CM/Rec(2020)1.

[33] This strategy has involved numerous organs and structures of the Council of Europe and has pursued three fundamental objectives: building online democracy; ensuring online protection and security for all; respecting and protecting the human rights of everyone in the digital world.

[34] C. SCHULMAN, A. SEGER, *op. cit.*

[35] Action against Cybercrime, Council of Europe: https://www.coe.int/en/web/cybercrime.

the Latin America and Caribbean region, including Benin, Brazil, Burkina Faso, Cape Verde, Chile, Colombia, Costa Rica, Dominican Republic, Fiji, Ghana, Mauritius, Morocco, Nigeria, Paraguay, Peru, Philippines, Senegal, Sri Lanka, East Timor, and Tonga. CYBERSOUTH focuses on the Southern Neighbourhood region, particularly Algeria, Jordan, Lebanon, Morocco, and Tunisia, while CyberEAST concerns Moldova, Armenia, Belarus, Georgia, Azerbaijan, and Ukraine.

The projects address the specificities of threats in different territorial contexts. For example, IPROCEEDS, which deals with the Western Balkans and Turkey, has provided in-depth training on investigations related to virtual currencies and the Darknet. It has emerged that, within the area considered by the project, only North Macedonia has a dedicated working group for monitoring and collecting information on illegal activities in the Darknet. On the other hand, Montenegro has limited investigative capabilities in cybercrime and digital forensics. Personnel from the new Special Public Prosecutor's Office of Serbia and the Department of Cybercrime of the Ministry of the Interior of Serbia have been trained. In Turkey, discussions have been held on the use of electronic evidence in criminal proceedings and the need to train prosecutors and judges in this field. In Bosnia and Herzegovina, the need to enhance interagency cooperation between prosecutors and law enforcement at the state, entity, and district levels has been highlighted.

Regarding this geographical area, particular emphasis has been placed on improving the relationship between cybersecurity and cybercrime. Most of the countries involved in the projects have completed the establishment or are in the process of expanding their Computer Incident Response Teams (CIRT). However, although CIRTs hold valuable data on incidents, crucial for law enforcement authorities in investigating and prosecuting cyber-attacks, the sharing of such information remains limited, making it difficult to assess the extent and trends of cybercrime and cybersecurity threats in this region, compromising the formulation of adequate strategies. To further enhance support in this region, consideration could be given to implementing measures aimed at increasing information sharing between CIRTs and law enforcement authorities.

CYBER-SECURITY IN SOUTHEAST ASIA: WHAT IS ASEAN DOING?

ELISA TINO

1. The Covid 19 pandemic has brought about a rapid change in our society. Indeed, it has forced to adopt rapid digitalization, and the migration of government, business and social activities online, in order to avoid the paralysis and subsequent collapse of the global economic and social system. Such digital transformation has thus resulted in an exponential growth of inter-state exchanges in cyber-space, which has inevitably been accompanied by an equally exponential growth in the risk of cyber-threats[1].

Actually, this problem is not at all new; in last decades, states with higher levels of digitalization have already experienced it and faced by adopting national laws and regulations governing the cyber-space[2]. However, the cross-border nature of cyber-threats have soon made it clear that individual state initiatives are inadequate and insufficient to prevent and efficiently manage them; the security of the cyber-space is a global problem, so it requires a choral and concerted effort. In particular, insomuch as the use and abuse of this complex, borderless and virtual space can impinge on economic development, public safety and even security across national borders in the physical world, the need to identify a set of norms to guide the behavior of states in cyber-space is felt to be imperative. These norms are deemed

[1] The term "cyber-threat" usually refers to a harmful activity committed with the intent of destroying, stealing, or disrupting data and digital life in general. In literature see M. DUNN-CAVELTY, *Cyber Threats*, in V. MAUER, M. DUNN-CAVELTY (eds.), *The Routledge Handbook of Security Studies,* New York, 2014, 180 ss.

[2] For an overview, see P. K. SINGH, *Laws on Cyber Crimes Alongwith IT Act and Relevant Rules*, Jaipur, 2007.

to be «an essential measure to reduce risks to international peace, security and stability»[3].

International efforts to identify them have been initially led by the Council of Europe, at regional level, and by the UN, at universal one. While the Council of Europe advocated for the conclusion of the first international treaty explicitly focusing on cyber-crime (the so-called Budapest Convention[4]), the UN activity concentrated around the work of two Groups tasked with examining the existing and potential threats from the use of information and communication technologies (ICT) by states, and the appropriate application of international law[5]. They are the United Nations Group of Governmental Experts (hereafter, UNGGE)[6] and the Open-Ended Working Group (hereafter, OEWG)[7].

---

[3] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98 of 24 June 2013, para. 16.

[4] The Convention on Cyber-Crime was signed in Budapest on November 23, 2001 (ETS No. 185) and it entered into force in 2004. It has currently been ratified by 75 states including non-member of the Council of Europe. It focuses on harmonizing laws and increasing cooperation across borders so that a range of cyber-crimes, such as a denial-of-service attack or the release of a computer virus, could be prosecuted in the multiple countries affected. Its legal content has been integrated by First Additional Protocol to the Convention on Cyber-Crime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189), and by Second Additional Protocol to the Cyber-Crime Convention on enhanced cooperation and disclosure of electronic evidence (CETS No. 224). The latter is not yet into force.

[5] The UN General Assembly placed cyber-security on its agenda in the late 1990s. See General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/Res/53/70 of 4 January 1999, where it recognized the benefits of scientific and technological advancement in information security, while noting its potential use for malicious purposes.

[6] In 2003 the UN General Assembly tasked the Secretary General with conducting a study about the security of global information and telecommunications systems, with the assistance of a Group of Governmental Experts (see General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/Res/58/32 of 18 December 2003). There were five Groups of Governmental Experts that examined the existing and potential threats from the use of ICTs by states, possible cooperative measures to address them, and the appropriate application of international law. The first UNGGE convened between 2004 and 2005, and a sixth round of negotiations concluded in 2021. Four rounds concluded with consensus reports, in 2010, 2013, 2015 and 2021.

[7] In December 2018 the UN General Assembly established the OEWG with the task to further develop rules and principles of responsible behavior of states and to consider initiatives of states aimed at ensuring security in the use of ICTs. It was also mandated to establish, under the UN auspices, regular institutional dialogue with the broad participation of states, and to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, and possible cooperative measures to prevent and counter such threats (see General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc.

After a start of work that did not live up to expectations[8], in its 2013 Report the UNGGE finally confirmed that «international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment»[9]. In its 2015 Report it went further: it demanded full respect for human rights (such as privacy, freedom of expression and free flow of information), and recommended a number of norms and guidelines outlining appropriate behavior of states in cyber-space[10]. They are eleven voluntary, non-binding norms that aim at promoting an open, secure, stable, accessible and peaceful ICT environment[11]; so, they do not replace or alter states' obligations or rights under international law – which are binding – but, rather, they provide additional and specific guidance on what constitutes responsible state behavior in the use of ICTs. These norms include interstate cooperation on security, due diligence, a commitment to not damage critical infrastructure and instead protect it, to respond to requests for assistance, to ensure supply chain security and to report ICT vulnerabilities[12].

The set of norms suggested by the 2015 UNGGE Report were then included in the 2021 final Report of the OEWG[13] and reiterated

---

A/Res/73/27 of 11 December 2018). The OEWG convened for the first time in 2019 and reported back to the General Assembly in 2020. In the same year, the General Assembly established a new five-year open-ended working group on security of and in the use of ICTs 2021–2025 (see General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/Res/75/240 of 4 January 2021).

[8] In its working in 2003-2004 and in 2016-2017, the UNGGE failed to achieve consensus and did not produce substantive reports.

[9] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/68/98 of 24 June 2013, para. 19.

[10] In particular, these norms were crafted to deal with state-to-state actions that could potentially carry the highest risks to international peace and security and the welfare of citizens. See UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc. A/70/174 of 22 July 2015.

[11] The purposes of this set of norms are to reduce risks to international peace and security, and to contribute to conflict prevention.

[12] It is worth noting that the eleven norms are part of a broader framework that also includes the recognition that international law applies to state conduct in cyber-space, a set of confidence-building measures and a commitment to coordinated capacity building. Those four components shape the UN framework of responsible state behavior in cyber-space.

[13] In particular, the OEWG, which worked in synergy with the GGE, reaffirmed the results of the GGE's previous reports, as well as that international law, and in particular the UN Charter, is applicable to cyber-space. Moreover, it recommended that states «further

by the new UNGGE established in 2019[14]. In particular, in its 2021 Report the latter offered an additional layer of understanding to help Governments with their implementation[15]. Moreover, while it reaffirmed the applicability of international law, and in particular the UN Charter, in its entirety to the ICT environment, it also noted the applicability of international humanitarian law in situations of armed conflict[16].

In identifying possible cooperative measures to address existing and potential threats in the sphere of information security and in elaborating the aforementioned set of norms, both the UNGGE and the OEWG were able to take advantage of valuable experiences emerging at the regional level. Indeed, in the last decade some regional organizations have proved to be relatively active in the field of cyber-security[17]; the Association of Southeast Asian Nations (hereafter, ASEAN) is among them[18].

According to statistical studies, more than half of the internet users in the world are in Asia[19], and in the last decade Southeast Asian

---

support the implementation and development of norms». See UN General Assembly, *Open-ended working group on developments in the field of information and telecommunications in the context of international security - Final Substantive Report*, UN Doc. A/AC.290/2021/CRP.2 of 10 March 2021.

[14] In 2019 the UN General Assembly mandated the Secretary-General to continue to study in order to promote common understandings and possible cooperative measures in the sphere of information security. For this purpose, it decided to establish another GGE advancing responsible state behavior in cyber-space in the context of international security. See UN General Assembly, *Advancing responsible State behaviour in cyber-space in the context of international security*, UN Doc. A/Res/73/266 of 2 January 2019.

[15] UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyber-space in the Context of International Security*, UN Doc. A/76/135 of 14 June 2021.

[16] Since 2019 many states (e.g. Germany, Italy, UK, Sweden, Ireland, Australia, Estonia, Finland, France, Israel, Iran, the Netherlands, New Zealand, the United States, etc.) have responded to the recommendations contained in the aforementioned Reports by transmitting to the UN their own position papers on the application of international law in cyber-space.

[17] Currently, a number of regional organizations and international fora are working on cyber-security issues. They include the Organization for Economic Cooperation and Development (OECD), the European Union (EU), the Council of Europe, the Organization of American States (OAS), the African Union (AU), as well as the G-7 and G-20, the NATO, the World Economic Forum, etc.

[18] So, it is not surprising that ASEAN member states participated in all the meetings of the UNGGE and the OEWG that have convened since 2004.

[19] See mainly C. H. HEINL, *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime,* in *Asia Policy*, 2014, 135; L. CHANG, *Cybercrime and Cyber Security in ASEAN*, in J. LIU, M. TEVOR, L. CHANG (eds), *Comparative Criminology in Asia*, New York, 2017, 2-3.

states have increasingly been the victims of cyber-attacks[20]. This explains why ASEAN, which counts both high-tech members (i.e. Singapore, Malayasia, Brunei Darussalam, Thailand and – somehow - the Philippines) and members having a lower level of digitalization (i.e. Myanmar, Cambogia, Laos, Indonesia, Vietnam)[21], have been dealing with cyber-crimes, cyber-threats and cyber-security since the early 2000s. This paper aims to shed the light on the ASEAN's efforts in this field. So, it will provide an overview of institutional and normative frameworks developed by the Organization over the years to address the challenges and problems of cyber-space[22], and it will assess whether and to what extent ASEAN has contributed to identify norms guiding states' behavior in cyber-space.

[20] For a brief report of cyber-attacks and accidents involving ASEAN member states in the last decade see B. Y. W. MANOPO, D. A. A. SARI, *ASEAN Regional Forum: Realizing Regional Cyber-Security in ASEAN Region*, in *Belli ac Pacis,* 2015, n. 1, 44-45; S. GOHWONG, *The Cyber-Attacks and Digital Economy in Malaysia during 1997-2016*, in *PSAKU International Journal of Interdisciplinary Research,* 2016, n. 2, 1-7; S. GOHWONG, *The Cyber-attacks in Vietnam during 2010-2016*, in *Asian Political Science Review*, 2017, n. 1, 51-55; ; L. CHANG, *op. cit.,* 3-6; S. GOHWONG, *The State of the Art of Cybersecurity Law in ASEAN*, in *International Journal of Crime, Law and Social Issues*, 2019, n. 2, 12. See also Interpol, ASEAN Cyber-threat Assessment 2020, https://asean.org/wp-content/uploads/2021/01/ASEAN_CyberThreatAssessment_2020.pdf; Interpol, ASEAN Cyber-threat Assessment 2021, https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

[21] About differences among ASEAN member states in dealing with cyber-security issues, see J. SUNKPHO, S. RAMJAN, C. OTTAMAKORN, *Cybersecurity Policy in ASEAN Countries* (2018), https://www.researchgate.net/publication/324106226; I. RAMADHAN, *Building Cybersecurity Regulation in Southeast Asia: A Challenge for the Association of Southeast Asian Nations (ASEAN),* in *Journal of Social and Political Sciences*, 983-985; K. ESTIYOVIONITA, A. SITAMALA, *ASEAN's Role in Cyber-Security Maintenance and Security Strategy through an International Security Approach,* in *Lampung Journal of Iternational Law*, 2022, 81-83.

[22] ASEAN approach to cyber-security has been mainly investigated in political perspective. In this sense see S. KHANISA, *A Secure Connection: Finding the Form of ASEAN Cyber Security Cooperation*, in *Journal of ASEAN Studies*, 2013, 41-53; C. H. HEINL, *op. cit.;* L. CHANG, *op. cit.;* C. TRAN DAI, M. A. GOMEZ, *Challenges and Opportunities for cyber Norms in ASEAN*, in *Journal of Cyber Policy*, 2018, 217-235; H. NASU et al., *The Legal Authority of ASEAN as a Security Institution*, Cambridge, 2019, 139-160; S. GOHWONG, *The State of the Art,* cit.; I RAMADHAN, *op. cit.;* K. ESTIYOVIONITA, A. SITAMALA, *op. cit.;* E. NOOR, *Positioning ASEAN in Cyberspace,* in *Asia Policy*, 2020, 107–114; X. CHEN, Y. YANG, *Different Shades of Norms: Comparing the Approaches of the EU and ASEAN to Cyber Governance*, in *The International Spectator*, 2022, n. 3, 48-65; J. DOSCH, *ASEAN's Governance and Management of Non-Traditional Security,* in J. DOSCH (ed.), *The Elgar Companion to ASEAN*, Chelterham, 2023, 93-107; K. L. TAY, *ASEAN Cyber-security Cooperation: Towards a Regional Emergency response Framework*, IISS Working Paper, June 2023, 1-27.

2. ASEAN is a regional organization comprising ten Southeast Asian states, namely Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam[23]. It was established in 1967 with the signing of the Bangkok Declaration[24], as a way to promote economic cooperation to manage conflicts in Southeast Asia, thus fostering peace and stability in the region[25], and it operated as *soft organization* for forty years[26]. Indeed, ASEAN had its legal foundation in a non-binding political document and originally made minimalism and informalism the hallmark of its organizational structure. Thus, common functions were carried out through a stable albeit not legally formalized apparatus of a predominantly inter-governmental nature[27] and the pursuit of statutory objectives relied primarily on soft law acts[28]. Overall, ASEAN's *modus operandi*

[23] About ASEAN see, *ex multis*, K. K. HOURN, D. MERICAN, *Peace & Cooperation in ASEAN*, London, 1997; H. DAVID, *Die ASEAN zwischen Konflikt, Kooperation und Integration*, Hamburg, 2003; C. B. ROBERTS, *ASEAN Regionalism*, London, 2003; P. C. SINHA (ed), *Handbook of ASEAN and Regional Cooperation. 12th Summit and Beyond*, New Delhi, 2007; E. L. FROST, *Asia's New Regionalism*, London, 2008; S. TIWARI (ed.), *ASEAN. Life after the Charter,* Singapore, 2010; O. VON FEIGENBLATT, *The Association of Southeast Asian Nations (ASEAN). Conflict and Development,* New Delhi, 2012; D. DESIERTO, D. COHEN (eds),
*ASEAN law and regional integration: governance and the rule of law in Southeast Asia's sing le market, A*bingdon/New York, 2021; L. JONES, *ASEAN, Sovereignty and Intervention in Southeast Asia,* New York, 2012; A. W. ZIE□TEK, G. GIL (eds), *ASEAN in a changing world*, Berlin, 2021; E. Y. JOONG LEE (ed.), *ASEAN international law*, Singapore, 2022; S. CHO, J. KURTZ, *Investing the ASEAN Way: Theories and Practices of Economic Integration in Southeast Asia,* Cambridge, 2023.

[24] *ASEAN Declaration*, Bangkok, 8 August 1967. The Bangkok Declaration was originally signed by Indonesia, Malaysia, Philippines, Singapore and Thailand in 1967, launching the start of ASEAN. Brunei joined in 1984, Vietnam in 1995, Laos and Myanmar in 1997, and Cambodia in 1999.

[25] The original five founders of ASEAN wanted to checkmate the spread of communism, bolster national sovereignty, and ensure that the numerous bilateral conflicts in the region were resolved peacefully.

[26] The expression "soft organization" usually refers to forms of association which are established and regulated by state manifestations of will expressed in political and diplomatic acts (that are not legally binding), and designed in such a way to favor less constraining options for the freedom of their member states. In literature see, among others, J. KLABBERS, *Institutional Ambivalence by Design. Soft Organization in International Law*, in *Nordic Journal of International Law*, 2001, 403; A. DI STASI, *About Soft International Organizations: An Open Question*, in R. VIRZO, I. INGRAVALLO (eds.), *Evolution in the Law of International Organizations,* Leiden, 2015, 44.

[27] The 1967 Bangkok Declaration did not endow the Organization with a permanent Secretariat which was then established in 1976 through the signing of an *ad hoc* international agreement. See Agreement on the Establishment of the ASEAN Secretariat (Bali, 24 February 1976).

[28] Over the years, ASEAN's regulatory production has primarily consisted of non-binding acts, which merely contain "commitments" of political content. In other words, instead of

consisted in building on small steps, voluntary, and informal arrangements towards more binding and institutionalized agreements. In their activities ASEAN and its member states were guided by the respect for the principle of sovereignty and its corollaries (e.g. independence, equality, territorial integrity, non-interference in the internal affairs, etc.) as contained in the Treaty of Amity and Cooperation in Southeast Asia[29]. So, in line with them, consensus was the privileged mode of decision-making. When member states failed to reach it, the use of the "ASEAN Minus X" mechanism was permitted. It allowed for flexible participation in cases where a member state was not yet ready to commit to a specific initiative or project[30]. Such organizational architecture and *modus operandi*, based on minimalism, informalism and flexibility, are usually referred to the expression *ASEAN Way*[31].

Actually, ASEAN remained faithful to this *Way* even when its member states decided to institutionalize their cooperation by adopting the ASEAN Charter[32]. Indeed, while making ASEAN a treaty-based organization, the entry into force of the Charter has not significantly changed its organizational architecture and *modus operandi*[33]. Since 2008, respect for state sovereignty, informalism, flexibility and consensus-based have continued to be ASEAN's

---

expressing a *voluntas obligandi*, these acts are expression of a *voluntas agendi* or *operandi.* Thus, ASEAN is regarded «an example of an organization assuming its use of soft law as a part of its legal policy». In this sense, see A. SCHIFANO, *Organizationhood in the Light of Asian Minimalism*, in *Chinese Journal of International Law*, 2023, 749.

[29] Treaty of Amity and Cooperation in Southeast Asia (Bali, 24 February 1976). It embodies universal principles of peaceful coexistence and friendly cooperation among states. It was amended three times, in 1987, 1998, and 2010 respectively, to allow for accession by states outside Southeast Asia, as well as for regional organizations whose members are sovereign states. As of July 2023, 51 states are parties to this Treaty.

[30] The "ASEAN minus X" mechanism was introduced in the 1980's and enables the Organization to overcome potential deadlocks on the road to progress in regionalization.

[31] See T. YUKAWA, *The ASEAN Way as a Symbol: An Analysis of Discourses on the ASEAN Norms*, in *The Pacific Review*, 2017, 1-17. It is worth noting that the distictive features of the *ASEAN Way* have been replicated in other Asian organizations. In this regard, see P. PENNETTA, *Il regionalismo multipolare asiatico,* Torino, 2003; A. SCHIFANO, *op. cit.*

[32] The 11th ASEAN Summit in 2005 adopted a resolution to formulate a Charter. On November 20, 2007, at the 13th ASEAN Summit, the draft Charter was formally adopted and passed on to the member states for ratification. It entered into force on December 15, 2008. The ASEAN Charter is the result of recognition by the member states that the Organization had matured to a point where it was ready for a higher level of cooperation.

[33] The 2007 Charter has institutionalized cooperation within ASEAN and consolidated its institutional existence. It has strengthened the ASEAN Secretariat, streamlined the decision-making, provided for permanent representatives posted to Jakarta and put in place a system of compliance monitoring and compulsory dispute settlement.

distinctive features[34]. Similarly, the goals it pursues remain effectively unchanged; indeed, ASEAN continues to promote regional peace and stability and to pursue the economic, social and cultural growth of the region. In other words, ASEAN remains a political and economic organization.

3. Neither (understandably) the 1967 Bangkok Declaration, nor the 2007 Charter expressly gives ASEAN jurisdiction over cyber-security issues[35]. However, they both confer upon it powers in security field. Indeed, pursuant to Article II of the Bangkok Declaration and Article 1 of the Charter, ASEAN aims to maintain peace and stability in the region, and it is therefore entitled to respond, in line with the UN Charter, to all forms of threats. Thus, ASEAN has ended up being (implicitly) responsible for cyber-security to the extent that peace and stability in the region are increasingly threatened by non-traditional threats, such as cyber-attacks. In other words, ASEAN's commitment to cyber-security has, albeit indirectly, its legal basis in the Organization's statutory acts.

The initial need for handling cyber-security issues arose from the broader economic imperative to strengthen the competitiveness of ASEAN's ICT sector. Since the early 2000s, ASEAN has set as its goal the deepening of connectivity in the region in order to promote the liberalization of trade in ICT products and services, the development of e-commerce and the strengthening of ICT infrastructure construction which, in turn, served as an enabler of socio-economic progress[36]. However, such economic growth and competitiveness needed not only connected but also secure information infrastructures[37]. Thus, cyber-security issues entered the

[34] See W. HUCK, *Informal International Law-Making in the ASEAN: Consensus, Informality and Accountability*, in *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht,* 2020, 101-138.

[35] Actually, neither the 1967 Bangkok Declaration nor the 2007 Charter explicitly provides for ASEAN's areas of competence, which can however be inferred from its objectives, as defined in Article II of the Bangkok Declaration and Article 1 of the ASEAN Charter.

[36] This objective materialized in the signing of the e-ASEAN Framework Agreement (Singapore, 24 November 2000), which is not yet into force. Then, ICT was listed among eleven priority sectors under the Framework Agreement for the Integration of Priority Sectors (Vientiane, 29 November 2004).

[37] See 3rd ASEAN Telecommunications and IT Ministers Meeting – Singapore Declaration (An Action Agenda) - 19 September 2003. See also Masterplan on ASEAN Connectivity: One Vision, One Identity, One Community ASEAN (Hanoi, 28 October 2010); ASEAN ICT Masterplan 2015 (Kuala Lumpur, 14 January 2011).

agenda of ASEAN's intergovernmental bodies[38] and soon became part of the overall plan to build a cohesive ASEAN Community based on three pillars comprising a political-security Community, an economic Community and a socio-cultural Community[39].

A quick reading of various blueprints and related non-binding documents approved by ASEAN Leaders over the years to build the foregoing Community highlights that cyber-security issues intersect with all three pillars. However, initially, these issues used to be treated as ancillary and incidental to the development of the three Communities, as reflected in the earliest official (non-binding) documents in which cyber-threats are mentioned[40]. Indeed, they offered no definition of "cyber-security" nor was any significance idea pointed out on how it would have been maintained. So, at an early stage, ASEAN decided not to develop a comprehensive regional strategy in this field; rather, its initial policy on cyber-security was based on the idea of securing cyber-space through the development of regional cooperation in the construction of resilient national systems. In particular, it urged member states to adopt domestic regulations[41],

[38] In particular, cyber-security issues were first addressed by ASEAN Telecommunication and IT Ministers Meetings and by ASEAN Ministerial Meetings on Transnational Crime. In 2004 the latter recognized cyber-crime as increasing transnational crime that affected ASEAN's security and urged for effective legal cooperation in combating it. Thus, the ASEAN Ministerial Meetings on Transnational Crime integrated cyber-crime among its eight priorities. See Joint Communiqué of the 4th ASEAN Ministerial Meeting on Transnational Crime (Bangkok, 8 January 2004).

[39] The decision to set up such a Community articulated in three pillars was agreed in the Declaration of ASEAN Concord II (Bali Concord II), which was endorsed at the 9th ASEAN Summit in 2003. It is worth noting that over the years, cyber-security issues have also been at the heart of ASEAN's external relations agenda. Thus, for instance, since 2009 Policy Meetings have been held annually among the ASEAN member states and Japan, with the purpose of enhancing international collaboration on this field (see, lastly, the 15th ASEAN-Japan Cybersecurity Policy Meeting, Tokyo, 4-5 October 2022). Similar meetings have been held with US since 2018 under the aegis of ASEAN-US Leaders' Statement on Cyber-security Cooperation (Singapore, 15 November 2018). See also ASEAN-EU Statement on Cyber-security Cooperation (Bangkok, 1 August 2019).

[40] See, for instance, Singapore Declaration (An Action Agenda), cit.; 2004-2010 Vientiane Action Programme (Vientiane, 29 November 2004); 2007 ASEAN Economic Community Blueprint (Singapore, 20 November 2007); 2009 ASEAN Political-Security Community Blueprint (Cha-Am, 1 March 2009); ASEAN Leaders' Statement on ASEAN Connectivity, (Hua Hin, 24 October 2009); 2010 Masterplan on ASEAN Connectivity, cit.; ASEAN ICT Masterplan 2015, cit.

[41] Over the years, most ASEAN member states have enacted legislation on electronic transactions and cyber-crime. Singapore was the first one; then, its example was followed by Malaysia, Philippines, Brunei, etc. For brief considerations about national legislations on cyber-security see S. GOHWONG, *The State of the Art,* cit., 12-23; H. NASU et al.,149-156; K. ESTIYOVIONITA, A. SITAMALA, *op. cit.,* 84-85.

to develop ICT capacity-building and to implement national emergency alert and response teams (known as Computer Emergency Response Teams - CERTs) by 2005, in accordance with common minimum performance criteria[42]. In sum, although its management came the prominence in building the ASEAN Community in its threefold articulation, cyber-security was originally viewed as a technical issue that primarily concerned national systems and required state intervention. So, ASEAN's primary purpose was to support its member states in reinforcing their own national security. To this end, it merely offered its intergovernmental bodies as platforms for member states to discuss cyber-related issues and to exchange information and best practices with the final aim to promote the identification of shared solution to common problems, thus creating a common cyber-view[43]. For this purpose, the ASEAN Network Security Action Council and Working Group on Cyber-crime were established respectively in 2012[44] and in 2013[45]. They both were in charge of coordinating ASEAN cyber-security cooperation activities in the digital sector and in the defense one respectively. In particular, the ASEAN Network Security Action Council is tasked with promoting cooperation among national computer emergency response teams, while the Working Group on Cyber-crime is a subsidiary body of Senior Officials Meeting on Transnational Crime acting as a platform for ASEAN member states to collaborate on capacity

[42] See 2003 Singapore Declaration (An Action Agenda), cit., para. 4. National CERTs were instrumental to develop a common framework for sharing expertise and cyber-security threat- and vulnerability-assessment information in real time. Most ASEAN member states successfully established CERT operations by 2005. Cambodia and Laos did so in 2008 and 2012 respectively.

[43] Cyber-security issues have been primarily dealt with by: the Ministerial Meeting on Transnational Crime and the Senior Officials Meeting on Transnational Crime; the Telecommunications and IT Ministers Meeting (then recalled Digital Ministers Meeting) and the Digital Senior Officials' Meetings; and the ASEAN Ministerial Meeting on Social Welfare and Development.

[44] See ASEAN ICT Masterplan 2010-2015, cit., 17 (Initiative 4.2.). The ASEAN Network Security Action Council is a technical forum gathering representatives from all ASEAN member states responsible for cyber-security and serving as an opportunity to build trust and promote collaborative efforts to create a secure cyber-space within the region. It is placed outside ASEAN's institutional structure as provided for in the 2007 Charter. It has convened meetings annually since 2013.

[45] The ASEAN Senior Officials Meeting on Transnational Crime decided to establish a Working Group on Cyber-Crime as a platform to discuss and adopt a coordinated approach to deal with cyber-crime, and to follow up on recommendations from other ASEAN-related fora. About its tasks see ASEAN Working Group on Cyber-Crime – Terms of Reference (Singapore, 27 May 2014).

building, training and sharing of information related to combating cyber-crime.

ASEAN's original approach to cyber-security and, in particular, its decisions not to endorse a regional strategy and not to address strict regulation or code of conduct is explained by diversity among member tates in terms of disproportionate technological development[46]. Such diversity, in tandem with the underlying socio-political milieu and the lack of trust given the diverse cultural and political context and history,
resulted in limited sharing of threat intelligence, as well as in profound differences in perceptions of cyber-space and its associated threats and, consequently, in differentiated national approaches to cyber-security. Against this backdrop, ASEAN has therefore made it a priority to contribute to the consolidation of a uniform "cyber-awareness" in all member states and to promote the establishment of a common and shared vision in the field of cyber-security.

4. 2016 marked a turning point in ASEAN's approach to cyber-security for two reasons.

Firstly, it was first created a platform exclusively dedicated to addressing cyber-security issues across ASEAN's various areas of competence: the Ministerial Conference on Cyber-security[47]. It is not properly an organ of ASEAN, as it stands outside its institutional structure, as defined in the 2007 Charter. Rather, it is an informal dialogue platform gathering Ministers and Senior Officials with expertise in cyber-security issues from each ASEAN member state. So, it has not replaced but has complemented ASEAN sectoral ministerial and sub-ministerial bodies increasingly facing cyber-security issues within the limits of their areas of competences. The creation of this Ministerial Conference is an indication of the

[46] In this regard, in literature see H. NASU, H TREZISE, *Cyber-security in the Asia-Pacific*, in N. TSAGOURIAS, R. BUCHAN (eds.) *Research Handbook on International Law and Cyberspace,* Cheltenham, 2015, 446-464; SUNKPHO, S. RAMJAN, C. OTTAMAKORN, *Cybersecurity Policy in ASEAN Countries,* 2018, https://www.researchgate.net/publication/324106226; E. KATANCHI, B. POURGHAHRAMANI, *Cyber Security Challenges in ASEAN Countries,* in *International Studies Journal*, 2021, 139-156; H. M. ALI, *"Norm Subsidiarity" or "Norm Diffusion"? A Cross-Regional Examination of Norms in ASEAN-GCC Cybersecurity Governance,* in *The Journal of Intelligence, Conflict, and Warfare*, 2021, 136-138.

[47] The inaugural meeting of the ASEAN Ministerial Conference on Cyber-Security took place on 11 October 2016 during the Singapore International Cyber Week and it usually takes place annually.

ASEAN's intention to elevate cyber-security to standalone issue, paving the way for deeper coordination of ASEAN efforts beyond the technical sphere towards a multidisciplinary approach[48]. And this has constituted a change from the approach followed up to that time.

The growing importance placed by ASEAN to cyber-security is further confirmed by the establishment of another body enriching the Organization's cyber-architecture: the Cyber-security Expert Working Group. Unlike the Ministerial Conference on Cyber-security, it is endowed with a sectoral scope; indeed, it was established in 2016 by the ASEAN Defense Ministers Meeting as a technical body serving to promote practical and effective cooperation among the member sin addressing cyber-security issues solely related to defense and military sectors[49].

While, as noted above, the creation of new bodies and platforms (especially the Ministerial Conference), dedicated to cyber-security, indicates the increased relevance the latter has assumed within ASEAN, the absence of adequate and tightly regulated coordination among them and with pre-existing ASEAN institutions has resulted in a fragmented architecture, and in the adoption of a plurality of non-binding acts that are often repetitive and lacking organicity[50]. To solve this problem and to strengthen cross-sectoral coordination on cybersecurity, the ASEAN Cyber-security Coordinating Committee was set up in 2020. It comprises representatives from relevant ASEAN sectoral bodies overseeing cybersecurity issues and serves as a formal organ to coordinate efforts and improve regional policy coherence in this field[51]. However, it is actually unable to lead the existing fragmentation to unity since it only meets annually.

Secondly, 2016 marked a turning point in approach to cyber-security since in that year ASEAN adopted a comprehensive regional plan in that field for the first time. The ASEAN Cybersecurity

---

[48] K. L. TAY, *op. cit.*, 7.

[49] See Concept Paper on the ADMM-Plus Experts' Working Group on Cyber-Security (Vientiane, 25 May 2016).

[50] See, for instance, ASEAN ICT Masterplan 2016-2020 (AIM 2020), August 2015; Master Plan for ASEAN Connectivity 2025, August 2016; ASEAN Political-Security Blueprint 2025, ASEAN Economic Community Blueprint 2025, and ASEAN Socio-Cultural Community Blueprint 2025, November 2015; ASEAN Digital Masterplan 2025, September 2016; ASEAN Declaration to Prevent and Combat Cyber-Crime, 13 November 2017.

[51] It stemmed from an initial proposal for better cyber-security policy coordination in ASEAN, as set out in the 2018 ASEAN Leaders' Statement, issued during Singapore's ASEAN Chairmanship. The inaugural meeting of the ASEAN Cyber-Security Coordinating Committee was held on 5 November 2020.

Cooperation Strategy, approved by the Telecommunications and Information Technology Ministers of member states, was a non-binding document providing the first ever roadmap for regional cooperation in the field of cyber-security[52]. It focused on strengthening CERT-CERT cooperation and capacity building, and on coordinating regional cybersecurity cooperation initiatives. It aimed to raise regional cyber-capabilities against ever evolving and increasingly sophisticated cyber-threats, and to avoid the duplication of resources. For this purpose, it recommended various initiatives. In particular, it suggested the adoption of the ASEAN CERT Maturity Framework focusing on two main areas of incident response: policy building and coordination among national CERTs, and cyber-security capacity building. The Framework should have addressed the challenge of CERT coordination due to the varying levels in capability by providing a common blueprint that enables national CERTs to self-assess their maturity levels. In essence, it should have been a feasibility study on establishing the ASEAN Regional Computer Emergency Response Team. The latter would have synergized the individual strengths and areas of expertise of the ASEAN national CERTs to bolster the overall effectiveness of regional incident response capabilities.

The Strategy approved in 2016 was updated in 2021 in order to respond to newer changes in the cyber and digital domain also caused by the Covid 19 pandemic. While continuing to build on existing achievements, ASEAN Cyber-Security Cooperation Strategy 2021-2025 aims to guide the creation of a safer and more secure cyberspace in the region and seeks to pursue a multi-disciplinary, modular, measurable multi-stakeholder approach to cyber-security. For this purpose, it identifies five areas of work: (1) Advancing Cyber Readiness Cooperation; (2) Strengthening Regional Cyber Policy Coordination; (3) Enhancing Trust in Cyberspace; (4) Regional Capacity Building; and (5) International Cooperation[53]. Under its aegis several projects and initiatives have been initiated. In particular, in January 2021, ASEAN Digital Ministers approved the

[52] See Joint Media Statement of the 16th ASEAN Telecommunications and Information Technology Ministers Meeting and Related Meetings, Bandar Seri Begawan, 26 November 2016, para. 7.

[53] It is worth noting that at the 6th ASEAN Ministerial Conference on Cyber-Security held in 2021, ASEAN member states discussed the update to the Cyber-Security Cooperation Strategy 2021–2025 and recognized the importance of strengthening cyber-security in supporting economic growth.

establishment of the ASEAN CERT Information Exchange Mechanism, which formalizes existing national CERT-level exchanges, thus helping the region develop a coordinated technical response to cyber-incidents. This Mechanisms represents a core component of the ASEAN Regional CERT, whose establishment was agreed by ASEAN member states in 2022. It covers eight functions, including facilitating coordination and information sharing between ASEAN member states national-level CERTs, and developing partnerships with industry and academia[54].

Additionally, in order to strengthen the region's cooperation in critical information infrastructure protection, ASEAN states have established cyberinformation-sharing mechanisms in both the financial
and defense sectors. Thus, the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP) was established in 2019 at the initiative of Central Bank of Malaysia. It allows ASEAN central banks to share cyber-threat intelligence and develop collaborative mitigating actions with ASEAN states which have engaged with the platform[55]. As far as the defense sector is concerned, in 2021 Ministers responsible for the matter created the ASEAN Cyber Defense Network (ACDN)[56]. It is a connecting structure of all cyber-defense operation centers of ASEAN defense establishments into a single network, providing a common communication platform. Moreover, it also aims to facilitate the exchange of knowledge and expertise between private-sector cyber experts and ASEAN cyber-defense staff through physical visits, conferences and using virtual platforms.

Then, with the view to enhancing regional capacity building, in 2023 ASEAN member states opened a Cyber-security and Information Centre of Excellence (ACICE) at Singapore's Changi Naval Base[57]. It is modelled on other multilateral 'fusion' centers in areas, such as

[54] The establishment of ASEAN Regional CERT strengthens the Organization's overall operational readiness in dealing with the fast-evolving cyber landscape by enabling stronger regional cyber-security incident response coordination. See Chairman's Statement of the 40th and 41st ASEAN Summits, Phnom Penh, 11 November 2022, para. 35.

[55] The ASEAN Cyber-Security Resilience and Information Sharing Platform was fully operationalized in February 2021.

[56] See Concept Paper on the establishment of ASEAN Cyber Defense Network (ACDN), as adopted by the 15th ASEAN Defense Ministers Meeting, 15 June 2021.

[57] The establishment of ACICE was approved by the 15th ASEAN Defence Ministers' Meeting in June 2021, while its Terms of Reference were approved by the 16th ADMM, in June 2022.

maritime security, and its purpose is to respond to the unique threats posited by cyber-security, disinformation and misinformation to defense establishments. Its opening allows ASEAN member states to bolster their defensive cyber-capacities through information sharing, training programs, and improved policy coordination[58].

5. As already said, cyber-security is a cross-cutting issue intersecting ASEAN political-security, economic and socio-cultural Communities. In particular, within the Political-Security Community, cyber-security has primarily been the domain of the ASEAN Regional Forum (ARF), as part of its focus on counter-terrorism and transnational crimes[59].

The ASEAN Regional Forum is a platform comprising 27 members mainly from the Asia-Pacific[60]. In recognition of security interdependence in the region, ASEAN established it in 1994[61] in order to promote peace and stability in the wider East-Asia region by advancing security dialogue and cooperation among the members[62]. Since 2004, the ASEAN Regional Forum has regularly organized workshops and seminars on cyber-space, with a particular focus on cyber-crime, cyber-terrorism, national capacity-building and the threat of "proxy actors". Its commitment to cyber-security had its consecration in the Statement on Cooperation in Fighting Cyber

[58] The ACICE will also focus on issues, such as fake news and misinformation, which is particularly difficult in Southeast Asia given the region's linguistic diversity. The activities of ACICE in building regional cyber-security posture are complemented by those of the ASEAN-Singapore Cyber-Security Centre of Excellence (ASCCE) and of the ASEAN-Japan Cyber-Security Capacity Building Centre (AJCCBC). The ASCCE was launched in 2019 as a physical training and policy research facility in Singapore for the benefit of all ASEAN member states.It offers training, workshops and exercises in areas such as international law, cyber-strategy, cyber-norms and other cyber-security policy issues, as well as CERT-related technical training. It also facilitates the exchange of open-source information on cyber-threats and best practices. It complements the aforementioned ASEAN–Japan Cyber-Security Capacity Building Centre, which was established in 2018 under the Japan–ASEAN Integration Fund as a physical training facility in Bangkok.

[59] H. NASU et al., *op. cit.,* 144.

[60] The current participants in the ASEAN Regional Forum are: Australia, Bangladesh, Brunei Darussalam, Cambodia, Canada, China, Democratic People's Republic of Korea, India, Indonesia, Japan, Lao PDR, Malaysia, Mongolia, Myanmar, New Zealand, Pakistan, Papua New Guinea, Philippines, Republic of Korea, Russia, Singapore, Sri Lanka, Thailand, Timor-Leste, United States, and Viet Nam. The European Union is a member of the ASEAN Regional Forum too.

[61] The 26th ASEAN Ministerial Meeting and Post Ministerial Conference (Singapore, 23-25 July 1993) agreed to establish the ASEAN Regional Forum. Its inaugural meeting was held in Bangkok on 25 July 1994.

[62] See 1st ARF Chairman's Statement, Bangkok, 25 July 1994.

Attack and Terrorist Misuse of Cyber-space issued in 2006[63]. It recognized «the serious ramifications of an attack via cyber-space to critical infrastructure on the security of the people and on the economic and physical well-being of countries in the region» and, therefore, it encouraged national and regional cyber-security regimes on the ground that «an effective fight against cyber-attacks and terrorist misuse of cyber-space requires increased, rapid and well-functioning legal and other forms of cooperation»[64]. Such a commitment was then reaffirmed in the Statement on Cooperation in Ensuring Cyber-Security[65] with a view to developing a specific cyber-security working plan[66].

Over the years the commitments made in the foregoing Statements and Working Plan have been mainly implemented in the form of various training at the regional level, with one of the focuses being how each member state responds and coordinates when cyber-incidents occur. Moreover, the ASEAN Regional Forum has been particularly keen on promoting cyber-confidence-building measures that are in line with ASEAN's diplomatic culture, which encourages the gradual downplaying and prevention of disputes through building confidence[67].

Additionally, in 2017 the ASEAN Regional Forum established the ARF Inter-Sessional Meeting on Security of and in the Use of ICTs in order to address the rapid growth of cyber-security threats. It serves as a specific platform for the member states of the Forum to promote mutual understanding, as well as to discuss and coordinate efforts on ICTs security, to implement the Working Plan on Security of and in the Use of ICTs. Then, an Open-Ended Study Group was created to discuss confidence-building measure that can reduce the

[63] ASEAN Regional Forum Statement on Cooperation in Fighting Cyber-Attack and Terrorist Misuse of Cyber-Space (Kuala Lumpur, 28 July 2006).

[64] Ivi.

[65] ASEAN Regional Forum Statement on Cooperation in Ensuring Cyber-Security (Phnom Penh, 12 July 2012).

[66] The ASEAN Regional Forum Working Plan on Security of and in the Use of Information and Communications Technologies was adopted at the 22nd ASEAN Regional Forum Meeting (Kuala Lumpur, 6 August 2015). This Working Plan serves to promote a peaceful, secure, open and cooperative ICT environment and to develop transparency and confidence-building measures to prevent conflict in cyber-space between the member states of the ASEAN Regional Forum through capacity building.

[67] In this sense see X CHEN, Y. YANG, *op. cit.*, 58. In essence, through the ASEAN Regional Forum, ASEAN has tried to facilitate the creation of a regional cooperation approach to cyber-governance that is (once again) primarily focused on the resilience of national capabilities and mutual confidence.

risk of conflict stemming from the use of ICT. This Study Group is an expert-level body subordinated to the foregoing Inter-Sessional Meeting, allowing for in-depth debates with a view to building consensus[68]. It is to be observed that these two bodies have complemented ASEAN architecture in the field of cyber-security, thus inevitably contributing to its fragmentation.

6. As already said, the 2021-2025 Strategy seeks to support the establishment of a rules-based multilateral order for cyber-space. This goal is in line with the position on cyber-security cooperation expressed by ASEAN Leaders in April 2018[69]. Indeed, on the occasion of the 32nd ASEAN Summit they adopted the landmark Statement on Cyber-security Cooperation, where they acknowledged the importance of promoting international voluntary cyber-norms of responsible state behavior, in order to foster trust and confidence and the eventual development of a rule-based cyber-space. So, they called for the identification of a «concrete list of voluntary, practical norms of state behavior in cyber-space (…) taking reference from the voluntary norms recommended in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the field of Information and Telecommunications in the Context of International Security (UNGGE)»[70]. In referring to the UNGGE in these terms, ASEAN Leaders showed that they agreed with its work and positions as far as the regulation of cyber-space is concerned. Indeed, their alignment with both UNGGE's and the OEWG's Reports was already evident in considerations expressed in the Preamble of the Statement on Cyber-Security Cooperation. It is affirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable and peaceful ICT environment and, in particular, it is argued that the principle of state sovereignty and its corollaries apply to the conduct by states of cyber-related activities[71].

[68] There have been five Open-Ended Study Groups since 2018, of which the Inter-Sessional Meeting adopted three proposals in total.

[69] ASEAN Leaders' Statement on Cyber-Security Cooperation (Singapore, 28 April 2018).

[70] ASEAN Leaders' Statement on Cyber-Security Cooperation, cit., 3.

[71] In this sense see also Statement on behalf of the Association of Southeast Asian Nations *(ASEAN)* delivered by H.E. Noor Qamar Sulaiman (Ambassador and Permanent Representative of Brunei Darussalam to the United Nations at the first substantive session of

What the Leaders' Statement only gave a glimpse of was instead clearly stated by the ASEAN Ministerial Conference on Cyber-Security shortly thereafter. On the premise that «international law, voluntary and non-binding norms of state behavior, and practical confidence building measures are essential for stability and predictability in cyber-space», the participants to the Conference agreed to subscribe in-principle to the eleven voluntary, non-binding norms recommended in the 2015 UNGGE Report[72]. So, for the first time, the member states of a regional organization formalized their acceptance of "UN cyber-norms". However, in doing so, they have stood as their passive recipients[73], instead of developing (or contributing to develop) new norms[74]. On the other hand, however, ASEAN's endorsement of UNGGE norms has not remained a dead letter. Rather, it has translated into a concrete commitment in their implementation. At the 2019 Ministerial Conference on Cyber-security, member states agreed to establish a working-level committee to develop a long-term regional action plan for the practical implementation on the UNGGE norms. Its draft was presented and adopted during the 2nd meeting of the Cyber-security Coordinating Committee in 2021. In its current version it identifies areas of capacity required to implement each of the cyber-norms and the ongoing, as well as planned, regional cooperation activities in these areas, in order to underpin ASEAN's active contribution to maintaining peace and security in the cyber-space. Firstly, the implementation of the norms will focus on the low-hanging fruit initiatives, i.e. capacity-building initiatives. During its last meeting in August 2023, the ASEAN Network Security Action Council discussed the implementation of this Regional Action Plan and encouraged member states to actively update initiatives supporting regional cooperation, capacity-building activities, and confidence-building measures to develop the necessary

---

the Open-Ended Working Group on Security of and in the use of information and communication technologies), New York, 13 December 2021, para. 4.

[72] See Chairmain's Statement of the 3rd ASEAN Ministerial Conference on Cyber-Security, Singapore, 19 September 2018, para. 9.

[73] *Contra*, see X. CHENG, Y. YANG, *op. cit.,* 58-60.

[74] Such an approach of passive acceptance has been further confirmed over the years. Indeed, the work of the UNGGE was recognised in the ARF Work Plan on Security of and in the Use of ICTs with «no intention to duplicate the work». Furthermore, the 6th iteration of the UNGGE and the adoption of the final reports of the OEWG (2019-2021) were welcomed by ASEAN in 2021. See Statement on Behalf of the Association of Southeast Asian Nations (ASEAN), cit., para. 2.

capabilities for implementing the eleven UNGGE norms[75]. However, it is yet unclear whether and to what extent ASEAN member states concretely observe these norms when actual cyber-incidents occur[76]. In this regard, in fact, it has been conveniently noted that «ASEAN States have so far refrained from 'naming and shaming' as they lack the means to accurately attribute the true source of cyber-attacks. Apart from a general statement that international law is applicable in cyber-space, the region lacks a perception of the application of international law»[77].

7. ASEAN has appeared early on to be cognizant that cyber-security is fundamental to regional stability, as well as its digital transformations and prospects in the emerging digital economy. However, dealing with it has confronted the Organization with the difficult task to balance the interests of individual members on the one hand, and the need for universally applicable regional norms on the other hand.

The analysis of institutional structure and key documents has revealed that ASEAN has performed such task by resorting to the tools of gradualness, flexibility and pragmatism underlying interstate cooperation in Southeast region since its establishment.

Indeed, instead of creating a tight binding regulation that would have harmonized domestic law in member states by limiting their sovereignty, ASEAN has preferred to engage in promoting national cyber-security resilience and in building more comprehensive efforts to address common cyber-threats, while strictly preserving state sovereignty. Thus, the discussion of cyber-security issues has been entrusted to bodies and platforms which are intergovernmental in nature and, in some cases (e.g. ASEAN Cyber-Defense Network, ASEAN Ministerial Conference on Cyber-Security, etc.) are not institutionalized. That is, they are located outside ASEAN institutional architecture as set out by the 2007 Charter. Additionally, confidence- and capacity-building measures, intended as practical solutions to establish region-wide cyber-norms, are formulated in non-binding acts

[75] See Final Statement of the 14th ASEAN Network Security Action Council, Bali, 22 August 2023.

[76] In this sense see N. VAN RAEMDONCK, *Cyber Diplomacy in Southeast Asia*, in EU Cyber Direct—EU Cyber Diplomacy Initiative Digital Dialogue, May 2021, 28, https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/2ZycxfN1/dd-southeast-asia-nb-fb-nyr-09-05.pdf

[77] *Ivi,* 4.

which are the result of intense consultations among ASEAN member states and of a consensus-based decision-making. In essence, the cyber-governance in the Southeast strictly complies with the *ASEAN Way*, inasmuch as it is informed by the principle of non-interference in states' domestic affairs, consensus-based decision-making, informal and minimal institutional mechanisms, flexibility[78].

Although ASEAN's commitment to create collective resilience and protect critical infrastructures while taking account of differences in countries' maturity and capacity is undeniable, its decision to opt for a flexible and pragmatic incremental approach has not been fully successful so far. Interpol's ASEAN Cyber-threat Assessment Reports have indeed outlined that since 2020 Southeast Asian states have been increasingly affected by cyber-attacks[79]. The limitations of ASEAN's cyber-security strategy lie primarily in the excessive fragmentation of its institutional architecture. It is loosely dispersed across various sectoral bodies and platforms that are usually uncoordinated[80].

Moreover, the various documents adopted over the years have failed to provide a definition of cyber-threat and cyber-crime, as well as a classification of cyber-incidents. Moreover, they have failed to identify a uniform risk assessment system so that when faced with the same incident, ASEAN member states can respond in the same way. In other words, ASEAN's strategy lacks «a common cyber-lexicon defining the respective impacts of a significant cyber-incident or cyber-emergency on critical information infrastructure»[81]. Clearly, this lack makes it even more difficult to reduce differences among member states in data protection legislation, and – more in general – in "cyber-culture". Finally, ASEAN member states are deemed to suffer the shortage of cyber-security professionals in terms of human talent and specific skillsets. This is considered a significant challenge for ASEAN in forming a regional emergency-response capability and it complements the absence of systematic and structured stakeholders in international discussions[82].

---

[78] In this regard, H. M. ALI, *op. cit.,* 128, observed that «ASEAN embodies cyber-norms which regulate behavior along the lines of intra-regional cooperation, wherein norms of international cooperation are rendered *subsidiary* to norms of regional autonomy». In this sense see also X. CHENG, Y. YANG, *op. cit.,* 58-59.

[79] See Interpol, *ASEAN Cyber-Threat Assessment 2020*, cit.; INTERPOL, *ASEAN Cyber-Threat Assessment 2021*, cit.

[80] K. L. TAY*, op. cit.,* 13.

[81] *Ibid*.

[82] *Ivi,* 14.

THE ACTIVITY OF THE ORGANIZATION OF AMERICAN STATES IN THE FIELD OF CYBERSECURITY·

MARCO FASCIGLIONE, MICHELE NINO

TABLE OF CONTENTS: 1. Introduction. – 2. Cybersecurity and Cybercrime in the Digital Society. – 3. The OAS Strategy on Cybersecurity. – 4. The OAS Agenda on Cybersecurity: the Cybersecurity Program. – 5. The OAS Program on Cybercrime and the International Cooperation in this Sector. – 6. Final Remarks.

1. The proliferation of telecommunications technologies and the increasing penetration of the Internet in the society represent growing trends in various states of the international community. These developments have also garnered significant attention in American states, driven by factors such as the liberalization of the telecommunications market, the widespread availability of mobile and wireless Internet technologies, and the expansion of broadband systems. Consequently, concerns about cybersecurity have risen at both national and regional levels and have led some American states to establish legal and policy frameworks to address cybersecurity issues. Such frameworks generally aim to implement a range of legal and policy measures for enhancing digital security and responding to cyberattacks[1]. However, many other countries in the region have yet to set forth such regulatory frameworks, or they are still in the process of developing them. In this context, the Organization of American States (OAS) is playing a pivotal role in supporting member states in

· This article is the result of joint efforts and discussions of the authors. However, in detail, Marco Fasciglione wrote paragraphs 1, 2, 5, while Michele Nino wrote paragraphs 3, 4, 6. This paper is part of research activities performed under the project «Security and Rights in the CyberSpace (SERICS)» (*Partenariato esteso 07: Cybersecurity, nuove tecnologie e tutela dei diritti* – PE00000014) of the National Plan of Recover and Resilience, funded by the EU programme *NextGenerationEU*.

[1] The federal administration of the United States, for instance, has adopted in 2023 an *Executive Order* which is meant to establish new standards in order to advance a coordinated, federal government-wide approach toward the safe and responsible development of AI, as well as better managing of cybersecurity risks (see *The White House*, *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, 30 November 2023). For a preliminary assessment, see: B. NEILL, J.D. HALLMARK, R.J JACKSON; D. DIASIO, *Key Takeaways from the Biden Administration Executive Order on AI*, 31 October 2023, www.ey.com/en_us/public-policy/key-takeaways-from-the-biden-administration-executive-order-on-ai.

establishing of legal and policy measures related to cybersecurity. Although a regional cybersecurity treaty is not yet in place, the OAS is actively promoting the formulation of rules and standards for cybersecurity and the fight against cybercrime[2].

This paper provides a brief overview of the main stages of inter-American cooperation in such matters, and analyzes the key aspects of the relatively recent programs initiated by the organs of the OAS in this field. To this end, after examining the notions of cybersecurity and cybercrime, the analysis focuses on the policies developed by the OAS in this area, which essentially follow a dual track: on the one hand, the tools aimed at promoting the creation of a regional framework for cybersecurity; on the other hand, the measures related to cooperation in criminal matters and aimed at countering cybercrime. The paper then delves into the functions of the main competent organs responsible for devising the overall OAS cybersecurity strategy. The final remarks highlight how the implementation of the OAS strategy on cybersecurity, which results from the coordinated action of a variety of bodies that work closely together, with the purpose of identifying forms and means of preventing, combating, and punishing cybercrime, has at the moment predominantly materialized through the adoption of non-binding acts. This situation, hence, is at the basis of the need for the adoption of binding instruments, including a future regional treaty to be negotiated under the aegis of the Organization, in order to effectively combat cybercrime in the American hemisphere.

2. The term cybersecurity is an information age terminology that was derived by merging the prefix – «cyber» with the word «security»[3]. It has been coined to refer to a multi-disciplinary aspect of information communications technology that deals with the legal, regulatory, technological and non-technological mechanisms that aim to protect computers, computer systems, computer networks, and digital technologies including the information stored or transmitted by them, from all forms of threats. Examples of such threats include unauthorized access or use of information, theft, modification,

[2] As to the normative harmonization of different legal systems in the perspective of international law, see G. RUOTOLO, *Internet (diritto internazionale)*, in *Enciclopedia del diritto*, 2014, 545 ss., 548.

[3] U.J. ORJI, *Cybersecurity Law and Regulation*, Nijmegen, 2012, 10-16.

disruption, corruption, and destruction[4]. One might be led to believe that the term cybersecurity would entail a concept with a limited scope, applicable exclusively to the world of computers. However, this is not the case. Indeed, the creation, management, and utilization of digital computing tools, as well as information and communication resources, have evolved into critical issues in contemporary society.[5] Therefore, the term under consideration represents rather a wide terminology that «covers broad subcategories ranging from cybersecurity to airport security to national security»[6]. In the absence of any unanimously accepted definition, cybersecurity may be defined as «the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber environment and organization, as well as users assets»[7]. In other terms it encompasses a range of governance measures, which typically include technical, organizational, policy, and legal aspects.

Technical aspects of cybersecurity governance essentially involve the development and implementation of necessary technical security measures for computer systems and network infrastructures. In addition, its organizational aspects concern the development of institutional capacities to promote cybersecurity, such as the establishment of law enforcement bodies, or the setting up of bodies charged with the task to manage cybersecurity incidents such as the establishment of Computer Emergency Response Teams (CERTs) to provide critical cybersecurity services such as prevention and early warning, detection, reaction, and crisis management. On the other side, legal aspects of cybersecurity governance deal with those legal measures that aim to promote cybersecurity and the development of a secure and sustainable information society. In this context, a crucial role is played by the adoption of rules aimed at prohibiting either the

[4] In this respect, «threat» refers to any «potential violation of the security» (see *International Telecommunications Union (ITU)*, *Security in Telecommunications and Information Technology: An Overview of Issues and the Deployment of Existing ITU-T Recommendations for Secure Telecommunications*, *Annex A: Security Terminology*, Ref. H.235 and X.800, Geneva, December 2003, 57. Natural disasters can also pose risks to the protection of IT systems and consequently constitute a «threat».

[5] L. FLORIDI (ed.), *The Cambridge Handbook of Information and Computer Ethics*, Cambridge, 2010, I ed., 4.

[6] P. SWIRE, L. STEINFELD, *Security and Privacy After September 11: The Health Care Example*, in *Minnesota Law Review*, 2002, 105.

[7] ITU High Level Experts Group [HLEG], *ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report*, Geneva, 2008, 27.

conducts that breach the security of computer systems or networks, or the attacks against critical information infrastructures. These rules, which can be enacted at both national and international levels, are based on the criminalization of actions that violate the confidentiality and integrity of computer systems, networks and data, or that improperly use such systems, networks, and information. The punitive mechanism of these regulations typically includes appropriate measures to combat such offenses, facilitating their detection, investigation by law enforcement authorities, and the prosecution of the offenders[8]. Furthermore, such rules can also extend criminalization to actions that involve an immoral or unlawful use of computers and computer networks, even when these actions do not in themselves constitute an attack on the security of computers or networked information infrastructures[9].

Summing up, on the one hand, the concept of cybersecurity cannot be confined solely to the prevention and criminalization of malicious acts against the security of computer systems and networks; on the other hand, the regulatory aspects of cybersecurity are the central element in respect to the control of cybercrime.

Conducts prohibited by cybersecurity law are commonly referred to as «cybercrimes» or «computer crimes». These terms are often used interchangeably to refer to instances where digital technologies are the target of a malicious or unlawful activity or the instrument for facilitating a crime or malicious activity. In other terms, «cybercrime» is used as an umbrella term to cover all forms of crime perpetrated with the help of computer resources regardless of whether the nature of the final target is a computer resource itself or not[10]. It therefore

[8] See the Preamble to the Council of Europe Convention on Cybercrime (CoE, *Convention on Cybercrime Budapest*, 23 November 2001, *European Treaty Series* No. 185).

[9] Examples of conducts falling within this category include the use of computer networks for activities such as the distribution or sale of prohibited pornography, including child pornography, the dissemination of xenophobic material, and copyright infringement. In the European regional context, the Council of Europe Convention on Cybercrime establishes under Articles 9 and 10 the obligation for contracting states to criminalize child pornography and copyright infringements, respectively. The Additional Protocol to the same Convention, concerning the criminalization of racist and xenophobic acts committed through computer systems, imposes a similar obligation on member states regarding the dissemination of xenophobic material (see CoE, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*, 28 January 2003, *European Treaty Series* No. 189).

[10] A definition of cybercrime is available in F. POCAR, *Note sullo sviluppo della normativa internazionale sui crimini relativi ai sistemi di informazione*, in AA.VV., *Studi in Onore di Umberto Leanza*, vol. I, Napoli, 2008, 629 ss., 633-635. Cybercrime has been also

includes traditional computer crimes as well as crimes against computer systems and networks[11]. Ultimately, the concept under review encompasses two categories of crimes that may be conceptually distinguished: cybercrimes in the *improper* sense and cybercrimes in the *proper* sense. Under the first meaning, the notion indicates common crimes established by criminal law that are *only incidentally* committed using a computer and the internet. Well-known examples include offenses like defamation (which can occur through email, chats, or websites), harassment (conducted through spamming or social networks), and more serious crimes, such as incitement to commit crimes, incitement to racial hatred, money laundering (also known as cyber-laundering), or child pornography[12]. Under the second meaning, cybercrime is used for describing those offences committed for the very purpose of targeting a computer system.

The absence of a universally accepted legal definition of cybercrime or computer crime is also evident in the practice. Cyber-security laws usually tend to avoid an explicit definition of these offences. As for instance, the Council of Europe Convention on Cybercrime, which is, at the moment, the only international treaty on the subject, does not explicitly define the terms «cybercrime» or «computer crime». However, the Convention, under its articles 2-10, criminalizes a range of offences according to four different categories, and namely: a) offences against the confidentiality, integrity and availability of computer data and systems; b) computer-related offences; c) content-related offences; and d) offences related to infringements of copyright and copyright-related rights. Under the Budapest convention these offences represent the minimum standard

---

defined as the complex of «computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks» (see C. HALE, *Cybercrime: Facts & Figures Concerning the Global Dilemma*, in *Crime and Justice International*, 2002, 65).

[11] M. GERCKE, *Understanding Cybercrime: A Guide for Developing Countries*, ITU, Geneva, 2009, 17.

[12] Of course, it cannot be ruled out that information technology tools may also be used to commit international crimes, leading to significant implications in terms of the punishment of such offences through the international criminal justice system (see, *ex multis*: M. ROSCINI, *Gravity in the Statute of the International Criminal Court and Cyber Conduct that Constitutes, Instigates or Facilitates International Crimes*, in *Criminal Law Forum*, 2019, 247 ss.).

of what can be regarded as cybercrime or computer crime[13]. Finally, and turning to the universal level, the United Nations General Assembly, through its Resolution 74/247, established an Open-ended *ad hoc* intergovernmental committee of experts with the task of developing an international convention on cybercrime[14]. The negotiations, which are still ongoing, have resulted in six working sessions and in a preliminary draft treaty that provides a definition of «cybercrimes» as «the use of information and communications technologies for criminal purposes», a definition which is reflected in the operative part of the draft treaty, but which is not included in Article 2, containing the 'definitions' used in the text (the so-called *Use of Terms*)[15].

3. Unlike what has happened in other regional contexts, in the American continent the debate about the introduction of regulatory and governance tools concerning cybersecurity is relatively recent[16]. The delay in the development of initiatives on cybersecurity is related to the fact that the diffusion of technologies in the Americas – with some limited exceptions – has only occurred in more recent times than in other regional experiences. Therefore, it is only around the beginning of the 2000s that the advent of the Internet and the growth of crimes committed using technologies began to raise concerns in the OAS member states and to push the need to address cybersecurity issues through the adoption of policies founded on regional cooperation.

The inter-American system regarding cybersecurity is complex and evolved, since it is based on the involvement of several actors –

---

[13] S. SCHJOLBERG, *The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva*, 2008, 8-9, www.cybercrimelaw.net/documents/cybercrime_ history.pdf.

[14] See *Countering the use of information and communications technologies for criminal purposes, Resolution adopted by the General Assembly on 27 December 2019*, UN Doc. A/RES/74/247, 20 January 2020.

[15] See *Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, Sixth session, New York, 21 August-1 September 2023, UN Doc. A/AC.291/22, 29 May 2023.

[16] For example, in the European regional context the debate about the international nature of the so-called computer crimes has been on the agenda of the Council of Europe institutions since 1976, when the topic was raised during some conferences, that were organized by the Council of Europe and were focused on the issue of economic crimes (Council of Europe, *Press release*, *Twentieth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime*, Strasbourg, 15-18 November 1976, *Summary of the Reports*, R(76) 13, Appendix 2, 4).

national and international public bodies as well as private stakeholders – which carry out their diversified functions in close cooperation and synergy, in order to build and strengthen the normative, economic and technical competencies of the OAS member states in this specific area. The origins of such system are to be found in the strategy developed in 2004 by the OAS General Assembly with Resolution XXXIV.O/04, which, inspired by a multidisciplinary and multidimensional approach aimed at creating and developing a real culture of cybersecurity of the OAS member states in this area, essentially represents the manifesto of the American organization in the field of cybersecurity[17].

The OAS approach towards the establishment of a detailed strategy on cybersecurity has its roots in two considerations. On the one side, the OAS has realized the importance assumed over time by the Internet, the related networks and technologies in the context of the development of the global economy and with a view to achieving the efficiency and productivity of commercial, industrial and intellectual activities in the American continent[18]. On the other side, the OAS has highlighted the necessity to counter pathological use of technological tools – such as, the commission of cyber crimes or the destruction of critical information systems, critical infrastructures and state economic and financial systems[19] – which constitute serious threats to cybersecurity and are capable of compromising the functioning of an entire country[20].

---

[17] General Assembly of the Organization of American States, *Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity*, AG/Res. 2004 (XXXIV-O/04), 8 June 2004. In reality, the first act that originally contained the strategy at issue is Resolution no. 1939 of the OAS General Assembly (General Assembly of the Organization of American States, *Development of an Inter American Strategy to Combat Threats to Cybersecurity*, AG/Res. 1939 (XXXIII-O/03), 10 June 2003) on which the more complex and detailed 2004 resolution is based. For an overview of important acts adopted by the OAS in the field of cybersecurity, see: Center for Cyber Security and International Relations Studies, *Organisation of American States*, www.cssii.unifi.it/vp-174-oas.html.

[18] AG/Res. 2004 (XXXIV-O/04), cit., 4.

[19] According to the definition provided by CICTE, critical infrastructure refers to «those facilities, systems, and networks, and physical or virtual (IT) services and equipment, the disabling or destruction of which would have a severe impact on populations, public health, security, economic activity, the environment, government services or the ability of the government of a member state to operate effectively» (Inter-American Committee Against Terrorism (CICTE), *Declaration Protection of Critical Infrastructure From Emerging Threats*, CICTE/doc.1/15, 20 March 2015, par. 11).

[20] AG/Res. 2004 (XXXIV-O/04), cit., 4.

These considerations have favored the development of an inter-American strategy on cybersecurity which, by expressly recalling some well-known resolutions adopted by the United Nations Security Council regarding cyberspace – those, in particular, intended to: combat the phenomenon of cyber crime; to build a global culture of cybersecurity; to protect critical information systems[21] –, is based on four pillars: 1. the strengthening of the knowledge of Internet users and operators with regard their security and computers, the threats related to the use of network and existing tools to defend themselves against risks related to cyberspace; 2. the promotion and reinforcement of public-private partnerships, in order to increase the education, awareness and cooperation with the private sector. This, in order to enable private stakeholders – which represent the main owners and operators of the critical and information infrastructures on which nations depend – to effectively protect such infrastructures[22]; 3. the identification and development of technical standards and best practices with a view to guaranteeing the security of information transmitted over the Internet and other communication networks; 4. the promotion of the adoption of legislation and policies on

[21] A/RES/55/63 on combating the criminal misuse of information technologies, 4 December 2000; A/RES/56/121 on combating the criminal misuse of information technologies, 19 December 2001; A/RES/57/239 on creation of a global culture of cybersecurity, 20 December 2002; A/RES/58/199 on the creation of a global culture of cybersecurity and the protection of critical information systems, 23 December 2003 (see: AG/Res. 2004 (XXXIV-O/04), cit., 2).

[22] In this regard, some important collaborations between the Organization of American States and the US company Amazon Web Services should be mentioned. In 2017 they entered into an agreement focused on the implementation of four objectives: 1. the organization of webinars on cybersecurity and IT transformation (in English, Spanish and Portuguese); 2. the participation in cybersecurity events organized by the OAS and held in member countries; 3. the development of white papers on cybersecurity policies and best practices; 4. the collaboration on the main political and legislative initiatives (AWS Public Sector Blog, *AWS Teams up with the Organization of American States on Cybersecurity*, aws.amazon.com). In 2018 the OAS and the US company prepared the first white paper entitled: «A Call to Action to Protect Citizens, the Private Sector and the Government» (www.oas.org/en/sms/cicte/awswhitepaper.pdf), which indicates not only a series of concrete measures to be adopted with regard to many sectors – such as citizenship and the private sector, operators of critical infrastructures, government and public administrations, cyber defense, the fight against cybercrime and the development of entrepreneurship and talent to guarantee cybersecurity – but also a methodology divided into seven phases for the development of national cybersecurity strategies (OAS Press Release, *OAS and Amazon Web Services Team Up for Increased Cybersecurity for North American and Latin American Citizens, Businesses and Governments*, www.oas.org/en/media_center/press_release.asp?sCodigo=E-015/18).

cybercrime, aimed at safeguarding network users and preventing the improper and criminal use of information and computerized systems[23].

To this end, the strategy developed by the OAS provides an institutional structure based on the activity and interaction of three bodies: 1. the CICTE (Inter-American Committee Against Terrorism), which has the task of preventing and countering terrorism in the Americas and promoting cooperation and dialogue between member states, in accordance with the principles of the OAS Charter and the 2002 Inter-American Convention against Terrorism[24]; 2. the CITEL (Inter-American Telecommunication Commission), which pursues the objective of facilitating and encouraging the development of both telecommunications and information and communication technologies in the American hemisphere in compliance with the principle of sustainable development[25]; 3. the REMJA – that is to say, Meetings of Ministers of Justices, other Ministers, Prosecutors and Attorney Generals of the Americas – which represent the main fora of the OAS and its member states in matters of criminal justice and international legal cooperation. In particular, these fora constitute an important meeting place of legal and judicial authorities of the Americas for the exchange of information, experiences and coordination of public policies, with the aim of strengthening judicial collaboration in the American continent[26].

4. As to far as the role of the CICTE is concerned, it is important to underline that it has the mandate to: develop the Inter-American agenda on cybersecurity; fight against cybercrime; support member states in countering new forms of cybercrime[27]. To this end such body is entrusted with the coordination of two specific programs: 1. the cybersecurity program; 2. the cooperation program on cybercrime.

---

[23] AG/Res. 2004 (XXXIV-O/04), cit., 5.

[24] CICTE (Inter-American Committee Against Terrorism), *What We Do*, www.oas.org/en/sms/cicte/.

[25] CITEL (Inter-American Telecommunication Commission), *About CITEL*, www.oas.org/ext/en/main/oas/our-structure/agencies-and-entities/citel/About/Details/category/citel/about-citel, par. 1.

[26] Cooperation in Justice-REMJA, *What is REMJA?*, www.oas.org/en/sla/dlc/remja-en/remja.asp.

[27] The CICTE was established by the OAS in 1999 with the aim of strengthening cooperation among member countries to prevent, combat and eliminate terrorist acts and activities (OAS, General Assembly, *Hemispheric Cooperation to Prevent, Combat and Eliminate Terrorism*, AG/RES. 1650 (XXIX-O/99), 7 June 1999).

The cybersecurity program was launched in 2008 with the aim of assisting the OAS member states to build the necessary technical and political competencies in cybersecurity matters. The program, which constitutes an integral part of the OAS strategy in this field, pursues the objective of guaranteeing «an open, secure, and resilient cyberspace throughout the Western Hemisphere»[28].

The program is based on three pillars. First, it provides OAS member states with assistance in the elaboration and development of cybersecurity policies and strategies, which involve all the interested stakeholders and are adapted to the legislative, cultural, economic and structural situation of each country. Second, the program contributes to improving and strengthening the competencies of national institutions in the cybersecurity sector, establishing CSIRTs at national level and providing state authorities with both individual technical support and targeted exercises and training courses. Third, the program carries out research and awareness-raising activities: a) preparing technical documents, toolkits and reports to guide policy makers, operators of critical infrastructures and representatives of both the private sector and civil society; b) highlighting developments related to cybersecurity; c) identifying the main issues and challenges concerning cybersecurity in the American hemisphere[29].

As part of these activities, the program has been characterized by significant publications concerning various issues related to cybersecurity in the American hemisphere[30].

As to the activity of the CICTE in the context of cybersecurity, it should be highlighted that it has the main mandate of defining and developing projects for the establishment of a network of specific bodies constantly operative in the American hemisphere (the so-called Computer Security Incident Response Teams – CSIRTs). These bodies have the task of rapidly disseminating information relating to cybersecurity and providing technical support whereas cyberattacks occur[31].

---

[28] OAS Cybersecurity Program, www.oas.org/en/sms/cicte/prog-cybersecurity.asp.

[29] Id.

[30] Cybersecurity Program: Publications, www.oas.org/en/sms/cicte/cybersecurity/publications/.

[31] The CSIRTs can be defined as bodies established with the task of providing information security services, prevention, detection, mitigation and response to cyber attacks that may take place in a given community. It may happen, in fact, that faced with a cyber attack, a body or organization may not have the knowledge or experience necessary to deal with it. In such situations, bodies such as CSIRTs can represent a fundamental tool for

In the strategic vision of the OAS, the CSIRTs established at national level must: be designated by each government and be accredited according to relevant norms of international law concerning cybersecurity; cooperate with each other and exchange information based on criteria of mutual trust; have secure infrastructures to manage confidential information; be able to interact with the private sector; consolidate the knowledge of their communities with a view to making them aware of the existence and identification of cybersecurity threats and of the tools needed to neutralize and counter such threats.[32] Furthermore, within the program at issue, it operates the CSIRT Americas Network – the OAS Network of Cyber Government Incident Response Teams, – which provides timely information on cybersecurity threats to 29 CSIRTs from 20 OAS member states.

In addition to those described above, the CICTE performs other additional functions. In particular, over the years this body has released a series of important documents, where it has asked the OAS member states to adopt several measures. This, in light of the needs increasingly expressed by state authorities to protect critical infrastructures from the growing and widespread terrorist attacks in the American continent – as well as from other emerging threats, such as the use by terrorist organizations of the Internet and information and technological systems to pursue their criminal objectives – and to make these infrastructures work in an adequate way, through effective and advanced cybersecurity programs[33].

More precisely, the CICTE has underlined the necessity for the OAS member states: a) to prepare a system against cyberterrorism, that implements not only the Inter-American Convention against terrorism, but also the pertinent universal legal instruments – *i.e.*, both the relevant resolutions adopted by the UN Security Council and the

---

developing a coordinated and efficient response to an attack, helping to mitigate its consequences. A CSIRT is generally equipped with an organizational structure that includes a series of consolidated processes, a catalogue of technological tools, a budget, a catalogue of services, specialized personnel, a network of contacts, a communication plan, and a legal framework that regulates its action. Together, these elements create a basis for managing cyber incidents and develop methods for supporting affected communities to the maximum extent possible (OAS, *A Practical guide for CSIRT. A Sustainable Business Model*, vol. 2, 2023, 7). In Italy, for example, the CSIRT is established at the National Cybersecurity Agency (ACN).

[32] AG/Res. 2004 (XXXIV-O/04), cit., 7.

[33] CICTE, *Declaration Protection of Critical Infrastructure From Emerging Threats*, 2015, cit., par. 13.

UN Global Counter-Terrorism Strategy developed by the General Assembly[34]; b) actively cooperate with each other in order to prevent terrorists from exploiting technologies, communications and network resources to incite acts of terrorism, in compliance with individual privacy, human rights and fundamental freedoms as well as the sovereignty of the individual states[35]. Furthermore, the CICTE has repeatedly highlighted the importance of identifying forms of public-private partnership in the fight against terrorism, with a view to ensuring both the good functioning of critical infrastructures and the cybersecurity of the OAS member countries[36].

As to the functions of the Inter-American Telecommunications Commission (CITEL) in the context of cybersecurity, it should be emphasized that this body plays a fundamental role, which consists in the identification and adoption of technical standards, aimed at ensuring the cyber and Internet security in the American hemisphere. In particular, the Commission's work is based on the awareness that the partnership between government authorities and industrial and commercial sectors represents a fundamental tool for guaranteeing the proper functioning of computer system networks in the American continent. Indeed, according to the structure created by the inter-American strategy, the identification of technical parameters that allow the development of cybersecurity solutions – which are defined, detailed and economically sustainable – must necessarily be achieved through an intense cooperation between telecommunications and information technology companies, on the one hand, and the governments of the OAS member states, on the other[37].

The CITEL carries out its functions in a structured, gradual and prospective manner. More precisely, the identification of technical

---

[34] Inter-American Committee Against Terrorism (CICTE), *Declaration Strengthening Cyber-Security in the Americas*, CICTE/DEC.1/12 rev. 1, 7 March 2012, par. 4; *Declaration Protection of Critical Infrastructure From Emerging Threats*, 2015, cit., par. 5 (see: Security Council, resolutions: 1267 (1999), 15 October 1999; 1373 (2001), 28 September 2001; 1540 (2004), 28 April 2004; 1624 (2005), 14 September 2005; 1631 (2005), 17 October 2005; 2133 (2014), 27 January 2014; 2170 (2014), 15 August 2014; 2178 (2014), 24 September 2014; General Assembly, *The United Nations Global Counter-Terrorism Strategy*, A/RES/60/288, 8 September 2006).

[35] CICTE, *Declaration Protection of Critical Infrastructure From Emerging Threats*, 2015, cit., par. 10.

[36] Id., par. 4-5, p. 8; Inter-American Committee Against Terrorism (CICTE), *Declaration Strengthening Hemispheric Cooperation and Development in Cybersecurity and Fighting Terrorism in the Americas*, CICTE/Dec 1/16, 26 February 2016, par. 22.

[37] AG/Res. 2004 (XXXIV-O/04), cit., 8-9.

safety standards and the consequent recommendation to the OAS member states to approve them represent the final outcome of a process characterized not only by the evaluation of several important elements (*i.e.*, the regional approaches to network security; the legislation and strategies adopted by states aimed at ensuring cybersecurity; the interconnections between the public and private sectors in this specific area; the existence of resources available to implement the identified standards), but also by the dialogue and confrontation with the OAS member states. Furthermore, some significant activities carried out by the Inter-American Telecommunications Commission should be noted, such as: the facilitation of the information sharing between member states to ensure secure networks; the technical assistance provided to these states, also through the support and collaboration of private stakeholders; the promotion of capacity-building and training programs in order to advance the process of disseminating technical information and practices related to cybersecurity issues in the Americas[38].

5. The OAS started its own cybercrime cooperation program in 1999. This program, together with the establishment of both the Inter-American Portal on Cybercrime, and the Working Group on Cybercrime, represents one of the most significant outcomes of the cooperation in the field of criminal investigations and prosecution of such crimes in the region, within the abovementioned REMJA meetings. In respect to cybercrime, REMJA Meetings serve the important role of assisting OAS member states in combating cybercrime, creating the conditions for public authorities – included law enforcement authorities and judicial bodies – to developing appropriate legal tools for preventing and prosecuting the commission of such crimes[39]. Aside the REMIJA Meetings, the Expert Group on Cybercrime is an organ established to enhance international cooperation in preventing cybercrime and in the investigative and enforcement phases. Generally speaking, REMJA and the Expert Group: a) provide support to states in the development and adoption of regulations aimed at punishing cybercrime, protecting computer systems, and preventing the use of computers for illegal activities; b)

[38] Id.
[39] Id., 10.

develop solutions to ensure cooperation in cybercrime matters among investigators and law enforcement authorities who investigate and prosecute cybercrime. The ultimate goal of REMJA Meetings and of the Expert Group is to guide OAS member states in the process of modernizing laws and regulations with the goal to combat cybercrime at both substantive and procedural levels[40].

Within the cybercrime program, the Expert Group's role is to facilitate the exchange of information and experiences among its members and to formulate basic recommendations to enhance and strengthen cooperation among the OAS member states, international organizations, and other international procedures. More specifically, as to the cooperation among national authorities in matters related to cybercrime, the Working Group plays a pivotal role in providing training for prosecutors and judges from Latin American countries on key issues, including the assessment of electronic evidence, conducting investigations, and prosecuting cybercrime offenses.

Another noteworthy activity of the Working Group is reflected in the promotion of legislative instruments among member countries. This includes the adoption (and the updating) of legislation and procedural measures necessary for the effective prosecution and adjudication of cybercrimes, as well as the enactment of laws required to ensure the collection and preservation of all forms of electronic evidence by service providers to guarantee the retention and retrieval of stored or transiting information.

The Working Group also has the responsibility to encourage the OAS member states to develop and implement national strategies that encompass measures for preventing, investigating, and prosecuting cybercrimes. Finally, the Working Group is charged with the task of promoting, among OAS member countries, the adhesion to the Convention on Cybercrime adopted, as mentioned above, within the framework of the Council of Europe. Article 37 of the CoE Cybercrime Convention, indeed, authorizes the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting states to the Convention, to invite any state, which is not a member of the Council of Europe and has not participated in its elaboration, to accede to the Convention. This overarching transregional scope of the Budapest Convention goes in the direction of establishing a common minimum

[40] Id., 10-11.

level of basic policy and legal strategies for countering transnational crime. This clearly entails the need for harmonizing national legislation within various legal systems, even transcending individual regional contexts[41].

6. This essay, after having examined the notions of cybersecurity and cybercrime, has analyzed the evolution of the OAS cybersecurity strategy. As it has been underlined, such strategy has the following objectives: a) the creation of a cybersecurity culture in the American continent; b) the establishment of a regional framework regarding cybersecurity; c) the identification of tools intended to facilitate the legal and judicial cooperation in criminal matters, in order to combat cybercrime.

The analysis conducted in this article allows to draw some conclusive remarks. On the one hand, it should be highlighted that the approach adopted by the OAS in this field is the expression of an important methodology which demonstrates a precise and appreciable will of the American Organization to identify forms and means of preventing, combating and punishing pathological uses of technological tools on the Internet and computer networks for criminal purposes. This approach has crystallized through a complex system, involving several bodies carrying out activities and functions in close cooperation with each other, and concerning various infrastructures in the American hemisphere, and has oriented policies and legislation of several OAS member states on cybersecurity.

On the other hand, it should be observed that the OAS's activity in this sector has mainly resulted in the adoption of non-binding acts, which are as such not capable of imposing duties on the member states of the Organization. Indeed, the implementation of the OAS strategy has led to the adoption of important soft law instruments having recommendatory nature and the identification of technical standards with the aim of guiding, assisting and supporting member states in the fight against cybercrime, by not providing legal obligations on them. It follows that the OAS strategy, which is based on the interaction and cooperation of different bodies and on the

[41] To date, the countries of the American continent that have accessed the Budapest Convention are: Argentina, Brazil, Canada, Chile, Colombia, Costa Rica, Ecuador, Guatemala, Mexico, Panama, Paraguay, Peru, the Dominican Republic, the United States of America, Trinidad and Tobago, and Uruguay (www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185).

assistance provided to states, lacks at the moment the legal force necessary to create an effective system capable of adequately addressing future threats and risks related to cyberspace that are seriously harmful to the overall functioning of an entire country.

In this regard, as it has been highlighted, if it is true that some states of the American continent have adhered to the Budapest Convention on Cybercrime, it is also true that many other American states have not done so, also in light of the fact that this convention is a European treaty instrument.

As a consequence, also in order to guarantee a legal harmonization between the various OAS member countries and to identify common parameters and principles binding them, it is necessary that in the immediate future the American organization – as the Council of Europe did with the Budapest Convention, and the African Union did with the Malabo Convention on Cyber Security and Personal Data Protection, that was adopted in 2014 and recently entered into force with the ratification of Mauritania – prepare a regional treaty instrument. This treaty, inspired in any case by the current strategy on cybersecurity, should have the objective of creating a certain legal system, which aims to effectively – and to a greater extent than today – combat cybercrime in the American hemisphere.

THE SHANGHAI COOPERATION ORGANIZATION AND CYBERSECURITY: A SINO-RUSSIAN APPROACH TO INTERNATIONAL LAW?

ANTONIO MARICONDA, PIERFRANCESCO ROSSI*

1. The term cybersecurity generally refers to "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack"[1]. This seemingly neutral definition has over time taken political and strategical connotations that are nowadays overriding[2]. Indeed, security threats from cyberspace became a primary concern for national defence policies, progressively inducing states to legislate on the matter[3]. The era of internet as a self-governing space is thus over[4], leaving room for a strong regulatory role of states[5].

---

* This article is the result of joint efforts and discussions of the authors. However, in detail, Pierfrancesco Rossi wrote Sections 1 and 6, while Antonio Mariconda wrote Sections 2, 3, 4 and 5.

[1] Merriam Webster Online Dictionary, available at <https://www.merriam-webster.com/>.

[2] More in detail on this topic, see N. THIBAULT, *Defining Cybersecurity*, in *Technology Innovation Management Review*, 2014, p. 13 ff. and, on the context-dependent nature of this definition, see European Union Agency for Network and Information Security, *Definition of Cybersecurity, Gaps and Overlaps in Standardisation*, 2015, available at <https://www.enisa.europa.eu>.

[3] For a detailed analysis of single countries' approaches to cybersecurity, see International Telecommunication Union, *Global Cybersecurity Index. Measuring commitment to cybersecurity*, IV ed., 2020, 32 ff.

[4] On this stance in the scholarship of 1990s, see D.R. JHONSON, D. POST, *Law and Borders-The Rise of Law in Cyberspace*, in *Stanford Law Review*, 1996, 1367 ff. and H.H. PERRITT, *Cyberspace Self-Government: Town Hall Democracy or Rediscovered Royalism*, in *Berkley Technology Law Journal*, 1997, 424.

[5] K. MAČAK, F*rom Cyber Norms to Cyber Rules: Re-engaging States as Law-Makers*, in *Leiden Journal of International Law*, 2017, 879 ff.

International law scholarship[6] and non-state actors[7] have been striving to legally frame this phenomenon since the 1990s. Yet, due to its politically sensitive nature, this task is far from without challenges. The epitome of this struggle are the discussions conducted within the United Nations fora in which states express their stance of international law and cyberspace, notably including the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE)[8] and the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG)[9]. In their meetings and the resulting non-binding reports, the only consensus that has been reached is that international law is applicable to the cyberspace[10]. When discussing in more detail how international law should operate, the debate turned in outright confrontation, preventing states to adopt common positions[11].

---

[6] See, above all, International Law Commission, *Report of the International Law Commission on the Work for the Fifty-eighth Session*, Annex D, *Protection of Personal Data in Transborder Flow of Information*, UN Doc. A/61/10, 1 May-9 June and 3 July-11 August 2006,490 ff and M.N. SCHMITT, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge, II ed., 2017. For an overview of the different approaches of international law scholarship, see G.M. RUOTOLO, *Abolish the Rules Made of Stone? Contemporary International Law and the models to Internet Regulations*, in *Italian Review of International and Comparative Law*, 2022, 254.

[7] Microsoft (A. MCKAY and others), *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World,* 2014, available at <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA>.

[8] Established pursuant to para. 4 of UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/60/45 of 6 January 2006.

[9] Established pursuant to UN General Assembly*, Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/73/27 of 11 December 2018.

[10] See, for the UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/68/98 of 24 June 2013, para. 8; UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/70/174 of 22 July 2015, para. 12; UN General Assembly, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Doc A/76/135 of 14 July 2021, para. 17. For the OEWG, see UN General Assembly, *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Final Substantive Report*, UN Doc A/AC.290/2021/CRP.2 of 10 March 2021, para. 2.

[11] For example, in 2017 the Working Group discussed the applicability of countermeasures, international humanitarian law and self-defence in cyberspace and did not adopt a final report because of the strong disagreement between States; M. SCHMITT and L. VIHUL, *International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber*

Therefore, despite some progress in 2021[12], disagreement persists about the operation of certain existing norms of international law to cyberspace.

In this normative process, the role of China and Russia stands out. Criticizing US supremacy in cyberspace, these states have played a pivotal role in debates over international cybersecurity law. Notably, their action has been twofold. On the one hand, they have advocated for cooperation in the cybersecurity domain, actively promoting it within the United Nations[13]. On the other, their dissent within these fora prevented the formation of a consensus on the application to cyberspace of existing legal frameworks, such as international humanitarian law, countermeasures or self-defence[14]. While such posture may appear inconsistent, it is arguably indicative of a political will to influence the creation of cyberspace norms: since international cybersecurity law is still in its infancy, China and Russia appear to be wishing to participate in its shaping, acting as norm makers instead of norm takers[15]. In doing so, they have generally refused to simply apply pre-existing international law to this new context, advocating instead the adoption of new instruments founded on their own

---

Norms, in *Just Security*, 2017, available at <https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/>.

[12] See M. SCHMITT, *The Sixth United Nations GGE and International Law in Cyberspace*, in *Just Security*, 2021, available at <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>.

[13] For example, the issue of cybersecurity entered the UN agenda in 1998 at the initiative of Russia, which led to the adoption of UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/53/70 of 4 January 1999. Russia's role was also pivotal in the following years, with a number of proposals on the matter then adopted by the UNGA. See UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/54/49 of 23 December 1999, UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/55/28 of 20 December 2000 e UN General Assembly, *Developments in the field of information and telecommunications in the context of international security*, UN Doc. A/RES/56/19 of 7 January 2002.

[14] See A. HENRIKSEN, *The End of the Road for the UN GGE Process and the Future Regulation of Cyberspace*, in *Journal of Cybersecurity*, 2019, 3. This approach is summarized by *Statement by the Representative of the Russian Federation at the fourth session of the UN Open-ended Working Group on Security of and in the use of ICTS 2021-2025*, 7 March 2023, available at <https://docs-library.unoda.org/OpenEnded_Working_Group_on_Information_and_Communication_Technologies__(2021)/ENG_Russian_statement_How_international_law_applies.pdf>.

[15] See M. SCHMITT, *Cybersecurity and International Law*, in R. GEIß, N. MELZER (eds), *The Oxford Handbook of the International Law of Global Security*, Oxford, 2021, 661 ff.

understanding of international law. Thus, the Sino-Russian practice on cybersecurity is a prime vantage point for capturing these two states' stance on international law.

For these reasons, an inquiry into the way these common views on cybersecurity and international law are formed and articulated is of keen interest. A prominent role in this regard is played by the Shanghai Cooperation Organization (SCO), an international organization whose members are China, India, Iran, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan and Uzbekistan. In essence, the SCO is an Asian regional organization with very broadly worded competences, but with security as its main focus. SCO practice on cybersecurity is extremely significant, as it preludes the positions taken by its members in UN cybersecurity fora. Therefore, since its leading members are China and Russia, main actors in this domain, SCO practice can be expected to considerably influence future developments in international cybersecurity law.

In light of the above, the aim of this contribution is to delve into SCO's cybersecurity practice, emphasizing that it reflects and makes apparent the Sino-Russian stance on international law. To this end, section 2 will describe the history, structure and guiding principles of the Organization, highlighting that it is mainly a tool for Chinese and Russian strategic interests and a product of their views on international law. Sections 3, 4 and 5 will describe the SCO cybersecurity practice, pointing out that its member states have throughout the years maintained a consistent approach on cybersecurity. Section 6 will conclude.

2. Regional cooperation in Central Asia traces its origins to the need to settle the border demarcation issues resulting from the fall of the Soviet Union[16]. To this end, and to enhance mutual trust with the newly independent Central Asian countries, China and Russia signed with Kazakhstan, Kyrgyzstan and Tajikistan the Shanghai Agreement on Confidence Building in the Military Field in the Border Area (1996) and the Agreement on Mutual Reduction of Military Forces in the Border Areas (1997)[17]. Moreover, the states of this group, referred

[16] See T. ATABAKI, J. O'KANE (eds.), *Post-Soviet Central Asia*, London-New York, 1998 and P. DUNAY, *Regional Security Cooperation in the former Soviet area*, in *Armaments, Disarmament and International Security SIPRI Yearbook 2007*, 2007, p. 165 ff.

[17] The Agreement on Confidence Building in the Military Field in the Border Area was signed on 26 April 1996 at Shanghai. The text is available at

to as the "Shanghai Five", signed several bilateral agreements to strengthen their cooperation[18].

When the Shanghai five were joined by Uzbekistan in 2001, the SCO was born. The Declaration on the Establishment of the SCO listed the objectives of the organization as follows: "strengthening mutual trust and good-neighborly friendship among the member states; encouraging effective cooperation among the member states in political, economic and trade, scientific and technological, cultural, educational, energy, communications, environment and other fields; devoting themselves jointly to preserving and safeguarding regional peace, security and stability; and establishing a democratic, fair and rational new international political and economic order"[19]. To pursue these aims, the Charter of the Organization identified several areas of cooperation, falling into six broader categories: disarmament, economic integration, environment, security, social affairs and telecommunications[20].

Beyond the vague wording of SCO documents, the reference to a new international order immediately stands out. It is evident that the intention of this group of states was to create "the only international organisation outside the sphere of influence of the United States and its allies"[21]. It was also immediately clear that the main field of operation of the new Organization would have been security[22], as its first act was the adoption of the Shanghai Convention on Combating

---

<https://peacemaker.un.org/sites/peacemaker.un.org/files/960426_AgreementConfidenceBuildingMilitaryFieldinBorderArea.pdf>. The Agreement on Mutual Reduction of Military Forces in the Border Areas was signed on 24 April 1997 at Moscow. The text is available at <https://cis-legislation.com/document.fwx?rgn=3872>.

[18] D. TROFIMOV, *Arms control in Central Asia*, in A.J.K. BAILES and others (eds.), *Armament and Disarmament in the Caucasus and Central Asia*, *SIPRI Policy Paper no. 3*, 2003, 46–56.

[19] Quoted from the Declaration on the Establishment of the Shanghai Cooperation Organization, which was signed on 15 June 2001 at Shanghai. Its text is available at <http://www.sectsco.org/html/00088.html>.

[20] Charter of the Shanghai Cooperation Organization (SCO), signed on June 2002 at Saint Petersburg and entered into force 19 September 2003, Art. 3 ("SCO Charter").

[21] S. KUMAR, *Why the SCO matters*, in *The Diplomat*, 29 June 2011, available at <https://thediplomat.com/2011/06/why-the-sco-matters/>.

[22] S. ARIS, *Eurasian regionalism: The Shanghai Cooperation Organization*, London, 2011, 75-76.

Terrorism, Separatism and Extremism[23], referred to as the "three evils" by SCO leaders[24].

The SCO has experienced rapid success, expanding its membership to India and Pakistan in 2017 and to Iran in 2023. Moreover, it has gradually strengthened its role in the international arena, forging relationships with the United Nations[25], international organizations[26], observer states[27] and dialogue partners[28]. Nowadays, the SCO covers the immense area from the White Sea to the South China Sea, including South Asian countries, and encompasses almost half of the world's population[29].

---

[23] Signed on 15 June 2001 in Shanghai and entered into force on 29 March 2003, available at <https://eng.sectsco.org/documents/?year=2001>.

[24] See S. ARIS, *The Shanghai Cooperation Organisation: "Tackling the Three Evils". A Regional Response to Non-Traditional Security Challenges or an Anti-Western Bloc?*, in *Europe-Asia Studies*, 2009, 457-482.

[25] See UN General Assembly, *Observer status for the Shanghai Cooperation Organization in the General Assembly*, UN Doc. A/RES/59/48 of 2 December 2004, providing the SCO with the observer status; UN General Assembly, *Cooperation between the United Nations and the Shanghai Cooperation Organization,* UN Doc. A/RES/64/183 of 18 December 2009, providing a framework for the cooperation between the United Nations and the SCO; UN General Assembly, *Cooperation between the United Nations and the Shanghai Cooperation Organization*, UN Doc. A/RES/65/124 of 13 December 2010 and UN General Assembly, *Cooperation between the United Nations and the Shanghai Cooperation Organization,* UN Doc. A/RES/67/15 of 19 November 2012 on the same issue. Moreover, the SCO has contacts with the UN Secretariat and the UN institutions represented in Beijing and representatives of the UN attend annual SCO summits upon the invitation of the country holding SCO's current presidency. Finally, the Organization established partnerships with the UN Economic and Social Commission for Asia and the Pacific (ESCAP), the UN Office on Drugs and Crime (UNODC), the UN Educational, Scientific and Cultural Organization (UNESCO), the UN Office for the Coordination of Humanitarian Affairs (UNOCHA), the Food and Agriculture Organization of the United Nations (FAO) For further information about the SCO cooperation with the UN, see <https://eng.sectsco.org/20170109/192193.html>.

[26] The SCO has established partnerships with the following International Organizations: the Commonwealth of Independent States (CIS), the Association of Southeast Asian Nations (ASEAN), the Collective Security Treaty Organization (CSTO), the Economic Cooperation Organization (ECO), the Conference on Interaction and Confidence Building Measures in Asia (CICA), the International Committee of the Red Cross (IRC), the World Tourism Organization (WTO), the Eurasian Economic Commission (EEC), and the League of Arab States (LAS).

[27] Islamic Republic of Afghanistan, Republic of Belarus and Mongolia have the status of Observer before the SCO organs.

[28] The Republic of Azerbaijan, the Republic of Armenia, the Kingdom of Bahrain, the Arab Republic of Egypt, the Kingdom of Cambodia, the State of Qatar, the State of Kuwait, the Republic of Maldives, the Republic of the Union of Myanmar, the Federal Democratic Republic of Nepal, the United Arab Emirates, the Kingdom of Saudi Arabia, the Republic of Turkey, the Democratic Socialist Republic of Sri Lanka.

[29] As recalled by the UN Secretary General in his remarks to the Shanghai Cooperation Organization Cooperation Council on 4 July 2023, available at

As for its structure, the SCO is very little institutionalized. It has only two standing bodies[30]: the Secretariat, which is the administrative organ of the Organization[31], and the Executive Committee of the Regional Anti-Terrorist Structure (RATS), entrusted with the task of coordinating member states' activities in combatting the "three evils" of terrorism, separatism and extremism[32]. Therefore, the Organization mainly provides a network for periodic meetings between political representatives of member states: the Heads of State Council is the supreme organ of the Organization and defines the priorities and main directions of its activities[33]; the Heads of Government Council reviews the budget and mainly focuses on economic cooperation[34]; the Council of Ministers of Foreign Affairs examines matters related to SCO activities and prepares the sessions of the Heads of State Council[35]; the Council of National Coordinators (senior diplomats) manage the SCO's current activities[36]. Finally, the heads of ministries can jointly address issues relating cooperation in the relevant areas and working groups of experts can be formed[37]. In light of this features, the SCO has been described not as a "normative" organization, but mainly as a forum in which member states frame their cooperation and reach common political positions[38].

It is evident from this brief description that China and Russia play a driving role in the SCO[39]. This emerges first and foremost from its

<https://www.un.org/sg/en/content/sg/statement/2023-07-04/un-secretary-generals-remarks-shanghai-cooperation-organization-delivered>.

[30] These two organs symbolized the "SCO's birth as a fully-fledged international organization", see W. SONG, *Interests, Power and the Shanghai Cooperation Organization (SCO)*", in *Journal of Contemporary China*, 92.

[31] SCO Charter, Art. 11.

[32] Agreement on Regional Anti-Terrorist Structure between the Member States of the SCO, signed on 7 June 2002 at Saint Petersburg, art. 3. The text is available at <https://eng.sectsco.org/documents/?year=2002>.

[33] SCO Charter, art. 5.

[34] Ibid., Art. 6.

[35] Ibid., Art. 7.

[36] Ibid., Art. 9.

[37] Ibid., Art. 8.

[38] E. TSYBULENKO, A. PLATONOVA, *Legal Instruments of the Shanghai Cooperation Organisation: A Case of Missed Opportunities?*, in *Central Asian Yearbook of International Law and International Relations*, 2022, 244 ff.

[39] On the Chinese leading role, see P. GUANG, *A Chinese perspective on the Shanghai Cooperation Organization*, in A.J.K. BAILES, P. DUNAY, P. GUANG and M. TROISTKIY, *The Shanghai Cooperation*, *SIPRI Policy Paper no. 17*, 2007, 48 ff. and European Parliament Think Tank, *China's leading role in the Shanghai Cooperation Organisation*, 2015, available at <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2015)564367>; On the Russian leading role see M. TROISKIY, *A Russian perspective on the Shanghai*

history, which testifies to how the organization came into being primarily to meet the needs of these two powers. More significantly, however, it emerges from its structure: consisting mainly of a set of governmental meetings and having limited institutionalization, the political clout of the most influential states manages to guide the organization's activities. In this regard, it is worth noting that the very choice to create an organization that is almost exclusively a forum for political discussion reflects the Chinese approach to law. Indeed, one of the hallmarks of the latter is to favor "political guidance" over the creation of binding norms[40]. In any case, even where institutionalization has occurred, Sino-Russian dominance has persisted. In this respect, suffice it to mention the structure of one of the two standing organs, the RATS, where China and Russia have the right to nominate more staff members than other states[41].

This leadership is not only political, but also axiological and legal. Indeed, the SCO guiding principles, often referred to as the "Shanghai Spirit"[42], blatantly mirror Sino-Russian stance of international law. Notably, the SCO embraces the view that "mutual trust, mutual benefit, equality, mutual consultations, respect for cultural diversity and pursuit of common development" as well as "non-alignment, non-targeting at other countries or regions and the principle of openness" have to be pursued and that they can only operate in a new rational international order, based on non-interference and respect for sovereignty[43]. Thus, the emphasis is on the autonomy of member states in pursuing these goals, making the SCO an organization founded on mutual trust and lacking a strong collective identity[44]. The Shanghai spirit is thus the backbone of the Organization, so fundamental that SCO leaders refer to it as "a consolidating component, a source of unity and spiritual power . . . a

---

Cooperation Organization, in A.J.K. BAILES, P. DUNAY, P. GUANG and M. TROISTKIY, *The Shanghai Cooperation*, *SIPRI Policy Paper no. 17*, 2007, 31 ff.

[40] See, in this regard, P. ROSSI, *China*, in F.M. PALOMBINO (ed.), *Duelling for Supremacy: International Law vs. National Fundamental Principles*, Cambridge, 2019, 58.

[41] See *The Shanghai Cooperation Organization: Internal Contradictions*, in *Strategic Comments*, vol. 12, no. 6, 2006.

[42] The Organization itself in its website and official documents often refers to the "Shanghai Spirit". See <https://eng.sectsco.org/20170109/192193.html>.

[43] Ibid.

[44] J. MACHAFFIE, *Mutual trust without a strong collective identity? Examining the Shanghai cooperation organization as a nascent security community*, in *Asian Security*, 2021, 349 ff.

common concept of security, a civilisation formula, a concept of development and a system of values"[45].

To understand why the "Shanghai Spirit" reflects the Sino-Russian stance of international law, it is necessary to read it in the context of these states' statements on international law. For example, the "Shanghai spirit" takes up almost verbatim the Maoist-era "Five Principles of Co-existance". These maxims, included in the final declaration of the 1955 Bandung Conference and become the ideological manifesto of the Non-Aligned Movement, were the "mutual respect for sovereignty and territorial integrity, mutual non-aggression, non-interference in each other's internal affairs, equality and mutual benefit, and peaceful coexistence"[46]. More recently, this adherence can be ascertained through Sino-Russian joint statements on international law. In these documents, often drafted in the aftermath of international crises, the two powers explicitly conveyed their vision of international law. Their key idea is to endorse a strictly literal interpretation of the UN Charter and of the Declaration on Friendly Relations, arguing that the entire international order must be grounded in the principles listed in Article 2 of the UN Charter[47]. Among these, the non-interference in internal affairs and the sovereign equality of states stand out. It follows that unilateral military interventions and unilateral sanctions are unlawful[48] and that international law must be interpreted in the light of different cultures and national identities. In this vein, "there is no one-size-fits-all template to guide countries in establishing democracy…A nation can choose such forms and methods of implementing democracy that would best suit its particular state" and "it is only up to the people

[45] *Press Conference by Secretary-General Zhang Deguang on the Eve of the Fifth Anniversary Summit of the SCO*, 6 June 2006, available at <www.sectsco.org/html/01006.html>.

[46] In this respect, see T. WANG, *International Law in China: Historical and Contemporary Perspectives*, in *Recueil des cours de l'Académie du droit international*, 1995, 263–287.

[47] L. MÄLKSOO, *Russia and China Challenge the Western Hegemony in the Interpretation of International Law*, in *EJIL: Talk!*, 2016, available at <https://www.ejiltalk.org/russia-and-china-challenge-the-western-hegemony-in-the-interpretation-of-international-law/>.

[48] *The Declaration of the People's Republic of China and the Russian Federation on the Promotion of International Law*, 26 June 2016, available at <https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/2649_665393/201608/t20160801_679466.html#:~:text=The%20People%27s%20Republic%20of%20China%20and%20the%20Russian,and%20promotion%20of%20peaceful%20cooperation%20among%20disputing%20parties>, paras. 3 and 6 ("2016 Declaration").

of the country to decide whether their State is a democratic one"[49]. The same holds true for human rights, which "must not be used to put pressure on other countries" or as a pretext to interfere in domestic politics of states[50]. In order to realize these principles, the establishment of a "new international order" is needed[51]. This would replace the Western-centred one, which endorse double standards in the interpretation of international norms[52].

This reading of the Shanghai spirit does not seem to be affected by India's accession into the SCO. Indeed, while India has historically been at the forefront of the development of contemporary international law[53], its presence in the SCO has not mitigated the Sino-Russian influence on the Organization's vision of international law. This is explained by the fact that India joined the Organization to promote some very specific strategic interests[54] and does not seem to want to be involved more than is necessary to resolve them[55].

In light of the above, it is clear that SCO member states, when referring to the Shanghai Spirit, and particularly when emphasizing sovereign equality, non-interference, and multiculturalism, draw on this stance of international law[56]. Therefore, more explicitly, the SCO and the Shanghai Spirit "can be seen as the institutionalization of the

---

[49] *Joint Statement of the Russian Federation and the People's Republic of China on the International Relations: Entering a New Era and the Global Sustainable Development*, 4 February 2022, available at <http://www.en.kremlin.ru/supplement/5770> ("2022 Declaration").

[50] Ibid.

[51] *China-Russia Joint Statement on 21st Century World Order*, 12 July 2005, available at <http://www.politicalaffairs.net/china-russia-joint-statement-on-21st-century-world-order/> and *Joint Declaration on a Multipolar World and the Establishment of a new International Order*, 23 April 1997, available at <https://archive.org/details/RussianChineseJointDeclarationOnMultipolarWorldEstblOfANewIntlOrder19977pgsPOL.sml>.

[52] 2022 Declaration and 2016 declaration, para. 6. See I. BRUNK, *China, Russia and International Law*, in *Lawfare*, 11 July 2016, available at <https://www.lawfaremedia.org/article/china-russia-and-international-law>.

[53] See B.N. PATEL, *India and International Law*, Leiden, 2005.

[54] G. SAINI, H. JACOB, *India, China, and the Shanghai Cooperation Organization: Bilateral Relations, Geopolitical Trends, and future Trajectory*, in *Council for Strategic and Defense Research*, 2022, 12 ff.

[55] C.R. MOHAN, *India and the SCO: All is not Well*, in *NUS Institute of South Asian Studies*, 10 July 2023, available at <https://www.isas.nus.edu.sg/papers/india-and-the-sco-all-is-not-well/>.

[56] T. AMBROSIO, *Catching the Shanghai Spirit: How the Shanghai Cooperation Organization Promotes Authoritarian Norms in Central Asia*, in *Europe-Asia Studies*, 2008, 1321 ff.

opposition of Moscow and Beijing[57] to the American-dominated, unipolar international order in which the US promotes democracy and universal human rights and has used these values to intervene in the domestic affairs of states seen by Washington as violating these norms (for example, Serbia in 1999 and Iraq in 2003)"[58].

In few domains this opposition appears more clearly than in SCO practice on international cybersecurity law, as will be further discussed in the next sections.

3. It has been noted that cybersecurity today dominates the SCO's political and military agenda[59]. Among other things, the Organization conducts joint cybersecurity drills, such as the one in 2017 simulating an online terrorist attack, its member states' competent ministries meet periodically to discuss the issue, Heads of State or Government frequently mention it in their joint declarations, and SCO representatives often participates in cybersecurity-related events around the world[60]. In essence, this practice is mainly composed of political declarations and debates, which the SCO does not report transparently in their entirety[61].

Thus, to figure out what the SCO's understanding of cybersecurity is, one must delve into the documents in which member states have expressed their views on the issue in more detail. The first

[57] In this regard, it is worth adding that China's approach to human rights has undergone a significant evolution over the years. Whereas in the Post-Mao era human rights were explicitly seen as an interference of Western countries in Chinese internal affairs, now the Chinese approach is more ambiguous. In fact, China is to date a party to six human rights treaties and calls out human rights in its constitution. However, it conducts at the same time a creeping contestation of existing international human rights law framework instrumentalizing the international legal lexicon. Notably, through the frequent invocation of the principle of sovereignty and of the need to tailor human rights protection to local needs and particularities, it subtly promotes a subordination of human rights to domestic law. See P. ROSSI, *China*, cit., 56 ff.; H. CHIU, *Chinese Attitudes toward International Law of Human Rights in the Post-Mao Era*, in V.C. FALKENHEIM (ed.), *Chinese Politics from Mao to Deng*, New York, 1989, 237; B. AHL, *The Rise of China and International Human Rights Law*, in *Human Rights Quarterly*, 2015, 637.

[58] Ibid., 1328-1329.

[59] E. MIKHAYLENKO, A. OSPANOVA, M. LAGUTINA, *The SCO and Security Cooperation*, in S. MAROCHKIN, Y. BEZBORODOV (eds.), *The Shanghai Cooperation Organization: Exploring New Horizons*, London, 2022, 44.

[60] The last meeting of competent ministries took place on 2 February 2024. The report is available at <https://eng.sectsco.org/20240202/1255002.html>. More generally, all the reports of these meetings and events are available at <https://eng.sectsco.org/>.

[61] Indeed, the organization's official documents report very generically on the debates that take place at these events.

was the SCO Plan of Action to Ensure International Information Security, agreed upon by SCO Heads of State in August 2007[62]. In execution of this plan, the SCO took several initiatives. Among them, the 2009 SCO Agreement on Cooperation in the Field of Information Security[63] stands out. With this instrument, the SCO created a principled legal framework for its member states' cooperation on cybersecurity.

Notably, the treaty identifies six major threats to information security[64] and binds member states to cooperate in order to cope with them. The main areas of this cooperation are the joint monitoring and response to cyberthreats, the fight against cybercrimes through adequate domestic legal frameworks, the interaction with other international organizations and between states in addressing the issue, the improving of the international legal framework and the exchange of information between state parties[65]. The Convention further stipulates that this cooperation has to take place consistently with universally recognized international norms and principles[66] and according to the agreed formats and mechanisms[67].

Although the Convention is only a framework agreement whose obligations are broadly worded, it is instrumental in describing the guiding principles of SCO action on cybersecurity. Indeed, it clearly underlies SCO member states' views on cybersecurity and, consequently, their stance on international law.

First of all, the Agreement employs the term "information security", rather than cybersecurity. This terminology is not neutral

---

[62] See U.N. General Assembly, *Developments in the field of information and telecommunications in the context of international security: Report of the Secretary-General*," U.N. Doc. A/64/129, 8 July 2009, reply received from Kazakhstan, para. 9.

[63] Agreement on Cooperation in Ensuring International Information Security between the member states of the Shanghai Cooperation Organization, signed on 16 June 2009 at Ekaterinburg. The text is available available at <https://eng.sectsco.org/documents/?year=2009>.

[64] Notably, Art. 2 of the Agreement identifies six "key threats to international information security: 1) Developing and using information weapons, preparing and conducting information warfare; 2) Information terrorism; 3) Cybercrime; 4) Use of a dominant position in the information space to the detriment of the interests and security of other States; 5) Dissemination of information prejudicial to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States; 6) Threats to secure and stable functioning of global and national information infrastructures that are natural and/or manmade".

[65] Ibid., Art. 3, which provides a detailed list of the major areas of cooperation.

[66] Ibid., Art. 4.

[67] Ibid., Art. 5.

but expresses SCO member states' view of cyberspace as subject to state control over information flow[68]. Indeed, the term cybersecurity, as employed by Western states and international organizations, refers to the technical protection of hardware, software and data against any threat stemming from accidental or malicious reasons[69]. Information security is a broader term, which also includes control over Internet content that may be detrimental to the political, economic and social order[70]. SCO member states favor this second conception, which entails that the state can influence what is published online[71]. Confirming this conception, the Agreement identifies the "Dissemination of information harmful to the socio-political and socio economic systems, spiritual, moral and cultural environment of other States" as one of the major threats to information security and Annex 2 to the Convention defines it as "distorting the picture of the political and social system of a State, its foreign and domestic policy, important political and social processes in the country, spiritual, moral and cultural values of its population"[72].

The vague wording of the Annex in defining the nature of the threat is functional in granting governments broad discretion in limiting internet content. This becomes all the more clear when looking at the domestic legislation of SCO member states. Narrowing the analysis to states that were SCO Members when the Agreement was drafted, China has the world's largest internet content control

[68] See K. GILES, *Russia's Public Stance on Cyberspace Issues*, in *4th International Conference on Cyber Conflict*, 2012, available at <https://ccdcoe.org/uploads/2012/01/2_1_Giles_RussiasPublicStanceOnCyberInformationWarfare.pdf>.

[69] C. CUIHONG, *Cybersecurity in the Chinese context: Changing concepts, vital interests, and prospects for cooperation*, in *China Quarterly of International Strategic Studies*, 2015, 475.

[70] Accordingly, the definition of information security provided by the "List of Basic Terms in the Field of International Information Security", Annex 1 to the Agreement on Cooperation in the Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization is very broad, i.e., "the status of individuals, society and the state and their interests when they are protected from threats, destructive and other negative impacts in the information space".

[71] B. TOSO DE ALCANTARA, *SCO and Cybersecurity: Eastern Security Visions for Cyberspace*, in *International Relations and Diplomacy*, 2018,552-553.

[72] List of Basic Types, Sources, and Features of Threats in the Field of International Information Security, Annex 2 to the Agreement on Cooperation in the Field of Ensuring International Information Security among the Member States of the Shanghai Cooperation Organization.

system, which is known as the "Great Firewall of China"[73]. The system makes use of both human censors and software to control online content considered harmful by the Communist Party[74]. This activity, which is entrusted to a specific body directly answerable to the Communist Party[75], finds its explicit legal basis in the 2017 Cybersecurity Law[76]. This act allows limitations on internet contents based on very vague grounds[77], provides a legal basis for the shutting down of the internet[78] and restricts the anonymity of users on the Web[79]. The same holds true for Russia. As in China, the body responsible for information security (the *Roskomnadzor*) is structurally dependent on the government[80]. Moreover, Russia launched a project of internet "sovereignization", that is the creation by law of a Russian internet segment working independently from the global internet[81]. This led to the adoption of legislative provisions allowing the extrajudicial blocking of web resources containing

[73] For further detail on this issue, see M. SVENSSON, *Human Rights and the Internet in China: new frontiers and challenges*, in S. BIDDULPH, J. ROSENZWEIG (eds.), *Handbook on Human Rights in China*, Cheltenham, 2019, 632 ff and R. CREEMERS, *The Chinese Conception of Cybersecurity: A Conceptual, Institutional, and Regulatory Genealogy*, in *Journal of Contemporary China*, 2024, 173-188.

[74] See G. AUSTIN, *Cybersecurity in China: The next wave*, Cham, 2018.

[75] The organ is called Central Leading Group on Network Security and Informatization.

[76] Law passed November 2016, effective from June 2017. The English Translation of this law is available at <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>.

[77] According to art. 12 of this act, "Any person and organization using networks shall abide by the Constitution and laws, observe public order, and respect social morality; they … must not use the Internet to engage in activities endangering national security, national honor, and national interests; they must not incite subversion of national sovereignty, overturn the socialist system, incite separatism, break national unity, advocate terrorism or extremism … create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts …".

[78] According to Art. 58 of this act, "To fulfill the need to protect national security and the social public order, and to respond to the requirements of major security incidents within the society, it is possible, as stipulated or approved by the State Council, to take temporary measures regarding network communications in a specially designated region, such as limiting such communications".

[79] For a detailed review on Chinese legislation on cybersecurity, see M. JIANG, *Cybersecurity Policies in China*, in L. BELLI (ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, Cham, 2021, 183 ff.

[80] A. SHCHERBOVIC, *Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the "Sovereignization" of the Internet in Russia*, in L. BELLI (ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, Cham, 2021, p. 68.

[81] Federal Law of 1.05.2019 No. 90-ФЗ On Introducing Amendments to the Federal Law on Communications and the Federal Law on Information, Information Technologies and

"extremist information"[82] and extending the right to access to data of law enforcement authorities[83]. Finally, all the Central Asian SCO member states have adopted measures restricting Internet content, limiting the anonymity of users and expanding the authorities' power for intervention[84].

In short, the concept of information security promoted by the Agreement finds its concrete implementation in the domestic laws of SCO member states[85]. It underlies the belief that public interests are superordinate to the human rights to freedom of expression and privacy in cyberspace. In this way, SCO member states explicitly challenge the Western conception of cybersecurity, officially informed by the balancing of individual and collective interests. While it attracted predictable criticism from UN Human Rights Treaty Bodies[86], this practice is of great relevance. Indeed, it signals that

[82] Federal Law of 28.12.2013 N 398-FZ On Amendments to the Federal Law "On Information, Information Technologies and the Protection of Information".

[83] Federal Law of 06.07.2016 N 374-FZ on Amendments to the Federal Law "On Countering Terrorism" and certain legislative acts of the Russian Federation regarding the establishment of additional counter-terrorism measures and ensuring public safety". This Law, often referred to as the Yarovaya law (after the Duma member who advocated it), attracted wide criticism in Russia and led the Russian government to collide with several internet service providers, such as Telegram. See O. CHISLOVA and M. SOKOLOVA, *Cybersecurity in Russia*, in *International Cyber Security Law Review*, 2021, 245 ff.

[84] See the Reports on freedom on the net by the NGO Freedom House, summarizing the measures adopted by these countries on cybersecurity: for Kazakhstan, available at <https://freedomhouse.org/country/kazakhstan/freedom-net/2023>; for Uzbekistan, available at <https://freedomhouse.org/country/uzbekistan/freedom-net/2023>; for Kyrgyzstan, available at <https://freedomhouse.org/country/kyrgyzstan/freedom-net/2023>; for Tajikistan, available at <https://freedomhouse.org/country/tajikistan/freedom-world/2023>.

[85] This is true also for the states that became SCO Members after the drafting of the Convention: see for Indian policies A. KOVACS, *Cybersecurity and data protection in India: an uneven patchwork*, in L. BELLI (ed.), *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, Cham, 2021, 133 ff.; Pakistani policies in M.R. SHAD, *Does Pakistan's first Cybersecurity Policy go far enough*, in *The National Interest*, 2022, available at <https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/does-pakistan%E2%80%99s-first-cybersecurity> and Iranian policies in M. COHOON, *Information Control in Iranian Cyberspace: a soft war strategy*, in *Arab Centre for Research and Policy Studies*, 8 May 2022, available at <https://www.dohainstitute.org/en/PoliticalStudies/Pages/information-controls-in-iranian-cyberspace-a-soft-war-strategy.aspx>.

[86] See *Comments Provided by David Kaye, the United Nations Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression about People's Republic of China Cybersecurity Law (Draft) Pending Before the 12th National People's Congress*, 4 August 2015, available at <https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=14423> and Human Rights Council, *Report of the Special Rapporteur on the situation of*

these states advocate a conception of cybersecurity aimed at explicitly criticizing existing international human rights law on the subject. This stands in stark contrast to what Western states do instead, officially promoting human rights in cyberspace, only to, as was recently revealed by Wikileaks, also initiate mass-surveillance programs[87].

We have so far described what is the conception that the Agreement brings out about the domestic legal framework on cybersecurity. Now, it is also crucial to emphasize what the agreement dictates regarding international relations. In this respect, Art. 2 mentions among the major threats to information security the "[u]se of a dominant position in the information space to the detriment of the interests and security of other States" and Annex 2 further explains that this threat "is caused by the unevenness in the development of information technologies in different countries and the current trend of the increased "digital gap" between developed and developing countries… Its features include monopolizing the production of software and hardware for the information infrastructure, limiting the participation of States in international information technology cooperation impeding their development and increasing their dependence of these countries from more developed countries; embedding hidden features and functions in software and equipment supplied to other countries to monitor and influence the information resources and/or critically important structures of these countries; controlling and monopolizing the market of information technologies and products to the detriment of the interests and security of the states". This threat is strictly linked with another one listed by Art. 2, which is the "Development and application of information weapons, preparation and conduct of information warfare", caused, according to the Annex 2, by the "the creation and development of information weapons posing a direct threat to critically important structures of states that may lead to a new arms race and is the main threat in the field of information security".

---

human rights in the Russian Federation, UN Doc. A/HRC/54/54 of 15 September 2023, 11, paras. 60-62.

[87] See E. MACASKILL and others, *NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained*, in *The Guardian*, 1 November 2013, available at <http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded>.

This wording is intended to refer quite explicitly to the position of dominance assumed by the United States in the field of technology[88]. By identifying this dominance as a danger, the agreement seeks to prevent even the mere development of potentially harmful technologies or a monopoly in software and hardware production. However, in order to change international law along these lines, SCO Member States needed to develop a legal framework shared with third States. For this reason, Art. 3 of the Agreement stipulates that one of the major areas of cooperation had to be "elaborating joint measures for the development of the provisions of the international law" in the field.

To this end, SCO member States have cooperated in drafting two Codes of Conducts, which will be the subject of the next section.

4. Aiming to spread the principles contained in the 2009 agreement to the universal level, SCO member states agreed in 2011 "to submit to the 66th session of the UN General Assembly a draft resolution on an international code of conduct in the area of information security"[89].

Thus, on 12 September 2011, four members of the SCO (China, Russia, Tajikistan and Uzbekistan) submitted a "Draft International Code of Conduct for Information Security" to the General Assembly[90]. This document, whose purpose was "to identify the rights and responsibilities of States in information space"[91], reiterated the principles composing the Shanghai Spirit and implemented in the 2009 Agreement.

In this vein, it called for compliance with the Charter of the United Nations and respect for sovereignty and human rights, taking

[88] See *Potomac Institute's Cyber Readiness Index 2.0*; the *Harvard Kennedy School's National Cyber Power Index* 2020; and *the International Institute for Strategic Studies, Cyber Capabilities and National Power: A Net Assessment*, 2021, demonstrating that the United States continues to lead when it comes to national cyber capabilities. As for scholarship, see K. POLLPETER, *Chinese writings on cyberwarfare and coercion*, in J.R. LINDSAY, T.M. CHEUNG, D. REVERON, *China and Cybersecurity: Espionage, strategy and politics in the digital domain*, 2015, 147.

[89] Speech by Dmitry Medvedev at a meeting of the Shanghai Cooperation Organisation Council of Heads of State in expanded format, 15 June 2011, available at <http://en.kremlin.ru/events/president/transcripts/11578>.

[90] UN General Assembly, *Letter dated 2011/09/12 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*". UN Doc. A/66/359 of 12 September 2011.

[91] Ibid., Purpose and Scope.

into account the diversity of history, culture and social systems of all countries[92]. Furthermore, it pledged states to prevent other states from using their infrastructures and technologies to undermine the right of the countries that have accepted the code of conduct[93]. Finally, the Code called for a non-military use of the cyberspace[94] and for a shared effort to cope with "the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment"[95]. We have already seen how these concepts are understood in SCO member states' approaches to international law. Suffice it to underline that this document is one of the clearest embodiments of this understanding.

However, perhaps the most controversial provision of this code is the call "to fully respect rights and freedom in information space, including rights and freedom to search for, acquire and disseminate information *on the premise of complying with relevant national laws and regulations*"[96]. Here the code effectively makes respect for fundamental rights and freedoms conditional on compliance with domestic law. In doing so, it makes explicit what was only implicitly suggested by the 2009 agreement: SCO member states intend to challenge the existing framework of international human rights law by stipulating that respect for human rights succumbs to national interests expressed in domestic law[97]. Therefore, the acceptance of the Code by the UN General Assembly would have meant an historical endorsement of this understanding at the universal level.

In contrast, the Code was not received with great enthusiasm by the Assembly and it was not adopted[98]. This can be traced back to three reasons. The first is that Western bloc states advocated for the application of existing international law norms to cyberspace[99]. Thus,

---

[92] Ibid., lett. a).
[93] Ibid., lett. d).
[94] Ibid. lett. b).
[95] Ibid., lett. c).
[96] Ibid., lett. f).
[97] J. KENNY, *Cyberoperations and the Status of due diligence obligations in International Law*, in *International and Comparative Law Quarterly*, 2023, 169-170.
[98] B. TOSO DE ALCANTARA, *SCO and Cybersecurity*, cit., 553.
[99] See for example, the US *International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World*, May 2011, 9 and, for scholarship, see J. A. LEWIS, *Liberty, Equality, Connectivity: Transatlantic Cybersecurity Norms, Report of the Center for Strategic and International Studies*, 2014, available at < https://www.csis.org/james-lewis-publications>.

according to these states, "to conclude comprehensive multilateral treaties, codes of conduct or similar instruments would not make a positive contribution to enhanced international cybersecurity"[100]. The second is the concern about states' overly broad leeway to restrict fundamental rights[101]. By subordinating respect for these to domestic law, the risk was to "give room for more self-selected processes and self-biased national narratives and thereby contribute to an alienation and even disengagement of States from their international legal commitments"[102]. The third is that, in calling upon states to prevent the misuse of their infrastructures and technologies, it espoused a multilateral approach, rather than a multistakeholder one[103]. In other words, it recognized a central role for states, excluding private stakeholders. Not reflecting the real balance of power in cyberspace, which is dominated by corporations, this too met with opposition from the Western bloc[104].

Since the failure of the 2011 Draft Code, several political and media events related to cyberspace took place. The most notable of these is perhaps the Wikileaks case in 2013, which brought to the headlines mass-surveillance programs carried out by Western

---

[100] See the United Kingdom, *Response to General Assembly resolution 68/243 Developments in the field of information and telecommunications in the context of international security*, 2014, available at <https://ccdcoe.org/uploads/2018/11/UN-14XXXX-ITISreplyUK.pdf>. See also, on this issue, M. KALJURAND, *United Nations Group of Governmental Experts: The Estonian Perspective*, in A. M. OSULA, H. ROIGAS (eds.), *International Cyber Norms: Legal, Policy & Industry Perspectives*, Tallinn, 2016, 123 and, as for scholarly skepticism, see J. GOLDSMITH, *Cybersecurity Treaties: A Skeptical View*, in *Lawfare*, 9 March 2011, available at <https://www.lawfaremedia.org/article/cybersecurity-treaties-skeptical-view>.

[101] J. CARR, *Problems with China and Russia's International Code of Conduct for Information Security*, in *Digital Dao*, 22 September 2011, available at <http://jeffreycarr.blogspot.com/2011/09/4-problems-with-china-and-russias.html>.

[102] A. PETERS, H. KRIEGER and L. KREUZER, *Due Diligence: The Risky Risk Management Tool in International Law*, in *Cambridge International Law Journal*, 2020, 134-135.

[103] On this difference, see A. SEGAL, *China and Information vs. Cyber Security*, in *Council on Foreign Relations blog*, 15 September 2011.

[104] See, for example, U.S. Department of State, *U.S. Intervention at the World Conference on International Telecommunications*, 13 December 2012, available at <http://www.state.gov/r/pa/prs/ps/2012/12/202037.htm>. C. KAUFFMANN, *Multistakeholder Participation in Cyberspace*, in *Schweizerische Zeitschrift für internationales und europäisches Recht,* 2016, 217 ff.; T. MAURER, *Cybernorms Emergence at the United Nations – An Analysis of the Activities at the UN regarding Cybersecurity*, in *Science, Technology, and Public Policy Program Explorations in Cyber International Relations Project of Harvard Kennedy School*, 2011, 25-26.

governments. This caused the issue of cybersecurity to be given central importance again on the international level[105].

All six SCO Member states (China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan) reacted to this changed framework by submitting to the UN General Assembly a new International Code of Conduct for Information Security on 9th January 2015[106]. The declared purpose of the Code was "to push forward the international debate on international norms on information security and help forge an early consensus on this issue"[107]. Thus, the underlying intention of sponsoring states was to attract a broad consensus, "taking into full consideration the comments and suggestions from all parties"[108]. For this reason, while the code broadly mirrored that of 2011, it had few notable differences prompted by this very aim[109].

First, the 2015 Draft Code repeatedly expressed appreciation for the UNCG's reports, which testifies how important this forum is to SCO member states[110]. This can be explained considering that, as mentioned, the UNCG in its reports came to very general conclusions, which can hardly invalidate the vision brought forward by SCO member states. Therefore, expressing appreciation for its work aimed to reassure third states with respect to the content of the Code, while not particularly affecting its substantive content[111].

Secondly, the call made by the 2011 Code not to proliferate "information weapons" was omitted. Indeed, that definition had been criticized because, given its broadness, it could have potentially included social medias used to organize protests against governments. So read, the provision would have resulted in a strong interference

---

[105] S. MCKUNE, *An Analysis of the International Code of Conduct for Information Security: Will the SCO states' efforts to address "territorial disputes" in cyberspace determine the future of international human rights law?*, 28 September 2015, available at <https://citizenlab.ca/2015/09/international-code-of-conduct/#7>.

[106] UN General Assembly, *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*, UN Doc. A/69/723 of 13 January 2015.. ("2015 Letter")

[107] Ibid., 1.

[108] Ibid.

[109] The Citizen Lab of Toronto University designed an interactive feature to compare the two Draft Codes, available at <https://openeffect.ca/code-conduct/>.

[110] 2015 letter, 3-4.

[111] S. MCKUNE, *An Analysis of the International Code of Conduct for Information Security*, cit.

with freedom of expression[112]. Thus, SCO member states left out this controversial provision to attract broader consensus[113].

Yet, the multilateral approach and the references to Western dominance as a threat persisted. What is more, the 2015 Code added that "States must play the same role in, and carry equal responsibility for, international governance of the Internet, its security, continuity and stability of operation, and its development"[114]. This makes clear that, as SCO member states see information security, the equality of states in Internet governance and the rejection of the multistakeholder approach are non-negotiable values. Hence, there remains on this point an unbridgeable gap with the Western bloc[115].

Finally, and most significantly, the 2015 Draft Code omitted the provision that made the protection of human rights conditional on the respect of domestic law. In its place, it stipulated that states shall "fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information, taking into account the fact that the International Covenant on Civil and Political Rights (article 19) attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection

---

[112] W. DETLEV, *The UN Takes a Big Step Forward on Cybersecurity*, in *Arms Control Today*, 4 September 2013, available at <https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity#source>; T. FARNSHWORTH, *China and Russia Submit Cyber Proposal*, in *Arms Control Today*, 2 November 2011, available at <https://www.armscontrol.org/act/2011-11/china-russia-submit-cyber-proposal>.

[113] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), *An Updated Draft of the Code of Conduct Distributed in the United Nations – What's New?*", available at <https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/#footnote_4_2722>.

[114] 2015 Letter, 5, no. 8.

[115] This contrast clearly emerged at the World Summit on the Information Society (WSIS) in 2012, during which Russia, China, and many developing countries have taken the view that multistakeholder approach naturally favors the West, given that ICT companies are mainly US-based. On the other hand, the United States have taken the view that the Multistakeholder approach was the only possible for internet governance. On this debate, see M. MUELLER, *ITU Phobia: Why WCIT was Derailed*, in *Internet Governance Project*, 18 December 2012, available at <http://www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/>; D.P. FIDLER, *Internet Governance and International Law: The Controversy Concerning Revision of the International Telecommunication Regulations*, in *ASIL Insights*, 7 February 2013, available at <http://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision>.

of national security or of public order (*ordre public*), or of public health or morals"[116].

This amendment aimed to overcome concerns raised with respect to the 2011 Code on human rights compliance, by harmonizing the issue with the ICCPR. However, such concerns persisted. Indeed, the 2015 Code's wording focuses on Art. 19 (3) of the ICCPR, selectively quoting only the grounds for the restriction of the freedom of expression[117]. This suggests SCO states' will to frame their domestic legislation as consistent with international human rights law[118]. However, it is worth noting that their understanding is blatantly incompatible with the UN Human Rights Committee's (HRC) reading of Article 19 ICCPR. Indeed, in its General Comment 34, the HRC held that restrictions "may not put in jeopardy the right itself" and that "the relation between right and restriction and between norm and exception must not be reversed."[119]Moreover, in the 2015 Code there is no mention at all of the right to privacy, which also makes plain that SCO member states did not consider amending their information security legislation which explicitly provides for mass-surveillance systems.

Despite these amendments from the 2011 version, the 2015 Code of conduct was also rejected. In fact, the international community's misgivings about excessive state control over cyberspace prevented again the formation of a broad consensus[120].

5. In recent years, the attitude of SCO member states towards the development of international cybersecurity law has slightly changed. Indeed, while they continued to stand out for their activism within the UNCG and the UNWG[121], they also worked to adopt new binding instruments on information security, departing from the strategy of non-binding codes of conduct.

This renewed approach was also expressly made manifest during the 13th Meeting of SCO National Security Council Secretaries, which

[116] 2015 letter, 5, no. 7.

[117] Ibid.

[118] S. MCKUNE, *An Analysis of the International Code of Conduct for Information Security*, cit.

[119] U.N. Human Rights Committee, *General comment No. 34, "Article 19: Freedoms of opinion and expression*, U.N. Doc. CCPR/C/GC/34, 2011, para. 21.

[120] B. TOSO DE ALCANTARA, *SCO and Cybersecurity*, cit., 553.

[121] On this activism, see A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023, 11 ff.

called for "intensifying practical cooperation in the field of international information security and drafting universal regulations, principles and norms of States responsible conduct in the media sector under UN auspices"[122]. In this vein, China and Russia signed a bilateral treaty on cooperation in ensuring international information security[123], largely restating the principles enshrined in the SCO 2009 Agreement[124]. Moreover, China signed a Bilateral Treaty with the US to normalize their cyber-cooperation[125]. Finally, and most significantly, Russia submitted to the UN General Assembly a Draft of a United Nations Convention on Cooperation in Combating Cybercrime[126].

This Draft Convention is founded on all the cornerstones of SCO's conception of cybersecurity: state sovereignty over cyberspace, sovereign equality of states, and non-intervention in the domestic affairs of other states[127]. The Draft aims to create a binding framework obliging states to criminalize certain cyber-related conducts and regulating their cooperation in dealing with cybercrime. These crimes are analytically listed in the Convention and cover various kind of behaviours, ranging from the unauthorized access to electronic information to phishing related offences, from child pornography to Information and Communication Technology (ICT) related theft[128]. In essence, this Draft Convention is intended to be the Sino-Russian response to the Council of Europe Convention on Cybercrime (Budapest Convention), which is the most prominent binding international instrument on cybercrime. Indeed, neither China nor

[122] Press release on the outcome of the 13th meeting of the SCO National Security Council Secretaries, 22 May 2018, available at <https://eng.sectsco.org/20180522/431989.html>.

[123] Signed in Moscow, on 30 April 2015 and whose English translation is available at <https://cyber-peace.org/wp-content/uploads/2013/05/RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf>.

[124] For a commentary of this Agreement, see A. SEGAL, *Peering into the future of Sino-Russian cyber security cooperation*, in *Texas National Security Review*, 10 August 2020, available at <https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/>.

[125] Signed in Washington on 25 September 2015, available at <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

[126] UN General Assembly, *Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General*, UN Doc. A/C.3/72/12 of 11 October 2017, available at <https://digitallibrary.un.org/record/1327693?ln=en>.

[127] Ibid., Art. 3.

[128] Ibid., Arts. 6-18.

Russia are parties to the latter Convention because they found its transnational approach to depart from the principles of state sovereignty and non-interference[129].

Western bloc states, for their part, consider this Draft Convention as a dangerous means of endorsing human rights violations by the sponsoring states and vigorously oppose its adoption[130]. In fact, the Convention drafting process fully espouses the SCO's approach to human rights in cyberspace. Particularly illustrative in this regard are China's attempts to include the crime of dissemination of false information in the Convention or the proposal by Malaysia, Singapore, Pakistan, Russia and other states to exclude the protection of privacy and personal data from due process safeguards[131].

Despite this radical divergence, the Convention negotiation process has moved forward. Indeed, in November 2019 the Resolution sponsored by Russia was approved by the General Assembly. Then, in December 2019, the General Assembly approved another Resolution creating an open Ad Hoc Committee (AHC) to "Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes"[132]. The AHC, operating under the auspices of United Nations Office on Drugs and Crimes (UNODC) convened its inaugural meeting on May 2021[133] and since then it held several meetings according to the relevant roadmap approved by the General

[129] N. PIJOVIĆ, *The Cyberspace 'Great Game'. The Five Eyes, the Sino-Russian Bloc and the Growing Competition to Shape Global Cyberspace Norms*, in *NATO CCDCOE Publications*, 2021, 226.

[130] See V. WEBER, *The Dangers of a New Russian Proposal for a UN Convention on International Information Security*, in *Council on Foreign Relations*, 21 March 2023, available at <https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security>. See also D. BROWN, *Cybercrime is Dangerous, But a New UN Treaty Could Be Worse for Rights*, in *Just Security*, 13 August 2021, available at <https://www.justsecurity.org/77756/cybercrime-is-dangerous-but-a-new-un-treaty-could-be-worse-for-rights/>.

[131] In this regard, see K. BANNELIER, *The U.N. Cybercrime Convention Should Not Become a Tool for Political Control or the Watering Down of Human Rights*, in *Lawfare*, 31 January 2023, available at <https://www.lawfaremedia.org/article/the-u.n.-cybercrime-convention-should-not-become-a-tool-for-political-control-or-the-watering-down-of-human-rights>.

[132] UN General Assembly, *Countering the use of information and communications technologies for criminal purposes*, UN Doc. A/RES/74/247 of 27 December 2019.

[133] The documents related to that session are available at <https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/Organizational_session>.

Assembly[134]. Between the 29th of January and the 9th of February 2024, the AHC held its concluding session, in which no consensus on an agreed text was reached. Thus, the Chair of the AHC and the Secretariat submitted a draft decision to the General Assembly stating that the AHC will hold an additional session at a date yet to be determined[135].

In the light of the above, it is not undue to infer that the future of the internet is being played out in the negotiation of this Convention. Two seemingly irreconcilable conceptions of state intervention in cyberspace are trying to reach a shared wording and 2024 will likely be a decisive year in this respect. In this process, SCO member states, especially Russia and China, retain a prominent role.

6. The practice reported in this contribution demonstrated that SCO member states have played a prominent role in international cybersecurity law. First and foremost, the activism of Russia and China in UN fora has prevented the formation of a shared *opinio* on the applicability of certain norms of international law in cyberspace. Furthermore, the consistent adoption since 2007 of political declarations, codes of conduct and binding agreements has clarified the key features of these states' stance on cybersecurity, namely: the pre-eminence of public interests over individual rights, sovereignty in the cyber space, non-interference in internal affairs, rejection of the multistakeholder approach, and the countering of cyberwar by preventing the formation of dominant positions in the cyberspace. This position stands as a stark alternative to that advocated by the Western bloc and this opposition came to its peak in the Draft Convention negotiations. The coming months may prove decisive in figuring out which approach will prevail.

However, what is worth noting as of now is how much SCO cybersecurity practice is a testbed for international law. Indeed, since

[134] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, *Proposed roadmap and mode of work of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*, UN Doc. A/AC.291/CRP.6 of 24 February 2022.

[135] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, *Draft decision submitted by the Chair of the Ad Hoc Committee*, UN Doc. A/AC.291/L.13 of 8 February 2024,

international cybersecurity law is still forming, each state is trying to shape it according to its own will. In doing so, it inevitably seeks to push forward its own vision of international relations. In the case of SCO member states, this implies an attempt to subordinate the operation of international law (especially human rights law) to domestic law. Therefore, while the future of international cybersecurity law is uncertain, current practice shows that there are states using this normative process as a platform to openly criticize existing international law and, among them, a prominent role is played by SCO member states.

THE COMMON AFRICAN POSITION ON THE APPLICATION OF INTERNATIONAL LAW TO THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES IN CYBERSPACE

SILVIA VENIER

1. As the penetration of digital technologies increases across the African continent and across all sectors[1], the governance of the cyberspace, including with respect to its security implications, is gradually being perceived as a policy priority. With billions of dollars lost annually from cybersecurity breaches[2], serious cyberattacks, some of which have also involved the headquarters of the African Union (AU) in Addis Ababa[3], are raising the warning on the urgency to govern the digital revolution. Considering that, along with weak technical and organisational protocols and poor digital literacy of users, the lack of adequate legislation often creates an environment conducive to cybercrimes[4], the adoption of criminal law provisions to

[1] According to statistics provided by the International Telecommunication Union (ITU), from 2005 to 2022 the percentage of individuals using the internet in Africa over the entire population increased from 2% to nearly 40%, see ITU DataHub available online. For an overview of the digital transition in Africa, see S.R. PONELIS, M.A. HOLMER, *ICT in Africa: Building a Better Life for all*, in *Information Technologies for Development*, 2015, 163.

[2] According to Interpol, the most prevalent form of transnational cybercrime in Africa is business email compromise (e.g. an email is sent to trick someone into sending money or divulging confidential data), which causes massive monetary losses without requiring sophisticated technical skills. Interpol, African Cyberthreats Assessment Report 2023, 14, available online.

[3] If the latest large-scale cyberattack against the AU headquarters occurred in March 2023, back in 2018 and 2020 western media reported that listening devices were found to have been installed in the Chinese-built AU headquarters in Ethiopia which, between 2012 and 2017, had allegedly been sending confidential data off to Shanghai, allegations that were denied by both Chinese and African leaders. See G. KADIRI, J. TILOUINE, *À Addis-Abeba, le siège de l'Union africaine espionné par Pékin*, *Le Monde*, 26 January 2018; R. SATTER, *Suspected Chinese Hackers Stole Camera Footage from African Union*, *Reuters*, 16 December 2020.

[4] N. KSHETRI, *Cybercrime and Cybersecurity in Africa*, in *Journal of Global Information Technology Management*, 2019, 79.

curb illegal activities committed online is the main focus of cyberspace governance.

Attention is also increasingly devoted towards harmonising legal and policy frameworks at the supranational level. In a continent that is experiencing rapid economic growth and where trade barriers are being dismantled through the Africa Continental Free Trade Area[5], diverging regulatory approaches to the cyberspace may represent an obstacle to such developments. Common minimum standards are expected to instil trust to online operations and enable the continent to «operate as one»[6], as also recognised by the AU Assembly when, in 2010, it called for harmonised rules on information and communication technologies (ICTs) to attract investments[7]. More recently, during the 2022 Lomé Summit on cybersecurity, African Heads of state and government confirmed their commitment towards ensuring that cybersecurity remains a top priority at the highest level of governance, suggesting that «the existence of binding rules […] is a *sine qua non* condition for the reinforcement of the citizens', companies' and administrations' confidence in the digital economy»[8].

A turning point in the efforts towards harmonised cybersecurity governance was the adoption in 2014 of the AU Convention on Cybersecurity and Personal Data Protection (Malabo Convention), which aims at setting forth «the security rules essential for establishing a credible digital space»[9]. The integration, in the same instrument, of provisions devoted to electronic transactions, data protection and cybersecurity, criticised by some as being overbroad[10],

[5] *Agreement Establishing the African Continental Free Trade Area*, adopted on 21 March 2018 and entered into force 30 May 2019. All legal sources are available on the AU website and were last accessed on 14 April 2024.

[6] UN Economic Commission for Africa, *Tackling the Challenges of Cybersecurity in Africa*, 4, available online.

[7] AU Assembly, declaration n. 1 (XIV) of 2 February 2010, *Addis Ababa Declaration on Information and Communication Technologies in Africa, Challenges and Prospects for Development*, preamble. See also, more recently, AU Assembly, declaration n. 3 (XXX) of 29 January 2018, *Declaration on Internet Governance and Development of Africa's Digital Economy*.

[8] *The Lomé Declaration on Cybersecurity and the Fight Against Cybercrime*, 23 March 2022, preamble (hereinafter Lomé Declaration).

[9] *African Union Convention on Cybersecurity and Personal Data Protection*, adopted on 27 June 2014 and entered into force 8 June 2023 (hereinafter Malabo Convention). For a discussion, see K. BALL, *African Union Convention on Cyber Security and Personal Data Protection*, in *International Legal Materials*, 2017, 164 ss.

[10] For an overview of the debate, see L.A. ABDULRAUF, C.M. FOMBAD, *The African Union's Data Protection Convention 2014: A Possible Cause for Celebration of Human Rights in Africa?* in *Journal of Media Law*, 2016, 67.

makes this convention a unique treaty globally. In the Chapter devoted to cybersecurity, it criminalises a broad range of cyber activities, requires states to promote education and training, and establishes procedures for investigation, prosecution, and international cooperation[11]. Yet, with only fifteen ratifications[12], the Malabo Convention experiences a low level of participation and weak implementation. In general, African states remain at varying levels of tackling cybersecurity and a unified cybersecurity governance agenda is still lacking[13].

Closely connected with the efforts towards ensuring a stable and secure digital environment to support economic and social growth, the national security implications of cyber threats are also being increasingly considered. The reliance on digital technologies of critical sectors implies that a disruption of the information infrastructure may significantly interfere with the delivery of key public services, in a manner that could trigger serious concerns[14]. Furthermore, experience has shown that online disinformation campaigns, with false information even more rapidly shared in case of use of automated artificial intelligence (AI) tools, have the potential to significantly alter democratic processes, especially elections[15]. There is thus an emerging perception of the need to promote a common understanding of norms for the peaceful use of digital technologies in inter-state relations and for responsible state behaviour in cyberspace, including with respect to the prevention and prosecution of illegal acts carried out by non-state actors that have repercussions in other states.

---

[11] Malabo Convention, Chapter III. states are required to adopt national policies and strategies (art. 24) and an adequate legal framework, having particular regard to the protection of critical infrastructures (art. 25); to promote education and training activities on cybersecurity targeted to different stakeholders and citizens (art. 26); to introduce specific types of criminal offences related to attacks on computer systems, digital data breach and content-related (art. 29) and to adapt certain offences to ICTs. African states are also party to legal and policy frameworks established by regional organizations, such as ECOWAS Council of Ministers, directive n. 1 of 19 August 2011, *Fighting Cybercrime within ECOWAS*.

[12] These include Angola, Cape Verde, Côte d'Ivoire, Congo, Ghana, Guinea, Mozambique, Mauritania, Mauritius, Namibia, Niger, Rwanda, Senegal, Togo, Zambia.

[13] N. IFEANYI-AJUFO, *Cyber Governance in Africa: at the Crossroads of Politics, Sovereignty and Cooperation*, in *Policy Design and Practice*, 2022, 149.

[14] U.J. ORJI, *Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa*, in *International Journal of Criminal Justice*, 2021, 60.

[15] The 2017 and 2022 general elections in Kenya are the often-cited example, see I.A. ABDIRAHMAN, *Exploring Co-Regulation as a Solution to Automated Disinformation in Kenya*, in *Journal of Intellectual Property and Information Technology Law*, 2023, 201.

On this issue, the Lomé Declaration suggested reinforcing cooperation on cybersecurity to support, *inter alia*, African cyberdiplomacy efforts towards «setting norm at the international level»[16].

The adoption, under the AU auspices, of the Common African Position (CAP) on the application of international law to the use of ICTs in the cyberspace is the most recent and interesting outcome of this trend. Before discussing the CAP in detail, the next section offers a brief overview of the cybersecurity governance efforts promoted at the AU level towards the harmonisation of legal and policy frameworks on ICTs as a tool to support economic and social growth and towards the advancement of a common understanding of how international law applies to the cyberspace.

2. In line with the objectives stated in its Constitutive Act[17], the AU is being projecting itself as a key player in the governance of the cyberspace. A few months after the adoption of the Malabo Convention, a Specialised Technical Committee (STC) on communications and ICTs (STC-CICT) was established under the responsibility of the AU Executive Council, which among its functions include to develop common frameworks for ICTs policy and regulation, also with respect to cybersecurity[18]. During its first session, the STC-CICT urged member states to ratify the Malabo Convention, to develop national cybersecurity legislations and to create national and regional computer emergency and incident response teams[19]. It then advised the Executive Council to endorse the AU Declaration on Internet governance and development of Africa's digital economy[20], to adopt cybersecurity as a flagship project of Agenda 2063[21], the continent's strategic framework for inclusive and

[16] Lomé Declaration, paras 5(b) and (d).

[17] Some of the AU objectives listed under art. 3 of the AU Constitutive Act are relevant to the goal of fostering the digital economy (to «achieve greater unity and solidarity» under para a, and to «accelerate the political and socio-economic integration of the continent» under para c) and of ensuring peace and stability in the cyberspace (to «defend the sovereignty, territorial integrity and independence of its Member States» under para b, to «promote and defend African common positions on issues of interest to the continent and its peoples» under para d, and to «promote peace, security and stability on the continent» under para f).

[18] AU Executive Council, decision n. 900 (XXVIII) of 28 January 2016, *Decision on the Specialised Technical Committees*, para 2. STC are AU organs composed of member states' ministers responsible for specific sectors.

[19] STC-CICT, declaration n. I of 4 September 2015, *2015 Addis Ababa Declaration STC-CICT-1*, para 16.

[20] AU Executive Council, decision n. 986-1007 (XXXII) of 26 January 2018, para 45.

[21] Ivi, para 46(i).

sustainable development, and to create an African Cyber Security Collaboration and Coordination Committee[22]. In 2019, it called for the establishment of a working group on AI to study the possibility to adopt a common African stance on AI[23], a draft of which was discussed in the committee's latest ordinary meeting held in 2023[24]. On that occasion, the STC-CICT reiterated the urgent need for a continental strategy on cybersecurity, which is still lacking[25].

Other relevant initiatives are pursued by the AU Commission under the Digital Transformation Strategy for Africa (2020-2023, DTS), which includes an «enabling environment, policy and regulations»[26] among its four foundational pillars and incorporates cybersecurity and data protection among its cross-cutting themes[27], and under the «Policy and Regulation Initiative for Digital Africa (PRIDA)», which is carried out in collaboration with the European Union and the International Telecommunication Union and aims, *inter alia*, at harmonising ICTs regulatory frameworks and at improving African stakeholders' capacity to participate in global internet governance forums.

Turning our attention to the national and regional security implications of the use of ICTs, these have been considered by the AU Peace and Security Council (PSC). Established in 2002 and placed under the authority of the AU Assembly to serve as a «standing decision-making organ for the prevention, management and resolution of conflicts»[28], the PSC has *inter alia* the responsibility to coordinate

[22] Ivi, para 46(ii). The terms of the reference of the expert group are available online.

[23] STC-CICT, declaration n. III of 26 October 2019, *2019 Sharm El Sheik Declaration STC-CICT-3*, para 15(a).

[24] See https://au.int/en/5thstccict.

[25] Of note is that the AU Assembly requested the AU Commission to «expeditiously develop a Continental Cyber Security Strategy and a Cybersecurity Model Law» when it endorsed the fifth report of the PSC in 2020, see AU Assembly, decision 755 (XXXIII) of 10 February 2020, *Decision on the Fifth Report of the Peace and Security Council of The African Union*, para 17.

[26] *The Digital Transformation Strategy for Africa (2020-2030)*, 12.

[27] Ivi, 55.

[28] *Protocol relating to the establishment of the Peace and Security Council of the African Union*, adopted at Durban on 9 July 2002 and entered into force on 26 December 2003 (Durban Protocol), art. 2(1). The PSC is composed by fifteen members elected by the AU Executive Council on the basis of the principles of equitable regional representation, periodical rotation and respect for constitutional governance and the rule of law. For an overview of the establishment and relevance of the PSC, see P.D. WILLIAMS, *The Peace and Security Council of the African Union: Evaluating an Embryonic International Institution*, in *Journal of Modern African Studies*, 2009, 603.

efforts to protect against international terrorism[29], to decide on any issue having implications for the maintenance of peace, security and stability on the continent[30], to ensure respect of the AU Non-Aggression and Common Defence Pact[31], whose broad definition of aggression has been found to easily accommodate also serious cyberattacks[32].

The PSC begun its considerations on the role of cybersecurity in the promotion and maintenance of peace in Africa in 2016, when it suggested that «cybersecurity concerns are broader than national security and they can become a planetary emergency with the potential of amplifying the traditional security threats»[33] and urged states «to develop cyber diplomacy capabilities and to actively participate in international meetings and debates on the governance of the internet and cybersecurity issues»[34]. This meeting was followed by a set of official statements on this topic, beginning with Communiqué 749 (2018) devoted to counterterrorism, which affirms the need to contrast the use of ICTs by terrorist groups, whether in their fundraising, narrative promotion, and recruitment[35]. In Communiqué 850 (2019), the PSC expressed «concern that a number of states are developing ICT capabilities for military purposes and that the use of

[29] Durban protocol, art. 7, para i.

[30] Ivi, art. 7, para r.

[31] *African Union Non-Aggression and Common Defence Pact*, adopted at Abuja on 1 January 2005 and entered into force on 18 December 2009 (Abuja Pact), art. 9. As of March 2024, it has been signed by 44 states and ratified by 22.

[32] As defined in the Abuja Pact, art. 1, aggression encompasses not only the use of armed force but also «*any other hostile act* by a State, a group of States, an organization of States or non-State actor(s) or by any foreign or external entity, against the sovereignty, political independence, territorial integrity and *human security* of the population of a State party» (emphasis added). Among the examples of such acts, under art. 1(c) the Pact refers to «*technological assistance* of any kind, intelligence and training to another State for use in committing acts of aggression against another Member State» (emphasis added). On the provisions of the Abuja Pact relevant to cybersecurity, see U.J. ORJI, *Interrogating African Positions on State Sponsored Cyber Operations: A Review of Regional and National Policies and Legal Responses*, in *Baltic yearbook of International Law*, 2022, 254 ss; ID., *Rethinking the African Union Non-Aggression Treaty as a Framework for Promoting Responsible State Behavior in Cyberspace*, in *MPIL Research Paper Series*, 2021, 77.

[33] AU PSC, press statement n. DCXXVII of 26 September 2016, 1.

[34] Ivi, 2.

[35] AU PSC, communiqué n. 749 (2018) of 27 January 2018, *Towards a Comprehensive Approach to Combatting the Transnational Threat of Terrorism in Africa*, para 19. For an assessment of the relevance of official statements and communiqués issued by the PSC, see WILLIAMS, *op. cit.*, 615-616.

ICTs in future conflicts between states is becoming more likely»[36] and that «increasing global threats to cybersecurity constitute serious threats to national, regional, continental and international peace and security»[37]. It then stressed some key steps to enhance cybersecurity at the national level, including to undertake regular cyber security risk assessments, enhance national cyber security capacities, redouble investments in education and public awareness raising campaigns, and take the necessary steps to own the national information infrastructure[38]. The importance of mainstreaming cybersecurity into all AU peace and security mechanisms was finally affirmed in Communiqué 1097 (2022), which for the first time urges states «to adapt to the digital era by enacting necessary legislations for ensuring compliance of international law and international humanitarian law in the use of emerging technologies and the new media»[39].

The inaugural engagement between the PSC and the AU Commission on International Law (AUCIL)[40] was finally welcomed in Communiqué 1120 (2022). In this statement, the PSC highlights the concern for «the targeting of government institutions and public infrastructures, the spread of misinformation and subversive activities and interferences with national processes including elections»[41] and «[a]cknowledges the application of international law to cyberspace» while referring in particular to the prohibition on the threat or use of force, the prohibition on intervention in the internal or external affairs of states, and the inviolability of the political independence, territorial integrity, and sovereignty of states as foundational rules of international law[42]. The document underlines «the urgent need for a

[36] AU PSC, communiqué n. 850 (2019) of 20 May 2019, *Mitigating the Threats of Cyber Security to Peace and Security in Africa*, preamble.

[37] Ivi, para 1.

[38] Ivi, paras 3-5.

[39] AU PSC, communiqué n. 1097 (2022) of 4 August 2022, *Emerging Technologies and New Media: Impact on Democratic Governance, Peace and Security in Africa*, para 11.

[40] The AUCIL was established on the basis of Article 5(2) of the AU Constitutive Act. The Statute of the AUCIL was adopted by the AU Assembly, decision 209 (XII) of 3 February 2009, *Draft Statute of the African Union Commission on International Law*.

[41] AU PSC, communiqué n. 1120 (2022) of 9 November 2022, *Inaugural Engagement between the Peace and Security Council and the AU Commission on International Law*, preamble. The statement was followed by two other communiqués in which an update was offered on the process of developing a CAP. See AU PSC, communiqué n. 1148 (2023) of 13 April 2023, *Cyber Security: Impact on Peace and Security in Africa*, paras 6 and 7, and communiqué n. 1171 (2023) of 24 August 2023, *Updated briefing on the Development of the Common African Position on Cyber-Security in Africa*.

[42] Communiqué n. 1120 (2022), para 3.

Common African Position on the application of international law on cyberspace, as well as the need for Africa to actively engage in the process of articulating the rules of international law»[43] and emphasises that «basic human rights and fundamental freedoms, especially the principles enshrined in the African Charter on Human and Peoples' Rights, and the fundamental principles of international humanitarian law are also applicable to cyberspace»[44].

The CAP on the application of international law to the use of ICTs in cyberspace was officially adopted by the PSC in Communiqué 1196 (2024) and was referred to the ordinary session of the AU Assembly held in February 2024 for consideration and endorsement[45]. In this statement, the PSC encourages states to consider issuing national positions in line with the CAP and to actively participate in regional and international multilateral forums on the governance of cyberspace[46]. The next section investigates the contents of the CAP more in detail.

3. Until today, the international process on clarifying norms for the governance of states' behaviour in cyberspace has seen only a marginal participation of African states and regional organizations, at least until the sixth UN Group of Governmental Experts (GGE) was established in 2019[47]. The CAP is a remarkable addition to this debate as it is the first statement that collects the views of a group of states and significantly contributes towards geographically diversifying the

[43] Ivi, para 4.

[44] Ivi, para 5.

[45] AU PSC, communiqué n. 1196 (2024) of 29 January 2024, *Draft Common African Position on the Application of International Law to the Use of Information and Communication Technologies in the Cyberspace* (hereinafter CAP). The CAP was included in the report of activities of the PSC that was adopted by the AU Assembly in February 2024, see *Report of the PSC of the AU on its activities and the State of Peace and Security in Africa, Reporting Period: January to December 2023*, para 16 and Annex I. Under para 36 of that report, the PSC invites the AU Assembly to officially endorse the CAP in the upcoming ordinary session. At the time of writing, no official decision or declaration by the AU Assembly explicitly endorsing the CAP is available yet on the AU website.

[46] CAP, paras 4 and 7.

[47] The UN GGE is mandated to advance international cooperation on responsible state behaviour in the cyberspace. Since when the process started in 2004, only few African states were selected to participate in the group, until the 2019-2021 GGE introduced the equitable regional distribution as a criterion to select the 25 participating states. Four African states, including Kenya, Mauritius, Morocco and South Africa, participated to that GGE. Kenya was the only African state to offer an official position on the application of international law to the cyberspace.

discussion. It provides rich evidence of *opinio juris ac necessitatis* on some hotly debated topics which often see diverging views of states.

The process that led to the adoption of the position was a multi-stakeholder capacity building initiative open to all AU states and other experts and led by the PSC and the AUCIL[48]. It fitted into the broader African practice of developing CAPs, diplomatically agreed texts that can take various formats, such as consensus papers, joint statements or declarations, generally without binding force, adopted to address common challenges and to serve as concerted policy priorities in global forums[49]. Scholars have noted that the development of CAPs, which are foreseen among the objectives of the AU[50], has become «a vital practice in the relationships between member states and the AU»[51].

The CAP on international law and cyberspace consists of a preamble and eleven sections: nine thematic sections on rights and obligations, a section on capacity building and a concluding paragraph. It begins by affirming that ICTs represent «an instrument of human interaction, a vehicle for social development, and an engine of economic growth, poverty eradication and sustainable development»[52] and that it is «in the interest of all states, societies and present and future generations to develop a global legal architecture that ensures that ICTs are used for peaceful purposes, and that prevents the malicious and criminal use of such technologies, guarantees that cyberspace remains open, secure, stable, accessible and peaceful, protects basic human rights and fundamental freedoms of individuals and peoples, and advances the common interest of mankind»[53]. According to the CAP, the views of all states on these

[48] See the overview offered by the AUCIL Special Rapporteur M. HELAL, *The Common African Position on the Application of International Law in Cyberspace: Reflections on a Collaborative Lawmaking Process*, *EJIL: Talk!*, 5 February 2024. The process proceeded in two – to some extent concomitant – stages: the organisation of three training sessions for African diplomats and experts (March – July 2023) and the actual drafting of the position (May – December 2023). It was supported by Canada, Germany and the United Kingdom.

[49] O. AYODELE, *Africa's International Relations and the Legend of 'Common Positions'*, in *African and Asian Studies*, 2023, 63.

[50] Among the objectives of the AU, art. 3, para d, includes «to promote and defend African common positions on issues of interest to the continent and its people».

[51] B. ADEOYE, *Common African positions on global issues. Achievements and realities*, Africa Reports, 2020, 3.

[52] CAP, para 2.

[53] Ivi, para 3.

themes have an equal weight[54] and the process of further expanding dialogue should be transparent, inclusive and multilateral[55]. The document is to be viewed as a non-exhaustive contribution to ongoing discussions, in consideration of the continuous and rapid technological developments, reserving the AU its position for all issues that are not dealt with in this statement[56].

The section devoted to sovereignty in cyberspace characterises territorial sovereignty as a primary rule of international law[57] and endorses what has been defined as a pure sovereignty approach[58], according to which states' sovereignty is violated simply by the penetration of a computer system located in its territory that occurs without the consent of the targeted state or any other lawful justifications. As is well known, along with cyberespionage[59], one of the most contentious issues in the current debate is indeed the legality of extraterritorial law enforcement operations carried out for different purposes, including to have direct access to evidence stored abroad or take down sites sharing criminal content. The CAP highlights that, by virtue of territorial sovereignty, states are entitled to exercise exclusive jurisdiction, including legislative, adjudicative and enforcement authority, over the components of cyberspace located in their territories[60]. Any enforcement operation on the territory of a foreign states thus violates that states' sovereignty regardless of whether it causes any physical or virtual harm[61]. It explicitly rejects any *de minimis* threshold[62], which is however somehow re-introduced

[54] Ivi, para 6. The right of all countries to participate in internet governance on equal footing has been in particular advocated by China, see Z. HUANG, Y. YING, *Chinese approaches to cyberspace governance and international law in cyberspace*, in N. TSAGOURIAS, R. BUCHAN (eds.), *Research handbook on International Law and Cyberspace*, Cheltenham, 2021, 549-550.

[55] CAP, para 4. The reference to multilateralism suggests that African states endorse the leading role of governments in defining the global cyberspace governance framework, as also outlined by the Chinese «multilateral plus multi-party» model, see Z. HUANG, Y. YING, *op. cit.*, 551-553.

[56] CAP, para 10.

[57] Ivi, para 13.

[58] K.J. HELLER, *In defence of pure sovereignty in cyberspace*, in *International Law Studies*, 2021, 1432.

[59] R. BUCHAN, *Cyberespionage and International Law*, Oxford, 2021.

[60] CAP, paras 13-14.

[61] Ivi, para 15.

[62] Ivi, para 16. Under the *de minimis* approach, low intensity cyber operations violate sovereignty only when they cause at least some kind of harm to the targeted state, such as physical damage or loss of functionality of the information infrastructure. The genesis of the *de minimis* approach is referred to be the Tallin Manual 2.0, see M.N. SCHMITT (ed.), *Tallin*

in the case of a cyber operation against the ICTs infrastructure of a foreign state that «causes effects, such as loss or impairment of functionality» on a third state, which may constitute a breach of the sovereignty of that latter state[63].

The CAP makes clear that seeking to codify rules on permissible enforcement activities in the cyberspace of foreign states poses significant risks given «the vast disparity of technical capability of States» that would carry the risk of abuses from the part of the most powerful actors[64], which is not surprising considering that African states are far more likely to be targeted by low intensity cyberoperations than to launch them. In any case, it has been noted that the fact that the CAP's determination that a state's cyber infrastructure is accorded the same protection as its physical territory is «a highly significant development that will go a long way to ensuring that cyberspace is a safe, secure, and peaceful domain»[65].

In section three, the CAP discusses the extent of requirements of due diligence, defined in line with well-established jurisprudence as not allowing knowingly the own territory to be used for acts contrary to the rights of other states[66]. The debate here mainly centres around determining the specific actions required to prevent and redress harmful behaviour of non-state actors or other states[67]. The CAP affirms that due diligence is an obligation of conduct that depends on the state's knowledge and capacity to act to prevent or halt the wrongful act[68] and has to be determined on a case-by-case basis[69]. The

Manual 2.0 on the International Law applicable to Cyber Operations, Cambridge, 2017, 20. Note that in this part dealing with violations of sovereignty, along with the «degree of infringement» the Tallin Manual also refers to «interference with or usurpations of inherently governmental functions», which is generally dealt with in the context of the prohibition of intervention principle (see below).

[63] CAP, para 16.

[64] Ivi, para 17.

[65] R. BUCHAN, N. TSAGOURIAS, *The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force*, *EJIL: Talk!*, 20 February 2024.

[66] Ivi, para 21. For an analysis of how due diligence applies to cyberspace under international law, see T. DIAS, A. COCO, *Cyber due diligence in international law*, Oxford Institute for Ethics, Law and Armed Conflicts, 2020, available online.

[67] For an overview of different positions endorsed by states on this point, see P. ROGUSKI, *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*, The Hague Program for Cyber Norms, 2020, 11, available online.

[68] CAP, para 22.

[69] Ivi, para 23.

unique challenges faced by developing countries and the importance of international cooperation and information sharing are emphasised[70].

Turning our attention to the section on prohibition of intervention in the internal and external affairs of states, while there is widespread consensus that this principle is extremely relevant to cyberspace and the CAP is no exception[71], the challenge is, once again, to clearly delimit the constitutive elements of a prohibited intervention (i.e. whether the act targets *domaine réservé* matters and whether it amounts to coercion) and their application to online activities[72]. The CAP suggests that this prohibition is a rule that applies to inter-state relations[73] and «protects against acts that impinge on matters within the domestic jurisdiction of States» which include the «inalienable right to choose their political, economic, social and cultural systems»[74]. Not surprisingly, the CAP thus proposes that this broad definition of matters that fall within the *domain réservé* of states (including also social and cultural systems) equally applies to cyberspace.

The position then goes on to discuss the actions that may amount to coercion, suggesting that further study and deliberation between states are required on this point[75]. In any case, according to the CAP, it is not necessary that the coercive act, understood «as a policy that is designed to impose restraints on the will of a foreign State», reaches the level of completely depriving a state of its freedom of choice or to compel that state to act or refrain from acting involuntarily, while

---

[70] Ivi, para 25. On this point, the Tallin Manual suggests that «[d]eveloped States will often be more capable of stopping harmful cyber operations that emanate from their territory than developing States» and that the criteria to determine the extent of the due diligence obligations depend on «the technical wherewithal of the State concerned, the intellectual and financial resources at its disposal, the State's institutional capacity to take measures, and the extent of its control over cyber infrastructure located on its territory», see M.N. SCHMITT (ed.), *op. cit.*, 47.

[71] CAP, para 29 stating that «the principle of non-intervention is especially pertinent in the context of cyberspace given the increasing connectivity between states and societies and provides greater opportunities for malicious actors, including States and non-State actors the acts of which are attributable to States, to misuse ICTs for the purposes of intervening in the internal and external affairs of States».

[72] I. KILOVATY, *The international law of cyber intervention*, in N. TSAGOURIAS, R. BUCHAN (eds.), *op. cit*., 99 ss.

[73] CAP, para 27.

[74] Ivi, para 28. For an overview of state views on the application of the principle of non-intervention to cyberspace, see W. OSSOFF, *Hacking the Domaine Réservé: the Rule of Non-Intervention and Political Interference in Cyberspace*, in *Harward Journal of International Law*, 2021, 310-320.

[75] CAP, para 32.

emphasising that unsuccessful threats to coercion are also unlawful under international law[76]. Noticeably, the CAP incorporates an expanded definition of coercion by referring to policies rather than actions, and a low threshold for the violation of the principle of non-intervention, which may occur only for the very fact of targeting certain critical sectors, including electoral processes[77]. For these reasons, it comes closer to the views of states that advocate for defining coercion as acting against another states' «freedom of control» which is broader than the «freedom of choice» definition[78].

In the section on the peaceful settlement of disputes, the CAP affirms that this obligation also applies to any dispute that may arise between states in relation to the use of ICTs or to diverging understandings of norms for responsible state behaviour in cyberspace[79]. In then proposes a unique view when it recognises the potential for ICTs to enhance the peaceful settlement of disputes, referring in particular to online mediation platforms and dispute resolution software, and urging states to invest resources in research and development on such tools[80].

The sixth section refers to the prohibition of the threat or use of force as a «rule of jus cogens and a fundamental and cardinal rule of general international law»[81], with the only two exceptions of self-defence against an armed attack and authorisation by the UN Security Council acting under Chapter VII of the UN Charter. The AU adopts the effect-based approach when it affirms that a cyberoperation would fall within the scope of the prohibition of the use of force when «the scale and effects of the operation are comparable to those of a conventional act of violence», including physical damage, injury, or

[76] *Ibidem*.

[77] On the application of the concept of coercion to online electoral interference, see S. WHEATLY, *Foreign interference in elections under the non-intervention principle: we need to talk about «coercion»*, in *Duke Journal of Comparative and International Law*, 2020, 161; N. TSAGOURIAS, *Electoral cyber interference, self-determination and the principle of non-intervention in cyberspace*, in D. BROADERS, B. VAN DER BERG (eds.), *Governing Cyberspace Behaviour, Power and Diplomacy*, Lahman, 2020, 45.

[78] N. TSAGOURIAS, R. BUCHAN, *op. cit.*; R. BUCHAN, J. DEVENNEY, *Clarifying Responsible Cyber Power: Developing Views in the U.K. Regarding Non-intervention and Peacetime Cyber Operations*, *Lawfare*, 20 October 2022. Under the Tallin Manual, coercion occurs only if the conduct succeeds in influencing the outcome of certain *domaine réservé* activities, see N.M. SCHMITT (ed.), *op. cit.*, 318.

[79] CAP, para 35.

[80] Ivi, para 37. The reference to the two tools probably derives from their growing use in the private sector.

[81] Ivi, para 38.

death[82]. The threshold seems high when the document refers as examples to «a cyber operation that destroys, inflicts damage or permanently disables critical infrastructures or civilian objects»[83].

This section then dwells on the elements to determine when a cyber operation amounts to an armed attack, as the gravest form of use of force that triggers the right to self-defence: these include the duration of the attack, the nature of the targets and location, the type of weapon used, and the extent of the damage caused[84]. The CAP takes note of the controversial notion of self-defence against imminent threats and favours a restrictive interpretation according to which self-defence is permitted only «if an armed attack occurs»[85]. Yet, it does not make any reference to self-defence's requirements of necessity and proportionality. Finally, according to the CAP, arming and training non-state actors, or providing technical assistance, could amount to a violation of the prohibition of the use of force[86].

The part on the application of international humanitarian law (IHL) in cyberspace distinguishes between international and non-international armed conflicts according to the generally agreed elements triggering the applicability of IHL in both contexts[87]. In this section, the CAP suggests that «the AU is mindful of the possibility that cyberoperations as in itself may trigger a non-international armed conflict», without clarifying if this could occur for international armed conflicts too[88]. Reference is then made to the principles that govern the means and methods of warfare, in particular distinction, proportionality and prohibition of unnecessary suffering[89]. The CAP

[82] Ivi, para 39. See similarly the Tallin Manual, N.M. SCHMITT (ed.), *op. cit.*, 330 and 333.

[83] CAP, para 40. For a detail discussion of the criteria to be used to assess the likelihood that states will characterise a cyber operation as a use of force, see N.M. SCHMITT (ed.), *op. cit.*, 334-336.

[84] CAP, para 41.

[85] Ivi, para 42. The Tallin Manual endorses a different view, see N.M. SCHMITT (ed.), *op. cit.*, 350.

[86] CAP, para 44.

[87] Ivi, paras 47-49.

[88] A careful reading of this paragraph suggests that this is due to the challenges in determining the level of intensity of armed violence that serves a non-international armed conflict determination, while in international armed conflict any use of armed force triggers IHL applicability. On whether cyberoperations may trigger an international armed conflict, the Tallin Manual concludes that «cyber operations alone have the potential for crossing the threshold», see N.M. SCHMITT (ed.), *op. cit.*, 384; as per non-international armed conflicts, it «achieved no consensus as to whether non-destructive but severe cyber operations may be considered in order to fulfil the intensity requirement», ivi, 389.

[89] CAP, paras 50-51.

makes clear that the ICT infrastructure associated with certain civilian objects, such as hospitals or humanitarian assistance facilities, enjoy additional specific protection[90]. An issue that could have been touched upon in this part was clarifying whether and to what extent cyber operations associated with armed conflicts may amount to war crimes and give raise to international criminal responsibility[91].

Section eight deals with international human rights law (IHRL). Following an introductory paragraph that refers to the universality, indivisibility and interdependence of human rights and to states' obligations to respect, protect and ensure[92], the CAP focuses on freedom of expression online, which must be protected by states[93]. In consideration of the widespread practice of filtering online content and services or general internet shutdowns[94], the position could have made more explicit that these may amount to a violation of IHRL. Reference could have been made to the Declaration of Principles on Freedom of Expression and Access to Information in Africa adopted in 2019 by the African Commission on Human and Peoples' Rights, which under Principle 38 requires states not to interfere with this right through the removal, blocking or filtering of content or the disruption of internet access for segments of the public or the entire population. Instead, the CAP generally refers to the fact that restrictions to freedom of expression must be provided by law and to what is strictly necessary in a democratic society, including to respect the rights of others and some public values such as national security, public order, public health or moral[95], which are often interpreted in not so properly strict terms by African states.

According to the CAP, responsible state behaviour includes an obligation not to engage in any conduct that may violate the right to privacy, such as the transnational interception of communication, indiscriminate surveillance and data misuse[96]. Interestingly, the CAP affirms not only the duty of states to protect persons against human rights violations committed online but also that «businesses

[90] Ivi, para 52.

[91] An affirmative position is endorsed by the Tallin Manual, N.M. SCHMITT (ed.), *op. cit.*, 391 ss.

[92] CAP, para 53.

[93] Ivi, para 54. Here the position could have been made clearer by the reiteration of the term «respect».

[94] Internet shutdown statistics are available at www.accessnow.org/campaign/keepiton/.

[95] CAP, para 54.

[96] Ivi, para 55.

enterprises that operate in the ICT sector have a responsibility to respect and protect human rights, especially the right to privacy and freedom of information, including by exercising due diligence to identify, prevent, mitigate and account for any adverse human rights impact of their activities»[97]. Here it could have been intriguing to know the position of African states on the right to be forgotten, which may become relevant in the near future in consideration of the exponential increase of internet usage across the continent[98].

The position then dwells on the relevance of ICTs for economic, social and cultural rights and on the obligation to cooperate to ensure the realization of the right to development[99]. A reference is made on the duty to bridge the digital divide, which could have benefitted from an explicit reference to the positive duty to provide education and training on ICTs, and to pay special regard to the persons in vulnerable situations, especially persons with disabilities who have the right to enjoy the benefits of ICTs. For those purposes, states shall ensure «that the design, development, and production of ICTs incorporates assistive and adaptive technologies»[100]. Finally, the AU calls for the responsible development and management of digital identity systems[101] and for considering the conclusion of agreements on mutual assistance in the area of combating all forms of cybercrimes[102].

The last thematic section deals with the rules of attribution of conduct to a state in cyberspace[103]. The CAP affirms that the customary rules as reflected by the International Law Commission Draft Articles on the Responsibility of states apply to online activities[104]. It goes on by clarifying that the burden of proof is on the state making the claim that another state has committed an

[97] Ivi, para 56.

[98] The right to be forgotten refers to the right to have some personal data removed from the internet. Experts of the Tallin Manual agree that, at present, there is no customary IHRL based obligation of states to require third parties to remove personal data from the internet, see N.M. SCHMITT (ed.), *op. cit.*, 196.

[99] CAP, para 57.

[100] Ivi, para 58.

[101] Ivi, para 59.

[102] Ivi, para 60. As known, this is a contentious issue in the international debates on cyberspace governance, with some states (including Russia and China) advocating for the adoption of such an instrument, while western states regarding this as problematic for fears that it may be misused by governments to facilitate or validate internet censorships practices.

[103] For an in-depth and updated discussion on this, see A. STIANO, *Attacchi informatici e responsabilità internazionale dello Stato*, Napoli, 2023.

[104] Ivi, para 61.

internationally wrongful act[105], with the required support of international information sharing. The last paragraph briefly touches upon the responses to internationally wrongful acts committed through ICTs, which must be in line with other obligations under international law[106].

Capacity building and international cooperation are discussed in section ten as essential to a digitally interdependent world. Reference is made to the importance of cooperating towards securing critical information infrastructures and to the fact that the «development dimension should be fully integrated into any future elaboration of international rules applicable to the cyberspace»[107]. Finally, the concluding paragraph takes up some considerations already mentioned in the preamble, such as that the CAP must be considered as a non-exhaustive articulation of the views of the AU[108], which are expected to be further elaborated considering technological developments and ongoing discussions on these themes.

4. In the process of defining what amounts to acceptable state behaviour in cyberspace, which is generally characterised by unsettled views and diverging opinions and permeated with ambiguity as states are inclined to maintain some sort of freedom to act, the CAP contributes clarifying African priorities and positions on some decisive points. Furthermore, in a context in which the lack of awareness amongst policy makers in some African countries results in the inability to adequately monitor and defend national networks, the organisation of capacity building and training activities represented an added value of the CAP drafting process and was paramount to ensure that representatives of African states had the knowledge to develop their positions on these complex themes.

---

[105] Ivi, para 62. The existence of a legal obligation to provide evidence of the basis upon which it attributed cyber operations to another state is endorsed by the Russian Federation in its national position, see UNGA, *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266*, 80. The Tallin Manual affirms the non-existence of a similar obligation, see N.M. SCHMITT (ed.), *op. cit.*, 83.

[106] CAP, para 63.

[107] Ivi, para 66.

[108] Ivi, para 68.

The document supports the application of relevant branches of international law to the cyberspace, even if the precise contours of some rules require further elaboration, as it is often the case for national statements. It nevertheless maintains that developing new norms may be necessary, given the unique characteristics and evolving nature of the cyberspace.

Not surprisingly the CAP includes some insights that bring it closer to the model of internet governance advocated for by non-Western countries, with an emphasis on the equal rights of states, the decisive role of governments and the crucial importance of capacity building and international cooperation. The position endorses a pure sovereignty approach to the cyberspace and affirms the duty of substantiating claims of internationally wrongful acts. Yet, a strong digital sovereignty perspective may also serve at validating censorship and massive shutdown practices over the internet as national security measures, which do not constitute rare occurrences in Africa.

On many other issues, however, the CAP aligns itself to western perspectives as reflected by the findings of the experts who drafted the Tallin Manual, as highlighted in the previous sections. Some interesting novelties are introduced, such as encouraging the use of ICTs in the peaceful settlement of disputes or highlighting the duties of business enterprises working in ICTs. Yet other important themes, such as the potential role of ICTs in the commission of the gravest crimes under international law, could have been considered.

In any case, the CAP remains an important contribution to the debate on the application of international norms to the cyberspace and a good start for any future deliberations on these matters.

Finito di stampare nel mese di settembre 2024
Presso la *Grafica Elettronica* Napoli

THE AUTHORS

ANNITA LARISSA SCIACOVELLI – Professor of International law, University of Bari Aldo Moro (Italy). Member of the Advisory Board, European Union Agency for Cybersecurity (ENISA). Member of the Defense Innovation Office, Chief of Defense Staff, Italian Ministry of Defense.

SEBASTIANO LAPISCOPIA – Colonel of the Italian Army. Former Head of the International Legal Affairs Office of the Italian Defense General Staff. Chief Editor of the review «Rassegna della Giustizia Militare», Italian Ministry of the Defense.

ARINDRAJIT BASU – PHD Candidate at the Leiden University, Faculty of Global Governance and Affairs. Digitalization and Human Rights Research Consultant with the United Nations Development Program (UNDP). Previously, Research Lead at the Centre for Internet&Society.

BHARATH GURURAGAVENDRAN – Graduate student at New York University (NYU). Research Consultant with NYU's Centre for Human Rights and Global Justice. Previously, Assistant Professor at Jindal Global Law School; Legislative Assistant to Member of Parliament (through the LAMP Fellowship).

KEIKO KONO – Visiting Researcher at the Meiji University Cybersecurity Laboratory, Tokyo. Previously, Post-Doctoral Researcher, University of Copenhagen. Former Senior Research Fellow of Public International Law and Cybersecurity, National Institute for Defence Studies (NIDS), Japanese Ministry of Defence. Former law researcher of NATO CCDCOE.

TAL MIMRAN – Associate Professor, Zefat Academic College. Academic Director, International Law Forum of the Hebrew University. Fellow at the Federmann Cyber Security Research Center, Law Faculty, Hebrew University. Previously, Legal Adviser, Israeli Ministry of Justice.

LIOR WEINSTEIN – Master's student of International Law (LLM), Hebrew University, Jerusalem. Researcher in Law and Technology and International Law, Tachilit Policy Center. Member of the International Law Forum, Hebrew University, and of the Federmann Cyber Security Research Center – Cyber Law Program.

ISAAC MORALES TENORIO – Senior Director for Cybersecurity & Data Privacy, LATAM, FTI Consulting. Previously, First General Coordinator for Multidimensional Security Issues, Mexico's Ministry of Foreign Affairs. Coordinator for Multidimensional Security. Member of the UN GGE to Advance Responsible Behavior in Cyberspace; Chairperson of the OAS Working Group on Confidence-Building Measures in Cyberspace.

MARIANA SALAZAR ALBORNOZ – Professor of International Law, International Humanitarian Law (IHL) and International Criminal Law (ICL), Universidad Iberoamericana, Mexico City. Previously, Rapporteur for International Law Applicable to Cyberspace and for Privacy and Data Protection, Inter-American Juridical Committee, Organization of American States.

PIETRO GARGIULO – Professor of International Law, University of Teramo (Italy). Editor in Chief, "La Comunità Internazionale" ("The International Community"), Quarterly of the Italian Society for International Organization (SIOI).

IVAN INGRAVALLO – Professor of International Law, University of Bari Aldo Moro (Italy). Associate Editor, "La Comunità Internazionale" ("The International Community"), Quarterly of the Italian Society for International Organization (SIOI).

ELENA DRAGO – Women4Cyber Chapters Coordinator. MA Philosophy, Politics and Economics in MED, University of Bari Aldo Moro (Italy).

ELISA TINO – Associate Professor of International Law, University of Naples "Parthenope" (Italy). Author of monographs and scientific articles concerning the law of international organizations and some topics of public international law.

MARCO FASCIGLIONE – Researcher of International Law and Human Rights Law, Co-Director of the Business and Human Rights Summer School, National Research Council (CNR, Italy). Member of Mission Appeals Tribunal (MAT), NATO.

MICHELE NINO – Professor of International Law, University of Salerno (Italy). Holder of the Course of the Law Clinic in "International Protection of Human Rights", University of Salerno.

ANTONIO MARICONDA – PhD candidate in International Law, University of Naples Federico II. Research Fellow, University of Milan 'La Statale' on the project "Arms, Peace, and Sustainability" (ArPeSu). Author of scientific articles on both public and private international law, published in Italian and international journals.

PIERFRANCESCO ROSSI – Assistant Professor of International Law, Department of Political Science, University of Teramo. Adjunct Professor at Luiss University, Rome. His main research interests are the jurisdictional immunities of states, international organizations and diplomatic and consular agents, and the interaction between international law and domestic legal orders.

SILVIA VENIER – Research fellow in International Law, Department of Social and Political Sciences, University of Trieste.