2021 13th International Conference on Cyber Conflict
Going Viral
T. Jančárková, L. Lindström, G. Visky, P. Zotz (Eds.)
2021 © NATO CCDCOE Publications, Tallinn

Covid-19 and the Cyber Pandemic: A Plea for International Law and the Rule of Sovereignty in Cyberspace

François Delerue
Research Fellow
Institut de recherche stratégique de l'École militaire (IRSEM)
Paris, France
francois.delerue@alumni.eui.eu

Abstract: There has been an important increase in threats and attacks in cyberspace during the Covid-19 crisis. Incidentally, States and other actors have condemned this *cyber pandemic* and highlighted the incompatibility of these behaviours with international law and the framework of responsible State behaviour.

From the perspective of international law, the rule of sovereignty appears to have a central role to play in addressing the malicious cyber activities that have taken advantage of the coronavirus pandemic. Indeed, most of these malicious cyber activities may only constitute breaches of sovereignty. Sovereignty is, however, among the most unsettled and contentious parts of international law, even among the so-called 'like-minded' States, which have expressed very different interpretations.

Building on these observations, the present article investigates the different types of cyber operations that unfolded during the Covid-19 pandemic and questions their characterization in relation to the rules and principles of international law. It assesses the theoretical role of the rule of sovereignty in crisis management during a cyber pandemic as well as its actual use in State practice. Ultimately, it demonstrates the centrality of this rule of international law and how the current sanitary crisis may constitute a plea for its application – or perhaps its rejuvenation – and for its further development in State practice.

Keywords: *Covid-19, coronavirus, international law, sovereignty, espionage, SolarWinds*

1. INTRODUCTION

States and other actors have condemned the Covid-19 cyber pandemic and highlighted the incompatibility of such behaviours with international law and with the framework of responsible State behaviour. Cyber threats fuelled by Covid-19 were notably discussed during two Arria-Formula meetings of the United Nations Security Council. The first, which took place on 22 May 2020, focused on *Cyber Stability, Conflict Prevention and Capacity Building* and was organized by Estonia, in cooperation with Belgium, the Dominican Republic, Indonesia and Kenya.[1] The second meeting, which occurred on 26 August 2020, was dedicated to *Cyber Attacks Against Critical Infrastructure*, and was organized by Indonesia, in cooperation with Belgium, Estonia and Vietnam, as well as the International Committee of the Red Cross.[2] Representatives of different States spoke at these Arria-Formula meetings and reaffirmed the importance of international law in the fight against the cyber pandemic. The United States representatives at these two Arria-Formula meetings of the UN Security Council, for instance, condemned these behaviours and recalled the importance of international law.[3] Moreover, some States condemned these behaviours in their contributions to the ongoing UN processes on the peace and stability of cyberspace.

In addition to these collective efforts, States have also unilaterally condemned the cyber operations that took advantage of the Covid-19 pandemic and those that targeted institutions involved in the management of the crisis. In condemning them, they generally reasserted the centrality of international law in ensuring the peace and stability of cyberspace, including in these difficult times. For instance, the European Union condemned the malicious cyber activities exploiting the coronavirus pandemic through a declaration by the vice-president of the European Commission, Josep Borrell, on 30 April 2020. In it, he 'call[ed] upon every country to exercise due

1 'Arria-Formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building' (*What's in blue*, 21 May 2020) <https://www.whatsinblue.org/2020/05/arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building.php> accessed 24 March 2021.

2 'Arria-Formula Meeting on Cyber-Attacks Against Critical Infrastructure' (*What's in blue*, 25 August 2020) <https://www.whatsinblue.org/2020/08/arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure.php> accessed 24 March 2021.

3 United States Mission to the United Nations, Ambassador Cherith Norman Chalet, 'Remarks at a UN Security Council Arria-Formula Meeting on Cyber Stability and Responsible State Behavior in Cyberspace (via VTC)' (United States Mission to the United Nations 2020) <https://usun.usmission.gov/remarks-at-a-un-security-council-arria-formula-meeting-on-cyber-stability-and-responsible-state-behavior-in-cyberspace-via-vtc/> accessed 24 March 2021; United States Mission to the United Nations, Rodney Hunter, 'Remarks at a UN Security Council Arria-Formula Meeting on Cyber Attacks Against Critical Infrastructure (via VTC)' (United States Mission to the United Nations 2020) <https://usun.usmission.gov/remarks-at-a-un-security-council-arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure-via-vtc/> accessed 24 March 2021.

diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law …'.[4]

Interestingly, however, we can observe a discrepancy between these general declarations and the condemnations in which the same States have denounced particular cyber operations that took advantage of the sanitary crisis. The United States, for instance, condemned the cyber operations that targeted a hospital in the Czech Republic in April 2020[5] and the Georgian Ministry of Health in September 2020.[6] Each time, they mentioned the 'framework of responsible State behavior in cyberspace, including nonbinding norms' but without making any reference to international law, nor stating which rule or principle of international law had been breached by these malicious activities. It is also conceivable that the United States considered these behaviours to be lawful and condemned them as unfriendly acts. These behaviours are likely to constitute violations of sovereignty, but their consequences were unlikely to have met the threshold of harm required by the United States as a criterion of a violation of sovereignty in cyberspace.[7]

Building on these observations, the present article explores the different types of cyber operations associated with the Covid-19 pandemic and questions their characterization in relation to existing rules and principles of international law. It assesses the theoretical role of the rule of sovereignty in the management of the cyber pandemic crisis, as well as its actual application and implementation in State practice. Ultimately, it demonstrates the centrality of this rule of international law and how the current sanitary crisis may constitute a plea for its application, if not for its rejuvenation, but also for its further development in State practice.

There are five sections in this article, the introduction being the first. The second section analyses the different types of cyber operations associated with the Covid-19 pandemic. The third section briefly introduces the international law applicable to cyber operations. The fourth section assesses the lawfulness of the cyber pandemic under international law. Finally, the fifth section discusses the role of the rule of sovereignty

4 European Union, 'Declaration by the High Representative Josep Borrell, on Behalf of the European Union, on Malicious Cyber Activities Exploiting the Coronavirus Pandemic' (Council of the European Union, 30 April 2020) <https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/> accessed 24 March 2021.

5 United States Secretary of State, Michael R. Pompeo, 'The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector' (U.S. Department of State, 17 April 2020) <https://cz.usembassy.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/> accessed 24 March 2021.

6 United States Embassy in Georgia, 'U.S. Embassy Statement on September 1, 2020 Cyberattack against Georgian Ministry of Health' (U.S. Embassy in Georgia, 1 September 2020) <https://ge.usembassy.gov/u-s-embassy-statement-on-september-1-2020-cyberattack-against-georgian-ministry-of-health/> accessed 24 March 2021.

7 United States, Brian J. Egan, 'Remarks on International Law and Stability in Cyberspace' (US Department of State 2016) <https://2009-2017.state.gov/s/l/releases/remarks/264303.htm> accessed 24 March 2021.

in managing the cyber pandemic crisis and how it may affect the different approaches adopted by some States in interpreting this rule of international law.

2. DECONSTRUCTING THE CYBER PANDEMIC

The Covid-19 pandemic has been marked by an important increase in the number of threats and operations in cyberspace. This cyber pandemic takes mainly two forms: first, some cyber threats have taken advantage of the pandemic-induced crisis; second, other cyber threats have been expressly directed at the health care sector and at the institutions involved in the management of the crisis. Among others, some States are believed to be responsible for a certain portion of these malicious cyber activities. The objective of the present section is to briefly introduce these different cyber operations and to identify which of them may have been conducted or sponsored by States and, incidentally, the rules and principles of international law that may be applicable in such cases.[8] Aside from the cyber pandemic, Covid-19 has also been accompanied by an *infodemic*; that is to say, disinformation campaigns that use the pandemic as a vector. Because the present article focuses on cyber operations, the infodemic lies outside its scope and is not studied here.[9]

The first category covers cyber threats that take advantage of the pandemic and may be qualified as opportunistic cyber operations. The spread of Covid-19 has been marked by an exponential digitalization of our lives, either for work, education or entertainment, or in our interactions with loved ones. Moving these activities online has created numerous new vulnerabilities that may be exploited by malicious actors. The fact that many workers have been working remotely – thus, shifting their activities to personal computers and networks that may not have the same security features as the ones usually used at the office – is also a source of vulnerability. The European Union Agency for Cybersecurity (ENISA),[10] Europol,[11] Interpol,[12] and

8 On the question of the attribution of cyber operations, see generally: François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 55–189; Dennis Broeders, Els De Busser and Patryk Pawlak, 'Three Tales of Attribution in Cyberspace. Criminal Law, International Law and Policy Debates' (The Hague Program for Cyber Norms, Policy Brief 2020) <https://www.thehaguecybernorms.nl/research-and-publication-posts/three-tales-of-attribution-in-cyberspace-criminal-law-international-law-and-policy-debates> accessed 24 March 2021; Kristen E Eichensehr, 'The Law and Politics of Cyberattack Attribution' (2020) 67 U.C.L.A. Law Review 520, 520–598; Michael N Schmitt and Liis Vihul (eds), *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 87–100.

9 See notably: Barrie Sander and Nicholas Tsagourias, 'The Covid-19 Infodemic and Online Platforms as Intermediary Fiduciaries under International Law' (2020) 11 JHLS 331, 331–347; Marko Milanovic and Michael N Schmitt, 'Cyber Attacks and Cyber (Mis)Information Operations During a Pandemic' (2020) 11 JNSLP 247, 266 et seq.

10 ENISA, 'COVID-19' (European Union Agency for Cybersecurity 2021) <https://www.enisa.europa.eu/topics/wfh-covid19> accessed 24 March 2021.

11 Europol, 'COVID-19 Sparks Upward Trend in Cybercrime' (Europol, 5 October 2020) <https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime> accessed 24 March 2021.

12 INTERPOL, 'COVID-19 Cyberthreats' (INTERPOL 2021) <https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats> accessed 24 March 2021.

the United States Cybersecurity and Infrastructure Agency (CISA)[13] – among many others – have drawn attention to these cyber threats. Notably, they pointed out that cybercriminals have been using the pandemic as a vector for phishing campaigns, ransomware attacks, and for spreading malware, online scams and disinformation campaigns. As cybercriminal activities are outside the scope of this article, they will not be further discussed.

In addition, the digitalization of the life of citizens throughout the world may have been exploited by some States. State agents and actors operating as their proxies may be using similar techniques, notably phishing campaigns, to take advantage of the vulnerabilities that arose from the digitalization of our societies. In weakening the cyber hygiene of individuals, especially as they continue working from home on personal devices and using less secure networks, the pandemic increases the potential for attacks and creates new opportunities for malicious actors to target these individuals. In doing so, the main objective is likely to gain access to the credentials of the targeted individuals and, ultimately, access to their devices to steal, compromise or destroy data.

Furthermore, the second category deals with cyber operations that target actors involved in the management of the Covid-19 crisis. The healthcare sector, in particular, faces numerous threats from cyberspace while they need to treat patients suffering from the coronavirus.[14] For instance, hospitals in various countries have been targeted by different cyber threats, such as ransomware attacks and Distributed Denial of Service (DDoS) attacks.[15]

Hence, in these challenging times, information is key. It appears that different actors have conducted cyber operations to get access to information and data on the spread of the virus and on the measures adopted in different countries. The Chinese cybersecurity company Qihoo 360 accused the advanced persistent threat (APT) known as DarkHotel, allegedly linked to South Korea, of having conducted a cyber espionage campaign against Chinese and international institutions, presumably to obtain information on the spread of the virus.[16] Similarly, APT 32, also known as OceanLotus Group, a group generally believed to be linked to Vietnam, has been

13 CISA, 'Coronavirus' (United States Cybersecurity and Infrastructure Agency 2021) <https://www.cisa.gov/coronavirus> accessed 24 March 2021.

14 Liviu Arsene, '5 Times More Coronavirus-Themed Malware Reports during March' (*Bitdefender*, 20 March 2020) <https://labs.bitdefender.com/2020/03/5-times-more-coronavirus-themed-malware-reports-during-march/> accessed 24 March 2021.

15 Matt Burgess, 'Hackers Are Targeting Hospitals Crippled by Coronavirus' (*Wired*, 22 March 2020) <https://www.wired.co.uk/article/coronavirus-hackers-cybercrime-phishing> accessed 24 March 2021; Emmanuel Paquette, 'En pleine crise du coronavirus, les hôpitaux de Paris victimes d'une cyberattaque' (*L'Express*, 23 March 2020) <https://lexpansion.lexpress.fr/high-tech/en-pleine-crise-du-coronavirus-les-hopitaux-de-paris-victimes-d-une-cyberattaque_2121692.html> accessed 24 March 2021.

16 Jeff Stone, 'A Chinese Security Firm Says DarkHotel Hackers Are behind an Espionage Campaign, but Researchers Want More Details' (*CyberScoop*, 6 April 2020) <https://www.cyberscoop.com/dark-hotel-qihoo-360-covid-19/> accessed 24 March 2021.

accused of having conducted cyber espionage activities against the staff of the Chinese Ministry of Emergency Management and of the Government of Wuhan.[17] At the global level, international organizations involved in the management of the sanitary crisis and the exchange of information have also been targeted.[18] The staff of the World Health Organization, for instance, has been targeted by phishing email campaigns.[19]

Additionally, the race for a vaccine against Covid-19 has been subjected to cyber operations targeting research institutions. Canada, the United Kingdom, and the United States have accused APT 29, also known as Cozy Bear, a group generally believed to be associated with Russian intelligence agencies, of using malware named WellMess or WellMail to target institutions involved in the development of Covid-19 vaccines.[20] Likewise, APT 38, also known as the Lazarus Group, and believed to be linked to North Korea, has been accused of targeting a pharmaceutical company developing a Covid-19 vaccine as well as a government institution involved in the management of the crisis.[21]

To sum up, the cyber operations in the second group show two different trends. On the one hand, some cyber operations aim at disrupting the daily management of hospitals; these activities normally do not match the usual profile of State conducted or sponsored operations. On the other hand, certain cyber operations strive to gather information on the spread of the virus, the management of the crisis by different actors, as well as to gain access to research on the development of a vaccine; the latter are more likely to be conducted or sponsored by States.

In conclusion, this section assessed the malicious cyber activities linked to the Covid-19 pandemic and showed that States are likely to conduct or sponsor operations to gather information and data, either targeting individuals that are more vulnerable in these challenging times or institutions involved in the management of the crisis and in the development of vaccines. The identification of the types of cyber operations that may have been conducted by States and their proxies allows us to assess their lawfulness

17 Raphael Satter and Jack Stubbs, 'Vietnam-Linked Hackers Targeted Chinese Government over Coronavirus Response: Researchers' (Reuters, 22 April 2020) <https://www.reuters.com/article/us-health-coronavirus-cyber-vietnam/vietnam-linked-hackers-targeted-chinese-government-over-coronavirus-response-researchers-idUSKCN2241C8> accessed 24 March 2021.

18 Kaspersky Lab (GReAT), 'APT Annual Review: What the World's Threat Actors Got up to in 2020' (*Securelist*, 3 December 2020) <https://securelist.com/apt-annual-review-what-the-worlds-threat-actors-got-up-to-in-2020/99574/> accessed 24 March 2021.

19 Joseph Menn and others, 'Hackers Linked to Iran Target WHO Staff Emails during Coronavirus' (Reuters, 2 April 2020) <https://www.reuters.com/article/us-health-coronavirus-cyber-iran-exclusi-idUSKBN21K1RC> accessed 24 March 2021.

20 UK NCSC, 'Advisory: APT29 Targets COVID-19 Vaccine Development' (United Kingdom's National Cyber Security Centre (NCSC) 2020) <https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development.pdf> accessed 24 March 2021.

21 Seongsu Park, 'Lazarus Covets COVID-19-Related Intelligence' (*Securelist*, 23 December 2020) <https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/> accessed 24 March 2021.

(Section 4). But, before that, the next section briefly introduces the international legal framework applicable to cyber operations.

3. INTERNATIONAL LAW APPLIES TO CYBER OPERATIONS

International law, and in particular the Charter of the United Nations, is the backbone of contemporary international relations and remains crucial in maintaining international peace and security. Nowadays, the applicability of international law to cyberspace is consensual among States and other actors: international law applies to cyberspace and cyber operations.[22] This has notably been affirmed by the consensual reports of the United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security in 2013 and 2015, and later confirmed by the majority of States on various occasions.[23] The question of the applicability of international law being settled, the debate has moved on to the question of how the rules and principles of international law are to be applied to cyberspace.

At the multilateral level, the effort to clarify the interpretation of the rules and principles of international law has already been undertaken by the third, fourth and fifth UN GGEs. The failure of the fifth UN GGE, in June 2017, actually resulted from this endeavour as it highlighted certain divergences among the participating States. The disagreement that erupted between the participating experts of the fifth UN GGE had nothing to do with the applicability of certain branches of international law to cyberspace but rather with the opportunity to enshrine a specific interpretation in the

22 See notably: Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge Studies in International and Comparative Law, Cambridge University Press 2012); Georg Kerschischnig, *Cyberthreats and International Law* (Eleven International Publishing 2012); Michael N Schmitt (ed), *The Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013); Katharina Ziolkowski (ed), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (NATO Cooperative Cyber Defence Centre of Excellence 2013); Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014); Scott J Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace* (Cambridge University Press 2014); Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014); Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfection of International Law* (Brill & Martinus Nijhoff Publishers 2015); Schmitt and Vihul (n 8); Henning Lahmann, *Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution* (Cambridge University Press 2020); Delerue (n 8).

23 See, for instance: UNGA 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013) UN Doc A/68/98 2013 8, para 19; UNGA '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/70/174 2015 12, para 24 et seq.

final report, as well as the particularities of interpreting them in the cyber context.[24] Today, these questions are again part of the mandate of the ongoing sixth UN GGE and of the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, created by UNGA Resolutions 73/266 and 73/27, respectively.

In recent years, there has also been important evolution in State practices regarding the international law applicable to cyberspace, in two main directions.

First, a growing number of States have publicized their approach on the rules and principles of international law applicable to cyberspace.[25] Two important caveats must be addressed though. On the one hand, fewer than a dozen States have made their interpretation public. On the other hand, the vast majority of the detailed approaches now publicized have been released by Western States. Therefore, the picture we have is geographically limited and partial. This second limitation may, however, recede in the future for two reasons. First, the recent publication by Iran of its approach may actually incentivize other non-Western States to follow suit.[26] It is indeed the first time that a non-Western State has publicly disclosed a detailed approach on this matter. Second, UNGA Resolution 73/266 requested that the States participating in the UN GGE submit their views on how international law should be applied to cyberspace. As such, there is a growing push for the States not taking part in the UN GGE to disclose their views as well, notably within the framework of the OEWG.

Second, States are increasingly developing and strengthening their practice on conducting and reacting to cyber operations. A growing number of States has been integrating cyber-related dispositions in their military manuals and domestic regulations on military and intelligence activities, a process that reflects, to some extent, their compliance with their international legal obligations. Yet, it is difficult to assess the compliance of their practice in conducting or sponsoring cyber operations, since it remains a predominantly covert practice. As for reacting to cyber operations, some States have developed a practice of 'naming and shaming' those States responsible for conducting malicious cyber activities. An important limitation to this observation is that these public attributions have only been done by a limited number of States,

24 François Delerue, Frédérick Douzet and Aude Géry, *The Geopolitical Representations of International Law in the International Negotiations on the Security and Stability of Cyberspace / Les Représentations Géopolitiques Du Droit International Dans Les Négociations Internationales Sur La Sécurité et La Stabilité Du Cyberespace* (IRSEM and EU Cyber Direct 2020) <https://eucyberdirect.eu/content_research/the-geopolitical-representations-of-international-law-in-the-international-negotiations-on-the-security-and-stability-of-cyberspace/> accessed 24 March 2021.

25 See the analysis in Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views' (Policy Brief, The Hague Program for Cyber Norms 2020) <https://www.thehaguecybernorms.nl/news-and-events-posts/policy-brief-application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views> accessed 24 March 2021.

26 Iran, 'General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat' (NOURNEWS Analytics & News Agency 2020) <https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat> accessed 24 March 2021.

usually Western ones, and predominantly by the Five Eyes Member States (Australia, Canada, New Zealand, the United Kingdom and the United States).[27] Interestingly, the vast majority of cases of the public attribution or condemnation of cyber operations have made no reference to international law. Only a few have come out to make loose references to international law or to the international rules-based order. None of these statements has ever clearly characterized which rule or principle of international law has been breached, nor referred to the categories of the international legal framework used to attribute and react to these acts.

Yet, other actors have been active in clarifying how international law applies to cyberspace and cyber operations. The most advanced example is the *Tallinn Manual* process initiated in 2009 by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE), which led to the publication of the *Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual 1.0)* in 2013[28] and the *Tallinn Manual on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0)* in 2017.[29] The NATO CCDCOE just announced the beginning of the work on a third version of the *Tallinn Manual*.[30] Another good example is the Cyber Law Toolkit, which offers an in-depth exemplification of the application of international law to cyber operations through scenarios.[31] Other actors, including some from the private sector, NGOs and expert groups, have addressed the questions pertaining to international law as part of the broader theme of the framework of responsible State behaviour – a framework that also includes norms of responsible behaviour and confidence-building measures. Moreover, recent initiatives and developments have demonstrated that international law applies, and offers a relevant legal framework, to the cyber operations that take advantage of the sanitary crisis, such as the Oxford Process.[32] Additionally, different academic publications have come to the same conclusion, such as, for instance, the seminal article by Marko Milanovic and Michael N. Schmitt.[33]

27 Florian J Egloff, 'Contested Public Attributions of Cyber Incidents and the Role of Academia' (2020) 41 Contemporary Security Policy 55, 61.

28 Schmitt (n 22).

29 Schmitt and Vihul (n 8).

30 'CCDCOE to Host the Tallinn Manual 3.0 Process' (NATO Cooperative Cyber Defence Centre of Excellence, 14 December 2020) <https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/> accessed 24 March 2021.

31 'International Cyber Law in Practice: Interactive Tookit' (Cyber Law Toolkit) <https://cyberlaw.ccdcoe.org/> accessed 24 March 2021.

32 Two online events gathered international lawyers to debate the rules and principles of international law applicable in such circumstances and led to the adoption of related statements: 'The Oxford Statement on the International Law Protections Against Cyber Operations Targeting the Health Care Sector' (Oxford Institute for Ethics, Law and Armed Conflict (ELAC), University of Oxford 2020) <https://elac.web.ox.ac.uk/the-oxford-statement-on-the-international-law-protections-against-cyber-operations-targeting-the-hea> accessed 24 March 2021; 'The Second Oxford Statement on International Law Protections of the Healthcare Sector During Covid-19: Safeguarding Vaccine Research' (Oxford Institute for Ethics, Law and Armed Conflict (ELAC), University of Oxford 2020) <https://elac.web.ox.ac.uk/article/the-second-oxford-statement> accessed 24 March 2021.

33 Milanovic and Schmitt (n 9).

This brief introduction to the debates surrounding the international law applicable to cyber operations leads to three observations. First, there is no contestation of the international legal framework applicable to cyber operations: the rules and principles of international law do apply to cyber operations. As highlighted regarding the failure of the fifth UN GGE in 2017, the disagreement is mainly political rather than legal. It did not show any opposition to the applicability of the rules and principles nor to their interpretation. Second, the international discussions, the unilateral statements by States on their respective approaches, the scholarly literature and all the other initiatives provide us with a good picture of the relevant rules and principles that are applicable to cyber operations, including in these challenging times of the current pandemic. However, the implementation of the international legal framework in State practice remains relatively limited. Third, despite the absence of opposition to the international legal framework, some divergences appear on its interpretation and on the concrete application of certain rules and principles. In fact, the interpretation of the rule or principle of sovereignty appears to be the most contentious issue, as shown in the next section.

4. APPLYING INTERNATIONAL LAW TO THE CYBER PANDEMIC

In this section, the objective is to assess whether the cyber operations conducted or sponsored by States during the pandemic constitute internationally wrongful acts. To be an internationally wrongful act, the action or omission must be attributable to a State and constitute a breach of an international obligation.[34] The question of attribution is not discussed in the present article and we will focus on the second element.[35] There are three main obligations that may be breached by cyber operations in general: the prohibition of the use or threat of force, the prohibition of intervention, and the rule of sovereignty.[36] In addition, the principle of due diligence appears to be particularly relevant in addressing cyber threats related to the Covid-19 pandemic.[37]

In a recent article, Marko Milanovic and Michael N. Schmitt assessed that the majority of cyber operations against healthcare facilities and capabilities may be violating the sovereignty of other States.[38] I agree with this assessment and this will be demonstrated in the present section. As discussed earlier, in taking advantage of the Covid-19

34 *Articles on Responsibility of States for Internationally Wrongful Acts* (adopted by the International Law Commission at its fifty-third session in 2001, annexed to General Assembly Resolution 56/83 of 12 December 2001, and corrected by Document A/56/49 (Vol I)/Corr4), Article 2. For a discussion on the characterization of cyber operations as internationally wrongful acts, see: Schmitt and Vihul (n 8) 84, rule 14; Delerue (n 8) 381.

35 Delerue (n 8) 55–189.

36 Schmitt and Vihul (n 8), rules 4, 66, 68–70; Delerue (n 8) 193–342.

37 François Delerue and Joanna Kulesza, 'Cybersecurity in the Year of the Plague: Due Diligence as a Remedy to Malicious Activities' (2020) 2 Tecnologie e Diritto 404, 404–419.

38 Milanovic and Schmitt (n 9).

pandemic, several States and their proxies have been predominantly conducting cyber operations aimed at gathering information and data, either by targeting individuals that are more vulnerable in these challenging times or institutions involved in the management of the crisis and in the race to find a vaccine. This section analyses these cyber operations in relation to the main rules and principles of the international law applicable to cyber operations.

A. The Cyber Pandemic and the Prohibition of the Use of Force

To constitute an unlawful use of force, a cyber operation would need to provoke physical damage, human injury or death.[39] There is no agreement on whether a cyber operation with no physical effect, but causing very significant damage in cyberspace, may amount to unlawful use of force.[40]

It is conceivable that some cyber operations taking advantage of the Covid-19 pandemic could have significant consequences and thus be characterized as unlawful uses of force. For instance, we could consider the example of a State-sponsored ransomware disrupting the normal running of a hospital, thus leading to the death of patients who could not receive the necessary care in time or because they received the wrong treatment.[41] That being said, none of the alleged State conducted or sponsored cyber operations that have occurred since the outbreak of Covid-19 came close to this required threshold of consequences. Therefore, even if it is theoretically possible, it seems highly unlikely that State conducted or sponsored cyber operations taking advantage of Covid-19 would constitute a use of force.

B. The Cyber Pandemic and the Prohibition of Intervention

To constitute an unlawful intervention, a cyber operation must meet three criteria, as stressed most famously by the International Court of Justice in the *Nicaragua* case.[42] First, an intervention must be carried out by a State or its proxy acting against another State. Second, the prohibited intervention concerns matters in which the targeted State is permitted to decide freely, encompassing external or internal affairs. Third, the element of coercion constitutes an essential component of a prohibited intervention.

39 Schmitt and Vihul (n 8) 329–338.

40 For instance, the French ministry of defence stated that 'France does not rule out the possibility that a cyberoperation without physical effects may also be characterized as a use of force', in: France, 'International Law Applied to Operations in Cyberspace' (ministère des Armées 2019) 7 <https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf> accessed 24 March 2021.

41 In September 2020, a ransomware attack, not attributed to a State, that targeted a hospital in Düsseldorf was believed to have contributed to the death of a patient by delaying her treatment. The subsequent investigation concluded, however, that the ransomware was not responsible for the death. Willian Ralston, 'The untold story of a cyberattack, a hospital and a dying woman' (*Wired UK*, 11 November 2020) <https://www.wired.co.uk/article/ransomware-hospital-death-germany> accessed 24 March 2021.

42 *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America)* (Merits) [1986] ICJ Rep 14, 107–108, para 205.

A prohibited intervention must constitute an attempt to coerce the targeted State by directly or indirectly interfering in the internal or external affairs of this State.[43]

The first two criteria are not specifically challenged by the features of the above-discussed cyber operations and are not discussed further for that reason. Conversely, assessing whether these cyber operations meet the third criterion is a trickier question. Indeed, the vast majority of cyber operations observed during the Covid-19 pandemic aimed at collecting data and information but did not have a coercive objective. The objective being to gather data and information to support the sponsoring State's policy and strategy and not to influence the targeted State.

True, the stolen data may be leaked or instrumentalized to coerce the targeted State. Yet, in such cases, the theft and the use of the data are two different acts,[44] the former being likely to constitute a breach of sovereignty while the second being more likely to be an unlawful intervention.

C. The Cyber Pandemic and Sovereignty

Cyber malicious acts taking advantage of the Covid-19 pandemic may, in most cases, constitute a violation of the sovereignty of the targeted States.[45] Indeed, most of these cyber operations aimed at penetrating computer systems and networks located on the territory of other States are meant to access and steal data. Unauthorized penetration into computer systems constitutes the basis of a violation of sovereignty. Yet, it must be noted that it remains one of the most contentious questions dealing with the international law applicable to cyber operations, since the States have adopted very different approaches, which I summarize below.

The different approaches revolve around three mains debates about sovereignty in cyberspace. First, whether sovereignty is a rule or a principle of international law. Second, on the reach of sovereignty when it is applied to cyberspace. Third, there remains a plurality of views on what may constitute a breach of territorial sovereignty in cyberspace.

First, the nature of territorial sovereignty in cyberspace is not settled. Sovereignty is a general principle of international law from which certain rules are derived, including the prohibition of the violation of territorial sovereignty.[46] Both rules and principles are sources of international law, and they are notably listed in Article 38 of the Statute

43 Philip Kunig, 'Intervention, Prohibition Of', *MPEPIL* (2008), para 1; Gaetano Arangio-Ruiz, 'Human Rights and Non-Intervention in the Helsinki Final Act' (1977) 157 RCADI 195, 257, 261 *et seq*.

44 Delerue (n 8) 241–256.

45 Milanovic and Schmitt (n 9) 252–256.

46 In outlining the Israeli perspective on the international law applicable to cyber operations, Roy Schöndorf wrote an interesting analysis of these different aspects of sovereignty in cyberspace: 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (9 December 2020) <https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/> accessed 24 March 2021.

of the International Court of Justice.[47] Rules refer to the actual norms of international law, from treaties or customary international law, for example. Furthermore, principles refer to the more abstract notions from which rules flow. While States agree on the existence of a general principle of sovereignty, they have divergent opinions on the rules flowing from that principle. Indeed, while some consider sovereignty only as a principle of international law in the cyber realm (e.g. the United Kingdom),[48] the majority argues that it is a rule.

Second, there is no consensus on what constitutes State sovereignty in cyberspace. For instance, there are ongoing debates over whether States are entitled to exercise sovereignty over data located on computers belonging to other entities which may or may not be located on the State's territory.[49] The confusion is amplified by the conflation between sovereignty as a political concept and sovereignty as defined by international law.

Third, there are multiple definitions of what may amount to a breach of territorial sovereignty when it comes to cyber operations. Among the limited number of States that have publicly disclosed their views on the matter, we can identify three main perspectives. In the first approach, any cyber operation that penetrates a foreign system or produces effects over it constitutes a violation of sovereignty. This is, for instance, the French approach.[50] Then, in the second approach, a cyber operation penetrating a foreign system constitutes a violation of sovereignty only if it meets a certain threshold of harm. This is the approach adopted in the *Tallinn Manual 2.0*[51] and by the United States.[52] It should be noted, however, that the position expressed recently by Paul Ney,[53] the General Counsel of the US Department of Defence, seemed to lean towards a third approach.[54] With that last approach, territorial sovereignty cannot be breached by a cyber operation unless it constitutes a violation of the principle of non-intervention. This is, for instance, the British approach.[55] These three different approaches have been formulated by Western States, usually considered to be 'like-minded' States, and it is plausible that other approaches may be expressed by other States in the future.

47 *Statute of the International Court of Justice*, annexed to the Charter of the United Nations, adopted 26 June 1945, entered into force 24 October 1945, 3 Bevans 1179, 59 Stat. 1031, T.S. 993, 39 AJIL Supp. 215 (1945).

48 United Kingdom, Jeremy Wright, 'Cyber and International Law in the 21st Century' (UK Attorney General's Office 2018) <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century> accessed 24 March 2021.

49 See, for instance, the discussion in: Roy Schöndorf (n 46).

50 France (n 40).

51 Schmitt and Vihul (n 8) 17–26, rule 4.

52 United States, Brian J. Egan (n 7).

53 Paul C Ney, Jr, 'DOD General Counsel Remarks at U.S. Cyber Command Legal Conference' (2020) <https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/> accessed 24 March 2021.

54 Michael N Schmitt, 'The Defense Department's Measured Take on International Law in Cyberspace' (*Just Security*, 11 March 2020) <https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/> accessed 24 March 2021.

55 United Kingdom, Jeremy Wright (n 48).

If we apply the three approaches to the malicious cyber operations taking advantage of the Covid-19 pandemic, they would constitute violations of sovereignty under the first approach but be deemed lawful under the third approach. Moreover, it seems doubtful that these cyber operations met the threshold of harm required by the States having adopted the second approach.

Aside from these three approaches, the *Tallinn Manual 2.0*, and some States such as the Netherlands,[56] have laid out another basis that may constitute a breach of the rule of sovereignty: when 'there has been an interference or usurpation of inherently governmental functions'.[57] There are two criteria to sustain this one: first, it must concern 'inherently governmental functions'. As rightly pointed out by Marko Milanovic and Michael N. Schmitt, while the management of the sanitary crisis is likely to be considered an inherently governmental function, it is more debatable regarding the provision of healthcare.[58] Consequently, this first criterion needs to be assessed on a case-by-case basis. According to the second criterion, the concerned cyber operation should be an interference or usurpation of these functions. As previously highlighted, most cyber operations within that purview aim at accessing and stealing data, without further action. Even if this data is linked to inherently governmental functions, it appears debatable – if not unlikely – that they may be seen as either a usurpation or an interference of these functions.

In conclusion, most cyber operations taking advantage of the Covid-19 pandemic are likely to constitute, in theory, violations of the territorial sovereignty of the affected States, yet unlikely to be considered as such by several States under their own interpretation of the rule in this particular context. For the majority of States that have expressed their views on the international law applicable to cyber operations, these cyber operations would fall short of a violation of sovereignty, either because they did not cause sufficient harm, they did not interfere or usurp inherently governmental functions, or because they did not constitute unlawful interventions.

5. THE NECESSITY OF AN EVOLUTION OF THE STATES' APPROACH ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS

This assessment of the lawfulness of the cyber operations that take advantage of the Covid-19 pandemic confirms that the main challenge is not the identification of the relevant rules or principles of international law but rather their interpretation and

56 The Netherlands, 'Letter to the Parliament on the International Legal Order in Cyberspace (Appendix on International Law in Cyberspace)' (Government of the Netherlands 2019) 3 <https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace> accessed 24 March 2021.

57 Schmitt and Vihul (n 8) 20–23, paras 10, 15–18. See also the analysis of this basis in the context of cyber espionage, in: Russell Buchan, *Cyber Espionage and International Law* (Bloomsbury Publishing 2018) 61.

58 Milanovic and Schmitt (n 9) 253, 255–256.

implementation by States. This assessment also highlights that the cyber operations taking place in these challenging times are similar to the ones usually conducted or sponsored by States: they are predominantly activities of cyber espionage. The situation is different not because the cyber operations are different but because their number may have increased and, more importantly, because their targets have received increased attention. Therefore, interest in this topic is not linked to an evolution in State practice in the specific context of the Covid-19 pandemic but rather to an evolution in the way we apprehend these matters in these challenging times.

International law offers a legal framework that applies to and regulates such behaviours; it also provides response mechanisms for the injured States, such as countermeasures.[59] Yet, several States and scholars have decided to take an unconventional approach to the rule of sovereignty in cyberspace by either denying its existence or conditioning it to a threshold of harm. Why such a specific approach in the cyber realm? In any other domain, the mere unauthorized trespassing of a border, for instance by an aircraft or boat, is enough to constitute a violation of sovereignty and no threshold of harm is required. In cyberspace, the trespassing of a border is constituted by the unauthorized penetration into a computer system regardless of the potential harm caused.[60] It has been argued that the addition of a threshold of harm as well as the opposition to the existence of a rule of territorial sovereignty in cyberspace was motivated by the willingness of States to avoid limitations on their espionage capabilities. Adopting an approach that is too broad on the rule of sovereignty in cyberspace would indeed contradict espionage activities that heavily rely on the penetration of foreign computer systems.[61]

Building on these observations, it may be asserted that, by highlighting State practice in cyberspace, the Covid-19 cyber pandemic calls upon us to reconsider two questions, starting with the different approaches to the rule of sovereignty in cyberspace that coexist. Then, we need to reassess the difficult equilibrium between the necessity to ensure the peace and stability of cyberspace through international law and the framework of responsible State behaviour, and the willingness of States to pursue certain unfriendly, if not adversarial, activities, such as intelligence gathering campaigns.

In fact, it may be time for States to rethink their approach to the rule of sovereignty in cyberspace and to decide whether such activities (i.e. cyber espionage campaigns) should be deemed unlawful or not, according to their approaches to how international law applies in cyberspace. If they are to be considered lawful, States may continue to condemn them: despite their lawfulness, they could be deemed unethical or immoral. In that case, however, States would deprive themselves of the lawful responses offered

59 Schmitt and Vihul (n 8) 111–134, rules 20–25; Delerue (n 8) 433–460.
60 Delerue (n 8) 215–219.
61 On the international law applicable to cyber espionage, see generally: Asaf Lubin, 'The Liberty to Spy' (2020) 61 Harvard International Law Journal 185; Buchan (n 57).

by the law of countermeasures, which are useful and relevant tools to compel the wrongful State to cease its behaviour and repair eventual injuries.

The recent SolarWinds case and the US 'defend forward' cyber strategy lead to a similar questioning. First, in the SolarWinds case, countless articles and comments have argued that SolarWinds constitutes an armed attack and that the United States would be entitled to invoke their right of self-defence in response.[62] Yet, as rightly pointed out by Jack Goldsmith, this seems to be purely a cyber espionage campaign in which State-backed hackers penetrated computer systems to access and steal data.[63] In that sense, the SolarWinds case is very similar to several cases of cyber operations that took advantage of the Covid-19 pandemic. They are cyber espionage activities pure and simple. By restraining the rule of sovereignty in cyberspace, States have made such activities lawful and have thus deprived themselves of the responses allowed by international law. Second, the implementation of the 'defend forward' cyber strategy by the United States is likely to take the form of cyber operations breaching given rules and principles of international law, predominantly the rule of sovereignty. In 2019, for instance, the *New York Times* reported that the US Cyber Command hacked the computer systems running the Russian power grid as a preparatory measure for potential further actions.[64] Such behaviours, which are to some extent comparable to the actions against SolarWinds, are likely to constitute blatant violations of the rule of sovereignty. These examples highlight the discrepancy that may exist between rhetoric and practice for some States.

In disregarding certain rules of international law in practice, as well as in limiting their reach through a particular interpretation of international law, States appear to be turning their backs on the international rules-based order. Such an approach bears the risk of endangering the international peace and stability of cyberspace. If international law is not perfect and has not prevented breaches of peace and aggressions in the past, it constitutes a powerful tool and the best regulatory framework at our disposal if we want to avoid turning cyberspace into a new Wild West.

62 See for instance, Thomas P Bossert, 'I Was the Homeland Security Adviser to Trump. We're Being Hacked.' *The New York Times* (16 December 2020) <https://www.nytimes.com/2020/12/16/opinion/fireeye-solarwinds-russia-hack.html> accessed 24 March 2021; Yevgeny Vindman, 'Is the SolarWinds Cyberattack an Act of War? It Is, If the United States Says It Is' (*Lawfare*, 26 January 2021) <https://www.lawfareblog.com/solarwinds-cyberattack-act-war-it-if-united-states-says-it> accessed 24 March 2021.

63 Jack Goldsmith, 'Self-Delusion on the Russia Hack' (*The Dispatch*, 18 December 2020) <https://thedispatch.com/p/self-delusion-on-the-russia-hack> accessed 24 March 2021.

64 David E Sanger and Nicole Perlroth, 'U.S. Escalates Online Attacks on Russia's Power Grid' *The New York Times* (15 June 2019) <https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html> accessed 24 March 2021.