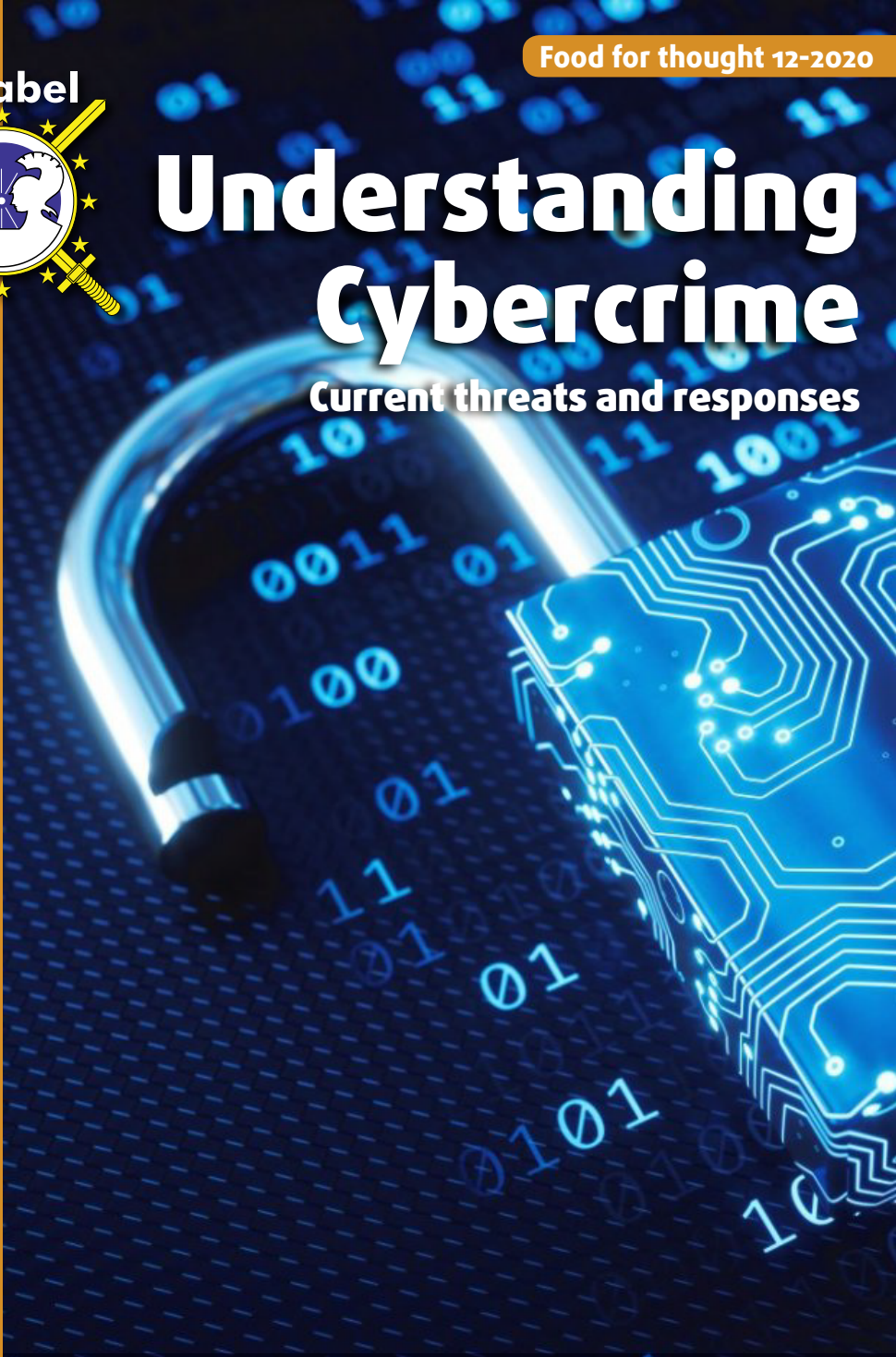
Finabel

Food for thought 12-2020

Understanding Cybercrime

Current threats and responses



AN EXPERTISE FORUM CONTRIBUTING TO EUROPEAN ARMIES INTEROPERABILITY SINCE 1953

FINABEL
European Army Interoperability Center

Written by
Christian Di Menna,
Candela Fernández Gil-Delgado,
Leandro Pereira Mendes and Milan Storms

This paper was drawn up by Christian Di Menna, Candela Fernández Gil-Delgado, Leandro Pereira Mendes and Milan Storms under the supervision and guidance of Mr Mario Blokken, Director of the Permanent Secretariat.

This Food for Thought paper is a document that gives an initial reflection on the theme. The content is not reflecting the positions of the member states but consists of elements that can initiate and feed the discussions and analyses in the domain of the theme. All our studies are available on www.finabel.org

TABLE OF CONTENT

LIST OF ACRONYMS

- **AI Artificial intelligence**
- **ARSIWA Draft Articles on the Responsibility of States**
- **CIA Central Intelligence Agency's**
- **DNC Democratic National Committee**
- **DoD Department of Defence**
- **DoS Denial of Service**
- **EU European Union**
- **IACs International armed conflicts**
- **ICJ International Court of Justice**
- **ICL The International Law Commission**
- **ICT Information and Communications Technology**
- **ICTs Information and Communication Technologies**
- **ICTY International Criminal Tribunal for the former Yugoslavia (ICTY)**
- **IEL International Environmental Law**
- **IHL International Humanitarian Law (IHL)**
- **IoT Internet of Things**
- **IP Internet Protocol**
- **IT Information technology**
- **NATO North Atlantic Treaty Organisation**
- **NIACs Non-international armed conflicts**

INTRODUCTION

Technology is embedded within almost every aspect of our daily lives, from the smartphones in our pockets to our computers, fridges, and door locks. Technology's exponential growth and its increasing effect upon daily lives shape how we live within a global society and, as expected, this process shows no sign of decreasing. In fact, we now rely on computer systems more than ever, as the Covid-19 outbreak has deeply affected the way people conduct their lives. For instance, digital technologies have been exponentially employed by governments, institutions, and businesses in order to mitigate the impact of social distancing. Notably, however, this technology is a double-edged sword. It makes our lives easier and more connected whilst enabling individuals and organisations to commit crimes remotely, creating new challenges for security professionals to overcome.

Offensive use of Information and Communication Technologies (ICTs) has been a recurrent subject since 2007, when Estonia was hit by a series of massive cyberattacks lasting

three weeks[1], resulting in a temporary disruption of service on many governmental and commercial websites and thus profoundly affecting the country's economy.[2] The attacks on Estonia brought cyberspace to the forefront of security discussions, raising awareness among states and international stakeholders about the diversity, extent, and gravity of vulnerabilities and weaknesses in this new and unique environment. Indeed, during the last decade, the international community has witnessed and experienced a considerable number of problematic episodes in cyberspace – the cyber intrusion at Sony Pictures Entertainment[3], the attack on France's TV5Monde[4], the Democratic National Committee (DNC) hack[5], to name a few.

Following these events, the North Atlantic Treaty Organisation (NATO) defence ministers officially recognised cyberspace as a new frontier of warfare at the 2016 Defence Ministerial Meeting, and that decision was endorsed at the 2016 Warsaw Summit. The Allies now "recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea". Certainly, this change comes as a response to the increasing number of cyber-attacks against both the organisation and its Member States. Similarly, in its 2017 Serious and Organised Crime Threat Assessment, the European Union (EU) has identified cybercrime as a priority crime threat, alongside trafficking in human beings, drug production, and migrant smuggling, among others.[6]

This *Food For Thought* begins with the chapter by Milan Storms, who presents the main concepts regarding cyberspace that are used in this report. In the next chapter, Leandro Pereira Mendes discusses the difficulty in attributing blame for cyberattacks, presenting the most oft-cited technical and legal hurdles of cyber-attribution. In chapter three, Christian Di Menna looks closely at the application of principles of International Environmental Law (I.E.L.), especially the duty of due diligence and "no-harm" principles in cyberlaw. In chapter four, Candela Fernández Gil-Delgado discusses the development of cyber armies, as well as future challenges to security professionals regarding cyberspace.

THE CONCEPTUAL FRAMEWORK OF CYBERCRIME

Before diving into the legal framework, this chapter provides an overview of the concepts and notions used in this *Food For Thought*. Technology is evolving faster than ever before; more data gets uploaded to the internet every day, and an increasing number of people are using these new forms of telecommunication. Apart from its exponential growth, we are ex-

1. Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, May 17, 2007. Available at. https://www.theguardian.com/world/2007/may/17/topstories3.russia.
2. Heather H. Dinniss, Cyber Warfare and the Laws of War, (Cambridge: Cambridge University Press, 2014), 38-39.
3. Andrea Peterson, "The Sony Pictures hack, explained", The Washington Post, December 18, 2014. Available at: https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.
4. Martin Untersinger, "Le piratage de TV5 Monde vu de l'intérieur", Le Monde, June 10, 2017. Available at: https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html.
5. Ellen Nakashima, "How the Russians hacked the DNC and passed its emails to WikiLeaks", The Washington Post, July 14, 2018. Available at: https://www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.
6. Europol, European Union Serious and Organised Crime Threat Assessment: Crime in the age of technology, European Policy Office 2017, p. 57. Available at: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017.

periencing that all aspects of life, including economy, defence and security, are increasingly interwoven with these new means of communication and technologies.[7] As a result, the number of threats concerning them is equally increasing.

Cybercrime has become a global problem due to the fact that it can be committed by anyone, from anywhere and at any time. As of July 2020, almost 4.57 billion users were active on the internet.[8] As every year passes by, cyberspace will encompass more data, resulting in an abundance of possibilities for criminals with malicious intent. But what exactly is *cyberspace*, how can it be defined? While many have tried to define the concept, this is not exactly easy to grasp. An Italian Cybersecurity report provided the following definition:

"Cyberspace is a set of interconnected computing infrastructures, including hardware, software, data and users as well as the logical relationships between them. It includes, among other things, the Internet, communication networks, process actuators systems and mobile devices equipped with a network connection."[9]

This definition provides a good starting point because it is sufficiently general to allow the newly established technologies to classify as part of 'cyberspace', and at the same time gives the reader a clear idea as to what cyberspace may encompass. When looking at other definitions of cyberspace, the core of the definition seems to boil down to the following: some sort of interdependent network of information systems, which could be the internet, telecommunications, computer systems etc.[10] Therefore, the main reason why it proves to be challenging to define cybercrime is exactly because cyberspace itself is a broad and constantly expanding concept.[11] Secondly, the term *cybercrime* comprises a body of different acts and conducts.[12] What makes the task of providing a definition even more troublesome is the fact that cybercrime is a borderless problem which can grasp every aspect of modern-day life. A good starting point, therefore, is to look at how different

7. Council of the European Union, Joint communication to the European Parliament, the Council, the European Economic and Social committee and the Committee of the regions regarding a cybersecurity strategy of the union, Brussels, 8 February 2013, JOIN/2013/01 final.
8. J. Clement, 'worldwide digital population as of July 2020', available at: https://www.statista.com/statistics/617136/digital-population-worldwide/#:~:text=How%20many%20people%20use%20the,in%20terms%20of%20internet%20users.
9. 2013 Italian Cyber Security Report, 'critical infrastructure and other sensitive sectors readiness, Research Center of Cyber Intelligence and Information Security "Sapienza" Università di Roma, available at: https://www.cybersecitalia.it/wp-content/uploads/2017/05/2013CIS-Report.pdf.
10. National institute of standards and technology, 'guide for conducting risk assessments', available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.
11. Harmandeep Singh Brar, 'cybercrimes: a Proposed taxonomy and challenges', Journal of computer networks and communications, Vol. 2018.
12. UNDOC, 'comprehensive study on cybercrime', February 2013, available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

legal instruments have defined the phenomenon as of yet. The only binding instrument regarding cybercrime at the time of writing, the Budapest Convention, provides a useful indication. Rather than giving a unique definition, the Convention provides four broad substantive categories of offences which can be classed as cybercrime. These categories are: 1) Offences against the confidentiality, integrity and availability of computer data and systems; 2) Computer-related offences; 3) Content-related offences; 4) Offences related to infringements of copyright and related rights.[13] The conceptual framework of the Budapest Convention paved the way for national and international rules, including EU policies, and is, therefore, a good indication of what can be defined as cybercrime.[14] Academic work has also tried to define cybercrime. Ultimately these definitions can be summarised as: "attacks against the confidentiality, integrity and availability of computer data or systems."[15] [16] It is important to keep in mind that cybercrime, as a concept, is the broadest possible notion in the spectrum of possible threats. For the sake of taxonomy, cybercrime requires to include concepts like cyberattacks, cyber warfare, cyberterrorism etc. in its definition. The previously mentioned categories of cyberattacks and cyber warfare deserve a detailed introduction, especially since chapter two will dwell more deeply on them. As with defining cybercrime, conceptualising cyberattacks can be quite challenging.[17] Hitherto there is no real practice in identifying cyberattacks and even less cyber warfare, says Hathaway.[18] A definition which has often been referred to is that of Richard A. Clarke, which states tha. cyberattacks are "actions taken by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[19] Even if this definition may sound too narrow, because of its focus on national states, it shows the distinction to be made between cybercrime, focused on individuals as perpetrators, and cyberattacks focused on state and non-state actors. This distinction is also made in some influential international legal instruments, like for example, the Tallinn Manuals (see legal framework).[20] When discussing its scope, the Manual expresses that cyber activities which do not reach the threshold use of force or which do not occur during an armed conflict will not be specifically looked at.[21] This seems to indicate that for cyber warfare or cyberattacks some sort of state or organisation involvement (e.g. certain non-state actors) is needed. This distinction separates cybercrime from the concepts of cyber warfare and cyberattacks, which will be studied in the following chapters. Cybercrime can, however, evolve into cyber warfare. Again, no single definition of cyber warfare exists. Maras provided a useful definition stating that cyber warfare can be described as a number of "cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack".[22] Therefore an important legal and conceptual difference ex-

13. Convention on cybercrime, Budapest 23 November 2001, ETS No. 185.
14. Francesco Calderoni, 'The European Legal Framework on cybercrime: striving for an effective implementation', Crime, Law and Social Change, 54(5), 339-357.
15. UNDOC, 'comprehensive study on cybercrime', February 2013, available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.
16. International Telecommunication Union, 'Understanding Cybercrime: A Guide for Developing Countries; Explanatory Report to the Council of Europe Cybercrime Convention', ETS No. 185; Fausto Pocar, 'New challenges for international rules against cyber-crime', European Journal on Criminal Policy and Research, 10(1):27-37; David Wall, Cybercrime: The Transformation of Crime in the Information Age, Cambridge Polity Press, 2007.
17. Oona Hathaway, 'The law of cyberattack', California law review, 100(4), 2011, 822-823.
18. Ibid, p.823.
19. Richard Clarke and Robert Knake, Cyber war: the next threat to national security and what to do about it, New York, HarperCollins publishers, 2010.
20. Michael Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge, Cambridge University Press, 2013..
21. Ibid, p. 18.
22. Marie-Helen Maras, Cybercriminolgy, Oxford, Oxford university press, 2016, 448p.

ists between cyberattacks and cyber warfare. To label an event as cyber warfare, an attack which amounts to an armed attack must have occurred. This is, however, not necessarily the case for cyberattacks.

Lastly, the notions of *cyberthreats* and *cyber operations* necessitate some explanation. The term *cyber operation* is most commonly referred to as any sort of action taken through cyberspace. In its most negative form, it is used for actions by states or non-state actors, when carrying out cyberattacks or when conducting cyber warfare. However, this does not mean that cyber operations are necessarily malign, offensive or contrary to international law. *Cyberthreats,* on the other hand, are more of a general concept. These could be described as "any malicious act that seeks to damage data, steal data, or disrupt digital life in general".[23] Examples of *cyberthreats* are: data breaches or Denial of Service (DoS) attacks where the attacker shuts down a machine or a network making it inaccessible to its intended users.[24]

Legal framework

The distinction made between cybercrime, cyber warfare and cyberattacks in the previous paragraph, on the other hand also finds its way into legal sources.

Cybercrime as a notion has been the subject of a limited number of binding international instruments, although their scope must be kept in mind, both substantively and geographically. The Budapest Convention by the Council of Europe concerning cybercrime is probably the most notable piece of hard law existing as of now.[25] Even though the convention is a binding instrument, it is important to remark that the instrument is *in se* regional. Since then, 66 Member States have acceded to the convention. The signatories exceed the 47 Member States of the Council of Europe, due to the possibility of non-member states to join the Convention.[26] The Budapest Convention provides that the signatory parties ensure that they will lay down the necessary legislation (or install the necessary jurisdiction) to establish certain acts as criminal offences under their domestic law. Seen that as of yet states have no criminal responsibility before the courts of other states since the Convention focuses on individuals as perpetrators. The notion of state crimes, which has proven to be very controversial, was left behind in 2001 during ARSIWA negotiations (Draft Articles on the Responsibility of States).[27] What has been installed is the notion of aggravated responsibility in case of gross and systematic failure by a state to fulfil its obligations arising under a peremptory norm of international law.[28] [29]

Therefore, the Budapest Convention is focused on making sure that states are holding perpetrators accountable within their jurisdiction rather than holding accountable the state itself as an entity.[30] In the next chapter, we will see that holding a state accountable for cybercrime or even cyber warfare may prove to be difficult. Even though the Budapest Convention is limited in scope, the

23. Hugh Taylor, 'What Are Cyber Threats and What to Do About Them', available at: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/.
24. X, 'What is a denial of service attack (DoS)?', available at: https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos#:~:text=A%20Denial%2Dof%2DService%20(,information%20that%20triggers%20a%20crash.
25. Convention on cybercrime, Budapest 23 November 2001, ETS No. 185.
26. Full list available at: fhttps://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
27. Gleider Hernandez., international law, Oxford, Oxford University Press 2019, p.403.
28. Article 40(2) International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, No. 10 (A/56/10), available at: https://www.refworld.org/docid/3ddb8f804.html; Gleider Hernandez, International law (Oxford, Oxford University Press, 2019).
29. Article 41 cites that when such a situation occurs states are obliged: to bring that situation to an end, not recognise as lawful that situation that has been created as a result of this breach and not to render any aid or assistance.
30. The Budapest convention defines jurisdiction as: 1) committed within its territory, 2) on board a ship or aircraft flagged or registered under the laws of that party, 3) by one of its nationals if the offence is punishable under the criminal law where it was committed and finally 4) if the offence is committed outside the territorial jurisdiction of any state.

need for a new global instrument may be put into perspective. The importance of the Budapest Convention cannot be underestimated in the sense that it has created a source of inspiration, especially regarding newly made or adapted national rules regarding cybercrime.[31]

As regards to cyberattacks and cyber warfare, attention must be shifted towards the sources of International Humanitarian Law (IHL) and the use of force, respectively *jus in bello* and *jus ad bellum* (granted that the threshold for *jus in bello* has been reached).[32] When looking at the sources of law, it should be noticed that cyber operations are really challenging the current framework of international law. One illustration that could exemplify the dangers of trying to qualify which legal framework could or should apply is that of the relation between cyberattacks and IHL. The 2013 Tallinn Manual states that it cannot be excluded that the rules of *jus ad bellum* and *jus in bello* apply to cyber operations.[33] *Jus in bello*, the rules that are applicable when an armed conflict is in place requires the qualification of a conflict as an armed conflict. The International Criminal Tribunal for the former Yugoslavia (ICTY) defined the notion of armed conflict since it has not been provided in any pre-existing legal framework.[34] It was set out as follows: "an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organised armed groups or between such groups within a State".[35] Cybercrime challenges this definition in the sense that the intensity of the violence is often not of a sufficient level to qualify as armed conflict. However, the consequences of cyberattacks may be as grave as situations which qualify as an armed conflict. Therefore, it could be argued that cyberattacks and cyber warfare are operating in a grey zone, hovering between peacetime rules and the rules of armed conflict.[36] The possible legal void that comes with cyber operations has been the subject of a lot of academic writings as of lately.[37] This exposes the possible problems of fitting cyber warfare into the existing framework of international law.[38] On a more positive note, this shows that cyber warfare requires further development which implicates possibilities to shape the future framework.

The relationship between customary international law and cyberattacks is especially challenging. The main reason is that the second of the two requirements for customary law, state practice (next to *opinio juris*), is lacking.[39] As of now, there has been no qualification of a cyberattack as an armed conflict and the application of IHL has not yet been triggered, which means no state practice is implied.[40] Finally, the Tallinn Manual, which has already been mentioned a couple of times, deserves special attention. It is an initiative of the NATO Cooperative Cyber Defence Centre of Excellence, drawn up by international experts. The manual defines the rights and obligations states bear

31. A world of difference: The Budapest convention on cybercrime and the challenges of harmonisation
32. For jus in bello to be applicable the situation needs to be qualified as an armed conflict, see ICTY 15 juli 1999, Prosecutor v. Dusko Tadić, IT-94-1-AR72.
33. Michael Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge: Cambridge University Press, 2013..
34. ICTY 15 juli 1999, Prosecutor v. Dusko Tadić, IT-94-1-AR72.
35. Ibid. p.70.
36. Oliver Fitton, 'Cyber operations and gray zones: challenges for NATO', Connections QJ, vol. 15(2),p.109-119.
37. For example: Oliver Fitton, 'Cyber operations and gray zones: challenges for NATO', Connections QJ, vol.15(2), p.109-119; ICRC, 'International humanitarian Law and Cyber Operations during armed conflicts', available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts
38. Eneken Tikk, 'International law in cyberspace, mind the gap', Research in focus, march 2020, available at: https://www.helsinki.fi/sites/default/files/atoms/files/tikk_2020_international_law_in_cyberspace.pdf.
39. See North Sea Continental shelf case; ICJ 20 February 1969, The North Sea Continental Shelf Case, I.C.J. Reports 1969, p.3.
40. Gleider Hernandez, international law, Oxford, Oxford University Press 2019, p.403.

under international law regarding cyber operations. It examines the relationship between cyber warfare and IHL, *jus in bello*. This means that its focus is on cyber operations being conducted by and against states, which is also the main focus of this *Food For Thought*.

THE ROCKY ROAD TO ATTRIBUTING BLAME FOR CYBERATTACKS

One threshold issue in discussing cyber-attribution involves the definition of attribution itself, a matter that certainly pervades all literature about this topic. At the most general level, 'attribution' refers to the identification of the responsible entity for a malicious cyberattack.[41] What is understood as" responsible entity" however, can vary. There are usually three types of answers: the specific computing device used to carry out an attack, the individual pressing the keys that launch an attack, and ultimately the party that supervised and controlled the attack.[42] According to Lin, even though "these three types of attribution are conceptually distinct, they are often related in practice".[43] Particularly, identifying the machine from which an attack was launched might provide some clues that may help unveil the human attacker's identity, which in turn can help determine the individual or entity responsible for authorising the cyber operation. Still, each of these types offer different challenges, increasing the difficulty of the attribution process.

Although attributing cyberattacks is not a new challenge[44], the debate on attribution is developing "surprisingly slowly".[45] Scholars and experts have been dwelling upon the subject, holding a full spectrum of views on it. At the positive end of the spectrum are those, like Rid and Buchanan, who argue that cyber-attribution is not only possible but "it has been happening successfully for a long

41. Kristen Eichensehr, "The Law & Politics of Cyberattack Attribution", UCLA Law Review, vol. 67, 2019, 5.
42. Herbert Lin, "Attribution of Malicious Cyber Incidents: From Soup to Nuts", Hoover Institution Aegis Paper Series on National Security, Technology, and Law, no. 1607, 2016 5.
43. Ibid., 13.
44. Marcus Schulzke, "The Politics of Attributing Blame for Cyberattacks and the Cost of Uncertainty", Perspective on Politics, vol. 16, no. 4, 2018, 955.
45. Thomas Rid and Ben Buchanan, "Attributing CyberAttacks", Journal of Strategic Studies, vol.38, 2015, 5.

time."[46] Lindsay strikes a more restrained yet positive note by characterising attribution as difficult but acknowledging that there are strong systems for identifying the source of intrusions and responding to attacks, with an increasing amount of investments being devoted to investigations.[47] At the other end of the spectrum, Singer and Friedman characterise attribution as "[p]erhaps the most difficult problem" in cyberspace,[48] and Eun and Aßmann argue that "determining the real aggressor is impossible unless the aggressor admits to it".[49] Shackelford further echoes this idea by affirming that sophisticated cyberattacks are "nearly impossible to trace to their sources".[50]

Why is attribution so difficult?

There are several answers to this question. First, many academics and experts suggest that the difficulty in attributing blame for cyberattacks is mainly caused by the intrinsic characteristics of the cyber domain.[51] The structural anonymity, which has been one of the hallmarks and biggest strengths of the Internet, provides the perfect venue for state and non-state actors to undertake malicious operations without fearing attribution or retaliation. The Internet, as Lindsay points out, "was designed to make connections easy and reliable even when the true identity of the connector and the path of the connection were unknown; security did not figure strongly in its early design".[52] Lupovici, however, seems to disagree on the premise that cyberspace is an inherently anonymous domain. Even though he recognises that some aspects of the Internet hinder attack attribution, he argues that anonymity is a socially attributed trait and, therefore, cyberspace could be structured in a way that does not uphold this characteristic.[53] Along this line of thinking, McConnell suggests that the only solution to the attribution problem is redesigning the Internet to make attribution and geolocation more feasible.[54] Such a change, however, would require a massive effort and probably would not help to prevent the increasingly sophisticated cyberattacks that are being launched today.[55] At the same time, reengineering the entire computer network would reduce its efficiency and dependability, and would bring into question the characteristics of the current Internet, such as freedom of action and privacy. Features treasured by many, including intelligence agencies.[56]

Second, cyber-attribution is further complicated by the fact that hackers have at their disposal a variety of programs, techniques and applications to conceal the identity of their own Internet Protocol (IP) addresses and thus to thwart detection. One common practice that attackers employ to hide their online trail is to break into poorly secured internet servers or even personal computers to use them

46. Ibid., 31.
47. Jon R. Lindsay, "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack", Journal of Cybersecurity, vol. 1, no. 1, 2015, 57.
48. P.W. Singer and Allan Friedman, Cybersecurity and Cyberwar: What Everyone Needs to Know, Oxford University Press, 2014, 73.
49. Yong-Soo Eun and Judith Sita Aßmann, "Cyberwar: Taking Stock of Security Warfare in the Digital Age", International Studies Perspectives, vol. 17, 2016, 355.
50. Scott J. Shackelford, "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem", Conference on Cyber Conflict (Tallinn: CCD COE Publications), 2010, 200.
51. Amir Lupovici, "The Attribution Problem and the Social Construction of Violence: Taking Cyber Deterrence Literature a Step Forward", International Studies Perspectives, no. 17, 2016, 322; Delbert Tran, "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack", Yale Journal of Law and Technology, vol. 20, 2018, 387.
52. Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare", Security Studies, vol. 22, no. 3, 2013, 375-76.
53. Amir Lupovici, "The Attribution", 330.
54. Mike McConnell, "Mike McConnell on how to win the cyber-war we're losing", The Washington Post, February 28, 2010. Available at: https://cyberdialogue.ca/wp-content/uploads/2011/03/Mike-McConnell-How-to-Win-the-Cyberwar-Were-Losing.pdf.
55. David D. Clark and Susan Landau, "Untangling Attribution", Harvard National Security Journal, vol. 2, 2011, 3. For instance, Rid argues that McConnell suggestion "is not only unrealistic, it would not even solve the problem at hand" (Thomas Rid, Cyber War Will Not Take Place, Oxford University Press 2013, 140-41). For Tran, "even if the Internet could arduously be redesigned to authenticate the source IP address of every bit of data sent over the Internet, these addresses would accomplish the goal of merely identifying the source machine of an attack, and not a person, thereby creating another degree of attenuation between an attack and the attacker" (Delbert Tran, "The Law", 390).
56. Ibid.

as proxies through which they can launch a cyberattack.[57] "The IP address, therefore, does not present the attacked state with a physical location to attribute the attack to or to retaliate in response. The detected server could be located in a neutral, friendly or even your own country."[58] According to Lipson, "an IP address is a poor surrogate on which to establish a basis for trustworthiness."[59] As Brenner effectively observed, "the Internet is one big masquerade ball. You can hide behind aliases, you can hide behind proxy servers, and you can surreptitiously enslave other computers without their owners' knowledge – and then use their computers to do your dirty work".[60] A prime example of a technology capable of concealing one's traces in cyberspace is the Central Intelligence Agency's (CIA) Marble Framework, which alters the language of the code from English to a foreign language, like Chinese, Russian, Korean, Arabic, and Farsi.[61]In this regard, Dinstein argues that future technological advancements will probably overcome the challenges that prevent cyber-attribution.[62] Indeed, governments are more capable of attributing responsibility for cyberattacks than they were a decade ago, thanks to technological advancements and innovations that have boosted states' confidence.[63] For example, in 2014, Canada revealed to possess robust systems in place that allow the detection of highly sophisticated attacks, even those launched by state-sponsored actors[64] and, in 2015, the United Kingdom's Chancellor affirmed that "we are increasingly confident in our ability to determine from where attacks come".[65]

It is important to bear in mind, however, that the technical realm is so "dynamic" that new technologies may both enhance and hinder states' ability to attribute malicious attacks,[66] generating "a cycle of escalating offensive and defensive capabilities".[67]

Third, even if it is possible to overcome all the technological issues mentioned above

57. Larry Greenemeier, "Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers", Scientific American, June 11, 2011. Available at: https://www.scientificamerican.com/article/tracking-cyber-hackers/.
58. Yong-Soo Eun and Judith Sita Aßmann, "Cyberwar", 355.
59. Howard F. Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues", Carnegie Mellon Software Engineering Institute, 2002, 56.
60. Brenner 2011, 13.
61. Milton Mueller et al, "Cyber Attribution: Can a New Institution Achieve Transnational Creditbility ?", The Cyber Defence Review, vol. 4, no. 1 ,2019, 110; John Leyden, "WikiLeaks exposes CIA anti-forensics tool that makes Uncle Sam seem fluent in enemy tongues", The Register, March 31, 2017. Available at: https://www.theregister.com/2017/03/31/wikileaks_cia/.
62. Yoram Dinstein, "Computer Network Attacks and Self-Defence", International Law Studies, vol. 76, 2002, 112.
63. Kubo Macák, "From Cyber Norms to Cyber Rules: Re-engaging States at Law-makers", Leiden Journal of International Law, 2017, 23
64. Canada, Statement by the Chief Information Officer for the Government of Canada (July 29, 2014).
65. United Kingdom, Chancellor's speech to GCHQ on cybersecurity (November 17, 2015).
66. William C. Banks, "State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0", Texas Law Review, vol. 97, no. 7, 2017, 1510.
67. The improvements in technical attribution might be matched over time by developments in attackers' abilities to conceal their identities, and this "cat-and-mouse game" will continue to cyber-attribution difficult. Kristen Eichensehr, "The Law", 9.

and identify the machine used to carry out a cyber operation with sufficient certainty, cyber-attribution remains challenging due to what has been defined as "human-machine gap"[68] or "entry-point anonymity".[69] That is to say, attribution can only be accomplished if the individual or organisation who was operating the computing device can also be identified. With this in mind, it should be noted that rarely does the location of a computer provide precise conclusions about the machine operator's identity.[70] Therefore, knowing that the cyberattack was executed from the territory of a state, or from the governmental cyber framework of a state, is not enough to attribute said attack.

Fourth, it may be quite difficult to determine the ultimately responsible entity as far as state responsibility is concerned. Even if it is possible to overcome all the technological challenges to identify the human attacker, the uncertainty about the connection of the individual pressing the keys to the state actor remains. Is the attacker an officially sanctioned government agent? Or is it a third party operating on its own? Deibert, Rohozinski, and Crete-Nishihata acknowledge that there is an increasing trend towards privateering cyberattacks, and states are particularly interested in this market since it "allows them to execute their missions once removed and clandestinely, thus offering plausible deniability and avoiding responsibilities under international law or the laws of armed conflict."[71]

Moving to the legal aspect of attribution, a state will only be held responsible for an internationally wrongful action that is attributable under public international law or that constitutes a breach of an international obligation of the state.[72] On this point, it is important to note that, traditionally, expectations for the attribution of state responsibility for acts of non-state actors were high.[73] According to the International Law Commission's (ILC) *Articles on Responsibility of States for Internationally Wrongful Acts*, a state can be held liable for the conduct of a non-state actor if the latter is "acting on the instruction of, or under the direction or control of" the state.[74] Unfortunately, the concepts of 'instructions', 'direct', and 'control' all need further explanation.[75] According to the commentary to the Articles on State Responsibility, 'instruction' comprises private individuals or groups acting as an auxiliary of the state.[76] More problematic issues, however, arise in determining the concepts of 'direction' and 'control', for the commentary falls short of explaining the difference between both of them. Rather, it only says that the terms are "disjunctive".[77] International courts also have failed to make a distinction with any level of detail between the three concepts. Therefore, as Schmitt puts it, "the prevailing approach tends towards a binary distinction in which either a state tells a non-state actor to perform an act (instruction or direction) or the state exercises 'effective control' over the non-state actor with respect

68. Robin Geiß and Henning Lahmann, "Freedom and Security in Cyberspace: Shifting the Focus away from Military Responses towards Non-Forcible Countermeasures and Collective Threat-Prevention", in Katharina Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy, 2009, 625.
69. Yong-Soo Eun and Judith Sita Aßmann, "Cyberwar", 355
70. William C. Banks, "State Responsibility", 1510.
71. Ronald J. Deibert, Rafal Rohozinski, and Masashi Crete-Nishihata, "Cyclones in Cyberspace: Information shaping and denial in the 2008 Russia-Georgia War", Security Dialogue, vol. 43, no. 1, 2012, 17.
72. International Law Commission, Draft Articles of Responsibility of States for Internationally Wrongful Acts, November 2001, Supplement No. 10 (A/56/10), art. 2. It is important to note that the ILC's rules are not a treaty and therefore they are not binding on any state. Yet, these rules were commended by the UN General Assembly in 2012 (UN Doc. A/RES/56/83) and have been mentioned 154 times by international courts, tribunals, and other bodies. (United Nations Legislative Series, Materials on the Responsibility of States for Internationally Wrongful Acts, 2012, ST/LEG/SER.B/25, viii).
73. Christian Payne and Lorraine Finlay, "The Attribution Problem and Cyber Armed Attacks", American Journal of International Law, vol. 113, 2019, 204.
74. Draft Articles of Responsibility of States for Internationally Wrongful Acts, art. 8.
75. Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace", The Yale Journal of International Law, vol. 42, no. 2, 2017, 9.
76. International Law Commission, Draft Article of Responsibility of States for Internationally Wrongful Acts with Commentaries, November 2001, Supplement No. 10 (A/56/10), art. 8, para. 2.
77. Ibid., para. 7.

to the act in question."[78]

The effective control test was coined by the International Court of Justice (ICJ) in its *Nicaragua v. United States of America* judgement.[79] Even though the Court does not provide a definition for the expression, it has asserted that a state's participation in the form of "financing, organising, training, supplying, and equipping" a non-state actor, it does not rise to the degree of effective control.[80] Hence, for example, supplying a terrorist group with malware would not result in state responsibility. In fact, even if the state plans the whole operation and selects the military targets, it still would not be enough to result in attribution.[81] Furthermore, taking into consideration the aforementioned technical challenges, determining that a hacker was under the effective control of a nation-state at a relevant time is probably impossible.[82]

In *Prosecutor v. Tadic*, the ICTY lowered the threshold by adopting the much less restrictive overall control test, which applies to an "organised and hierarchically structured group".[83] In light of the latter, the overall control test seems inappropriate for cyberspace, where the activity is more decentralised and rarely follows a hierarchical form. According to the International Court of Justice (ICJ) in *Bosnia and Herzegovina v. Serbia and Montenegro*, the "overall control test is unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a state's organ and its international responsibility."[84] Therefore, one is left to question the legal validity of this test. Regardless of whether effective control or overall control ultimately suits the cyber domain, the attribution bar continues to be extremely high. As a result, states are prevented from adopting any lawful response to cyberattacks, including their inherent right to self-defence, encouraging retaliatory operations outside the existing legal structure.[85] Against this background, some scholars have suggested that one possible solution to these legal challenges is to lower the attribution standard. Schmitt, for instance, defended an indirect responsibility approach by which a state might be held responsible for the consequences of non-state actors' unlawful operations on its territory "when it fails to take reasonably available measures to stop such acts in breach of its obligations to other states."[86] Lowering the attribution bar, however, increases the chances of misattribution and conflict escalation.

Fifth, another factor that contributes to the difficulty of attributing cyberattacks is the presence of dynamic and sophisticated non-state actors. Traditionally, states and non-state actors were distinguished by significant imbalances not only in legal status but also in resources and capabilities. The cyber domain, however, seems to offer great opportunities for non-state actors to challenge and, in some situations, to overcome states' hegemony.[87] Indeed, today these entities need as much or more attention than any other international player due to their ability to profoundly disturb international peace and security. Never-

78. Michael N. Schmitt, "Grey Zones", 9.
79. International Court of Justice, Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, 27 June 1986, para. 115.
80. Ibid.
81. Ibid.
82. Christian Payne and Lorraine Finlay, "Addressing Obstacles to Cyber-Attribution: A model based on state response to cyber-attack", The George Washington International Law Review, vol. 49, 2017, 563.
83. United Nations, International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, Prosecutor v. Dusko Tadic, Case no. IT-94-1-A, Appeals Chamber, Judgment, 15 July 1999, para. 120.
84. International Court of Justice, Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), 26 February 2007, para. 406.
85. Christian Payne and Lorraine Finlay, "The Attribution", 205.
86. Michael N. Schmitt, "Cyber Operations and the Jus ad Bellum Revisited", Villanova Law Review, vol. 56, 2011, 580.
87. Michael N. Schmitt and Sean Watts, "Beyond State-Centrism: International Law and Non-State Actors in Cyberspace", Journal of Conflict and Security Law, vol. 21, no. 3, 2016, 595.

theless, these actors "enjoy a relative degree of impunity" for the harmful effects of their actions[88] since international law does not offer a tailored framework based on which non-state actors can be held responsible for unlawful acts.[89] In this sense, an adequate legal response to the attribution problem should address the inexistence of attribution mechanisms for malicious cyber operations launched by non-state actors.

Finally, attributing blame for malicious cyber operations is vastly time-consuming and expensive,[90] limiting the number of actors that can bear the cost of it and, thus, hampering attribution. The investigation of cyberattacks is a complex process that requires detailed analysis of technical data as well as a deep comprehension of political and economic motivations.[91] Consequently, as Sheldon points out, "the forensics of attribution can rarely, if ever, give immediate results and can take days if not weeks to provide solid technical evidence."[92] Moreover, former U.S. Deputy Secretary of Defence William Lynn III recognised the struggle to attribute blame for cyberattacks, observing that "[t]he forensic work necessary to identify an attacker may take months if identification is possible at all."[93] Cyber-attribution, however, is nearly useless if it takes too long and is not able to identify all the actors involved in the attack.[94] These are the numerous hurdles, both technological and legal, that have been oft-mentioned as a hindrance to the development of an effective governing legal framework for cyberattacks.[95] Despite the fact that previous lit-

88. Luke Chircop, « A Due Diligence Standards of Attribution in Cyberspace", International and Comparative Law Quarterly, vol. 67, 2018, 647.
89. d'Aspremont et al., "Sharing Responsibility Between Non-State Actors and State in International Law: Introduction", Netherlands International Law Review, vol. 62 2015, 53-54.
90. Marcus Schulzke, "The Politics", 956.
91. John S. Davis II et al., Stateless Attribution: Towards International Accountability in Cyberspace, (California: RAND Corporation, 2017), 2.
92. John Sheldon, "Geopolitics and Cyber Power: why geography still matters", American Foreign Policy Interests, vol. 36, no. 5, 2014, 289-90
93. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy", Foreign Affairs, vol. 89, no. 5, 2010, 99.
94. John P. Carlin, "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats", Harvard National Security Journal, vol. 7, 2016, 409. The duration of the investigation is relevant for cyber-attribution because if a targeted state takes too long to respond, any countermeasures adopted may be seen as punishment, forbidden under public international law. On the other hand, if a targeted state engages in countermeasures too early and has wrongfully attributed the cyberattack, it will have committed an internationally wrongful act itself.
95. According to Shackelford, "the international law doctrine of attribution is in fact an essential ground for regulating cyberattacks" (Scott J. Shackelford, "From Nuclear War to Net War: Analogising Cyber Attacks in International Law", Berkeley Journal of International Law, vol. 21, no. 1, 2008, 233).

erature on cybersecurity perceived the attribution problem as an insurmountable technical issue, recent scholars and experts have begun to acknowledge that actual attribution might not be rocket science after all.[96] As Carlin aptly puts it, "although attribution is difficult, it is far from impossible".[97]

CYBERCRIME: THE APPLICATION OF THE DUTY DILIGENCE AND NO HARM PRINCIPLE

International Humanitarian Law, also called "the law of war", protects people who take no part in hostilities and restricts available means and methods of warfare.[98] This body of law applies to international armed conflicts (IACs) and non-international armed conflicts (NIACs). As common art. 2 of the 1949 Geneva Conventions states, an international armed conflict: "...may arise between two or more of the High Contracting Parties, even if the state of war is not recognised by one of them".[99] On the other hand, common art. 3 of the 1949 Geneva Convention applies for non-international conflicts saying that, "In the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties, each Party to the conflict shall be bound to apply, as a minimum, the following provisions…". The Geneva Conventions were born after the Second World War and applied for a war between states. Next to that, IHL has four core principles that apply to armed conflicts: military necessity, humanitarian, distinction and proportionality principles.

The cyber domain is completely revolutionary. As defined by Kurbalija "internet is an intense transborder digital interaction"[100] with unresolved issues. For instance, in a traditional conflict, linking the attack to a state organ is not a problem, but in cyber operations, there is a big issue as there are many hurdles in attributing attacks to states[101] and, since cyberattacks seem not to have the scope of a conventional conflict, the evaluation of the attacker's identity is particularly hard.[102]

Scholars state that an armed attack can occur as akinetic attacks but also as the use of virtual force if the attack is intended to alter the other country's powers by disrupting the country's fundamental infrastructure.[103]

Another important point related to IHL is the possibility of self-defence. States have not been eager to view the attacks that have occurred so far, as acts of war, and therefore they could not lawfully respond to these attacks in active defence because they were in fear of violating the law of war.104 To apply IHL, a cyberattack must fulfil all the conditions of an armed conflict. The application of

96. "Actual attribution of cyber events is already more nuanced, more common, and more political than the literature has acknowledged so far" (Thomas Rid and Ben Buchanan, "Attributing", 6).
97. John P. Carlin, "Detect, Disrupt, Deter", 409.
98. Henckaerts, J-M., Doswald-Beck, L. (2005). Customary International Humanitarian Law Volume I: Rules, Cambridge University Press, xvi-xix
99. Common Art. 2 1949 Geneva Conventions
100. Jovan Kurbalija, "State Responsibility in Digital Space", Diplo 2016
101. Cyber-attacks in the context of international humanitarian law, Oslo University, 2013
102. Emilia Rantala, Applicability of rules of armed conflict in international cyber warfare, Tallinn University, 2018
103. Simmons, N. (2014) A Brave New World: Applying International Law of War to Cyber-Attacks – Journal of Law & Cyber warfare, Vol. 4, 42-43 in Emilia Rantala, Applicability of rules of armed conflict in international cyber warfare, Tallinn University, 2018
104. Carr, J. (2012). Inside Cyber Warfare, 2nd Edition, Sebastopol: O'Reilly Media, Inc. 2 in Emilia Rantala, Applicability of rules of armed conflict in international cyber warfare, Tallinn University, 2018

IHL seems to be problematic and there is an actual need for legal response. There is a clear difference between real conflict and cyberattacks. The cyber domain could not be taken into consideration at the time of the Geneva Conventions since, in those times, computer technology was not as developed as nowadays. The solution proposed in this chapter is based on the principles of IEL, the duty of due diligence and the "no-harm" principle. These principles could be applied to cybercrime with some adaptations and modifications. In fact, IEL has a very concrete and strong application in several fields and in many judgments of the ICJ. The starting point of this analysis is the restrictive approach in the field of state responsibility of the ILC Draft Articles on Responsibility of States for Internationally Wrongful Act (hereinafter Draft Articles) and of the Tallinn Manual. The innovative solution to overcome this restrictive approach comes from authors that found a new strategy in applying IEL principles to cyberlaw with the necessary adaptations. This approach is based on some specific obligations that define the duty of due diligence in cybercrime.

Legal basis on the Responsibility of the State

The current main legal framework on the responsibility of the State is based on the Draft Articles, which is considered the codification of International Customary Law on state responsibility[105]. The Draft Articles have two levels of responsibility: the first regarding specific obligations and the second regarding the consequences of the violation. The second level effectively concerns state liability. In the next paragraphs, the Draft Articles will be analysed more in detail. The UN GGE (Government Group of Experts) adopted a restrictive approach towards these articles and their relation to cybercrime. It stressed that in cases of state responsibility, the geographical origin of an Information and Communications Technology (ICT) operation is not sufficient to attribute this activity to a particular state.[106]
The same restrictive approach is followed by the Tallinn Manual on the International Law Applicable to Cyber Warfare, the law of armed conflict in digital space.[107] Margulies argues that the high threshold of the Tallinn Manual could make state responsibility completely impracticable in digital space.[108]
Concerning the Draft Articles, this limited approach could collide with the "no-harm" principle in which the state is responsible for preventing any transboundary harm.[109]
Innovative solutions to fill this limited approach come from a specialised field of international law, in particular, from IEL. Since both environmental and cyber operations are concerned with the possible liability of states for acts originating in their country, causing harm in another state, it may be useful for cyberlaw to get inspiration from IEL. The delicate balance between restrictive rules on state responsibility and the "no-harm" principle is addressed to some other areas of international law with pronounced trans-boundary aspects, such as: environment, watercourses, nuclear activities, law of the sea and outer space.[110]

Innovative solutions from International Environmental Law

Cyber activities have a transboundary nature

105. General Assembly resolution 56/83, Responsibility of States for Internationally Wrongful Acts, A/RES/56/83 in Kurbalija, State Responsibility in Digital Space, DIPLO 2016
106. Para 28 UN GGE Report (2015)
107. Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge 2013 in Kurbalija note 100
108. Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility", 14 Melbourne J. Of Int'l L. (2013), p. 496 in Kurbalija note 100
109. See note 100
110. See note 100

because they can cause harm to other countries. The relevance of this threat could be compared to environmental threats. The starting point of this comparison is Principle 2 of the Rio Declaration: "States have, [...] the sovereign right to exploit their own resources pursuant [...] and the responsibility to ensure that activities within their jurisdiction or control do not cause damage to the environment of other States or of areas beyond the limits of national jurisdiction."[111] This rule is one of the bases of the duty of due diligence. It is an evolving principle of international law[112] whose rule applies if a responsible state complies with certain obligations and standards, whereas these are not clearly defined. Due to this legal gap, more specific rules have been drafted in order to develop other concepts such as the "no-harm" principle.

As stated in the Draft Articles, this principle requires states to take measures to protect persons or activities beyond their respective territories in order to prevent harmful events and outcomes.[113] The customary nature of the "no-harm" principle is confirmed by many Conventions, Court Cases and Policy Documents. The most important ruling of the ICJ is contained in the *Trail Smelter case*[114], in which the Court affirmed: "No State has the right to use or permit the use of its territory in such a manner as to cause injury [...] when the case is of serious consequence and injury is established by clear and convincing evidence. "[115]

Other ICJ rulings are the *Corfu Channel United Kingdom v. Albania case* in 1949[116] which stated about omission of the international obligation as a state responsibility, and the *Gabcikovo-Nagymaros* case[117] [118] in 1997 which confirms the "no-harm" principle.[119] Moreover, this principle was used in several Conventions such as the UN Convention of the Law of the Sea, the Convention on Biological

111. Rio Declaration on Environment and Development, Rio de Janeiro, 14 June 1992, Principle 2
112. International Law Association, Study Group on Due Diligence in International Law, Second Report, 2016
113. Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, with commentaries, UN 2001, Commentary to Art 3, 154, para (7) in Takano, Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications, Laws 2018,7,36
114. More details in Chapter 1 of this paper
115. Reports on International Arbitral Awards, Trail Smelter case (United States, Canada), 16 April 1938 and 11 March 1941, vol. III
116. Michael Waibel, "Corfu Channel Case". He describes this case as "UK and Albania called on the court to decide whether Albania was responsible for the explosion where two British ships struck mines in the channel and whether the UK's mine-sweeping operation violated Albania's sovereignty since the British navy had carried out a unilateral mine-sweeping and evidence-gathering operation within Albanian territorial waters".
117. Stephen Deets, "Solving the Gabcikovo-Nagymaros Dam Conflict", She describes the following "In 1977 Czechoslovakia and Hungary agreed to build a barrage complex on the Danube River with large dams at Gabcikovo (Czechoslovakia) and Nagymaros (Hungary). According to the treaty, the jointly-owned and -operated system would "strengthen the fraternal relations of the two states and significantly contribute to the bringing about of the[ir] socialist integration." In reality, however, it sparked a controversy between these two neighbors that has plagued Hungarian-Slovak relations for more than two decades".
118. Mara Tignino, "The role of international case law in implementing the obligation not to cause significant harm International Court of Justice". As she says "This case was the first ICJ dispute where issues of international environmental law were examined in depth.
119. States are only required to prevent harm caused as a result of an active disposition on or over their territory, which does not include the omission of protective measures. See Takano, note 113 and Case concerning the Gabcikovo–Nagymaros Project (Hungary/Slovakia), ICJ Rep. 1997 41, para 53

Diversity, Convention for the Protection of the Ozone Layer, Outer Space Treaty, Marine Pollution Convention, London Dumping Convention, and the UN Watercourse Convention.[120] Besides, the Budapest Convention on Cybercrime specifies that states have the responsibility to prevent the use of their territories by non-state actors to conduct cyberattacks against other states.[121]

Due Diligence and Cyberlaw

After the analysis of the principles of duty of due diligence and "no-harm", the next step would be to explain how these principles, normally used in IEL, apply to cyberlaw. The attribution of responsibility in cyber cases is very difficult due to technical and legal aspects. Internet architecture is complex, and the certainty required by legal evidence makes responsibility hard to attribute. Starting from traditional international law, we will adapt them to cyberlaw.

The first step of the due diligence analysis is defining the concept of *harmful conduct*. The ILC has established four criteria for which the harmful activity must (1) be a human activity; (2) be within the territory or control of one state; (3) give rise to harm or capable of giving rise to harm; and (4) be done to persons or things within another state.[122] These criteria will be adapted to cybercrime as follows.

Relating to the first point, cybercrime requires a broad definition of human activity due to the potential spreading of cyber activities. If due diligence would require a "continuous control", state responsibility could be really limited. A human activity could be defined as cybercrime if programming had a human origin.[123] Concerning the second point, it is clearly difficult to determine the location of origin of the attack and whether a crime occurs under the control of a state. Nevertheless, the responsibility of the state is making the best efforts to avoid and prevent transboundary harm originated in its territory or through its cyberinfrastructure.[124] The third and fourth criteria can be analysed together as they are intertwined. Even if the concept of harm from environmental law could be a restriction, a large part of cybercrime activities could qualify as such. As Ortner argued, a cyberattack can also have physical consequences, but in any case, the harm has to be more than the legal minimum to qualify as such.[125] [126]

There are several points of view on the principle of due diligence. Koivurova explains that "State's conduct is compared to what a 'reasonable' or 'good' government would do in a specific situation of transboundary harm."[127] As stated by Ortner, in the field of cybercrime, there are two criteria to determine whether a state has acted according to the due diligence or not. The first point is the degree of technological development of a country and the second point is the degree of control that the state has over the cyberinfrastructure. Depending on the seriousness of the threat, the due diligence will be consequently anal-

120. Convention on the Law of the Sea, Dec. 10, 1982, 1833 U.N.T.S. 397; United Nations Convention on Biological Diversity, June 5, 1992, 31; Vienna Convention for the Protection of the Ozone Layer, Mar. 22, 1985, T.I.A.S. No. 11097;United Nations (1966) Treaty on principles governing the activities of states in the exploration and use of outer space, including the Moon and other celestial bodies (the "Outer Space Treaty") referenced 610 UNTS 205 – resolution 2222(XXI) of Dec 1966; Convention for the Prevention of Marine Pollution from Land-Based Sources, June 4, 1974 1546 U.N.T.S. 119. Convention on the Prevention of Marine Pollution by Dumping of Waste and Other Matter, 1972; Convention on the Law of the Non-Navigational Uses of International Watercourses, GA Res.51/229 (21 May 1997)

121. See note 100

122. Daniel Barstow Magraw, "Transboundary Harm: The International Law Commission's Study of "International Liability", 80 AM. J. INT'L L., 305, 310 (1986) in Daniel Ortner, Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans- boundary Cybercrime, 2015 BYU L. Rev. 177 (2015)

123. Daniel Ortner, Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans- boundary Cybercrime, 2015 BYU L. Rev. 177 (2015)

124. Ibid.

125. Ibid.

126. Ibid.

127. Timo Koivurova, Due Diligence, in Max Planck Encyclopedia of Public International Law (2010).

ysed. Nonetheless, the expected due diligence of a state is based on minimum conditions.[128] As Kurbalija stressed, the duty of due diligence is going to develop thanks to state practice in dealing with cyberattacks. He argued that this is the basis to create norms through international customary law.[129] He mentioned Graham proposing some steps to determine the due diligence obligation. The main phases of his proposed method are: (1) to enact stringent criminal laws, (2) to conduct detailed investigations, (3) to prosecute and (4) to cooperate with victims' states.[130]

Regarding the Tallinn Manual 2.0, prepared by an international group of experts and NATO, article 6 states about the due diligence concept that "A State must exercise due diligence in not allowing its territory, or cyberinfrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for other States."[131] This rule does not indicate any practical steps to be taken regarding due diligence.[132]Authors defined more thoroughly what kind of specific requirements a state has to take into consideration in its conduct of due diligence. The broader obligations are: prevent, protect, prosecute and redress.[133] This theory came from a similar framework of ILC that was adaptable to cybercrime.

The first of the obligations is prevention. It is made possible through the implementation and adoption of laws and policies on cybercrime. The International Tribunal for the Law of the Sea provides three principles to prevent transboundary harm that could also be applied to cyberlaw: the precautionary approach, best practices and the impact assessments.[134]

Second, the obligation to protect denotes actions taken by law enforcement. In other words, it ensures that state officials will be trained specifically for this purpose, enabling institutional capacity to not only monitor, but also respond to cybercrime. The *Pulp Mills Argentina v. Uruguay case*[135] gives the common basis to these two obligations (prevention and protection), which is named "cooperation". The judgment states that the cooperation between the parties was "necessary in order to fulfil the obligation of prevention"[136] while also stressing the necessity of cooperation when responding to acts causing transboundary harm in order to prevent similar future events.

Third, and according to Ortner, a state is obliged to prosecute in case of transboundary harm.[137] In this case, the due diligence principle imposes that the legal system forbids and punishes wrongful acts, and it also prevents additional violations. An important component of this obligation is the development of extradition protocols which are one of the practical outcomes of cooperation between states combating cybercrime.

Fourth and last, redress means to assist the victims of transboundary harm. It is the last of the obligations of the duty of due diligence and the least defined. The non-discrimination

128. Daniel Ortner, Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans- boundary Cybercrime, 2015 BYU L. Rev. 177 (2015)
129. See note 100
130. Ibid.
131. Rule 6, Tallinn Manual 2.0
132. Takano, Due Diligence Obligations and Transboundary Environmental Harm: Cybersecurity Applications, Laws 2018,7,36
133. See note 119
134. A precautionary approach means preventing transboundary harm through specific law. Best practice is the requirement to use the best technology available to develop protocols to prevent cyberattack#. Finally, the impact assessment is the consideration of the impact of its policies on the proliferation of cybercrime.
135. Panos Merkouris, "Case Concerning Pulp Mills on the River Uruguay (Argentina v. Uruguay): Of Environmental Impact Assessments and "Phantom Experts". He claims that "The dispute arose from the authorisation by Uruguay of the CMB1 pulp mill and the actual construction of the Botnia pulp mill and its associated facilities on the banks of the River Uruguay, which constitutes an international boundary between the two sovereign States of Argentina and Uruguay".
136. Pulp Mills Case, Argentina vs Uruguay, 2010 ICJ, Reports 2010, p. 14
137. See note 119

principle has to be applied to the victims since the states have to offer the same level of assistance as for their nationals. In cybercrime, the redress duty is articulated within two possible approaches: access to justice and compensation.[138]

The role of non-state actors within the "no-harm" principle

The role of non-state actors is central in cybercrime since the control of the cyberinfrastructure is held by the private sector 90% of the time.[139] As Buchan said, the state is not responsible for the conduct of a harmful non-state actor due to a territorial link alone.[140] The ICJ ruling in the *Gabcikovo-Nagymaros case* confirms that states have to prevent transboundary harm when it is caused by a national disposition as long as there is an opportunity to do so and if it is foreseeable that the disposition could cause harm.[141]
In case of private activity, the state must apply a regulatory framework to prevent violation in its territory of legal rights under customary law. The respect of due diligence is aimed at individuals acting in a state's jurisdiction. States incur responsibility in case they fail to take positive action in relation to the conduct of a non-state actor operating within their jurisdiction. Even if there is not a direct responsibility of a non-state actor to respect due diligence, states have the obligation to ensure that international law is respected.[142]
As explained in chapter two, identifying the perpetrators of a cyberattack is very difficult. This is one of the main reasons why attribution is not easy at all. Hemen suggests the definition of "imputed responsibility", premised on the state's failure to implement the duty to prevent its territory from being used to attack other states.[143] In case a state is unwilling to investigate and prosecute the attackers, the non-state actor's connection to the state shall be presumed, and the attacks may be impliedly attributed to the latter.[144]

THE FUTURE OF CYBER WARFARE

According to Theiler, it is often said that September 11th 2001 was the day when everything changed. Perhaps not so much for our daily lives, but in the field of security, it was the beginning of a new era.[145] Even though 9/11 can not be considered as a result of cberattacks,[146] [147] it paved the way for future cybercrimes. Artificial machines can easily

138. See note 122 "Concerning the access to justice approach, states shall offer compensation to the victim or allow effective civil litigation against who made the attack; concerning the compensation approach there are several possibilities: reparation, compensation for damages or other form of economic redress. These approaches could meet a state's international obligation to provide redress"
139. Shackelford, Scott J. 2014. Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge: Cambridge University Press. In Takano, see note 131
140. Buchan, Russell. 2016. Cyberspace, non-state actors and the obligation to prevent transboundary harm. Journal of Conflict and Security Law 21: 429–53. In Takano, see note 131
141. Bremer, Nicolas. 2017. Post-environmental impact assessment monitoring of measures or activities with significant transboundary impact: An assessment of customary international law. RECIEL 26: 80–90. In Takano see note 131
142. See note 131
143. See Office of General Counsel, Department of Defense, An Assessment of International Legal Issues in Information Operations (May 1999), reprinted in Thomas Wingfield. See particularly Convention on Cybercrime, Council of Europe, Nov. 23, 2001, 41 I.L.M. 282, 2296 U.N.T.S. 167, which criminalises cyber-attacks and confirms the duty of states to prevent their territories from being used by non-state actors to conduct these attacks against other states; In Hemen Philip Faga, Baltic Journal of Law & Politics 10:1 (2017): 1–34
144. Vincent-Joel Proulx, "Babysitting Terrorists: Should States Be Strictly Liable for Failing To Prevent Transborder Attacks?" Berkeley J. Int'l L. 23 (2005): 622-641. In Hemen Philip Faga, Baltic Journal of Law & Politics 10:1 (2017), 1-34.
145. Olaf Theiler, "New threat. the cyber-dimension", NATO's review, September 4, 2011. available at https://www.nato.int/docu/review/articles/2011/09/04/new-threats-the-cyber-dimension/index.html
146. Sergio G. Eissa, Sol Gastaldi, Iván Poczynok, María Elina Zacarías Di Tullio, "El ciberespacio y sus implicancias en la defensa nacional. Aproximaciones al caso argentino"
147. Ibid. However, the authors establish tha. in relation to the attack of September 2001"[t]here has not yet been an act of cyberterrorism with physical damage and material effects, but the technology of cyberattacks is clearly evolving from a simple nuisance to a serious threat to information security and even to critical national infrastructures"

be controlled by attackers causing devastating outcomes. As Wheeler said "[the] more I speak to people, the more they think that the next Pearl Harbor is going to be a cyberattack" and adds "that the most horrifying cybersecurity attack is going to have its own name and [it] is going to involve something more terrifying than we've thought of yet."[148] Since this accident, our traditional perception of security collapsed. Threats no longer had a clear sender, and cyberwarfare operations became so powerful since cybercrimes, next to cyberattacks, could be launched instantly, without any evidence, making them hard to predict or even counter, impacting systems around an entire country, knocking out emergency services for days, disrupting the economy and weakening military responsiveness.[149] With the constant use of the Internet of Things (IoT), territorial borders ceased to make sense, as did military dominance of space and time.[150] As a result of it and since the development of new technologies - including artificial intelligence (AI) -, cyber warfare is now considered the fifth domain of military operations next to land, air, sea and space, given the fact that a person equipped with a machine can cause more damage to the infrastructures of a country than thousands of soldiers.[151] This fact has been supported by Lynn[152] after the U.S cyberattacks in 2008 stating that "cyber is a new domain of warfare, like land, sea, air and as the domains they are, this new domain needs policies, doctrine, planning, resources and strategy like the other ones"[153] and as such "[it] must be recognised as a territory of dominance […] as far as war is concerned". Even if this statement was also supported by Gazula, who declared that "with the development of information technology (IT), cyberspace is becoming another battlefield following the land, sea, air and outer space" some other authors claimed that cyberspace could not be considered as a future battlefield.[154] In this line, Cavelty has flatly stated that "[m]ilitaries cannot defend the cyberspace of their country – it is no space where troops and tanks can be deployed because the logic of national boundaries does not apply" while Anderson agrees with her by considering that "traditional concepts of national defence cannot be applied in cyberspace."[155]

However, and regarding cyberattacks, It was not until the 2007 incidents in Estonia that full political attention was given to this growing source of threats to public security and state stability. Estonia was struck by a 22-days cyberattack campaign. The attack was part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn.[156] After three weeks of massive cyberattacks, it became clear that societies in NATO countries were suffering from high digital vulnerability.[157]

One year later, in 2008 and coinciding with the cyberattacks on Georgia[158], the United States experienced an unprecedented attack within the Department of Defence (DoD),

148. Natasha Turak, "The next 9/11 will be a cyberattack security expert warns", 2018, https://www.cnbc.com/2018/06/01/the-next-911-will-be-a-cyberattack-security-expert-warns.htm. .
149. Maxwell Davies, "What is the future of cyber warfare", June 27, 2018, available at https://blog.v-hr.com/blog/what-is-the-future-of-cyber-warfar.
150. European Commission, "A strategic reflection about a European approach to Internet of Things –the next revolution" defines IoT as "a set of products, services and processes that virtualises the real-world things for digital processing whose outcome is a digital representation of the real world that can interact with digital systems and applications and is susceptible to Internet business models"
151. Juan M. Padrón and Ángel Ojeda-Castro, "Cyber warfare: artificial intelligence in the frontlines of combat", International Journal of Information Research and Review, June, 2017
152. Cyberattack on United States DoD, Homeland security digital library, October 2008, available at https://www.hsdl.org/c/tl/2008-cyberattack-united-states-dod/
153. Ibid.
154. Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies" May 2017, Cybersecurity Interdisciplinary Systems Laboratory (CISL)
155. Brad Bigelow, "What are Military Cyberspace Operations Other Than War?
156. Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective Cooperative" Cyber Defence Centre of Excellence.
157. Olaf Theiler, "New threats: the cyber-dimension", September 2011
158. Omar El Bakioui, "Cyber-Security and Cyber-Warfare: Is cyber warfare is the most important future threat?",
He recognises that "there were three types of cyberattacks that affected Georgia: (i) the DDOS cyberattacks addressed to Georgian websites including media outlets, large banking sites and other smaller websites; (ii) the defacing of specific politically and economically prominent websites; parliamentary, governmental and national bank sites were all tackled; (iii) the perpetrators dispensed dangerous software, malware, in an attempt to infiltrate and worsen the cyberattacks".

an attack considered as the worst breach of U.S. military computers in history where they suffered a major failure in its defence network putting millions of files at risk. A virus created by a foreign AI was placed within the Army's computer systems[159] in the Middle East and it spread the malicious code throughout the DoD network.[160]

Most of the subjects who committed these attacks were non-state actors. As we already know, within cyberspace, there is a distinction between states and non-state actors regarding the kind of actions carried out to launch cyberattacks; on the one hand, states remain the most dangerous actors in cyberspace. However, due to high-level digital espionage and sabotage, they will end up losing their strength and sooner or later, they will become secondary actors in the cyber arena. On the other hand, there are non-state actors[161] who are more and more involved in cybercrimes[162] since they have the potential to employ digital force or, to be involved in cyber military. Authors like Sigholm refer to the current situation by considering that "Although nation-states might seem to be the most likely main players in a future full-scale cyberwar, recent events have shown that non-state actors might also play a key role during such events, and almost certainly will do so during low-intensity cyber-skirmish".[163] Bussolati reinforced this by saying that "one of the most remarkable elements of past cyber events is the substantial involvement of non-state actors" as well as "their […] future role in cyber warfare".[164]

After the occurrence of these events and with the rise of these acting subjects, cybercrime itself became a new reality in which predictions and hypotheses made thirty years ago in the well-known article "Cyberwarfare is coming", eventually became real facts.[165] Growing awareness of the seriousness of cyberthreats and cybercrimes[166] was further heightened by the incidents of the following years, hinting at the potential of cyber warfare[167] as well as its

159. La Nación, "Este es el cibercomando de EE.UU que Trump utiliza contra Teherán y Moscú", june 27, 2019, available at https://www.lanacion.com.ar/tecnologia/este-es-cibercomando-eeuu-trump-utiliza-teheran-nid2261797
160. William J. Lynn III, "Defending a New Domain: Cyber Security," 2010.
161. According to Bussolati, they can be classified in five categories: (a) individual hackers; (b) criminal organisations; (c) cyber mercenaries; (d) hacktivists; (e) patriotic hackers.
162. Ibid. According to him "Estonian and Georgian incidents where analysis of these incidents indicated the likely involvement of hacker groups".
163. Johan Sigholm, "Non-State actors in cyberspace operations", January 2013, available at https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations
164. Nicolò Bussolati, "The rise of Non-State actors in Cyber warfare", Oxford University Press, 2015. p. 102-126
165. John Arquilla, David Ronfeldt, "Cyberwar is coming!", available at https://www.rand.org/pubs/reprints/RP223.html
166. Harsh Shrivastava, Neha Kumari, "Chapter 9 The Role of Artificial Intelligence in Cyber Security". In the article the sort out three different types of threats leading to Cyber warfare: (a) Espionage (b) Sabotage (c) Propaganda."
167. Gema Sánchez Medero, "Stuxnet and anonymous", September-November 2012, derecom

impacts on critical national infrastructures.[168] [169] In this regard, Allen stated that "[in] this digital age […] destroying critical national infrastructures such as automated power plants, stock markets and transportation systems could disable this nation without firing a shot."[170]

In the end, as Wright writes, "[t]he future of cyber warfare will be determined by two things: the mindset (policies, strategies) and the technologies (tools)."[171]

Cyber armies within cyberspace

During the last years, warfare and militaries have evolved and have made extensive use of technology to implement and adapt in different ways, means and ends to achieve the military intention which is directly in line with the nation states' political objective.[172] The *militarisation of cyberspace*[173], the legality of cyber armies and their future role, are some of the questions that keep arising these days. This matter lacks any solid response yet due to the fact that cyberspace is not hegemonised by a single actor.

As pointed out before, the event of September 2001, together with the Estonian (2007), Georgian (2008), U.S (2008) cyberattacks and the disclosure of the Stuxnet virus (2010) led to an increasing militarisation of cyberspace and cybersecurity issues. It is this outcome that makes necessary, in the words of Bergtora, "[a] considerable militarisation of cyberspace that goes in tandem with a growing government-interest in controlling popular uses of the internet."[174]

Regarding the future of armed forces and their involvement in the new cyberspace, some experts agree that "through cyber operations will be a significant component of future conflicts, the role of the military in cybersecurity will be limited and needs to be carefully defined" adding that "future conflicts between nations will most certainly have a cyberspace component, but this will just be an accompanying element of the battle".[175] Indeed, the future role of armed forces within cyberspace is already on its way: *cyber departments* such as the United States Cyber Command or specifically trained units like in Sweden have been created.[176] Nevertheless, some others have argued that military operations in cyberspace outside the context of armed conflict should be limited to the protection of military networks and information systems.[177]

In any case, the creation of these cyber-bodies *ergo* a cyber army, according to Broeders, "will have need of a broader group of military professionals to integrate the new cyber capacity into the military organisation at large, but the bottleneck lies in creating a contingent of military hackers."[178]

One of the likely cyberwarfare scenarios for armed forces would be the creation of a legally constituted cyber army, where cyber commands and cyber soldiers would lead cyber operations in cyberspace, if redundancy may

168. Aydin Direskeneli, "Cyber warfare and critical infrastructure security", For him "Today, critical infrastructures are managed centrally by using IT infrastructure and that is why security of critical infrastructures has become a main problem on its own".
169. Ibid. For instance, "in december 2015, the world witnessed the first known power outage caused by a malicious cyberattack where three utilities companies in Ukraine were hit by BlackEnergy malware, leaving hundreds of thousands of homes without electricity for six hours. Another example would be, back in 2013, Iranian hackers breached the Bowman Avenue Dam in New York and gained control of the floodgates. Oil rigs, ships, satellites, airliners, airport and port systems are all thought to be vulnerable, and media reports suggest that breaches have occurred".
170. Terrence S. Allen Major, 2017, InterAgency Journal Vol. 8, Issue 3
171. Aaron Wright, "The future of cyber conflict" August 4, 2020, Available at https://cove.army.gov.au/article/the-future-cyber-conflict
172. Michael Aschmann, J.C Jansen van Vuuren, Louise Leenen, "Cyber Armies: The Unseen military in the grid", March 2015
173. Lior Tabansky, "The current state of cyber warfare", Tel Aviv University, may 2015, Available at https://www.cybersecurity-review.com/articles/the-current-state-of-cyber-warfare/
174. Kristin Bergtora Sandvik, "Towards a Militarisation of Cyberspace?" Peace Research Institute Oslo
175. Myriam Dunn Cavelty, "The Militarisation of Cyber Security as a Source of Global Tension", Strategic trends 2012"
176. Henry Montgomery,"Sweden to train 'cyber soldiers' during military service, January 16, 2019, Available at https://www.thelocal.se/20190116/sweden-to-train-cyber-soldiers-during-military-service
177. Ibid 154.
178. Dennis Broeders, Investigating the Place and Role of the Armed Forces in Dutch Cyber SecurityGovernance, July 2015, ResearchGate

be applied. The concept of a cyber command with its defensive, offensive, research and development capabilities will allow military networks as well as strategic government networks to be defended and protected against a cyberattack. Thus, the cyber command would be established where a number of its operational activities would not be very different from the police, prosecution and military domains, leading therefore to enhanced cooperation between both police, military and the intelligence community.[179]Schoka says that "cyber command's current approach to conducting computer network operations focuses heavily on the review and approval process. In addition to ensuring legal compliance with the myriad of authorities and orders pertaining to cyberspace operations, review processes focus on risk management."[180] For every operation, the cyber command executes, joint leaders and operation planners must meticulously calculate and evaluate the risks associated with that particular operation.[181] Currently, it is said that there are at least 100 different cyber commands around the world today belonging to a range of state and non-state actors[182] due to the increased involvement of the military in cyber defence. This situation has led to growing concern about cyberspace operations prompting states to armed conflict and creating a strategically unstable situation with the potential for state cyber-operations to lead to unintentional escalation of tensions and conflicts.[183]

From now on, we can expect cyber armies will have a significant role to play within the next generations of military warfare and development in modern warfare. Cyberwarfare is a reality, and the implementation of cyber armies in the different countries with a mandate to execute defensive and offensive actions is important. In order words, the existence of a cyber army ensuring surfaces and gaps of cyberspace are guarded while allowing nation states to be able to ensure cyber sovereignty is necessary.

Future challenges and possible solutions

Some of the biggest challenges faced in cyber warfare are: (a) the unpredictability of cyberwar in the long term as today's solutions may not be effective against future warfare tactics; and (b) a clear lack of international rules concerning cyberspace (especially between the three "cyber superpowers" China, Russia, and the United States[184]) and intelligence agencies[185] indicating that we are facing a cybersecurity crisis.[186] Michael Robinson, Kevin Jones, Helge Janicke write about the issues that cyber warfare will create in the upcoming years saying "the majority of challenges presented by cyber warfare cannot be solved from the perspective of just one discipline". In the same line, Van der Meer highlights how states can respond to massive cyberattacks targeting their society. Nevertheless, this question cannot be answered on a solid basis since there is not any legal binding act that can resolve

179. Ibid.
180. Andrew Schoka, "Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat", April 2019, available at https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/
181. Ibid.
182. John D. Winkler, Timothy Marler, Marek N. Posard, Raphael S. Cohen, Meagan L. Smith, "Reflections on the Fture of Warfare and Implications for Personell Policies of the U.S Departement od Defense" Available at https://www.rand.org/content/dam/rand/pubs/perspectives/PE300/PE324/RAND_PE324.pdf
183. Gary D, Brown Rusi, "State Cyberspace Operations Proposing a Cyber Response Framework" September 2020, Royal United Services Institute for Defence and Security Studies.
184. Matthew Crandall and Bradley Thayer "The Balance of Cyberpower", November 25, 2018. For them "there are other important actors in cyberspace, including Estonia, France, India, Iran, Israel and North Korea".
185. Ibid 148
186. Kubo Mačák, "Is the International Law of Cyber Security in Crisis?", 8th International Conference on Cyber Conflict" For him "Several indicators suggest that the international law of cyber security is in the midst of a crisis. First, proposals of internationally binding treaties by the leading stakeholders, […] have been met with little enthusiasm by other states […] Second, states are extremely reluctant to commit themselves to specific interpretations of the controversial legal questions and thus to express their opinio juris. Third, instead of interpreting or developing rules, state representatives seek refuge in the vacuous term 'norms'".

this issue. Yet, the author has identified seven measures contained in what is called the "The Diplomacy Tool Box" which focuses on deterring cyberattacks with the prospect of political and economic sanctions.[187] Therefore, the exposure of the attackers, and thus removing their 'cloak of invisibility', is an important first step in holding perpetrators accountable.[188] The possible measures to counter cyberattacks would be the following:

a. *Acquiescence and strengthening cybersecurity* by simply acknowledging that the cybersecurity measures in the case are not adequate;
b. *Diplomatic protests* by communicating the allegedly responsible state about the cyberattack. As an example of these protests could be the expulsion of some diplomats or other officials representing the accused state;
c. *Legal measures* by sending a clear, public signal that the attackers have been identified and will face repercussions within a legal framework;
d. *Political and economic sanctions* might definitely have some deterrent value, especially for countries that strongly depend on imports and/or exports since it may prohibit certain economic transactions with the country behind the cyberattacks.
e. Beyond these diplomatic actions, we can find the non-diplomatic actions for when states need to respond to large-scale cyberattacks. These actions normally involve the presence of the armed forces and/or security forces:
f. *Retaliation in cyberspace:* to a large-scale cyberattack by retaliating with a counterattack in the same dimension that the offender has used: cyberspace;
g. *Covert retaliation in cyberspace*: Launching a covert counter - cyberattack, lowering the risk of escalation and international condemnation;
h. *Military retaliation*: Military retaliation may send the crystal-clear message that cyberattacks are not tolerated – thus deterring any potential cyberattack in the near future. Yet, it bears the risk of triggering a military response from the other side as well and thus starting a dangerous escalation process.

Finally, scholars think that using *blockchain* to overcome cybersecurity could be useful to prevent society from being affected by full-scale cyber warfare in the next decade. Blockchain[189] is going to be one of the best means of defence against cyberattacks since it is based on two organisational features: sovereign decentralisation, and record-keeping autonomy[190] which means it can protect data from intruders, and keep systems secure[191] by providing one of the best employable tools to protect data from hackers, preventing potential fraud and decreasing the chance of data being stolen or compromised. Blockchain technology could allow records to be created and verified at a greater level of speed, security and transparency.[192] The impossibility of a task like taking down a whole chain increases along with the number of users on a network: which would mean that the more users there

187. Cyberattacks: EU ready to respond with a range of measures, including sanctions', Press release 357/17, European Council, 19 June 2017.
188. Sico van der Meer, State-level responses to massive cyberattacks: a policy toolbox, Clingendael, December 2018.
189. Yulia Horbenko, "Using Blockchain Technology to boost cyber security", She writes "Blockchains are distributed networks that can have millions of users all over the world. Every user can add information to the blockchain and all data in the blockchain is secured through cryptography. Every other member of the network is responsible for verifying that the data being added to the blockchain is real. This is done using a system of three keys (private, public, and the receiver's key) that allow members to check the veracity of the data while also confirming who it comes from" available at https://steelkiwi.com/blog/using-blockchain-technology-to-boost-cybersecurity/
190. Renny Rueda, Eldar Šaljić, Duško Tomić, "The Institutional Landscape of Blockchain Governance. A Taxonomy for Incorporation at the Nation State", February 2020, Volume 9, Issue 1, Pages 181-187,
191. Ibid.
192. Philip Bucher, "How blockchain technology could change our lives", European Parliamentary Research Service.

are, the lower the risk of getting attacked by hackers. Some international actors have already tested blockchain in order to prevent cyberattacks in their national IT systems, for instance: (a) the Estonian government has experimented with blockchain implementations enabling citizens to use their ID cards to order medical prescriptions, vote, banking etc; (b) African countries such as Ghana, Kenya and Nigeria have begun to use blockchains to manage land registries; (c) the UK also has trialled the use of blockchain technology for welfare payments.[193]

It is completely true that the future of warfare will be shaped by how these technological advances are assessed and adopted to overcome the challenge of cybercrime. The overview given by Cavelty shows that states confronted with a massive cyberattack have several tools available to respond, varying from silent acquiescence and diplomatic protests to counter-attacks by cyber or conventional military means.[194] In the long term, and looking into the future, just as Cavelty writes, "international cooperation and norm-setting seem to be more viable in preventing large-scale cyberattacks than a cycle of attacks and counter-attacks escalating into yet higher levels of cyber destruction."[195]

CONCLUSION

Cyberspace develops at lightning speed. During the last decades, people have been increasingly using technology in their daily lives and, thus, becoming overdependent on ICTs. New invasive technologies have never been as dangerous as they are now and in the future. Moreover, the speed at which they are developing and the lack of a legal framework are leaving states with uncertainty in responding to cyberattacks. One of the possible solutions to make up for the lack of regulation described by this report would be the application of the principles of "no-harm" and due diligence contained in IEL. Specifically, this study delved into IEL norms as a solution to current and emerging issues in cybersecurity, cyber conflict, and cyber defence, instead of using other international law frameworks that have been proposed for cyberspace such as IHL.[196]

One of the most active subjects in cybercrime are non-state actors. Entities that take advantage of "invisibility" and "difficulty" of attribution as a result of the impossibility of "tracking" their steps in a dimension that does not even exist in the material domain. These two shortcomings -lack of international regulation and the impossibility of attributing the attacks- lead to the third shortcoming: lack of state responsibility for the launched cyberattacks. Undoubtedly and like any other international issue, the problems in cyberspace cannot be tackled by only one state, regardless of how powerful and influential it is. This is why it is necessary that states come together in order to create a more stable and reliable cyber environment, especially given the fact that, since states are all organised by auto-

193. Ibid.
194. Ibid 174.
195. Sico van der Meer, "Enhancing international cyber security. A key role for diplomacy", Security and Human Rights, Vol. 26 (2015) p. 193-205
196. Jason Healey and Hanna Pitt, "Applying International Environmental Legal Norms to Cyber Statecraft", Journal of law and policy for the information society

mated computer programs, it is possible to hack them and to alter them, unleashing catastrophic consequences much more disastrous than many past kinetic wars.

In the same line, cyber warfare is also hitting hard in the military field, especially by launching cyberattacks motivated by intellectual, economic, and political reasons that in the end unleash conflicts between countries that are willing to demonstrate their strength through cyberspace. Regarding military operations (*cyber operations*), cyberattacks must also be considered a threat, as they are increasingly likely to combine with computer attacks carried out to shut down the opponent's networks and systems or direct public opinion in favour of one of the contenders.

In this report, some solutions to defend states from cyberattacks were given, which have been gathered from authors who recommend a series of acts either at a general level, through diplomatic actions backed by national rules, either at a specific level, such as the use of AI, and more specifically, the use of blockchain to protect them from such attacks and achieve better security in the cyber domain.

The cyber-arena is still an unforeseeable domain where the only certainty is that cyberspace is here to stay and is expected that next generation and future ICTs will become a platform, if not already, for most of the businesses worldwide. Taking into account the expectations surrounding the development of cybercrime, each state should increase its own security measures against cyberattacks and, in order to do this as effectively as possible, governments should establish, if not yet done so, an agency whose sole focus is on cyberspace and cyberattacks.[197]

197. Philipp Hälsig, "Measures to prevent cyber warfare attacks and information warfare", Model United Nations International School of The Hague 2013.

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Chiefs of Staff in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and *ad hoc* coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 38 – GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at **www.finabel.org**

European Army Interoperability Centre

www.linkedin.com/in/finabelEAIC @FinabelEAIC @FinabelEAIC

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 441 79 38