2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Cyber Law and Espionage Law as Communicating Vessels

Dr. Asaf Lubin
Post-Doctoral Cyber Research Fellow
Fletcher School of Law and Diplomacy
Tufts University
Medford, MA, United States

Abstract: Existing legal literature would have us assume that espionage operations and "below-the-threshold" cyber operations are doctrinally distinct. Whereas one is subject to the scant, amorphous, and under-developed legal framework of espionage law, the other is subject to an emerging, ever-evolving body of legal rules, known cumulatively as cyber law. This dichotomy, however, is erroneous and misleading. In practice, espionage and cyber law function as communicating vessels, and so are better conceived as two elements of a complex system, Information Warfare (IW). This paper therefore first draws attention to the similarities between the practices – the fact that the actors, technologies, and targets are interchangeable, as are the knee-jerk legal reactions of the international community. In light of the convergence between peacetime Low-Intensity Cyber Operations (LICOs) and peacetime Espionage Operations (EOs) the two should be subjected to a single regulatory framework, one which recognizes the role intelligence plays in our public world order and which adopts a contextual and consequential method of inquiry. The paper proceeds in the following order: Part 2 provides a descriptive account of the unique symbiotic relationship between espionage and cyber law, and further explains the reasons for this dynamic. Part 3 places the discussion surrounding this relationship within the broader discourse on IW, making the claim that the convergence between EOs and LICOs, as described in Part 2, could further be explained by an even larger convergence across all the various elements of the informational environment. Parts 2 and 3 then serve as the backdrop for Part 4, which details the attempt of the drafters of the *Tallinn*

Manual 2.0 to compartmentalize espionage law and cyber law, and the deficits of their approach. The paper concludes by proposing an alternative holistic understanding of espionage law, grounded in general principles of law, which is more practically transferable to the cyber realm.

Keywords: *international law, information warfare, espionage, cyber law, Tallinn Manual 2.0, sovereignty, diplomatic law, consular law, general principles of law*

1. INTRODUCTION

Here is a story in two parts. In Part I, the Defense Minister for the Republic of Scamdinavia is honey-trapped by an attractive showgirl. During the course of their secret affair, the showgirl introduces the Minister to a senior naval attaché from the Embassy of Cyberia. The Minister, who quickly befriends the attaché, invites the latter to visit his home. Upon arrival, the attaché creates a diversion and seizes the opportunity to enter the Minister's private office, placing a pen-shaped recording device on his desk and photographing top-secret documents pertaining to the Department's security contracts and research spending. As a result, a number of top-secret Department of Defense projects are jeopardized, and the Minister is forced to resign.[1]

The second part begins with a series of phishing emails, sent to a number of major corporations across Scamdinavia, by a private hacking group with support and direction from Cyberia's central intelligence agency. The emails contain a trojan downloader. Within an eight-month period, roughly 50,000 computers are infected by the malicious code. Exploiting zero-day vulnerabilities in Microsoft XML Core Services, the malware begins modifying Windows registries, poisoning local DNS caches, disabling antivirus programs, and sequencing certain information harvesting and hard disk wiping processes. As a result of the attack, a number of financial institutions in Scamdinavia are unable to provide services and take weeks to fully restore functionality, causing significant economic losses. To make matters worse, the

1 This hypothetical is loosely based on one of the biggest spy scandals and political controversies of the Cold War era, the 1961 Profumo Affair. At the centre of the public blunder stood John Profumo, then Secretary of State for War, who was discovered to have had a sexual affair with model and showgirl Christine Keeler. Keeler was also romantically involved with Evgenii Ivanov, a senior naval attaché at the Soviet Embassy and an officer of the Soviets' Main Intelligence Directorate. At Keeler's invitation, Profumo and Ivanov met and soon became friends. Relying on his intimate access to Profumo's home and office, Ivanov was able to photograph highly classified documents pertaining to allied contingency plans for the Cold War defense of Berlin, as well top-secret specifications of US spy planes and nuclear weapons. Secretary Profumo initially denied the allegations of impropriety raised against him, but he eventually was forced to resign from his post, a fact that played a role in hastening the end of Harold Macmillan's term as Prime Minister. For further reading see JONATHAN HASLAM, NEAR AND DISTANT NEIGHBORS: A NEW HISTORY OF SOVIET INTELLIGENCE, 207-209 (2015); Leon Watson, *I Did Betray My Country: Fifty Years After Profumo's Resignation, Christine Keeler Confesses She Passed Secrets to Russians*, DAILY MAIL (9 June 2013), available at http://goo.gl/kPyXQT.

secret data of major government contractors is breached, and a number of top-secret Department of Defense projects are jeopardized.[2]

Existing legal literature would have us assume that these two hypothetical scenarios are doctrinally distinct. The first scenario is a textbook example of interstate spying, and insofar as it is regulated at all, it is only subject to the scant, amorphous, and under-developed legal framework of *espionage law*.[3] The second scenario, on the other hand, involves an example of what is colloquially termed a "cyber attack", which is subject to an emerging, ever-evolving body of legal rules, known cumulatively as *cyber law*.[4] This dichotomy, however, is erroneous and misleading. In practice, espionage and cyber law function as communicating vessels, and so are better conceived as two elements of a complex system, Information Warfare (IW). The paper draws attention to the similarities between the practices – the fact that the actors, technologies, and targets are interchangeable, as are the knee-jerk legal reactions of the international community. In light of the convergence between peacetime low-intensity cyber operations and peacetime espionage operations, the two should be subjected to a

2 This hypothetical is inspired by the events that transpired in South Korea on 20 March 2013 and are commonly known as the "Dark Seoul" incident. The attack, which occurred at approximately 2:15pm, hit television broadcasters YNT and MBC, as well as banks KBS, Shinhan, Nonghyup, and Jetu. South Korea's communicating regulator, Park Jae-Moon, released a statement suggesting that: "unidentified hackers used Chinese IP addresses to contact servers of the six affected organizations and plant malware which attacked their computers." Based on previous practice of North Korea to spoof Chinese IP address, a number of high-ranking officials from South Korea pointed their finger to Pyongyang. For further reading see Jonathan A.P. Marpaung & HoonJae Lee, *Dark Seoul Cyber Attack: Could it Be Worse*, 6th Conference of Indonesian Students Association in Korea (7 July 2013), available at http://goo.gl/MgCI9u; *China IP Address link to South Korea Cyber-Attack*, BBC News (21 March 2013), available at http://goo.gl/wm43kQ.

3 As Prof. Chesterman has argued, intelligence exists "in a legal penumbra, lying at the margins of diverse legal regimes and at the edge of international legitimacy." Elsewhere he noted that: "despite its relative importance in the conduct of international affairs, there are few treaties that deal with it directly. Academic literature typically omits the subject entirely or includes a paragraph or two defining espionage and describing the unhappy fate of captured spies. For the most part, only special regimes such as the laws of war address intelligence explicitly. Beyond this, it looms large but almost silently in the legal regimes dealing with diplomatic protection and arms control." See Simon Chesterman, *The Spy Who Came In From the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L. L. 1071, at 1072, 1130 (2006); Richard Falk, foreword, in ESSAYS ON ESPIONAGE AND INTERNATIONAL LAW v, v (Roland J. Stranger ed., 1962) ("traditional international law is remarkably oblivious to the peacetime practice of espionage. Leading treatises overlook espionage altogether or contain a perfunctory paragraph that defines a spy and describes his hapless fate upon capture"); Christopher D. Baker, *Tolerance of International Espionage: A Functional Approach*, 19 AM. U. INT'L. L. REV.1091, 1091 (2004) ("Espionage is curiously ill-defined under international law, even though all developed nations, as well as many lesser-developed ones, conduct spying and eavesdropping operations against their neighbors"); Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SEC. L. & POL'Y 115, 116 (2014) ("there is a long-standing (and cynically named) 'gentleman's agreement' between nations to ignore espionage in international law").

4 *See e.g.*, MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2nd ed., 2017); UN General Assembly Resolution on an International Code of Conduct for Information Security, UN Doc. A/66/359 (14 September 2011); Elaine Korzak, *UN GGE on Cybersecurity: The End of an Era?*, THE DIPLOMAT (31 July 2017), available at http://goo.gl/BSWfnm; Louise Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations, in* 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (Czosseck & Ziolkowski eds., 2012); Joseph S. Nye Jr., *The World Needs New Norms on Cyberwarfare*, THE WASHINGTON POST (1 October 2015), available at http://goo.gl/NuC4z7; Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT ON THE ISSUES (14 February 2017), available at goo.gl/4xPN7F.

single regulatory framework, one which recognizes the role that intelligence plays in our public world order and which adopts a contextual and consequential method of inquiry.

Part 2 of this paper provides a descriptive account of the unique symbiotic relationship between espionage and cyber law. It further explains the reasons for this dynamic and applies its findings to the two hypothetical scenarios introduced above. Part 3 then situates the discussion surrounding this relationship within the broader discourse on IW, making the claim that the convergence identified in Part 2 could further be explained by an even larger convergence across all the various elements of the informational environment. Parts 2 and 3 serve as the backdrop for Part 4, which details the attempt of the drafters of *Tallinn Manual 2.0* to compartmentalize espionage law and cyber law, and the deficits of their approach. The paper concludes by proposing in Part 5 an alternative holistic understanding of espionage law, grounded in general principles of law, which is more practically transferable to the cyber realm.

2. LAW OF COMMUNICATING VESSELS

> "If you had a bent tube, one arm of which was the size of a pipe-stem and the other big enough to hold the ocean, water would stand at the same height in one as in the other. Thus discussion equalizes fools and wise men in the same way, and the fools know it."
>
> -Oliver Wendell Holmes[5]

The experiment described in the quote, what Justice Holmes called the "hydrostatic paradox of controversy", is merely the Justice's cynical take on a classic principle of fluid mechanics, according to which the levels of homogenous liquid in a system of connected containers will always aspire to be equal, since the pressures on those levels are equal. Thus, if additional liquid is added to one vessel, the liquid will immediately find a new equal level in all connected vessels. This image of the "communicating vessels" experiment carries with it a powerful metaphor, which has been used across the humanities and social sciences, from construing surrealist thought,[6] to characterizing international policies on torture.[7] In this paper, I argue that the trite principle could also be helpful in describing the dialectical relationship between espionage law and cyber law.

What do I mean by "espionage" and "cyber"? It is worth recalling that: "no

5 2 JOHN T. MORSE, LIFE AND LETTERS OF OLIVER WENDELL HOMES 40 (1896). The statement was made by Holmes in response to an article in *The Nation* which harshly criticized his philosophy.

6 ANDRÉ BRETON, COMMUNICATING VESSELS (Translated by Mary Ann Caws & Geoffrey Harris, 1990).

7 STEVEN DEWULF, THE SIGNATURE OF EVIL: (RE)DEFINING TORTURE IN INTERNATIONAL LAW 535-551 (2011).

internationally recognized and workable definition of 'intelligence collection' exists."[8] Similarly "there are no common definitions for Cyber terms – they are understood to mean different things by different nations/organizations".[9] Given these innate ambiguities, it is important that I provide working definitions for both terms at the outset of this paper. To begin with, I am only interested in those cyber and espionage operations that occur in peacetime, given that wartime spying and cyber warfare are more constrained by the rules of international humanitarian law, and in any event occur at a far lesser rate than their peacetime equivalents. Limiting myself to peacetime cyber operations further narrows the scope of cyber activities to be examined, as it excludes from review those operations that by their scale and effect are likely to trigger an international armed conflict or to provoke responses in self-defense. Our attention thus automatically shifts to Low-Intensity Cyber Operations (LICOs). These are "below-the-threshold" operations which have not only proven to be significantly costly in recent years, but are in fact commonplace, as Michael Schmitt notes: "Few, if any, cyber operations have [ever] crossed the armed attack threshold".[10]

With Espionage Operations (EOs), I tend to cast the net quite wide, using the terms "espionage", "intelligence collection", "surveillance", and "reconnaissance" interchangeably, thus rejecting method-based definitional distinctions. Instead, I use the term EOs to mean a peacetime operation which encompasses the following four elements: (1) the operation involves the gathering, analysis, verification, and dissemination of information of relevance to the decision-making process of a State or States or otherwise serves some State interests; (2) the operation is launched by agents of a State or States, or those with a sufficient nexus to the State or States in question; (3) the operation targets a foreign State or States, their subjects, associations, corporations, or agents, without the knowledge or consent of that State or those States; and (4) the operation involves some degree of secrecy and confidentiality, as to the needs behind the operation and/or the methods of collection and analysis employed,

8 Sulmasy and Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L. L. 625, 637 (2007).

9 *Cyber Definitions*, NATO Cooperative Cyber Defence Centre of Excellence, available at http://goo.gl/wtAkWP.

10 Michael N. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA. J. INT'L L. 697, 698 (2014). For further reading on the nature of LICOs see: Beatrice Waldon, Note, Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law, 126(5) YALE L. J. 1242 (2017). See also James R. Clapper, Statement of the Record, US Cybersecurity and Policy, Senate Armed Services Committee (29 September 2015), available at goo.gl/aWSgKH (where Clapper makes an alarming prediction: "we foresee an ongoing series of low-to-moderate level cyber-attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security").

so to ensure its effectiveness.[11] Notice that I exclude from review various forms of unconcealed open-source intelligence gathering, such as reading a newspaper, visiting a social media website, or gathering information in the course of routine diplomatic relations (element 4). I further exclude from my analysis domestic forms of surveillance focusing solely on interstate activities, launched by one State and its proxies (element 2) against another State and its proxies (element 3).

Already visible is the close proximity in nature between EOs and LICOs, for our definition of LICOs could also be limited only to interstate interactions (especially if we are to distinguish between LICOs and more local forms of domestic cyber crime). The only difference, therefore, between EOs and LICOs rests on the first element. Unlike EOs, LICOs can only be employed against electronic information (as opposed to non-electronic physical properties, *e.g.* a passport kept in a dresser or printed bank records stored in a cabinet). Moreover, LICOs are different as they may extend beyond the mere passive copying and storing of data to other more aggressive and coercive forms of electronic intrusion (e.g. altering, removing, disrupting, degrading, or destroying certain information, programs, systems, or networks).[12]

Therefore, if we put EOs and LICOs in a Venn diagram (see below in Figure 1), not only will the circle-circle overlap be significant (encompassing different types of cyber espionage and electronic surveillance operations), but the remaining sets will share profound similarities. I provide below a list of hypothetical examples of operations which are either exclusively EOs, exclusively LICOs, or in between, to exemplify those similarities.

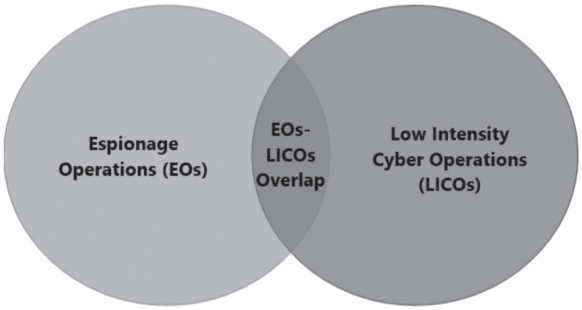
It is this affinity between EOs and LICOs that creates the "communicating vessels" phenomenon. Any attempt to modify or extend existing bodies of international law to better regulate LICOs will inevitably result in tidal waves that will engulf EOs.

11 This definition mirrors in some respects, and departs from in others, the definition put forward by Dermarest: "espionage can be defined as the consciously deceitful collection of information, ordered by a government or organization hostile to or suspicious of those the information concerns, accomplished by humans unauthorized by the target to do the collecting" (Geoffrey Dermarest, *Espionage in International Law*, 24 DENV. J. INT'L L. & POL'Y 321, 326). Note that as highlighted in Dermarest's definition, and as a general rule, intelligence operations involve some degree of secrecy and confidentiality to ensure their effectiveness (operations *de cape et d'épée*, coupled with some degree of deceitful intent). That said such is not always mandated (*e.g.* open source intelligence collection).

12 Note that my definition of EOs excludes "covert action" operations. These types of activities have a different primary purpose than the acquisition of intelligence. They seek the "purposive attenuation of the options of the target", influencing economic, ideological, political, diplomatic, and military conditions abroad. See W. MICHAEL REISMAN AND JAMES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS, AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW 10-12 (1992) (Reisman and Baker provide a useful list of examples of covert activities ranging from psychological operations and disinformation to political assassinations). If I were to include covert action into the definition of EOs, additional similarities between EOs and LICOs will surface (consider, for example, Russian interferences in elections as reflecting both covert action and a "below the threshold" cyber intrusion). In other words, expanding the definition of EOs to include covert action will entail extending its purpose beyond "mere passive copying and storing of information to other more aggressive types" of intrusions (namely the disruptive, degrading, and destructive kind).

Conversely, any attempt at normative compartmentalization or regulatory insulation could be equated to challenging a law of physics and would not pass the smile test.

FIGURE 1: VENN DIAGRAM OF EOS AND LICOS INTERSECTION



Exclusively EOs:

- Launching a spy satellite into space to engage in geo-spatial monitoring of a rogue country.
- Placing human agents in a major oil company, gathering information about its strategic plans.
- Gathering information about a government ministry relying on diplomatic engagements and open source materials.
- Placing cameras and microphones in the apartment of cyber criminals and monitoring their business dealings.
- Entering a training camp for a terrorist organization and seizing certain documents relating to an impending attack.

Exclusively LICOs:

- Jamming the communications links of a commercial satellite and sending it false GPS coordinates.
- Launching a ransomware attack against a major oil company, shutting down its operations for a short period.
- Launching a DDoS operation against a non-essential government service website.
- Hacking the devices of cyber criminals and blocking their access to a certain cryptocurrency.
- Installing malware on laptop computers at a terrorist training camp, circumventing a terrorist plot by altering certain data stored therein.

EOs-LICOs Overlap:

- Hacking a spy satellite for the purpose of gathering information about its technical specifications.
- Installing malware on the tablet of an oil company's CEO to gather information about the company's strategic plans.
- Hacking the DNS server of a government ministry and monitoring the internet activities of the ministry's staff.
- Hacking the devices of cyber-criminals and monitoring their business dealings by remotely activating certain sensors.
- Installing spyware on laptop computers at a terrorist training camp, and seizing certain documents relating to an impending attack.

To further my point, let us examine some areas of convergence between peacetime EOs and LICOs. First, both passive intelligence collection and mildly more aggressive cyber intrusions are launched by the same primary actors – State intelligence and security agencies and/or their proxies – and using the same advanced technological tools. Unit 8200 of Israel provides one good example,[13] and APT33 with its ties to Iran's Cyber Army offers another.[14] This reality is owed in part to the fact that traditional EOs now rely heavily on cyber techniques to increase their likelihood of success and broaden their scope of impact. For 16th century Sir Francis Walsingham, the father of modern intelligence agencies, "a global mass surveillance program involved paying off travellers in the ports of Lyon and merchant adventurers in the bazars of Hamburg".[15] Today, we cannot imagine an intelligence agency that would be satisfied with such low-tech techniques. SIGINT-based tools, such as the hacking of connected devices and the interception of electronic communications (either targeted or in bulk) have now significantly overshadowed the old historical techniques. The rise to predominance of Cyber-HUMINT, as its own distinct discipline, proves that even the most traditional of spying methodologies is not immune from this wave of digitalization.[16] Once an agency controls a band of cyberspies, calibrating between passive collection and moderately more offensive intrusions is left to its discretion and capacity limitations. So it is not surprising that the NSA is hoarding zero-day

13 John Reed, *Unit 8200: Israel's Cyber Spy Agency*, FINANCIAL TIMES (10 July 2015), available at goo.gl/951paE.

14 Eric Auchard, *Once 'Kittens' in cyber spy world, Iran gains prowess: security experts*, REUTERS (20 September 2017), available at https://goo.gl/DCmDkf; Jaqueline O'Leary *et al., Insight into Iranian Cyber Espionage*, FIREEYE (20 September 2017), available at https://goo.gl/vcS6Wc.

15 Asaf Lubin, *A Principled Defence of the International Human Right to Privacy: A Response to Frédéric Sourgens*, 42(2) YALE J. INT'L. L. 1, 2 (2017).

16 Andy Greenberg, *Cyberespionage is a Top Priority for CIA's New Directorate*, WIRED (9 March 2015), available at goo.gl/YWp5Zx (discussing the CIA's "digital overhaul" and quoting Jim Lewis from the Center for Strategic and International Studies, who notes: "Those 'humint' operations, as the intelligence community calls them, typically involve real spies on the ground, unlike the NSA's remote cyber espionage or the cyberwarfare activities of the Pentagon's Cyber Command. 'This kind of cyber activity has become increasingly important to them' … That combination of humint and digital operations could mean a spy infiltrating an organization to plant spyware by hand, for instance, or a digital investigation to check the bona fides of a source or agent. 'If you think of NSA operations as a vacuum cleaner and Cyber Command as a hammer, this is a little more precise, and it's about supporting human operations'").

vulnerabilities,[17] that the CIA controls a whole vault of cyber tools,[18] or that the FBI hacks thousands of foreign computers in the dark web with a trove of malware.[19]

Second, both EOs and LICOs thrive on "plausible deniability" and demand increased levels of deception and secrecy, intrinsically resisting mechanisms of accountability. Think of an undercover agent who is masquerading one day as a 30-year-old Danish female protester at a reproductive rights rally and the next day as a 55-year-old German wheelchair-bound male social worker. Now think of the Chinese hacker who is spoofing his way through the Tor network, one day hijacking the computer of a real Danish protester and the next adopting the online identity of an actual German social worker. Both operations, due to their unique nature, create similar and significant evidentiary hurdles for assigning individual and State responsibility under traditional international legal frameworks.[20]

Finally, both EOs and LICOs target information in ways that are non-kinetic and below-the-threshold, triggering the same knee-jerk international legal reactions. The victims of spying and cyber operations have a limited basket of potential claims that they might raise for a violation of international law, namely: violations of sovereignty, territorial integrity, the principle of non-intervention, the prohibition on extraterritorial enforcement, certain human rights abuses (such as the rights to privacy and freedom of expression), certain property rights abuses (including IP rights), and other potential State and individual immunities and privileges, depending on the subject matter of the operation.[21] What is more, common to both EOs and LICOs is the fact that the international norms enumerated in the above list are sufficiently under-defined to leave ambiguity as to whether an actual violation of a primary rule of international law had occurred. The *Tallinn Manual 2.0* was in this regard an attempt to clarify (if not codify) the "key aspects of the public international law governing 'cyber operations' during peacetime".[22] Put differently, the experts in *Tallinn 2.0* sought to elucidate the law of LICOs in isolation from the law on EOs. As I will show later, this unfortunate compartmentalized approach adopted by the *Manual*'s authors proves counterproductive at offering effective regulation. For now, let me conclude this section by showing in Table 1 how the two hypotheticals that opened this paper exemplify the convergence between EOs and LICOs.

17 *See e.g.*, Andy Greenberg, *The Shadow Brokers Mess is What Happens when the NSA Hoards Zero-Days*, WIRED (17 August 2016), available at goo.gl/zUdceh.

18 *See e.g.*, Lorenzo Franceschi-Bicchierai, *The secret-spilling organization launches a new series where it will release the source code of alleged CIA tools from the Vault 7 series*, MOTHERBOARD (9 November 2017), available at goo.gl/5C8eyN.

19 *See e.g.*, Joseph Cox, *The FBI Hacked over 8,000 Computers in 120 Countries Based on One Warrant*, MOTHERBOARD (22 November 2016), available at goo.gl/wWRtm2.

20 *See e.g.* John S. Davis *et al., Stateless Attribution: International Accountability in Cyberspace*, RAND CORPORATION (2017), available at https://www.rand.org/pubs/research_reports/RR2081.html; Dieter Fleck, *Individual and State Responsibility for Intelligence Gathering*, 28 MICH. J. INT'L. L. 687 (2007).

21 For potential violations from EOs, *see generally* Chesterman, n. 3. For potential violations from LICOs see Waldon, n. 10, at 1469-1477.

22 MICHAEL N. SCHMITT (ED.), TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (2nd ed., 2017) 3.

TABLE 1: AREAS OF CONVERGENCE BETWEEN EOS AND LICOS AS REFLECTED IN THE HYPOTHETICALS

	Part I: Classic EO	Part II: Classic LICO
Instigator	Cyberia's Intelligence	Private Hackers with Support from Cyberia's Intelligence
Tech Employed	Recording Device and Photography	Malware Capable of Both Copying Data and More Disruptive Functions
Accountability Thwarting Mechanism	Unidentified Showgirl, Clandestine Operation	Untraceable Phishing Emails and Hard-To-Detect Trojan Downloader
Goal of Operation	Information on Top Secret DOD R&D Projects	Information on DOD R&D Projects, Economic Disruption and Losses
Potential International Law Violations	Sovereignty, Non-Intervention, Diplomatic Law, Privileges and Immunities, Property Rights, Privacy Rights	Sovereignty, Non-Intervention, Privileges and Immunities, Property Rights, Privacy Rights

3. INFORMATION WARFARE: COMMUNICATING VESSELS WITHIN A UNIFIED SYSTEM

Dr Martin Libicki of the RAND Corporation gave one of the keynote addresses in the 8th International Conference on Cyber Conflict. In his remarks, he made the claim that the old 1990s DoD catch-phrase "Information Warfare" (IW) was making a comeback.[23] IW as a unified theory suggests that "competition over information would be the high ground of warfare,"[24] and that such competitions would involve "the protection, manipulation, degradation and denial of information".[25] It employs the following litmus test: "If information is used to perpetrate an act that was done to influence another to take or not take actions beneficial to the attacker then it can be considered IW".[26] Due to this broad test, different scholars at different times have introduced different elements that form part of IW. Libicki, for example, in his 1995 short monograph *What Is Information Warfare*, introduced it as a heptagon of methods of varying maturity, encompassing:

23 Martin C. Libicki, *The Convergence of Information Warfare*, STRATEGIC STUD. Q. 49, 50 (2017) ("given today's circumstances, in contrast to those that existed when information warfare was first mooted, the various elements of IW should now increasingly be considered elements of a larger whole rather than separate specialties that individually support kinetic military operations").

24 *Id*., at 49.

25 MARTIN C. LIBICKI, WHAT IS INFORMATION WARFARE? X (1995).

26 A. JONES AND G. KOVACICH, GLOBAL INFORMATION WARFARE: THE NEW DIGITAL BATTLEFIELD 5 (2nd ed., 2016).

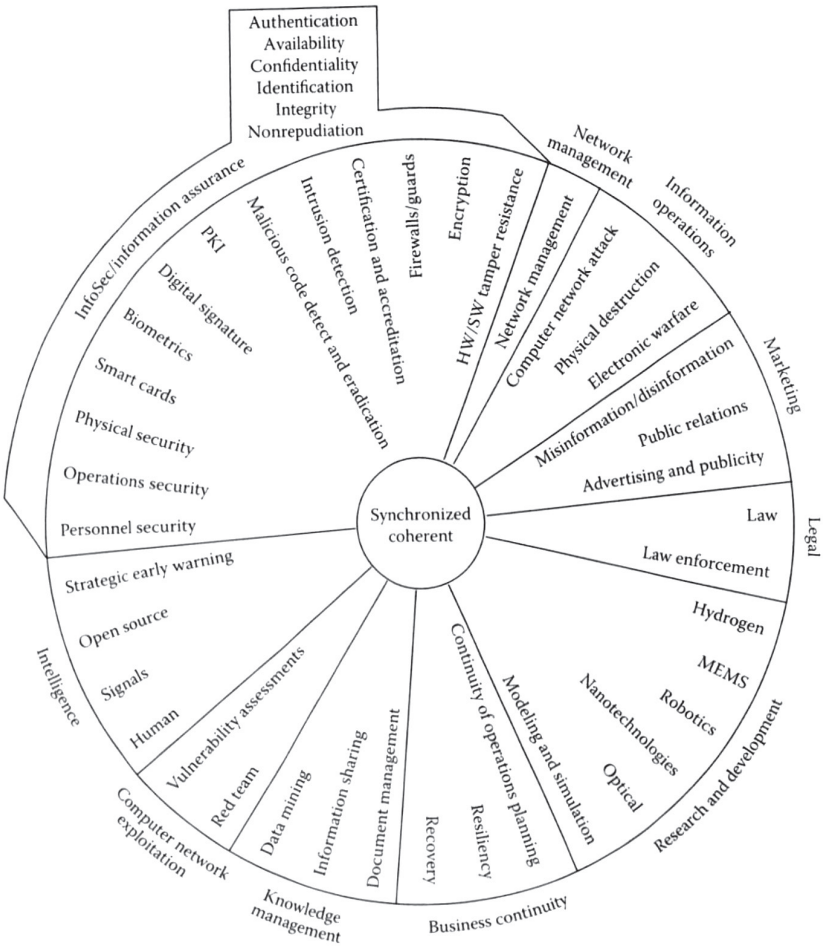
> "(i) command-and-control warfare (which strikes against the enemy's head and neck); (ii) intelligence based warfare (which consists of design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space); (iii) electronic warfare (radio-electronic or cryptographic techniques); (iv) psychological warfare (in which information is used to change the minds of friends, neutrals, and foes); (v) 'hacker' warfare (in which computer systems are attacked); (vi) economic information warfare (blocking information or channelling it to pursue economic dominance); and (vii) cyberwarfare (a grab bag of futuristic scenarios)".[27]

Jones and Kovacich go even further, arguing that IW covers a whole spectrum of elements including, *inter alia*: lawfare, business continuity, knowledge management, information security, computer network exploitation, and intelligence.[28]

27 Libicki, n. 25, at X. Note that today Libicki seems to take a far more condensed approach to the elements encompassing IW, suggesting it covers ISR operations (intelligence, surveillance, and reconnaissance), electronic warfare (EW0, psychological operations (PSYOP), and Cyber Operations. *See* Libicki, n. 23, at 49. Directive 3600.1 of the US DoD similarly adopted this multi-dimensional approach in defining IW's core and supporting capabilities. The original directive was adopted in 1996 but has since been amended twice in 2006 and 2013. In its latest iteration it defines "Information Operations" as "the integrated employment, during military operations, of information-related capabilities (IRC) in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" (DODD O-3600.01, Information Operations (IO) 12 (2 May 2013), available at goo.gl/wJJX6T). The directive proceeds to note that IRCs constitute "tools, techniques, or activities" employed within a dimension of the information environment. These can include, but are not limited to, "a variety of technical and non-technical activities that intersect the traditional areas of electronic warfare, cyberspace operations, military information support operations (MISO), military deception (MILDEC), influence activities, operations security (OPSEC), and intelligence." *Id*., at 1.

28 *See* Jones and Kovacich, n. 26, at 6.

FIGURE 2: JONES AND KOVACICH'S ELEMENTS OF INFORMATION WARFARE



Regardless of which model of IW you adopt, all seem to include both certain EOs and LICOs as components of the broader theater of informational conflict. Libicki argues that the recent convergence of the IW's various elements, and the theory's broader resurgence as a unified doctrine, can be explained by three emerging circumstances:

> "First, the various elements can use many of the same techniques, starting with the subversion of computers, systems, and networks, to allow them to work. Second, as a partial result of the first circumstance, the strategic aspects of these elements are converging. This makes it more likely that in circumstances where

> one element of IW can be used, other elements can also be used. Hence, they can be used together. Third, as a partial result of the second circumstance, countries – notably Russia, but, to a lesser extent, North Korea, Iran and China – are starting to combine IW elements, with each element used as part of a broader whole."[29]

I highlight the discourse on IW because I feel it is important that we place the unique dialectical relationship between EOs and LICOs within a broader informational enviornment. These are two communicating vessels which form part of an even larger machine and the operating logic of that machine, as laid down in the above quote by Libicki, helps further explain the special relationship of EOs and LICOs. Assistant Secretary of Defense Eric Rosenbach once referred to cyber operations as filling the gap between diplomacy and economic sanctions on the one hand, and military action on the other. He called this gap, "the space between" and claimed that cyber operations within this space assist policy-makers in achieving their national interest.[30] The imagery of the space between is useful, but unlike Rosenbach's depiction, it encompasses much more than just cyber operations. A far larger spectrum of informational action, both cyber and non-cyber, occupies this "space between", with intelligence gathering and covert action constituting a significant and historical component. Any attempt at regulating some aspects of this space, in isolation from others, would be ill-fated.

4. THE COMPARTMENTALIZATION APPROACH AND THE TALLINN MANUAL 2.0

Against this backdrop, I want to begin portraying what was attempted in the *Tallinn Manual 2.0*. Rule 32 on "peacetime cyber espionage" is located in Section 5 of the *Manual*, which covers those cyber operations that the Group of Experts (GoE) deemed to be "not *per se* regulated by international law". According to the GoE, customary international law "does not prohibit espionage *per se*",[31] and therefore

29 *See* Libicki, n. 23, at 50.

30 For further reading see Thomas E. Ricks, *The Future of War: Cyber is Expanding the Clausewitzian Spectrum of Conflict*, FOREIGN POLICY (13 November 2014), available at goo.gl/1Nrsmi.

31 Note that the Experts rely on a single source to make this claim, basing themselves on the Office of General Counsel, Department of Defense Law of War Manual. However, paragraph 16.3.2, to which they cite, makes no reference to a lack of customary regulation of espionage under international law, quite the opposite is speaks clearly of "long-standing and well-established considerations" and "long-standing international norms" which govern this practice. *See* DEPARTMENT OF DEFENSE, LAW OF WAR MANUAL 990 (2016) ("international law and long-standing international norms are applicable to State behavior in cyberspace, and the question of the legality of peacetime intelligence and counterintelligence activities must be considered on a case-by-case basis. Generally, to the extent that cyber operations resemble traditional intelligence and counter-intelligence activities, such as unauthorized intrusions into computer networks solely to acquire information, then such cyber operations would likely be treated similarly under international law. The United States conducts such activities via cyberspace, and such operations are governed by long-standing and well-established considerations, including the possibility that those operations could be interpreted as a hostile act.")

determinations of lawfulness should be made on a case-by-case basis taking into account the particular methods employed in the conduct of the specific EO.[32] This allowed the GoE to avoid the need to address the hot potato of comprehensively explaining the law and practice of government espionage. What is more, it furthered the GoE's desire to compartmentalize spying, in its traditional sense, from the more specific cyber espionage and LICOs which regulation the *Manual* sought to elucidate. But as Chesterman has taught us, claiming that espionage is not *per se* regulated under international law is nothing more than a straw man: "Intelligence is less a lacuna in the legal order than it is the elephant in the room".[33] Well, the elephant was alive and well during the *Tallinn Manual* plenary sessions. It swayed its trunk and stomped its feet; but was nonetheless ignored.

Tossing to the side the question of the lawfulness of peacetime intelligence gathering, the GoE dodged the need to speak in higher granularity as to the conduct of interstate spying. Instead, the way was paved for the experts to engage in more general and casuistic reasoning. Throughout their commentary, the experts extract and extend legal rules from a series of tailored hypothetical scenarios, of their own design, which they then analyse in isolation from one another and in accordance with predominantly treaty norms. This "divide-and-conquer" approach is far from harmonious and results in a series of fragmented statements made throughout the *Manual*, each with varying degrees of consensus behind it. Every one of these statements can be compared to liquid being added to one of the vessels. Due to the communicative nature of cyber law and espionage law, as discussed above, any regulation of cyber espionage put forward by the experts – that is to say any regulation of the EOs-LICOs overlap area in our original Venn diagram – automatically sends equilibrium-adjusting tidal waves across the entire system. The experts did not acknowledge these tidal waves, nor did they address the impractical legal realities that they would inevitably create. Let us take up only two examples within the limits of this paper.

The GoE took a territorially protectionist approach to sovereignty violations. According to them:

> "[I]n the cyber context [...] it is a violation of territorial sovereignty for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there."[34]

32 *Tallinn Manual 2.0*, n. 22, at 169-170 ("while the International Group of Experts agreed that there is no prohibition of espionage per se, they likewise concurred that cyber espionage may be conducted in a manner that violates international law due to the fact that certain methods employed to conduct cyber espionage are unlawful").

33 Chesterman, n. 3, at 1072.

34 *Tallinn Manual 2.0*, n. 22, at 19. This rule is then extended to the territorial sea (Rule 48) and the territorial airspace (Rule 55). The GoE is most explicit in the context of the physical tapping of submarine communication cables for the purpose of collecting data. The GoE agreed that "doing so in the territorial or archipelagic waters of another State constitutes a violation of that State's sovereignty". *Id*., at 257.

The GoE provide the example of an agent of one State who uses a USB flash drive to introduce malware into cyber infrastructures in another State and claim that this would result in a sovereignty violation.[35] The caveats provided ("in the cyber context", "cyber operations", etc.) are an attempt at compartmentalization, and have little meaning. If spies cannot clandestinely use a USB flash drive in the territory of a foreign country without it resulting in a sovereignty violation, it follows that they cannot also take photographs, handle HUMINT sources, or steal physical documents in that territory. Especially not in an age where all of these activities *de facto* require some form of cyber enabling. Going down this rabbit-hole, under basic rules of syllogistic logic, if every act of territorial spying results in a sovereignty violation, and every sovereignty violation is a violation of international law,[36] then territorial spying violates international law. Lo and behold, the same experts that concluded that espionage was not "prohibited *per se*", have just *per se* prohibited espionage in its most elementary form.[37] Their approach would seem to suggest that the only lawful way to conduct espionage in the 21st century is either by remote means,[38] or with consent (from the targeted State) or authorization (from the UN Security Council).

A second example comes in the form of the applicability of diplomatic and consular law to cyber espionage. The GoE argues that if a sending State launches spyware from within its diplomatic mission against the cyber infrastructures of another State that would constitute "an abuse of the diplomatic function and therefore an internationally wrongful act."[39] Similarly, if the receiving State or third States intercepted the electronic communications of diplomatic missions and consular posts, they would be violating "the confidentiality of diplomatic and consular communications",

35 *Ibid*. Note that the GoE later backtrack this definitive statement, arguing that they could not agree "on the lawfulness of close access cyber espionage operations, such as the insertion of USB flash drive into a computer located on one State's territory by an individual acting under the direction or control of another State". *Id*., at 171.

36 AJIL Unbound has recently held an online symposium titled "sovereignty, cyberspace, and Tallinn Manual 2.0" which focused on whether sovereignty constitutes a stand-alone binding international legal norm that may be violated. In this debate, I second the view put forward by Phil Spector that there is ample evidence to assert that sovereignty is in fact a binding rule. *See* Phil Spector, *In Defense of Sovereignty, In The Wake of Tallinn 2.0*, 111 AJIL UNBOUND 219 (2017).

37 Not only that, but the experts also claim that certain LICOs employed to enable spying operations, e.g. using cyber intrusions to 'herd' the target's communications to a platform more susceptible to surveillance, might itself trigger separate grounds for sovereignty violations. *Tallinn Manual 2.0*, n. 22, at 172.

38 *Id*., at 19 ("the mere interception of wireless signals from outside the target state's territory does not constitute a violation of that State's sovereignty"). Though even on the point of remote surveillance, there was those experts who argued that a severity test should be employed and that if the consequences suffered from the remote surveillance were so severe, they might too result in a sovereignty violation (*Id*., at 171). Put differently, for certain members of the GoE even spying from outer space, the high seas, or international airspace, might violate sovereignty if they reach a certain degree of severity. This echoes to me the Soviet concept of "danger theory" pushed, and rejected, in the 1960s following the U2 Spy Plane incident. The crux of the Soviet position was that sovereignty might be violated without incursions into national territory, so long as certain national rights were endangered due to a particular surveillance practice. For further reading *see* Joseph R. Soraghan, Reconnaissance Satellites: Legal Characterization and Possible Utilization for Peacekeeping, 13(3) McGill L. J. 458, 471-472 (1967) (quoting the work of Ronald Christensen, he notes that Soviet Russia regarded "her sovereignty rights as going beyond her territorial borders, ceasing, it seems, not even at the borders of another state, and, perhaps pervading the entire universe. No one anywhere, she says, has the right to endanger the Soviet Union").

39 *Id*., at 211-212, 229.

which is central to their function, and therefore will also result in an internationally wrongful act.[40] Once again, note that the repeated references to cyber technologies are inconsequential. The GoE, in essence, is banning espionage from within or against diplomatic missions, regardless of the method employed. If you cannot do it with a malware, there is nothing to justify doing it with your bare hands. The fact that "diplomacy and intelligence gathering have always gone hand in hand,"[41] and that the practice of spying from and on diplomatic missions is as historical as it is commonplace,[42] was not even mentioned in *Tallinn Manual 2.0*, let alone addressed or resolved. Consider the following three reported allegations from the past two decades: (1) In the lead-up to the UN Security Council vote authorizing the use of force against Iraq in 2003, the US and the UK spied on every single delegation to the Security Council;[43] (2) During the G20 talks in Toronto in 2010, the US and Canada spied on large numbers of heads of states and other diplomats in attendance;[44] (3) Between 2012-2017 Chinese agencies used backdoors into computer networks at the African Union Headquarters (networks which they had paid for and installed as a gift) in order to spy on the various delegations.[45] If one wanted to apply *Tallinn Manual 2.0* rules to these three operations, one would have to conclude that all of them violated international law. The same experts who sought to isolate intelligence gathering – to not *per se* address its lawfulness – ended up banning some of the most basic methods through which it is acquired and thereby the practice as a whole. Attempting to only regulate LICOs resulted in tidal waves that inadequately constrained EOs.

In attempting to cage the espionage elephant (by limiting their analysis to specific and self-selected cases of cyber espionage), the GoE found themselves engaging in textual treaty derivation which regurgitated the myth system while ignoring the operational code.[46] The experts did not appreciate fully what CIA analyst James Jesus Angleton

40 *Id*., at 221.

41 Chesterman, n. 3, at 1072.

42 Craig Forcese, *Spies Without Borders: International Law and Intelligence Collection*, 5 J. NAT'L SEC'Y L. & POL'Y 179, 197 (2011); Ashley Deeks, *An International Legal Framework for Surveillance*, 55(2) VIRG. J. INT'L L. 291, 313 (2015) (citing Antonin Scalia who at the time of working for the DOJ OLC drafted a memorandum which concluded that "the practice of spying on foreign missions was so widespread that the "inviolability" provision of the VCDR should not be read to prohibit such activities).

43 *See e.g*. Martin Bright and Peter Beaumont, *Britain spied on UN allies over war vote*, THE GUARDIAN (7 February 2004), available at http://goo.gl/fXhd8U.

44 *See e.g*. Paul Owen, *Canada 'allowed NSA to spy on G8 and G20 summits*', THE GUARDIAN (28 November 2013), available at http://goo.gl/HJB6mD.

45 *See e.g*. Reuters, *China rejects claim it bugged headquarters it built for African Union*, THE GUARDIAN (29 January 2018), available at http://goo.gl/i5yt2g.

46 As Professor W. Michael Reisman noted "in law things are not always what they seem," and one needs to be particularly mindful of the existence of "two 'relevant' normative systems: one which is supposed to apply and which continues to enjoy lip service among elites and one which is actually applied". Reisman describes the tension between the myth and the code as a "dynamic process" and a "symbiotic relationship". Acknowledging that the international law governing EOs and LICOs does not exist solely in the myth or solely in the code, but rather in the space between the two, would have benefited the quality of *Tallinn Manual 2.0*'s overall analysis. For further reading see W. Michael Reisman, *On the Causes of Uncertainty and Volatility in International Law, in* THE SHIFTING ALLOCATION OF AUTHORITY IN INTERNATIONAL LAW: CONSIDERING SOVEREIGNTY, SUPREMACY AND SUBSIDIARITY 44-45 (Tomer Broude & Yuval Shany eds., 2008).

described as the "wilderness of mirrors" that is part and parcel of spycraft. Explaining the legal intricacies of espionage requires one to embrace the notion that all law inevitably involves certain forms of *lex simulata* and *lex imperfecta*. Merely citing the law-in-the-books, while avoiding the-law-in-action, pays a disservice to the experts' overall courageous goal of legal elucidation and codification. The *Tallinn Manual 2.0* could have (and should have) engaged in a far more deliberate, nuanced, and comprehensive investigation into the international law of intelligence, which would have inspired the development of more harmonious and sensible cyber norms with practicability for both scholars and practitioners.

5. PROPOSING AN ALTERNATIVE HARMONIOUS ACCOUNT

The *Tallinn Manual 2.0* could have started by acknowledging that customary international law recognizes a sovereign nation's right to spy – because it does. Our international legal order, and within it more specifically our "contemporary global security system", is dependent upon a "reliable and unremitting flow of intelligence to the pinnacle elites".[47] A plethora of legal sources, enshrined in both treaty and custom, effectively recognize the existence of a derivative liberty right of States to peacetime intelligence gathering. These sources include:

1. The right of States to survival, recognized by the ICJ in the Nuclear Weapons advisory opinion[48] (and the related collective right of self-determination of peoples);
2. The laws on the use of force (and their recognition of both a customary and a Charter-based right for individual and collective self-defense);
3. Collective monitoring obligations under UN and Treaty Law (as encompassed for example in the fields of disarmament and counter-proliferation law, counter-terrorism law, sanctions regimes, environmental law, disaster relief, and the fight against illicit trafficking);
4. International human rights law (and the obligation of States to respect and ensure the right to life, liberty, and security of all persons subject to their jurisdiction, as well as the discretion of States to derogate from certain rights in times of emergency as well as balance them off in the name of protecting national security interests);

47 Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 TEMP. L.Q. 365, 434 (1973).

48 Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, 226, 263 (8 July 1996) ("The Court cannot lose sight of the fundamental right of every State to survival and thus its right to resort to self-defense in accordance with Article 51 of the Charter, when its survival is at stake").

5. International humanitarian law (and the obligation of States to develop "effective intelligence gathering systems", already in peacetime and in preparation for armed conflict, so to be able "to collect and evaluate information concerning potential targets" during the war);[49] and
6. International Accountability Regimes (certain obligations and requirements derived from both international criminal law and the frameworks governing State responsibility for internationally wrongful acts).

Within the scope of this paper, I cannot delve into a comprehensive analysis of each of these sources. Instead, let me focus on the right of self-defense, as a single example. Dating back to the Caroline incident of 1837, the right of a State to engage in pre-emptive self-defense in order to avert an attack that is "instant, overwhelming, leaving no choice of means, and moment of deliberation"[50] has been extensively analysed.[51] Even those who still maintain, based on the wording of UN Charter Article 51, that a right of self-defense applies only "if an armed attack occurs," cannot ignore diverse and robust subsequent practice by States.[52] The 2004 High-level Panel on Threats, Challenges, and Change established by the UN Secretary-General thus recognized that "a threatened State, according to long established international law, can take military action as long as the threatened attack is imminent, no other means would deflect it, and the action is proportionate."[53] Regardless of what interpretation of "imminence" one adopts, from a classically restrictive "Pearl Harbor"-type position to a highly permissive "Bush doctrine"-type position,[54] both ends of the spectrum, and everything in between, will embrace a State's derivative right to engage in peacetime intelligence gathering. For how else will a State know when a threat reaches whatever level of imminence is deemed sufficient to justify military action? If a State is entitled to retaliate against imminent threats to its survival, by definition it must be allowed to engage in peacetime espionage to gather the information necessary to reach that very conclusion.

Even were we to adopt the formalistic and anachronistic approach that only Article 51 holds (and therefore that a State may only react to an imminent threat by seeking

49 *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia*, ICTY, ¶29 (June 2, 2000), available at http://goo.gl/btGZ6y.

50 *See generally*, R.Y. Jennings, The Caroline and McLeod Cases, 32 AM. J. INT'L L. 82 (1938).

51 For a summary of the literature, see Christopher Greenwood, *Self-Defence*, MAX PLANCK ENCYCLOPEDIA PUB. INT'L. L. (Apr. 2011), available at http://goo.gl/zwaErV. For a more recent review of the literature, see Monica Hakimi, *North Korea and the Law on Anticipatory Self-Defense*, EJIL: TALK! (Mar. 28, 2017), available at http://goo.gl/4XPZeb.

52 W. Michael Reisman & Andrea Armstrong, The Past and Future of the Claim of Preemptive Self-Defense, 100 AM. J. INT'L. L. 525, 526 (2006) (noting that anticipatory self-defense was not, in their view, "in the contemplation of drafters of the Charter, though claimed by many to have been grafted thereon by subsequent practice," followed by a showing of such practice through case studies).

53 *Secretary General's High-Level Panel on Threats, Challenges, and Change, A More Secure World: Our Shared Responsibility*, UNITED NATIONS 63 (2004), available at http://goo.gl/JxTQKb.

54 For more moderate interpretations, see Daniel Bethlehem, *Principles Relevant to the Scope of a State's Right of Self-Defense Against an Imminent or Actual Armed Attack by Nonstate Actors*, 106 AM. J. INT'L L. 769 (2012); Jeremy Wright, The Modern Law of Self-Defense, EJIL: TALK! (Jan. 11, 2017), available at http://goo.gl/1QCaHH.

Security Council authorization) there would still be a derivative right for States to engage in peacetime intelligence gathering. For how else will a delegation be able to prove to the Security Council that a threat is mounting, so to convince its members to vote in favour of an authorization of the use of force? To the extent that the United Nations does not have its own intelligence capacities, the Security Council must rely on Member States in order to fulfil its mandate of maintaining peace and security. Note in this regard that the UN Security Council has in fact acknowledged the function that Member States' intelligence plays in its ability to exercise this mandate. Most recently it adopted this view in Resolution 2396, concerning threats to international peace and security caused by terrorist acts. Acting under Chapter VII the Council not only called on Member States to "intensify and accelerate" their peacetime intelligence collection efforts, it went on to suggest exactly what measures they should employ. The Council decided that Member States "shall develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data". Other measures ordered by the Council were certain capabilities for the collection, processing, and analysis of passenger name record (PNR) and advance passenger information (API) data, the development and implementation of watch lists and databases on suspected terrorists, and increased cooperation with information communication technology companies in gathering a myriad of digital records and their later sharing through bilateral and multilateral arrangements.[55]

By recognizing that a right to spy exists as a matter of customary international law, the international community inexplicitly created a caveat to the myth system enshrined, *inter alia*, in Articles 2(1), 2(4), and 2(7) of the UN Charter, as well as in certain international legal regimes (such as the ones governing diplomatic and consular relations). Countries are willing to accept as tolerable certain assaults on their territorial sovereignty, political independence, their jurisdiction to determine their domestic affairs, and immunities and privileges, in the name of maintaining the important functions that intelligence plays in our public world order.[56] So long as the surveillance serves the *raison d'être* of our international system, the fundamental goals of all law – "the minimization of violence, the maintenance of minimum order, and as approximate an achievement of the politics of human dignity as each situation allows"[57] – the practice will be stomached even by those who have been discontentedly

55 UN Security Council Resolution 2396 concerning Threats to International Peace and Security Caused by Terrorist Acts, UN Doc. S/RES/2396 (21 December 2017).

56 For more on this function see Myres S. McDougal, Harold D. Lasswell & W. Michael Reisman, *The Intelligence Function and World Public Order*, 46 TEMP. L.Q. 365 (1973).

57 W. Michael Reisman, *Editorial Comment: Assessing Claims to Revise the Laws of War*, 97 AM. J. INT'L L. 82, 83 (2003).

subjected to it.[58] Note that this position was suggested, though ultimately not adopted, by a minority of the experts in *Tallinn Manual 2.0*:

> "A few of the experts were of the view that the extensive State practice of conducting espionage on the target State's territory has created an exception to the generally accepted premise that non-consensual activities attributable to a State while physically present on another's territory violate sovereignty. They emphasized, however, that this exception is narrow and limited solely to acts of espionage"[59]

Of course, acknowledging the right to spy would only be the first step in articulating the broader law on espionage. A fundamental source of international law mostly ignored by the GoE is that of general principles of law, which stand on the same footing as treaties and custom.[60] One of the typical uses of general principles is as "standard clarifiers", serving the purpose of defining "the depth and contours of broad or amorphous legal provisions" where international conventions and customs offer little organizational help.[61] One such general principle is the principle of "Abuse of Rights". Sir Hersch Lauterpacht recognized that "there is no legal right, however well established, which could not, in some circumstances, be refused recognition on the ground that it has been abused".[62] Applying the Abuse of Rights doctrine to our newly articulated Right to Spy creates the basis for the *Jus Ad Explorationem* (the law governing the launching of EOs). When spying is launched to achieve goals other than the ones for which it was originally intended, the particular operation will no longer be tolerable. Spying may only serve the national security interests of a State or the

58 Note that stomaching it from an international law point of view is different from domestically prohibiting spying and working extensively to prevent it. This is the essence of the "liberty right" to spy, as a weaker right, that does not create an obligation on third parties to condone or facilitate it. This GoE acknowledged the practice of State domestic criminalization of espionage, see *Tallinn Manual 2.0*, n. 22, at 174 ("States are entitled to, and have, enacted domestic legislation that criminalises cyber espionage carried out against them").

59 *Id*., at 19. See also at 171 ("A few of the experts took the view that [territorial cyber espionage] would not be unlawful, suggesting that acts of espionage represent an exception to the prohibitions of violations of sovereignty and intervention").

60 In the Introduction to *Tallinn Manual 2.0*, Professor Schmitt addresses which "rules and commentary" guided the GoE. It is quite visible from his description that the experts were solely interested in articulating treaty and customary international rules. The third source of international law, that of general principles, is not once mentioned by the project director in that section and is rarely brought up as such throughout the *Manual*. *Id.*, at 3-5.

61 Alain Pellet, *Article 38*, in THE STATUTE OF THE INTERNATIONAL COURT OF JUSTICE: A COMMENTARY 731, 850 (Andreas Zimmermann et al. eds., 2nd ed., 2012) (noting that the ICJ "will usually only resort to [General Principles of Law] in order to fill a gap in the treaty or customary rules available to settle a particular dispute"); CHARLES T. KOTUBY JR. AND LUKE A. SOBOTA, GENERAL PRINCIPLES OF LAW AND INTERNATIONAL DUE PROCESS: PRINCIPLES AND NORMS APPLICABLE IN TRANSNATIONAL DISPUTES 31-32 (2017) ()the authors cite the example of the ICSID tribunal using general principles to determine the precise content of the "fair and equitable treatment" standard, taking this interpretive approach due to the fact that "treaties and international conventions. … are not of great help to this end").

62 SIR HERSCH LAUTERPACHT, THE DEVELOPMENT OF INTERNATIONAL LAW BY THE INTERNATIONAL COURT 164 (1958).

broader interests of maintaining peace and security for the international community in general.[63] Thus, for example, if spying is done for the purpose of advancing the personal economic interests of a particular leader or those of specific corporations or industries,[64] or if it is conducted to facilitate a dictatorship or to commission an internationally wrongful act,[65] such spying operations are used "for an end which is different from which the right has been created",[66] and would therefore constitute an abuse of that very right.

Moreover, even in cases where the operation does serve a lawful purpose, but in its choice of means or targets (the *Jus In Exploratione*) the State adopts certain measures which are either customarily prohibited (*e.g.* torture and other cruel, inhuman or degrading treatment; or arbitrary interference with the customary human rights to privacy or freedom of expression), or which go beyond "unexpressed but generally accepted norms and expectations",[67] the operation might nonetheless be deemed unlawful. Again, general principles of law such as good faith, proportionality, rule of law, effectiveness, fairness, and comity,[68] might serve as useful tools in both interpreting existing treaty and customary norms (*e.g.* determining what constitutes as torture, or other cruel inhuman or degrading treatment; determining what violates the international human rights to privacy and freedom of expression) and clarify standards where the law has not yet caught up with the development of new surveillance and

63 *See* Asaf Lubin, *The Dragon-Kings Restraint: Proposing a Compromise for the EEZ Surveillance Conundrum*, 57 WASHBURN L. J. 1, 56 (2018).

64 Note that this idea was entertained to some degree by certain members of the GoE. *See Tallinn Manual 2.0*, n. 22, at 169, fn 386 (citing the 2015 US-Chinese commitment not to support cyber-enabled theft of intellectual property, and to a similar commitment taken by the G20 leaders that same year, the GoE cautioned that States may have committed themselves *inter se* to certain restrictions on industrial espionage. Nonetheless the GoE stopped short of determining that such practice was unlawful).

65 This resembles the position of the GoE that cyber espionage operations may be unlawful if they "constitute an integral and indispensable component of an operation that violates international law." *See Id*., at 171-172.

66 Alexandre Kiss, *Abuse of Rights*, MAX PLANCK ENCYCLOPEDIA OF INTERNATIONAL LAW, para. 5 (2006).

67 Roger D. Scott, *Territorially Intrusive Intelligence Collection and International Law*, 46 A.F. L. Rev. 217, 226 (1999) ("as long as unexpressed but generally accepted norms and expectations associated with espionage are observed, international law tolerates the collection of intelligence").

68 None of these general principles were sufficiently addressed in *Tallinn Manual 2.0*. Quite the opposite, the GoE even challenged the customary nature of proportionality as a binding legal requirement (*Tallinn Manual 2.0*, n. 22, at 204-205). For an analysis of proportionality as a general principle of international law *see* Kotuby and Sobota, n. 61, at 114-119. Similarly, an array of human rights standards, common to surveillance jurisprudence, and their applicability to both LICOs and EOs were hardly addressed by the authors. These include *inter alia* the principles of legality, necessity, proportionality, ex ante authorization, minimization procedures and safeguards from abuse, *ex post* review, independent oversight, non-discrimination, notification requirements, and access to remedy and justice.

cyber technologies.[69] Of course, making these determinations requires the use of contextual and consequential methods of inquiry.[70]

Determining the lawfulness of a particular LICO, including specifically cyber espionage operations, is not for the fainthearted. One should be willing to engage the *Jus Ad Explorationem* and the *Jus In Exploratione*, in light of the function that intelligence plays in our public world order, and in view of a contextual- and consequential-based analysis. It is therefore the reality that in some instances foreign agents introducing USB flash drives filled with spyware into national cyber infrastructures might indeed violate the international law of espionage, whereas in other instances they might not. We consider the intrusion on sovereignty or on diplomatic immunities only as factors in a far more layered legal analysis. This type of nuanced application will be relevant to all of the other hypotheticals introduced in the *Manual*: from certain cyber intrusions that 'herd' a target's communications to a platform more susceptible to surveillance, through tapping underwater submarine cables in the territorial sea, to spying on diplomats at the United Nations. Some of these might meet the above standards and criteria and would therefore be tolerated and stomached by the international community; others might not and would therefore be condemned, potentially even triggering State obligations for reparation. Far from rushing to provide rigid rules, *Tallinn Manual 2.0* should have recognized the symbiosis that exists across the informational domain, as manifested in the communicative nature of cyber and espionage law and should have thus been more modest in its approach. Instead of a rulebook, the GoE should have provided government lawyers with a map and a compass.

6. CONCLUSION

Dr Seuss taught us that "sometimes the questions are complicated and the answers are simple". In the area of cyber and espionage law, however, both the questions and the answers are complicated. This places a burden of humility on rule prescribers and rule appliers. In this paper, I have tried to highlight how, in our liberal rush to demonstrably regulate the cyber domain, a pursuit that we undertake for all the right reasons and with all the right intentions, we might end up leaving scorched earth.

69 M. Cherif Bassiouni, *A Functional Approach to "General Principles of International Law"*, 11 MICH. J. INT'L. L. 768, 777 (1989-1990) (where he suggested that general principles prevent "the static application of anarchic norms and procedures to what is admittedly an evolving legal process designed to frame or regulate the dynamic exigencies and needs of a community of nations with changing interests and mutable goals and objectives. To state that international law has faced and is likely to face increasing new challenges, if for no other reason than to meet the fast-growing and changing technological advances, is a truism. Thus the demands on international law must be accommodated through an expanded usage of 'General Principles'").

70 Reisman and Baker take this analysis a step further by applying a similar methodology (though at a higher level of abstraction) to the regulation of covert action. *See* W. MICHAEL REISMAN AND JANES E. BAKER, REGULATING COVERT ACTION: PRACTICES, CONTEXTS AND POLICIES OF COVERT COERCION ABROAD IN INTERNATIONAL AND AMERICAN LAW (1992).

When policy-makers are provided with sufficiently accurate information as to the levels and types of threats posed by their adversaries, their intentions, and capabilities, they are more likely to calibrate their responses properly, and are less likely to rely on force as a means for guarding against startling attacks or strategic surprises. Intelligence gathering, in this context, serves a stability-enhancing function in public world order, by increasing the potential for pacific settlement of disputes and reducing the chances for violence. As George Washington said: "To be prepared for war is one of the most effectual means of preserving peace".[71] The communicative nature of cyber law and espionage law entails that we need to take a degree of caution so that we do not regulate the former to a point where we can no longer benefit from the positive functions served by the latter.

A legal regime that tries to address LICOs without being mindful and cognizant of the tidal waves that such regulations will inevitably create for EOs is one that is doomed to be rejected by States. Far more troubling, however, is the fact that such a legal regime will not even serve our initial goals of enhancing the rule of law, stability, and the peaceful resolution of conflicts. The former President of the Republic of Estonia, Toomas Hendrik Ilves, opens *Tallinn Manual 2.0* by criticizing those who rely on realpolitik to dismiss international law as mere "window-dressing".[72] I share his criticism, but to adopt a set of rules that only echo the myth system while ignoring the operational code will only give fuel to those who scoff at the power of international law to effectively shape and bound government actions and expectations.

71 President George Washington, First Message to Congress on the State of the Union (Jan. 8, 1790).
72 *See Tallinn Manual 2.0*, n. 22, at xxiii.