ARTICLE

Mind the Gap(s) – The Need to Resolve Uncertainties in the International Law of Cyber Warfare

SHIRAN SHAHAF*

Emerging evidence demonstrates the growing significance of cyber operations in the context of armed conflicts and aggression. Despite increasing concerns of the international community, no specialised international legal regime has been developed to govern and control these operations. Instead, the law of armed conflict (LOAC) is applied to cyber operations that are conducted during armed conflicts. While the implementation of LOAC to evaluate the legality of cyber operations is important and valuable, this branch of law has not yet developed enough to resolve several core legal issues that are at the heart of cyber operations. These legal uncertainties, gaps and unsettled issues, have been referred to in the literature as "grey zones." Existing studies questioned whether clarifying these grey zones is desirable, given the uniqueness and sensitivities of cyber operations. This Article first identifies and analyses the main grey zones in the application of LOAC on cyber operations. It then focuses on the question of whether these gaps and uncertainties should be clarified, placing this Article in a growing conversation about legal cynicism and the politicization of international law. In particular, it argues that these gaps contribute to the marginalization of international law and frustrate its role in guiding human behaviour during armed conflicts.

* PhD candidate, Deakin University Faculty of Business and law; MA in European Studies, Hebrew University of Jerusalem; BA in International Relations and Arabic Language and Literature, Hebrew University of Jerusalem. I wish to thank A/Prof. Shiri Krebs for her guidance, advice, and inspiration throughout the whole research project. All errors are my own.

INTRODUCTION

In 2010, the Iranian nuclear systems were penetrated by the "Stuxnet" worm. This computer worm caused serious and irreversible physical "damage to the uranium-enriching infrastructure at the Natanz nuclear facility" and interfered with its processes.[1] The Stuxnet incident, allegedly conducted by state actors,[2] physically abused another state's infrastructure, thus illustrating the growing relevance of cyber warfare capabilities, the new risks to national security posed by cyberspace,[3] and mainly the need for international legal rules to regulate cyber operations.[4]

The Stuxnet incident is not an isolated event. A new era has begun, one in which ongoing global technology changes are occurring.[5] "More than 2.7 billion people use the internet" worldwide, and the majority of developed states use computers and computer networks to manage their national infrastructures.[6] The global technological change and the rise of cyberspace throughout the last few decades have had a substantial impact on states' security concerns, and national cybersecurity has become a highly important issue in states' "foreign and domestic policies."[7] All states are vulnerable to cyber operations: those that are technologically advanced, as well as those that lack technological development.[8] Thus, concerns regarding the ability to hinder or de-escalate cyber operations have been expressed by the international community.[9] For example, "the United Nations (U.N.) General Assembly has acknowledged that cyberattacks put the peace and security of the world at risk and have the capacity to undermine the security and integrity of critical national infrastructures, which provide services in the civil and military domains."[10] Also, the United States government has

1. Ido Kilovaty, *Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare*, 5 AM. U. NAT'L SEC. L. BRIEF 90, 91 (2014).

2. *Id.* at 92. Today, it is widely accepted that both the United States and Israel were responsible for this cyber operation.

3. *Id.*

4. Oona A. Hathaway et al., *The Law of Cyber Attack*, 100 CAL. L. REV. 817, 817 (2012); Michael N. Schmitt, *The Law of Cyber Warfare: Quo Vadis?*, 25 STAN. L. & POL'Y REV. 269, 299 (2014); John Richardson, *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*, 29 J. MARSHALL. COMPUT. & INFO. L. 1, 27 (2011).

5. Paul Przemyslaw Polanski, *Cyberspace: A New Branch of International Customary Law?*, 33 COMPUT. L. & SEC. REV. 371, 371 (2017).

6. Waseem Ahmad Qureshi, *Cyberwarfare: A Tortuous Problem for the Law of Armed Conflict?*, 28(1) TUL. J. INT'L & COMPAR. L. 1, 2 (2019).

7. Ilona Stadnik, *What Is an International Cybersecurity Regime and How We Can Achieve It?*, 11(1) MASARYK UNIV. J. L. & TECH. 129, 129-30 (2017).

8. Qureshi, *supra* note 6, at 2.

9. *Id.*

10. *Id.*; *See also* G.A. Res. 56/19, U.N. Doc. A/RES/56/19, at 1–2 (Jan. 7, 2002); G.A. Res. 58/32, U.N. Doc. A/RES/58/32, at 2 (Dec. 8, 2003); G.A. Res. 59/61, U.N. Doc. A/RES/59/61, at 2 (Dec. 3, 2004); G.A. Res. 60/45, U.N. Doc. A/RES/60/45, at 2 (Dec. 8, 2005); G.A. Res. 61/54, U.N. Doc. A/RES/61/54, at 2 (Dec. 6, 2006); G.A. Res. 62/17, U.N. Doc. A/RES/62/17, at 2 (Dec. 5, 2007);

expressed concerns over the growing risk that cyber activities pose to its national security.[11] Thus, as states continue to advance technologically, international law rules that govern use of force must be adjusted, through a process of conflict and contestation, cooperation and growth.[12]

However, despite this growing international concern, international law of armed conflict (LOAC) has yet to develop an adequate fitted model. In the past two decades, extensive scholarship in international law has analysed the rules governing cyber warfare, and, in particular, the application of the traditional law of armed conflict to cyber operations. Yet, not all the rules of international law apply flawlessly to cyber operations due to a poor match between existing rules and the challenges of cyber. Furthermore, some of the applicable rules generate significant legal disagreements and unsettled issues.[13] In 2017, Michael Schmitt published an Article in which he discussed some of these unsettled issues, which he termed "grey zones."[14] Schmitt highlighted three reasons justifying the need for clarification of these grey zones: First, "*uncertainty can lead to escalation*" as states may interpret and respond to certain actions differently.[15] Second, "clarification of grey zone issues will also enhance *deterrence* in cyberspace."[16] Third, "legal clarity breeds international *stability*;" and the clarification of grey zones can reduce the likelihood that states will use them in a way that leads to instability.[17] While accepting Schmitt's general arguments for clarifying grey zones in international law governing cyber operations, this Article advances a fourth argument for clarification, placing the implications of "grey zones" in the emerging debate about cynicism and backlash in international law. Existing literature identifies legal cynicism as a prevalent problem in international law and, specifically, in the law of armed conflict.[18] Based on this literature, I argue that existing legal grey zones trigger cynical attitudes towards international law and make people less trusting of it. Further, these grey

---

G.A. Res. 63/37, U.N. Doc. A/RES/63/37, at 2 (Dec. 2, 2008); G.A. Res. 64/25, U.N. Doc. A/RES/64/25, at 2 (Dec. 2, 2009); G.A. Res. 65/41, U.N. Doc. A/RES/65/41, at 2 (Dec. 8, 2010); G.A. Res. 66/24, U.N. Doc. A/RES/66/24, at 2 (Dec. 2, 2011); G.A. Res. 67/27, U.N. Doc. A/RES/67/27, at 2 (Dec. 3, 2012).

11. Adam P. Liff, *Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War*, 35 J. STRATEGIC STUD. 401, 401–02 (2012).

12. Troy Anderson, *Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals*, 34 ARIZ. J. INT'L & COMPAR. L. 135, 135 (2017).

13. Kilovaty, *supra* note 11, at 95–96.

14. Michael N. Schmitt, *Grey Zones in the International Law of Cyberspace*, 42(2) YALE J. INT'L L. ONLINE 1 (2017).

15. *Id.* at 21 (emphasis added).

16. *Id.* (emphasis added).

17. *Id.* (emphasis added).

18. Shiri Krebs, *All Is Fair In Law and War? Legal Cynicism in the Israeli-Palestinian Conflict*, *in* CYNICAL INTERNATIONAL LAW? 235, 235 (Bjornstern Baade et al. eds., 2021); *See also* additional literature in Section IV below.

zones weaken the ability of international law norms to effectively guide states' behaviour during either peacetime or armed conflicts. This legal ambiguity, also known as "grey zones" by Schmitt, will enable states to use international law as a tool to justify their actions.

Hence, the main questions this article seeks to clarify are: what are the current grey zones and controversies concerning the legal regime governing cyber operations? And, how do these gaps contribute to the marginalization and politicization of international law? This Article begins in Section I with definitions of key terms, including "cyberattack," "cyber warfare," and "cyber operation." This Article only covers cyber operations governed under the law of war, namely *jus ad bellum* and *jus in bello,* although there could be other laws, international or domestic, governing cyber operations. Cyber operations conducted outside these two branches of law are not covered in this Article. Section II then identifies core differences between cyber operations and other types of armed conflicts. These differences are the basis for identification of existing grey zones discussed in Section III. Section III begins with a description of the international efforts invested to regulate cyber operations, including the *Tallinn Manual*, and shows that despite these efforts, cyber warfare is currently not sufficiently regulated by existing legal norms. Then, based on the accepted notion that international law of war generally applies to cyber operations, Section III identifies the existing grey zones - legal gaps and unsettled issues - deriving from the application of international law to cyber operations. This Article extends and expands upon Schmitt's pioneering work in several ways.[19] First, it updates and enhances our understanding of the grey zones, for example by identifying countermeasures, which are not yet addressed by existing literature. Second, it provides an updated analysis of existing core disagreements, including those relating to the use of force and self-defence. Finally, by adopting the arguments of legal cynicism, Section IV demonstrates that the clarification of grey zones, as articulated by Michael Schmitt, in cyberspace is needed not only to prevent misinterpretation of the law or to promote international stability, but also to strengthen and reclaim international law as a normative framework guiding behaviour during armed conflicts.

I. DEFINITIONS

The literature on this topic utilises different concepts and definitions of cyber tools and methods, resulting in confusion concerning the scope and meaning of core terms such as "cyberattack," "cyber operation," and "cyber

19. Schmitt, *supra* note 14.

warfare."[20] In addition to detailed legal definitions, some authors use these terms colloquially, broadly signifying any use of cyber means in various contexts.[21] For purposes of clarity and consistency, this Article uses the term "*cyberattack*," as defined below, as its core term used to reference the cyber equivalent to the traditional "armed attack" concept. The term "*cyber operation*" is defined as "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace."[22] The term "*cyber warfare"* is used to refer more broadly to any cyber operation that occurs during an armed conflict, regardless of whether the operation can be considered as an armed attack or not; the term *"cyber warfare*" includes both cyberattacks and cyber operations.[23]

The most important definition central to this Article is the definition of "cyberattack," which refers to a cyber operation that according to *jus ad bellum*, crosses the line of an armed attack. Within *jus in bello*, LOAC applies to cyber operations conducted during an armed conflict (which do not necessarily rise to the level of cyberattack).[24] The traditional distinction between *jus ad bellum* and *jus in bello* also applies to cyberspace.[25]

Despite the significance of the term "cyberattacks" for the application of LOAC, existing literature includes various inconsistent definitions of this term. Analysing these definitions in the existing literature (including when referred to as "cyber warfare"), this Article identifies four main elements that are included in most definitions: (i) the identity of the attacker (state or non-state actor); (ii) the means of the operation (computer system or network); (iii) the target of the operation (computer system or network); and (iv) the effects of the operation (physical damage, reasonably expected such damage or damage caused to the functionality of physical objects).[26] Among the existing legal definitions, there is a consensus, articulated by Charles G. Billo and Welton Chang, that the *means* of the operation must be computers,

---

20. *See, e.g.*, Kilovaty, *supra* note 1, at 92; Hathaway et al., *supra* note 4, at 826–37; Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 A.F. L. REV. 121, 125–27 (2009); TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 15 (Michael N. Schmitt ed., 2013).

21. *Id.*

22. Memorandum from the Vice Chairman of the Joint Chiefs of Staff to Chiefs of the Military Services, Commanders of the Combat Commands and Directors of the Joint Staff Directorates on Joint Terminology for Cyberspace Operations 8 (2011) (available at https://info.publicintelligence.net/DoD-JointCyberTerms.pdf).

23. *Cyber Warfare*, HOW DOES LAW PROTECT IN WAR?, https://casebook.icrc.org/glossary/cyber-warfare (last visited Feb. 24, 2023).

24. Schmitt, *supra* note 20, at 75–78. For further information regarding *jus ad bellum*, see *infra* notes 132-33 and accompanying text; For further information regarding *jus in bello*, see *infra* note 201 and accompanying text.

25. *Id.* at 5.

26. The definition in Hathaway et al. also relates to the motive of the attack – ". . . for a political or national security purpose." *See* Hathaway et al., *supra* note 4, at 826.

computer systems, computer networks and so forth.[27] Also, it is generally agreed that the operation can be either offensive or defensive.[28] As identified in the Tallinn Manual, the main two controversies concerning the scope of the definition relate to the identity of the attacker and the effects of the operation. The first controversy refers to cyber operations that are carried out by non-state actors, asking whether they are considered "cyberattacks" under the law of armed conflict.[29] The second controversy concerns whether an operation must result in physical damage in order to be considered a cyberattack, or whether physical damage that was reasonably expected is sufficient, even if the actual outcomes of the attack did not have such effect.[30]

The most comprehensive legal document which defines "cyberattack" is the *Tallinn Manual*.[31] The *Tallinn Manual* (Rule 30) defines a cyberattack as a "cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[32] In relation to the identity of the attacker, the *Tallinn Manual* mentions that "in special circumstances, the conduct of non-state actors may be attributable to a state" (Rule 6).[33]

In respect to the effects of the operation, the *Tallinn Manual* takes the view that actual physical damage is not required, as long as it falls within the definition of a cyberattack mentioned above.[34] It further clarified that the word "cause" refers to "any reasonable foreseeable consequential damage, destruction, injury or death,"[35] and not only to the "effects on the targeted cyber system."[36]

---

27. *See, e.g.*, CHARLES G. BILLO & WELTON CHANG, CYBER WARFARE 3 (2004); NILS MELZER, CYBERWARFARE AND INTERNATIONAL LAW 4 (2011); MARIAROSARIA TADDEO, AN ANALYSIS FOR A JUST CYBER WARFARE (2012); Schaap, *supra* note 20.

28. *See, e.g.*, BILLO & CHANG, *supra* note 27, at 3; TADDEO, *supra* note 27; *Cyber Warfare*, *supra* note 23.

29. Schmitt, *supra* note 20, at 58.

30. *Id.* at 56–57.

31. *Id.*; *See* Part III(A).

32. Also, the majority of the Tallinn Group added to that definition incidents where the operation interferes with the functionality of an object "if restoration of functionality requires replacement of physical components." Schmitt, *supra* note 20, at 106, 108.

33. *Id.* at 32.

34. *Id.* at 106; See, for example, Rule 51 ('proportionality'), which explains that "the use of the words *expected* and *anticipated* indicates that the application requires an assessment of the reasonableness of the determination at the time the attack was planned, approved or executed." *Id.* at 162.

35. *Id.* at 107.

36. *Id.*

For clarity and simplicity, this Article adopts the definition of the *Tallinn Manual* for cyberattack, noting the existing controversies and varying interpretations.[37]

II. LEGAL CHALLENGES RELATING TO CYBERSPACE

Oona Hathaway writes that the typical areas of warfare include land, air, sea, and space; however, she notes that the increasing weaponization of the cyber world has led to the acknowledgement that cyberspace is another important aspect of warfare.[38] However, "[t]he definition of cyberspace proposed by the [United States] National Military Strategy for Cyberspace Operations [is] 'a domain characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures.'"[39]

Due to its distinctive features, cyberspace is different from the conventional, physical-kinetic sphere.[40] Firstly, cyber operations are actions conducted via the internet.[41] Due to technological advancements, states heavily rely on computers and digital networks to manage their "critical infrastructure."[42] Governments (and societies more broadly) are highly dependent on infrastructure which generally consists of essential services, including those related to communications, funds and so forth.[43] Vulnerability within these infrastructures exposes states to the risk of massive damage if these systems are interrupted.[44] Moreover, the internet does not have an organized structure,[45] which means that there is no clear separation between military and civilian networks and infrastructures; they are inherently interconnected and difficult to distinguish.[46] In other words, military codes sent through cyberspace are divided up into several data packages and may be sent through various civilian routes, and pass through

37. Kilovaty, *supra* note 1, at 98 ("The term 'cyber warfare' is not defined in the *Tallinn Manual*, despite being regularly used throughout it.").

38. Hathaway et al., *supra* note 4, at 827.

39. Schaap, *supra* note 20, at 126 (citing C. Todd Lopez, *Fighting in Cyberspace Means Cyber Dominance*, A.F. PRINT NEWS (Feb. 28, 2007), https://www.af.mil/News/Article-Display/Article/127803/fighting-in-cyberspace-means-cyber-domain-dominance).

40. Kilovaty, *supra* note 1, at 93. *See also* Gary D. Brown, *International Law Applies to Cyber Warfare: Now What?*, 46 SW. L. REV. 355, 357 (2017).

41. Yohannes Eneyew Ayalew, *Cyber Warfare: A New Hullaballoo under International Humanitarian Law*, 6 BEIJING L. REV. 209, 210 (2015).

42. Kilovaty, *supra* note 1, at 94.

43. *Id.*

44. *Id.*

45. Erki Kodar, *Applying the Law of Armed Conflict to Cyberattacks: From the Martens Clause to Additional Protocol I*, 15 ESTONIAN NAT'L DEF. COLL. PROC. 107, 128 (2012).

46. Kilovaty, *supra* note 1, at 94; Kodar, *supra* note 39, at 128.

a variety of civilian systems.[47] Thus, numerous civilian cyber systems, including "servers, routers, cables or satellites, as well as software," are used in each cyber operation and might be considered as legal military objectives to attack.[48] "For example, it is estimated that approximately 98 per cent of US government communications use civilian-owned and -operated networks."[49] Due to this interconnection, it is difficult and sometimes impossible to differentiate between military and non-military objects, which makes it difficult to apply the LOAC principle of distinction to cyber operations.[50]

Secondly, unlike kinetic war, cyber operations may cause serious damage to critical infrastructure without causing any physical damage;[51] operations within cyberspace may cause severe non-physical damage, including the destruction of banking systems and computers, harm of sensitive information and data, damage to government digital networks, and disruption of essential governmental services.[52] Although these effects are all severe, they are not physical. For example, unlike Stuxnet which resulted in physical damage, most cyber operations had serious effects but caused no physical destruction, such as the cyber operations on Estonia in 2007 and on Georgia in 2008.[53] The difference between physical and non-physical damage is highly significant in terms of applying the law; for example, as Russell Buchan has argued, "Article 2(4) [of the *Charter of the United Nations ("UN Charter")*] is an effects-based prohibition," meaning that only cyber operations that cause "physical damage will be regarded as an unlawful use of force."[54] Thus, cyber operations that do not reach this level will not constitute a violation of Article 2(4).[55]

Thirdly, a key problem relating to cyber operations is identifying where the attack is coming from and who is responsible for it.[56] Not only are cyber operations usually conducted clandestinely, but cyber attackers can also use technology to create false identifiers, which could cause confusion and

47. Robin Geiß and Henning Lahmann, *Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space*, 45 ISR. L. REV. 381, 385 (2012).

48. *Id.* at 385–86.

49. *Id.*

50. *Id.*

51. Noah Simmons, *A Brave New World: Applying International Law of War to Cyber-Attacks*, 4 J. L. & CYBER WARFARE 42, 74 (2014); Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SEC. L. 211, 212 (2012). Of course, cyber operations may also cause physical damage and even fatalities. Such effects, as previously discussed, distinguish cyber operations from cyberattacks.

52. Ayalew, *supra* note 41, at 210; Buchan, *supra* note 51, at 212.

53. Kilovaty, *supra* note 1, at 91–92; Schaap, *supra* note 20, at 146.

54. Buchan, *supra* note 51, at 212.

55. *Id.*

56. Jenny Döge, *Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime*, 48 INT'L L. ARCHIVE 486, 487 (2010).

delays in accurate attribution.[57] Cyber operations are frequently harder to identify and assess than conventional kinetic attacks. Such an analysis might call for the use of sensitive technology capabilities and information that states would rather keep secret. As a result, it is more difficult to attribute cyber operations.[58] Lorraine Finley and Christian Payne articulate that these technical difficulties have legal consequences: a state might misattribute a cyber operation and accidently use self-defence to attack the wrong third party. Also, because it takes time to identify the attacker, a state might not satisfy the factors of immediacy and necessity which are needed to legitimately use self-defence.[59]

Fourthly, unlike physical attacks, cyberspace actions are immediate. For cyber operations, no physical arrangements or deployments, such as military forces, are necessary.[60] Likewise, cyber operations can occur instantaneously, as they do not have the geographical distance barrier.[61]

Finally, while in the past states had exclusive use of weaponry and military facilities, cyber methods are easily reachable.[62] No one has exclusive control over cyberspace, thus both states and non-state actors can utilise it to further their ends.[63] For example, weak states or non-state actors who could not afford significant military expenses to participate in kinetic armed attacks may have the capability to do so now, by more affordable and quicker means.[64]

III. APPLYING INTERNATIONAL LAW TO CYBER WARFARE

The initial international step to regulate cyber warfare was the United Nations General Assembly First Committee (1998).[65] The Russian Federation initiated a call for "a cyber arms-control treaty" while the position of the United States was that "the same laws that apply to the use of kinetic weapons should apply to state behaviour in cyberspace."[66] This Committee has produced a draft resolution that was adopted as Resolution

57. Kilovaty, *supra* note 1, at 94.

58. Lorraine Finlay & Christian Payne, *The Attribution Problem and Cyber Armed Attacks*, 113 AJIL UNBOUND 202, 203 (2019).

59. *Id.* at 203–04.

60. Kilovaty, *supra* note 1, at 94–95.

61. *Id.* at 95; Brown, *supra* note 40, at 358.

62. Brown, *supra* note 40, at 358. Although, today physical weapons are also available to many non-state actors.

63. Kilovaty, *supra* note 1, at 95.

64. *Id.*; Nevertheless, powerful, rich, and developed countries still have a significant advantage in this domain. Also, conducting cyber operations does require some level of expertise.

65. G.A. Res. 53/70, U.N. Doc. A/Res/53/70 (Jan. 4, 1999).

66. Tim Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?*, at 20 (Cambridge, Mass.: Belfer Ctr. for Sci. & Int'l Affairs, Harv. Kennedy Sch., Discussion Paper 2011-11).

53/70 without a vote.[67] When the Draft Resolution went to recorded vote in 2005, the United States was the only country that voted against it.[68] Yet, during the following years, the United States proposed several draft resolutions aimed at creating "a global culture of cyber-security."[69] In 2000, the Third Committee of the General Assembly produced Draft Resolution 55/593.[70] This draft resolution was "introduced by the United States and 38 other member states including the Russian Federation, France, Israel, and the United Kingdom…" and was adopted as Resolution 55/63 ["Combating the criminal misuse of information technologies"], also "without a vote."[71] The Third Committee produced some more resolutions on the same subject.[72] In 2002, during the Second Committee, draft resolution 57/239 was presented by the United States, entitled "Creation of a Global Culture of Cyber-security."[73]

In 2004, a Group of Governmental Experts (GGE) was founded by the United Nations and has held five sessions to date.[74] Three of the sessions are considered to be successful in "outlining the global cybersecurity agenda and introducing the applicability of international law to state behaviour in cyberspace."[75] As explained by Eneken Tikk-Ringas, the first session (2004/2005) was unsuccessful in producing a report, due to lack of consensus.[76] The second GGE session (2009/2010) aimed to continue studying the current and emerging information security threats and ways to resolve them.[77] This session started the discussion among states regarding standards of use related to information and communication technology (ICT).[78] Tikk-Ringas continues her explanation by stating that the third GGE session (2012/2013) focused on states' behaviour and expanded the discussion into two separate dialogues: "applicability of international law [to ICT] and norms of responsible state behaviour."[79] Prior to the third session, in 2011, Russia, China, Tajikistan, and Uzbekistan offered an "International

67. *Id.* at 21.

68. *Id.* at 22.

69. *Id.* at 35-36, 43.

70. *Id.* at 35; G.A. Res. 55/593, U.N. Doc. A/Res/55/593 (Nov. 16, 2000).

71. Maurer, *supra* note 66, at 35; *see* G.A. Res. 55/63 (Jan. 22, 2001).

72. Maurer, *supra* note 66, at 36-37; *see, e.g.*, G.A. Res. 63/195 (Mar. 10, 2009); G.A. Res. 64/179 (Mar. 26, 2010); G.A. Res. 65/232 (Mar. 23, 2011).

73. Maurer, *supra* note 66, at 43.

74. Stefan Soesanto & Fosca D'Incau, *The UN GGE is dead: Time to fall forward*, EUROPEAN COUNCIL ON FOREIGN RELS. (Aug. 15, 2017), https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance#.

75. *Id.*

76. Eneken Tikk-Ringas, *International Cyber Norms Dialogue as an Exercise of Normative Power*, 17 GEO. J. INT'L AFF. 47, 50 (2016).

77. *Id.*

78. *Id.*

79. *Id.*

code of conduct for information security."[80] Moreover, the third session was notable because Russia and China, for the first time, publicly stated that "international law is applicable to cyberspace."[81] The fourth GGE session (2014/2015) dealt with "norms, rules, and principles for the responsible behaviour of States (chapter 3) separately from how international law applies to the use of ICTs (chapter 6)."[82] The former was considered to be "'voluntary, non-binding norms' that do not seek to limit or prohibit action that is otherwise consistent with international law."[83] The United States used the fourth GGE session to verify "existing principles of international law… identify and analyze rules and norms of behaviour that should govern the use of cyberspace."[84] The report of the fourth session "relates to the inherent right of self-defence under Article 51 of the UN Charter and affirms the IHL [international humanitarian law] principles of humanity, necessity, proportionality and distinction."[85] This session was significant and invited experts from many UN Member States, including "Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, the Russian Federation, Spain, the United Kingdom of Great Britain and Northern Ireland and the United States."[86] The consequent reports of those sessions reflect some of the points on which consensus was achieved between the Member States.[87]

Opposed to these three successful sessions, "the fifth and…last session" so far (2017) failed as a result of "fundamental disagreements" between the 25 members of the GGE group. [88] Therefore, this session, similar to the first one, also did not produce a consensus report.[89]

The UN activities mentioned above and the resolutions that have been adopted over time by different committees show that international cyber norms are slowly emerging, even though this process is highly dynamic.[90]

---

80. Maurer, *supra* note 66, at 5.

81. Elaine Korzak, *UN GGE on Cybersecurity: The End of an Era?*, DIPLOMAT (July 31, 2017), https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

82. Tikk-Ringas, *supra* note 76, at 50.

83. *Id.*

84. *Id.* at 51.

85. *Id.*

86. U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 3, U.N. Doc. A/70/174 (July 22, 2015).

87. U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 5, U.N. Doc. A/68/98 (June 24, 2013).

88. Soesanto & D'Incau, *supra* note 74 ("[F]undamental disagreements emerged between the Group's 25 members, particularly on the right to self-defence and the applicability of international humanitarian law to cyber conflicts.").

89. *Id.*

90. Maurer, *supra* note 66, at 47.

Tim Mauer explains that the main reasons for this dynamism are (i) domestic circumstances that impact the relations of different States and other actors and (ii) external factors that impact and alter the perspectives of key decision-makers.[91] It could be said that states play an important role in norm emergence; Russia and the United States had a critical role as the most significant counterbalance within the process.[92] Germany, Canada and the United Kingdom contributed funding for many research initiatives.[93] Surprisingly, China's contribution was not considerable except for its "co-sponsorship of the resolution in the First Committee."[94] Mauer posits that states can be considered as norm initiators; while they are mostly motivated by their personal interests, they are also influenced by "altruistic motives and a logic of appropriateness."[95] Thus, governments should put greater emphasis on creating their own cyber behaviours and strategies in order to establish a foundation for customary international law.[96]

A. The Tallinn Manual Project

In addition to the UN activities, in 2013 an international group of experts ("the Tallinn Group") created the *Tallinn Manual on the International Law Applicable to Cyber Warfare* that was initiated and supported by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE).[97] The purpose of the *Manual* was to create "a non-binding document applying the existing law to cyber warfare."[98] The international processes, including the *Tallinn Manual* projects, have focused on the application of LOAC to the actual challenges and circumstances of cyber warfare.[99] This includes the application of customary international law (CIL),[100] treaty law, including the Geneva Conventions of 1949,[101] the Additional Protocols of

91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.*
96. Soesanto & D'Incau, *supra* note 74.
97. Schmitt, *supra* note 20, at 1; An updated edition was published in 2017: TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 1 (Michael N. Schmitt ed., 2d ed. 2017).
98. Schmitt, *supra* note 20, at 1.
99. *Id.*
100. *Id.* at 8.
101. *See* Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31; Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85; Geneva Convention Relative to the Treatment of Prisoners of War, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287.

1977,[102] and The Hague Conventions of 1899 and 1907,[103] as well as the UN Charter.[104] Despite the international efforts described above and the significant development with the *Tallinn Manuals*, attempts to create binding international law applicable to cyber warfare have been unsuccessful.

Additionally, while the Tallinn process and manuals provide useful commentary on the application of existing international law to cyber operations, this interpretation is not universally accepted, and several significant issues remain highly contested (as will be detailed in sub-sections B through F below).[105] Indeed, most scholars agree that "international law applies to cyber warfare."[106] For example, the UN Secretary-General has acknowledged that "international law, and in particular, the Charter of the United Nations, is applicable [to cyberwarfare]."[107] Likewise, Harold Koh, legal advisor to the U.S. Department of State, "has stated that international law does apply to activities in cyberspace."[108] Finally, the Tallinn Group unanimously concluded that "both the *jus ad bellum* and *jus in bello* apply to cyber operations."[109] However, some of the issues raised by cyberattacks are not clearly addressed by existing international law.[110] This gap is

102. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3; Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), June 8, 1977, 1125 U.N.T.S. 609.

103. Convention (II) with Respect to the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, July 29, 1899, 32 Stat. 1803; Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land, Oct. 18, 1907, 36 Stat. 2277; Hague Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310; Döge, *supra* note 47, at 487; Ayalew, *supra* note 41, at 213; 1949 Geneva Convention I-IV; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of international Armed Conflicts (Protocol I) June 8, 1977, 1125 U.N.T.S. 3; Hague Conventions of 1899 and 1907.

104. U.N. Charter; Schmitt, *supra* note 20, at 8-9; Michael Gervais, *Cyber Attacks and the Laws of War*, 1 J. L. & CYBER WARFARE 8, 25 (2012).

105. This question has been a matter of controversy. The few scholars who claim that international law norms do not apply to cyber warfare argue that in reality, and as stated by Bradley Raboin, "the paradigm and structure of international law" cannot adapt to cyber warfare; *see*, *e.g.*, François Delerue, *International Cooperation on the International Law Applicable to Cyber Operations*, 24 EUR. FOREIGN AFF. REV. 203, 204 (2019); Bradley Raboin, *Corresponding Evolution: International Law and the Emergence of Cyber Warfare*, 31 J. NAT'L ASS'N ADMIN. L. JUDICIARY 602 (2011); Jordan Peagler, *The Stuxnet Attack: A New Form of Warfare and the (In)Applicability of Current International Law*, 31 ARIZ. J. INT'L & COMP. L. 399 (2014).

106. Brown, *supra* note 40, at 355.

107. *Id.* at 355 (citing U.N. GAOR, 68th Sess., U.N. Doc. A/68/98 (June 24, 2013)).

108. Peagler, *supra* note 105, at 411; *See also* Brown, *supra* note 40, at 355 (citing Harold Hongju Koh, *International Law in Cyberspace*, 54 HARV. INT'L L. J. ONLINE 1, 3 (2012)).

109. Schmitt, *supra* note 20, at 5.

110. *See*, *e.g.*, Gervais, *supra* note 104, at 10; Rex Hughes, *A Treaty for Cyberspace*, 86 INT'L AFF. 523 (2010); Dan-Iulian Voitasec, *Applying International Humanitarian Law to Cyber-Attacks*, 22 LEX ET SCIENTIA INT'L J. 124 (2015); Christopher Rosana Nyabuto, *A Game of Code: Challenges of Cyberspace as a Domain of Warfare*, 3 STRATHMORE L. REV. 49 (2018); Döge, *supra* note 56; Brown, *supra* note 40.

understandable given that the domain of cyberspace was not in existence when these laws (both customary and treaty law) were established,[111] and therefore states have not taken this type of warfare into account.[112]

Accordingly, while many of the current treaties and agreements under international law apply to cyberattacks, they do not do so explicitly.[113] The UN Charter, for example, offers a legal framework for an international convention regulating cyber operations, yet it seems that it is unable to address all the complexities involved in such a war.[114] In his Article, Schmitt identifies seven key grey zones concerning the application of international law to cyber warfare, including sovereignty, use of force, self-defence, and attribution.[115] This Article adopts and discusses these seven grey zones, as well as countermeasures. Also, under the grey zone of "use of force," this Article discusses the three approaches scholars have previously suggested to evaluate legitimacy of use of force: the effect-based, the instrument-based, and the target-based approaches.[116] In addition, under the grey zone of "self-defence," this Article identifies two more unsettled issues, and under the grey zone of "LOAC" it identifies one more unsettled issue. The following sections describe these main grey zones and emphasize the difficulty in applying the LOAC to cyber operations through the examples of both the 2010 Stuxnet incident against Iran and the 2007 cyber operations against Estonia.

B. Sovereignty and Non-intervention

The first challenge is applying the principles of state sovereignty[117] and non-intervention[118] to cyber operations. Under the principle of sovereignty, "hostile cyber operations directed against cyber infrastructure located on another state's territory… constitute, inter alia, a violation of that state's sovereignty whenever they cause physical damage or injury."[119] Thus, the unsolved question is regarding "cyber operations that neither cause physical damage nor amount to an intervention nevertheless violate the targeted

111. Schmitt, *supra* note 20, at 3; Kilovaty, *supra* note 1, at 95.

112. Döge, *supra* note 56, at 487-88. *See also* Kilovaty, *supra* note 1, at 95.

113. Alexi Franklin, *An International Cyber Warfare Treaty: Historical Analogies and Future Prospects*, 7 J. L. & CYBER WARFARE 149, 151 (2018).

114. Brett Epstein, *The Rules of Cyber-Welfare: What Are the Issues with These Rules, How Can the US Respond to an Attack When Applying These Rules, and Should New Rules Be Enacted?*, 18 HOLY CROSS J. L. & PUB. POL'Y 247, 286, 299 (2014) (citing U.N. Charter arts. 2, 51).

115. Schmitt, *supra* note 14, at 4-19.

116 Hathaway et al., *supra* note 4, at 845.

117. Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep 14, ¶ 202 (June 27).

118. *Id.* at ¶ 205 ("The principle forbids all states or groups of states to intervene directly or indirectly in the internal or external affairs of other states.").

119. Schmitt, *supra* note 4, at 274-75.

state's sovereignty."[120] For example, as posited by Michael Schmitt, State A has three alternatives to oversee cyber operations conducted by State B: i) using servers in State A's own territory to capture and intercept signals; ii) inserting malware into State B's network remotely; or iii) using a hard drive to implant the malware.[121] Schmitt analyses these three alternatives, and he begins by stating that the first alternative does not raise any legal issues because it neither involves coercion nor causes any physical injury. Also, espionage is not forbidden under international law.[122] After analysing the first, Schmitt moves to the third alternative, stating that it would be considered a breach of State B's sovereignty because the operation is taking place on its territory without States B's permission.[123] Schmitt concludes with an analysis of the second alternative, which he reminds us remains controversial: "[d]oes the remote implantation of the malware into State B's cyber systems…violate State B's sovereignty?"[124] Schmitt states that the Tallinn Group could not agree on whether it is considered a violation of sovereignty when a malware is implanted in a territory of another state and does not cause any physical damage.[125] Also, while traditionally only actions conducted by states could be considered as a violation of sovereignty, "some scholars [argue] that cyber operations conducted by non-State actors may also violate a state's sovereignty."[126]

With regards to the grey zone of non-intervention, "international law prohibits external intervention in the domestic affairs of another state due to the protective principles of territorial sovereignty and sovereign equality."[127] An action does not need to "cause physical damage or injury" in order to be considered as a violation of non-intervention principle, but it needs a coercive intent.[128] Coercion means taking actions in order to deny the free choice from another state.[129] The Tallinn Group agreed that cyber operations aimed at coercing the government may be considered as "a prohibited 'intervention'" or even "prohibited 'use of force.'"[130] Further, an

120. *Id.* at 275.

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. Schmitt, *supra* note 20, at 16. The *Tallinn Manual* does not mention the different views of the International Group of Experts regarding this issue.

126. *Id.* at 18.

127. U.N. Charter art. 2, ¶ 7; Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT'L. SEC. J. 146, 161 (2019); Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep 14, ¶ 205 (June 27).

128. Schmitt, *supra* note 4, at 275.

129. Schmitt, *supra* note 14, at 8.

130. Schmitt, *supra* note 20, at 17.

armed cyber-attack could trigger "the right of… self-defence," and actions that are not qualified as an armed attack but in other ways violate international law "may entitle the target State to resort to countermeasures."[131] The issue of coercion remains unsettled; there are different viewpoints regarding which cyber operations qualify as coercive in the intervention context.[132]

C. Jus ad Bellum: Use of Force, Armed Attack, and Self Defence

Jus ad bellum determines whether resorting to force is legal. Core questions under *jus ad bellum* are: (i) "when does a cyber operation constitute a wrongful use of force in violation of Article 2(4) of the United Nations Charter and customary international law?"[133] and (ii) "when would a cyber-attack rise to the level of an armed attack justifying self-defence under Article 51 of the U.N. Charter?"[134]

With regard to the first question, it is agreed that "a cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force" (*Tallinn Manual*, Rule 11).[135] The Tallinn Group reached consensus on the point that cyber operations resulting in physical damage, such as damage to computer hardware, can be comparable to kinetic operations in its scale and effects and considered as use of force.[136] However, they did not reach a similar consensus concerning cyber operations that lack physical consequences.[137] Dan Efrony and Yuval Shany identify that this "lack of consensus…under *jus ad bellum*" is a major inadequacy of the *Tallinn Manuals*.[138]

As stated by Oona Hathaway, the literature on this topic discusses three different approaches to analyse use of force: the effect-based, the instrument-based, and the target-based approaches.[139] As will be demonstrated below, and as articulated by Reese Nguyen, each of these

---

131. *Id.*

132. Schmitt, *supra* note 14, at 8.

133. Michael N. Schmitt, *Cyber Operations and the Jud Ad Bellum Revisited*, 56 VILL. L. REV. 569, 570 (2011). U.N. Charter art. 2, ¶ 4 ("All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.").

134. Hathaway et al., *supra* note 4, at 841; U.N Charter art. 51 ("[n]othing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations.").

135. Schmitt, supra note 20, at 45.

136. Dan Efrony & Yuval Shany*, A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 590 (2008).

137. *Id.*

138. *Id.* at 590.

139. Hathaway et al., *supra* note 4, at 845. *See also* Simmons, *supra* note 51, at 53; Gervais, *supra* note 104, at 29; Kilovaty, *supra* note 1, at 109.

approaches has significant shortcomings as they cannot comprehensively differentiate cyber operations from conventional attacks.[140]

The effect-based approach assesses use of force according to how serious the consequences are.[141] The gravity of the effects is determined by seven criteria as suggested by Schmitt ("Schmitt Analysis"): severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy and responsibility.[142] "Despite being the leading approach" among scholars,[143] the main problem with these criteria is that they are ambiguous and impractical in assessing whether an attack qualifies as an armed attack,[144] and they do not offer appropriate direction to decision-makers.[145] For example, the application of these criteria against the 2007 cyber operations on Estonia is ambiguous. While Schmitt states that according to the criteria these cyber operations can be considered as use of force because they were severe, invasive, and unnecessary, and also their effects were immediate, direct, and difficult to quantify,[146] other scholars interpreted this case contrarily. These scholars argue that while the cyber operations against Estonia were indeed immediate, the consequences were minimal: they were' not extremely serious due to the fact that there was no physical harm or damage to property, and the disruption caused merely a temporary inconvenience in terms of access to websites.[147] According to these scholars, the attack was intrusive and illegal, yet the ultimate consequences could not be considered a use of force.[148] Despite its weaknesses and even though it needs further refinement and broader consent in assessing use of force, the effect-based approach appears the most practicable approach when it comes to cyber operations.[149]

The instrument-based approach focuses on the way cyber operations are conducted.[150] Under this approach, only use of conventional weapons is relevant in order to qualify a cyber operation as use of force.[151] The main problem with this approach is that cyber operations normally do not employ ordinary military equipment and weapons and do not have the physical

140. Reese Nguyen, *Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare*, 101 CAL. L. REV. 1079, 1117 (2013).

141. Simmons, *supra* note 51, at 58.

142. Schmitt, *supra* note 133, at 575. *See also* Simmons, *supra* note 51, at 59; Gervais, *supra* note 104, at 31; Hathaway et al., *supra* note 4, at 847.

143. Simmons, *supra* note 51, at 61; Hathaway et al., *supra* note 4, at 845; Kilovaty, *supra* note 1, at 123.

144. Kilovaty, *supra* note 1, at 123.

145. Hathaway et al., *supra* note 4, at 848.

146. Schmitt, *supra* note 133, at 575, 577.

147. Nguyen, *supra* note 140, at 1123.

148. *Id.*; Gervais, *supra* note 104, at 32-33.

149. Kilovaty, *supra* note 1, at 123.

150. Gervais, *supra* note 104, at 29; Simmons, *supra* note 51, at 54.

151. Simmons, *supra* note 51, at 54-55; Hathaway et al., *supra* note 4, at 845-46.

attributes of military actions.[152] Therefore, under this approach, rarely will a cyber operation escalate to the of use of force threshold.[153] For example, according to this approach, neither Stuxnet nor the cyber operations against Estonia would be regarded as use of force: in both incidents non-traditional weapons were used.[154] Most scholars have rejected this approach for being "outdated and under-inclusive."[155]

Reese Nguyen explains that the target-based approach is based on the entity being targeted; for example, an attack on critical infrastructure, such as important "systems and assets," can be considered a use of force.[156] This approach focuses on "critical infrastructure with special status"[157] and defines "any cyber operation against such infrastructure as an 'armed attack.'"[158] This approach is itself limited though, especially since different countries may have different definitions of "critical infrastructure."[159] For instance, the US Congress defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[160] Second, while the previous approach was criticized for being under-inclusive, scholars argue that the target-based approach is "over-inclusive" as it extends the chances that a cyber operation might be considered as use of force.[161] This might undermine international security by increasing the likelihood of war.[162] According to this approach, it is sufficient that a cyber operation would merely attack a highly important infrastructure of a state in order to be considered as a use of force justifying self-defence as a response.[163] For example, under this approach, Iran should have been allowed to respond with force to the Stuxnet operation.[164] Similarly, the cyber operations against Estonia should have been considered a use of force, even though not much damage was done.[165]

---

152. Simmons, *supra* note 51, at 54-55; Hathaway et al., *supra* note 4, at 845.

153. Simmons, *supra* note 51, at 54-55; Hathaway et al., *supra* note 4, at 845-46.

154. Nguyen, *supra* note 140, at 1119.

155. Kilovaty, *supra* note 1, at 123; Hathaway et al., *supra* note 4, at 846.

156. Nguyen, *supra* note 140, at 1119.

157. *Id.*

158. Simmons, *supra* note 51, at 56; Hathaway et al., *supra* note 4, at 846; Nguyen, *supra* note 140, at 1119.

159. Nguyen, *supra* note 140, at 1119.

160. *Id.*; Critical Infrastructure Protection Act of 2001, 42 U.S.C. § 5195c(e) (2006).

161. Kilovaty, *supra* note 1, at 123.

162. *Id.*; Hathaway et al., *supra* note 4, at 847.

163. Hathaway et al., *supra* note 4, at 846-47.

164. Nguyen, *supra* note 140, at 1121.

165. *Id.*

Next, with regard to the second question of self-defence, according to the International Court of Justice (ICJ), "not every use of force rises to the level of armed attack."[166] It is essential to understand the difference between a use of force and an armed attack as the former seeks to "determine whether a state has violated Article 2(4) of the United Nations Charter and the related customary international law prohibition,"[167] while the latter determines "whether the target state may respond to an act with a use of force without itself violating the prohibition on using force."[168] "Only in the event that the use of force reaches the threshold of an armed attack, is a state entitled to respond using force in self-defence."[169] Thus, it is necessary to consider the "scale and effects" of a cyber operation in order to determine whether it reaches the level of an armed attack.[170] The "scale and effects" criteria were introduced in the ICJ *Nicaragua* judgment to differentiate actions that are considered armed attacks and actions that are not.[171] The ICJ "distinguish[es] the most grave forms of the use of force (those constituting an armed attack) from other less grave forms but provided no further guidance in this regard."[172] Therefore, the dispute regarding the "scale and effects" criteria is still unresolved.[173] The Tallinn Group agreed that "any use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement" to be considered as an armed attack.[174] However, they did not reach a consensus on the exact point of the severity of injury and damage in terms of how much harm a cyber operation needs to cause to people or property in order to qualify as an armed attack.[175] In fact, the international community has never managed to unambiguously identify any international cyber operations approaching the level of an armed attack, including incidents such as the 2007 cyber operations against Estonia.[176] The Tallinn Group

166. Schmitt, *supra* note 20, at 55 (citing Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep 14, ¶ 191 (June 27)).

167. *Id.* at 52; *see supra* note 133 and accompanying text.

168. Schmitt, *supra* note 20, at 52; U.N. Charter art. 51.

169. Schmitt, *supra* note 20, at 55.

170. *Id.* at 52, 54.

171. *Id.* at 55.

172. *Id.* (citing Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep 14, ¶ 195 (June 27)).

173. Schmitt, *supra* note 20, at 55.

174. *Id.*

175. *Id.* at 56.

176. *Id.* at 57-58; "Following the relocation of a Soviet-era statue in Tallinn in April of 2007, Estonia fell under a politically motivated" series of cyber-attacks "lasting twenty-two days" which targeted websites of Estonian organizations, including the Estonian Parliament, banks, ministries, newspapers and broadcasters; Rain Ottis, *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*, (2008), CCDCOE, https://ccdcoe.org/library/publications/analysis-of-the-2007-cyber-attacks-against-estonia-from-the-information-warfare-perspective/; Duncan B. Hollis,

unanimously determined that "the scale and effects threshold was not reached."[177] As for the 2010 Stuxnet attack, only some members of the Tallinn Group took the position "that the operations had reached the [level of an] armed attack" due to the fact that the Iranian centrifuges were seriously harmed.[178]

Additionally, the Tallinn Manual brings to light some more issues that remain unsettled with regards to cyber operations that trigger the legal right to self-defence. First, it is not clear whether a state can legally respond to several cyber operations that, if carried out separately, would not qualify as an armed attack.[179] The Tallin Group inquired as to whether these cyber operations could be considered an armed attack when accumulated.[180] The Tallinn Group agreed that these small operations can be considered as a complex armed attack if they are related to each other, they were carried out by "the same originator," and they reached a necessary scale when combined.[181] The second unsettled issue relates to cyber operations that are carried out by non-state actors. It was agreed by the Tallinn Group that such operations, conducted by either individuals or group of people, may qualify as an armed attack if they are attributed to a state or under its guidance.[182] However, it remains controversial whether cyber operations that were carried out by non-state actors without any guidance of a state can be considered as an armed attack and justify a response of self-defence.[183] Most of the Tallinn Group experts concluded that States have the "right of self-defence… [against] armed attacks by non-State actors, such as terrorists and rebel groups," and extended this right to cyber operations also; only a few experts of the Tallinn Group thought otherwise.[184] For example, even though they were carried out by a non-state actor, the 9/11 terrorist attacks by Al Qaeda against the United States were classified "as an armed attack triggering the inherent right to self-defence."[185] The third unsettled issue relates to cyber operations that result in extensive and adverse consequences without causing any injury, death, damage or destruction.[186] Some of the Tallinn Group experts argued that the nature of the consequences is what

Why States Need an International Law for Information Operations, 11 LEWIS & CLARK L. REV. 1023, 1024-25 (2007); Nguyen, *supra* note 140, at 1127.

177. Schmitt, *supra* note 20, at 57-58.

178. *Id.*

179. *Id.* at 56.

180. *Id.* at 56. According to the I.C.J. Oil Platforms case, "[e]ven taken cumulatively (Iran's attacks) … do not seem to the Court to constitute an armed attack on the United States," triggering the right to self-defence; Oil Platforms (Iran v U.S.) 2003 I.C.J. 161 ¶ 192 (Nov. 6).

181. Schmitt, *supra* note 20, at 56.

182. *Id.* at 58.

183. *Id.*

184. *Id.* at 59.

185. *Id.* at 58.

186. *Id.* at 56.

matters - only cyber operations that harm people or cause physical damage to property should be considered armed attacks; others focused on the extent of the consequences, as illustrated by the example of an "incident directed against the New York Stock Exchange that causes the market to crash."[187] As such a scenario may cause no more than economic damage, it was controversial among the Tallinn Group experts.[188] Finally, the last unsettled issue relates to the effects of the cyber operation.[189] The Tallinn Group "agreed that all reasonably foreseeable consequences" should be considered in order to qualify a certain cyber operation as an armed attack.[190] For example, cyber operations "targeting a water purification plant" should be considered as an armed attack as their effects are reasonably expected - people can become very ill or even die as a result of "drinking contaminated water."[191] Yet, the Tallinn Group did not reach a consensus as to whether these effects need to be intentional. For example, they provided the example of "cyber espionage by State A against State B that unexpectedly results in significant damage to State B's cyber infrastructure."[192] Most of the Group argued that "intention is irrelevant in qualifying an operation as an armed attack and that only the scale and effects matter."[193]

In summary, *jus ad bellum* refers to situations in which states are permitted to use force.[194] Due to several disagreements concerning *jus ad bellum* issues in the cyber field, the current norms are insufficient and do not provide States clear guidelines regarding the prohibition to use force and the right to self-defence.[195] First, in relation to the use of force issue, there was no consensus amongst the Tallinn Group regarding cyber operations that lack physical consequences. Second, there are some disagreements under the issue of self-defense; a consensus could not be reached as for the damage that might be caused to people or property when determining the scale and effects.[196] Also, there was no consensus amongst the Tallinn Group as to whether some specific scenarios justify self-defense as a response, such as (i) scenarios in which non-state actors, rather than states, carry out cyber operations,[197] and (ii) scenarios in which cyber operations resulted in serious effects, but do not harm people or property. [198] Thus, the literature has

187. *Id.*
188. *Id.*
189. *Id.* at 57.
190. *Id.*
191. *Id.* at 56-57.
192. *Id.* at 57.
193. *Id.*
194. Schmitt, *supra* note 4, at 279.
195. Hathaway et al., *supra* note 4, at 821.
196. Schmitt, *supra* note 20, at 55-56.
197. Schmitt, *supra* note 20, at 58.
198. *Id.* at 56.

explored three approaches in order to determine whether a state can legitimately use force: the "effect-based," the "instrument-based," and the "target-based" approaches.[199] However, the approaches themselves have weaknesses that makes this determination difficult.[200]

D. Jus in bello: The Law of Armed Conflict (LOAC)[201]

LOAC refers to cyber operations performed during an armed conflict.[202] The controversy is "whether cyber operations themselves can trigger an armed conflict and thereby bring LOAC into operation."[203] The *Tallinn Manual* takes a supportive stance regarding international armed conflicts, but adopts a more subtle stance with regards to non-international armed conflicts.[204] Etian Diamond explains that "international armed conflicts" involve two or more States, while "non-international armed conflicts" require that "at least one of the belligerent parties is a non-state actor."[205]

The *Tallinn Manual* defines international armed conflicts as "[inter-state] hostilities, which may include or be limited to cyber operations" (Rule 22).[206] This means that LOAC can apply to cyber operations that reach the level of "hostilities."[207]

The *Manual* provides that "hostilities may involve any combination of kinetic and cyber operations, or cyber operations alone."[208] Further, "hostilities exist whenever one state engages in 'cyber attacks' (Rule 30) against another."[209] Rain Liivoja and Tim McCormack analyse, "whether, and if so what kind of, cyber operations falling below the intensity of an attack could nonetheless trigger an armed conflict."[210] Little direction could be found in the *Manual* regarding this matter.[211] Accordingly, it seems that the only

199. Hathaway et al., *supra* note 4, at 845.

200. Nguyen, *supra* note 140, at 1117.

201. LOAC aims to defend individuals that are not engaged in the combat. Also known as international humanitarian law (IHL): Ayalew, *supra* note 41, at 212.

202. *Id.* at 215. *See* Kodar, *supra* note 45, at 109; Voitasec, *supra* note 110, at 124; Brown, *supra* note 40, at 356.

203. Rain Liivoja & Tim McCormack, *Law in the Virtual Battlespace: The Tallinn Manual and the Jus in Bello*, 15 Y.B. OF INT'L HUMANITARIAN L. 45, 51 (2012).

204. *Id.*

205. Etian Diamond, *Applying International Humanitarian Law to Cyber Warfare*, 67 L. & NAT'L SEC 67, 71-72 (2014).

206. Liivoja & McCormack, *supra* note 203, at 51 (citing Schmitt, *supra* note 20, at 79).

207. *Id.*

208. Schmitt, *supra* note 20, at 82.

209. *Id.*

210. Liivoja & McCormack, *supra* note 203, at 52.

211. *Id.*

cyber incidents that reach the level of an "attack" can be regulated under LOAC Rules.[212]

With regards to non-international armed conflicts, the *Manual* defines them as "protracted armed violence, which may include or be limited to cyber operations [between certain armed groups]" (Rule 23).[213] The *Manual* also mentions that LOAC can apply only if the conflict reaches a "minimum level of intensity" and the parties involved in the conflict, such as "individual… or groups of hackers," show a "minimum degree of organization."[214] This means that "cyber operations in and of themselves will only in exceptional cases amount to non-international armed conflict."[215]

One of the main challenges with *jus in bello* is applying LOAC "principles of distinction, proportionality and precaution" to cyber operations.[216] These principles are "codified in the First Additional Protocol to the Geneva Conventions (Additional Protocol I) [[217] and]… customary international law [and are] applicable both in international and non-international armed conflicts."[218] The principle of distinction limits the legitimate targets only to "combatants or military objects" in order to protect civilians.[219] However, cyberspace is a domain being used by both the army and the civilian population, which makes distinction much more challenging,[220] yet still possible, as in the case of Stuxnet. Further, "most international cyber infrastructure[s are]…in practice…dual-use infrastructure[s]" that serve both military and civilian needs, such as "computers, routers, cables, and satellites."[221] Therefore, the most important concern regarding this matter is whether it is possible to guarantee that cyber operations are focused solely on military goals and that ongoing precautionary measures are implemented to protect "civilian infrastructure."[222] The Stuxnet virus is an example of a cyberattack against a particular military computer system. However, attacks

212. Michael N. Schmitt, *Cyber Operations and the Jus in Bello: Key Issues*, 87 INT'L L. STUD. 89, 90 (2011); Diamond, *supra* note 205, at 75.

213. Liivoja & McCormack, *supra* note 203, at 51; Schmitt, *supra* note 20, at 84.

214. Liivoja & McCormack, *supra* note 203, at 51; Schmitt, *supra* note 212, at 105-06.

215. Liivoja & McCormack, *supra* note 203, at 51 (citing Schmitt, *supra* note 20, at 85).

216. Diamond, *supra* note 205, at 75.

217. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3.

218. Diamond, *supra* note 205, at 75.

219. Kodar, *supra* note 45, at 117; "Article 48 of *Additional Protocol I* requires the parties to a conflict to at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly direct their operations only against military objectives."; Schmitt, *supra* note 212, at 90 (citing Article 48 of *Additional Protocol I*, *supra* note 102).

220. Ayalew, *supra* note 41, at 221.

221. Cordula Droege, *Get off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians*, 94 INT. REV. RED CROSS 533, 562-63 (2012).

222. Ayalew, *supra* note 41, at 221.

on computer networks may happen randomly and harm civilian targets (both people and property) and not only military ones.[223]

Another critical question, posed by Yohannes Eneyew Ayalew, concerns the personnel who usually conduct cyber operations, namely hackers: "[a]re [they] a legitimate target?"[224] Are they protected under LOAC? Since many of them are civilians, the LOAC should, in principle, defend them from hostile attacks. However, some scholars argue that there is no justification to protect hackers that participate in a cyber-attack.[225]

The second principle is proportionality. Under this principle, attacks are not allowed if they "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."[226] This principle tries to reduce the harm that can be done to material items and civilians while yet achieving the "military advantage gained from the attack."[227] There is a real threat that cyber operations would have a severe impact on civilian facilities, given the "dual-use nature of most cyber infrastructure" and the "interconnectedness of cyberspace."[228] A central challenge of practicing proportionality in cyber operations is assessing whether "damage" also includes in its definition "loss of functionality."[229] This issue of whether "loss of functionality" is considered as damage was discussed among the Tallinn Group experts.[230] Most of the group argued "that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components."[231] Schmitt provides the example of a cyber operation that halts the functioning of an electrical grid and necessitates a replacement of critical parts of the system.[232] The second unresolved issue in this regard is determining whether any unintended civilian harm might be disproportional when taking into account the military benefit.[233] In fact, Diamond emphasizes that it is never easy to accurately evaluate and foresee the damage that might be caused to civilians compared to the military advantage

223. Droege, *supra* note 221, at 539-40.

224. Ayalew, *supra* note 41, at 221.

225. *Id.*

226. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 51 ¶5(b), June 8, 1977, 1125 U.N.T.S. 3. Diamond, *supra* note 205, at 78-79.

227. Kodar, *supra* note 45, at 118 (citing Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 57 ¶ (2)(a)(iii), June 8, 1977, 1125 U.N.T.S. 3).

228. Droege, *supra* note 221, at 571, 573.

229. *Id.*; Diamond, *supra* note 205, at 79.

230. Schmitt, *supra* note 20, at 108.

231. *Id.*

232. *Id.*

233. Diamond, *supra* note 205, at 79.

that could be achieved, but evaluating this proportionality in cyberspace is even harder due to the "interconnected nature of cyberspace."[234]

Another important principle is precaution. LOAC "requires belligerents to take precautions in attack,[235] as well as precautions against the effects of attack."[236] While combatants may be obligated to take all reasonable steps to keep their military and civilian cyber systems distinct, the integrated nature of military and civilian cyber systems makes this extremely unlikely.[237] Therefore, applying the precaution principle to cyber operations is also complicated due to technical challenges.[238]

It is important to also mention cyber operations occurring outside of an armed conflict. LOAC applies only to cyber operations conducted "during armed conflict," thus, cyber operations conducted "outside the context of armed conflict", which are not covered by LOAC, may fall under other laws.[239] While the first *Tallinn Manual* only addressed *jus ad bellum* and *jus in bello*, "*Tallinn Manual 2.0* [also] examines key aspects of the public international law governing 'cyber operations' during peacetime."[240] It "does not deal with international criminal law, trade law or intellectual property…[n]or …with either private international law or domestic law," but it does relate to "other public international law regimes."[241] For example, Rule 32 relates to "[p]eacetime cyber espionage."[242] The Tallinn Group agreed that "[a]lthough peacetime cyber espionage by States does not *per se* violate international law," cyber espionage that, for example, "violate[s] the international human right to privacy" is illegal.[243]

In summary, while LOAC generally applies to cyber operations conducted during armed conflict (international and non-international), the application of its principles presents several difficulties, mostly due to the cyber world's "interconnected nature."[244] First, since "international cyber infrastructures" are "dual-use" (military and civilian) applying the principle of distinction becomes challenging as it necessitates differentiating

234. *Id.*

235. *Id.* (citing Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, *supra* note 102, at art. 57.).

236. *Id.* (citing Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S. 3, *supra* note 102, at art. 58.).

237. Diamond, *supra* note 205, at 80.

238. Droege, *supra* note 221, at 574.

239. Brown, *supra* note 40, at 362-63.

240. Schmitt, *supra* note 97, at 3.

241. *Id.*

242. *Id.* at 168; ("Although peacetime cyber espionage by States does not *per se* violate international law, the method by which it is carried out might do so.").

243. *Id.* at 168-70.

244. Diamond, *supra* note 205, at 75, 79.

"between civilians and combatants and between civilian objects and military objectives."[245] Also, it is not clear whether hackers who are civilians participating in the conflict can be "legitimate target[s]."[246] Further, applying the principle of proportionality is challenging. This principle requires taking into account the expected damage to civilians while achieving military advantage from the operation. Again, since "cyber infrastructures" may be "dual-use," it is difficult to assess whether the expected damage might be disproportionate and harm also civilians.[247] Lastly, precaution is also difficult to apply since cyberspace is interconnected, and it is hard to distinguish infrastructures used by the military and civilians.[248] Regarding cyber operations to which LOAC does not apply, we can find cyber operations conducted outside armed conflict or non-international cyber operations in which the involved party cannot prove itself as an "organisation."[249] Such situations are covered by other bodies of law rather than LOAC.[250]

E. Countermeasures

Since the question regarding the permitted legal response to cyber operations "that do not reach the level of an armed attack" remains unsettled, scholars have suggested that states can use countermeasures, rather than self-defense, to respond to such cyber operations.[251] Countermeasures are permitted, under some circumstances, as a "response to low-intensity attacks"; they are not being used merely in military situations, but also as a response to "political and economic wrongs."[252] For example, actions such as "hacking into a network" or "destroying data" in a way that interferes with any other states' internal affairs or violates its sovereignty may warrant countermeasures.[253] Further, using countermeasures as a response does not require using force.[254] The legal logic behind the countermeasure's alternative is that cyber armed attacks are

245. Droege, *supra* note 221, at 571, 561-63; Ayalew, *supra* note 41, at 220-21.

246. Ayalew, *supra* note 41, at 221.

247. Droege, *supra* note 221, at 571, 573.

248. Diamond, *supra* note 205, at 78, 80.

249. Liivoja & McCormack, *supra* note 203, at 51.

250. Brown, *supra* note 40, at 362.

251. Simmons, *supra* note 51, at 68; *see also* Hathaway et al., *supra* note 4, at 857; Michael N. Schmitt, *Below the Threshold Cyber Operations: The Countermeasures Response Option and International Law*, 54 VA J. INT'L L. 697, 700 (2014); Kilovaty, *supra* note 1, at 107; Troy Anderson, *Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals*, 34 ARIZ. J. INT'L & COMPAR. L. 135, 147-48 (2017).

252. Gervais, *supra* note 104, at 57.

253. Simmons, *supra* note 51, at 68.

254. Katharine C. Hinkle, *Countermeasures in the Cyber Context: One More Thing to Worry About*, 37 YALE J. INT'L L. ONLINE 11, 21 (2011).

rare. As mentioned previously, "[f]ew, if any, cyber operations have crossed the armed attack threshold," while those that do not reach this point are more prevalent.[255] Therefore, theoretically, states may find countermeasures useful for responding to cyber operations deemed to be an "internationally wrongful act" but not an "armed attack."[256]

Appealing as this option may be, it is not free from challenges.[257] The main challenge being that countermeasures aim to repair the damage that was done, and "to return a situation to lawfulness."[258] Additionally, Article 52 on State Responsibility states that, if the victim state decides to take countermeasures, the hostile state must be informed of the intended action; [259] and the victim state needs to start a negotiation in which it asks the hostile state to stop its "internationally wrongful act," while providing the latter enough time to do so.[260] Implementing these rules in a cyber context may be challenging and any such negotiation may be ineffective, as the hostile state may "within a short time" utilize any notification to "'immunize itself from countermeasures'" and thereby frustrate the purpose of notification."[261] Michael Schmitt provides an example of an attack against a state's financial system. Schmitt posits that in the event that a significant, unlawful cyberattack is conducted against a victim state's financial system, the latter may respond by using cyber countermeasures to deny the aggressor state access to its financial institutions. With that said, if the victim state essentially warned the aggressor about its intentions, the aggressor state could quickly "transfer assets out of the country" or remedy the system's weaknesses, which would limit the victim state's ability to conduct countermeasures.[262]

Thus, as Oona Hathaway and her co-authors point out, international law norms governing countermeasures are not comprehensive when it comes to addressing the issue of states' responses to cyber operations.[263] Indeed, Katharine Hinkle suggests that this legal framework "is far from ready to take on the challenges of the digital age."[264] Therefore, the level of

255. Schmitt, *supra* note 251, at 698.

256. *Id.* at 699-700; Simmons, *supra* note 51, at 68.

257. Simmons, *supra* note 51, at 68.

258. *Id.* at 69 (citing International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, art. 49(1), G.A. Res. 56/83 annex, U.N. Doc. A/RES/56/83 (Jan. 28, 2002)).

259. Simmons, *supra* note 51, at 69; Schmitt, *supra* note 251, at 716-17; International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, art. 52 ¶ (1)(b), U.N. Doc. A/RES/56/83 (Jan. 28, 2002).

260. Schmitt, *supra* note 251, at 716-17.

261. *Id.* at 717; Simmons, *supra* note 51, at 69; Hinkle, *supra* note 254, at 18 (citing Draft Articles, Article 52, cmt. 6).

262. Schmitt, *supra* note 251, at 717.

263. Hathaway et al., *supra* note 4, at 859.

264. Hinkle, *supra* note 254, at 21.

harm that a cyber-countermeasure might result in may be difficult to correctly predict due to the "interconnected…nature of cyber systems."[265]

F. Due Diligence

Another important issue is the due diligence rule (*Tallinn Manual 2.0*, Rule 6).[266] According to the *Tallin Manual*, this regulation is founded on a fundamental principle of international law, which holds that states have an obligation to take reasonable precautions to prevent the use of their sovereign territory against other states.[267] The due diligence principle "requires that states not allow the use of their territory to carry out cyber operations against other states."[268] Thus, a state might be responsible for stopping an action carried out in its territory, even if this state was not at all involved.[269]

Dan Efrony and Yuval Shany state that the main challenge in applying the due-diligence principle is related to the "problem of attribution."[270] The problem is that the victim state needs to provide a piece of proof that connects the operation to the territory of the violating state in order for the latter to take "responsibility for lack of due-diligence," however, in cyberspace states are hesitant to do so and subsequently disclose their identity. Therefore, the victim state might not provide this kind of proof.[271] This makes the due diligence principle less applicable in the field of cyberspace.[272] Another unsettled issue relates to the question of whether "transit states" are included in the due diligence principal requirements or if it only applies to the jurisdictions where the breaching cyber operations are carried out.[273]

G. State Responsibility for Cyber Operations and the Legal Standard for Attribution

In addition to the grey zones in the interpretation of the relevant legal rules, cyber operations often raise problems relating to identifying the responsible actors. As Lorraine Finlay and Christian Payne articulate, this

265. Schmitt, *supra* note 251, at 726.

266. Schmitt, *supra* note 97, at 30 (citing U.S. v. Ariz., 120 U.S. 479, 483 (1887); S.S. Lotus (Fr. v Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10; Island of Palmas (U.S. v. Neth.), 2 R.I.A.A. 829, 839 (1928); Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. 4, 22 (Apr. 9); U.N. Doc. A/CN.4/1/Rev.1 ¶ 57 (Feb. 10, 1949)).

267. Schmitt, *supra* note 97, at 30.

268. Kilovaty, *supra* note 127, at 176 (citing Schmitt, *supra* note 20, at 30).

269. Kilovaty, *supra* note 127, at 176.

270. Efrony & Shany, *supra* note 136, at 644-45.

271. *Id.*

272. *Id.*

273. Schmitt, *supra* note 14, at 12-13.

issue of responsibility and attribution is divided between technical and legal characteristics.[274] The "technical problem" is to pinpoint the source of a specific cyber operation.[275] The "legal problem" is to determine the criteria for faulting a state for cyber operations "by nonstate actors."[276] The main reason for these problems, as articulated by Efrony and Shany, is that cyberspace possesses distinct features, such as providing a platform for people to act clandestinely.[277] The possibility to conduct cyber operations clandestinely relying on capabilities to hide IP addresses, as well as the reliance on "hacker groups or 'hacktivists'" rather than formal state institutions, generates these issues.[278]

However, in order to attribute responsibility, it is necessary to identify the physical computers and devices used by the attacker and identify the state responsible for that attacker.[279] A victim state could legally respond to an attack only after identifying these details.[280]

Beyond these factual challenges, the legal standard of attributing cyber operations to states is also challenging. Under Article 2 of the *Responsibility of States for Internationally Wrongful Acts*, a state can be held responsible for "an internationally wrongful act…consisting of an action or omission" if it is "(a) []attributable to the State under international law; and (b) [c]onstitutes a breach of an international obligation of the State."[281] Also, "States are legally responsible for the conduct of their governmental organs or entities."[282] Nevertheless, "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[283]

Literature discusses two different legal standards of control, yet there is not yet a consensus on which one is more applicable to international law.[284]

---

274. Finlay & Payne, *supra* note 58, at 203.

275. *Id.*

276. *Id.* at 204.

277. Efrony & Shany, *supra* note 136, at 632; Finlay & Payne, *supra* note 58, at 203.

278. Simmons, *supra* note 51, at 101-03; Scott J. Shackelford & Richard B. Andres, *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, 42 GEO. J. INT'L L. 971, 982, 984 (2011).

279. Shackelford & Andres, *supra* note 278, 984-85.

280. *Id.* at 985.

281. Michael N. Schmitt, *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict*, *in* PROCEEDINGS OF A WORKSHOP ON DETERRING CYBERATTACKS 151, 158-59 (2010) (citing Resolution adopted by the General Assembly, *56/83 Responsibility of States for internationally wrongful acts*, art. 2., U.N. Doc A/RES/56/83 (Jan. 28, 2002)).

282. Schmitt, *supra* note 281, at 157 (citing Resolution adopted by the General Assembly, *56/83 Responsibility of States for internationally wrongful acts*, art. 4, U.N. Doc. A/RES/56/83 (Jan. 28, 2002)).

283. Resolution adopted by the General Assembly, *56/83 Responsibility of States for internationally wrongful acts*, art. 8, U.N. Doc. A/RES/56/83 (Jan. 28, 2002). Schmitt, *supra* note 281, at 157.

284. Schmitt, *supra* note 281, at 157-58.

According to the *Nicaragua* case,[285] the U.S. had to have "'effective control' over the non-state actor group [the *Contras*]" in order to be found liable for the actions of the *Contras*.[286] The ICJ *Nicaragua* case and *Bosnia Genocide* judgement discuss the term "complete dependence" in the context of *effective control*; "the evidence available to the Court indicates that the various forms of assistance provided to the *[C]ontras* by the United States have been crucial to the pursuit of their activities, but is insufficient to demonstrate their complete dependence on the United States [*sic*] aid."[287] This means that a non-state actor must be under the "complete dependence" of a state in order for the latter to be found responsible for the operation.[288] The *Nicaragua* case also adds that:

> United States participation, even if preponderant or decisive, in the financing, organizing, training, supplying and equipping of the *contras*, the selection of its military or paramilitary targets, and the planning of the whole of its operation, is still insufficient in itself, on the basis of the evidence in the possession of the Court, for the purpose of attributing to the Unites States the acts committed by the *contras* in the course of their military or paramilitary operations in Nicaragua…. would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State.[289]

Accordingly, *effective control*, as articulated in Nicaragua, means that the State must have either "directed or enforced" the specific unlawful operations.[290] In the *Tadic* case, *the International Criminal Tribunal for the Former Yugoslavia* (ICTY) adopted the *overall control* standard, which is more tolerant and provides that a state can be responsible for an operation conducted by a certain group (or individual), which was endorsed by a state.[291]

The *effective control* test is problematic when applied to cyberspace due to the high level of proof that is unlikely to be achieved given the difficult task

---

285. Military and Paramilitary Activities In and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep 14, ¶ 202 (June 27).

286. Gervais, *supra* note 104, at 44; Schmitt, *supra* note 281, at 157-58.

287. Shackelford & Andres, *supra* note 278, at 986 (citing *Nicar. v. U.S.*, 1986 I.C.J. at ¶ 110); Antonio Cassese, *The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 EUR. J. INT. L. 649, 650 (2007) (citing Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Montenegro), Judgment, 2007 I.C.J. 43, ¶ 386-94 (Feb. 26)).

288. Shackelford & Andres, *supra* note 278, at 975.

289. *Nicar. v. U.S.,* 1986 I.C.J. at ¶ 115.

290. *Id.*

291. Shackelford & Andres, *supra* note 278, at 975, 986-87 (citing Prosecutor v. Tadíc, Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (Int'l Crim. Trib. for the Former Yugoslavia, Oct. 2, 1995)).

of identifying the origin of a cyber operation.[292] Further, even the tolerant *overall control* standard has been criticized as unrealistic when it comes to the attribution of cyber operations.[293] This is because attributing a cyber operation to a certain state depends on the ability to prove the extent of the involvement of a state, such as if a state "direct[ed] private individuals or groups to conduct the operations."[294] This kind of proof is also hard to achieve as cyber operations can be carried out by non-state actors without expending a large amount of funds and with different technology than States.[295] Thus, attributing an action of a non-state actor to a state might be very difficult.[296] Michael Schmitt and Liis Vihul point out that it is still unknown whether the Russian Federation was in some way involved in the "2007 cyber operations" against Estonia that were partially conducted by a hacking group named the Nashi youth.[297]

The Tallinn Group noted that, "[i]nternational law regulates cyber operations by non-State actors [that are not attributed to a State] only in limited cases."(Rule 33).[298] First, it applies Article 11 of *the Articles of State Responsibility*, providing that a state is allowed to acknowledge a cyber operation conducted by a non-state actor as its own conduct.[299] The Tallinn Group further stated that "cyber operations conducted by non-State actors that are not attributable to States" cannot breach international law rules, such as the principles of sovereignty and non-intervention and cannot be considered as use of force. Also, states are not permitted to use countermeasures as a result of such operations.[300] Yet, cyber operations carried out by non-state actors on a "territory" of a state, but not stopped by that state, would be a violation of due diligence.[301] Also, under some circumstances, the law of self-defence [302] and LOAC may control cyber operations carried out by non-state actors.[303]

To summarize, there are both technical and legal hurdles when attributing cyber operations to states.[304] The technical problems relate to the

---

292. Shackelford & Andres, *supra* note 278, at 987; *see also* Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility*, MELBOURNE J. INT'L L. 496, 514, 418-19 (2013).

293. Margulies, *supra* note 292, at 514, 518-19.

294. Schmitt, *supra* note 281, at 158.

295. Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyber Space: The Evolving International Law of Attribution*, 1 FLETCHER SEC. REV. 55, 56 (2014).

296. *Id.*

297. *Id.*

298. Schmitt, *supra* note 97, at 174.

299. *Id.* at 99.

300. *Id.* at 175.

301. *Id.*

302. Schmitt, *supra* note 97, at 175.

303. *Id.* at 175-76, 373.

304. Finlay & Payne, *supra* note 58, at 203.

ability to gather the necessary data, as usually the origin of the operation is unknown.[305] The legal challenge is that even when information becomes available, the legal standards of control that have been applied successfully to traditional attacks are not appropriate to cyber operations given the technical challenges.[306] The problem of attributing cyber operations to States will remain unsettled as long as states will be silent and reluctant to disclose their actions.[307] Further, we can also find evidence of legal cynicism in the application of the standards of attribution, as will be discussed below.[308]

H. Summary

Using Schmitt's article as a starting point, this section identified eight core grey zones concerning the applicability of international law to cyber operations: sovereignty, non-intervention, use of force, self-defence, the law of armed conflict (LOAC), countermeasures, due diligence, and attribution. Under each of these grey zones there are several issues and questions which remained unresolved among scholars, experts, and States. With regards to sovereignty and non-intervention, Michael Schmitt poses the question as to whether something like the "implantation of malware," resulting in no physical damage, breaches the principle of sovereignty.[309] This section also analysed whether cyber operations carried out by non-state actors can breach the principle of sovereignty.[310] The last question involves determining which parameters to use when qualifying a cyber operation as "coercive" when assessing a potential violation of the principle of non-intervention.[311]

With regards to use of force, there is no consensus of whether a cyber operation qualifies as a use of force if it does not result in physical damage.[312] Under the grey zone of self-defence there were five unsettled issues as summarized by Schmitt regarding regulating cyberwarfare. First, there is no consensus as to the threshold of destruction that needs to be reached in order to qualify a cyber operation as an armed attack, thus allowing a state to act in self-defence.[313] Second, it is not clear if a "series of cyber incidents that fall below the threshold of an armed attack" permit a state to act in self-

305. *Id.*
306. *Id.* at 204; Efrony & Shany, *supra* note 136, at 636.
307. Efrony & Shany, *supra* note 136, at 636.
308. *See* Part V, below.
309. Schmitt, *supra* note 4, at 275.
310. Schmitt, *supra* note 20, at 18.
311. Schmitt, *supra* note 14, at 8.
312. Efrony & Shany, *supra* note 136, at 590.
313. Schmitt, *supra* note 20, at 56.

defence.[314] The third unsettled issue is whether cyber operations that are conducted independently by non-state actors are thus armed attacks which would justify a state acting in self-defence.[315] Another unsettled issue concerns actions that do not cause "injury, death, damage or destruction" but result in "negative effects."[316] The last question, which relates to the issue of "reasonably foreseeable consequences," is if the perpetrator's intent in regard to the outcome of a cyber operation matters.[317]

Under the grey zone of LOAC, there were four questions provided by Ayalew and Diamond, deriving from the application of the principles of distinction, proportionality and precaution. The first question is whether it is legal to target hackers who are civilians participating in the conflict (distinction).[318] The second question is whether "loss of functionality" is also included in the definition of "damage" when speaking about the resulting harm of a cyber operation (proportionality).[319] The proportionality analyses also encompasses whether any "incidental damage" to civilians might be caused even if there is a "military advantage" from the operation.[320] The last question involves which precautions to take while conducting cyber operations as required by LOAC.[321]

With regards to countermeasures, Schmitt raises the question as to whether it is possible to apply the requirement of notification under countermeasures to cyber operations.[322]

The due diligence principle has generated two main questions discussed in the literature. First, Efrony and Shany discuss the question of how the victim state can provide proof of the absence of due diligence of another state if the former refuses to disclose its identity;[323] and the second, raised by Schmitt, is whether the due diligence principle applies merely to states in which the cyber operations originated or whether it also includes "transit States."[324] Finally, this Article, examining work by Lorraine Finlay and Christian Payne, recognizes technical and legal problems relating to state responsibility and attribution in the field of cyberspace.[325]

Supporting the argument among scholars that these unsettled issues need to be resolved in order to advance the creation of an international

314. *Id.* at 55, 56.
315. *Id.* at 58, 59.
316. *Id.* at 56.
317. *Id.* at 57.
318. Ayalew, *supra* note 41, at 221.
319. Diamond, *supra* note 205, at 79.
320. *Id.* at 79.
321. *Id.* at 79-80.
322. Schmitt, *supra* note 251, at 717.
323. Efrony & Shany, *supra* note 136, at 644–45.
324. Schmitt, *supra* note 14, at 12-13.
325. Finlay & Payne, *supra* note 58, at 203.

cyber warfare regime,[326] the next section will show why it is so important to resolve these issues and to define the current ambiguous legal situation of cyberspace in general.

IV. LEGAL CYNICISM AND CYBERSPACE

It seems that the application of international law to real-world situations involves some subjective elements.[327] However, Shiri Krebs reflects on current scholarship when arguing that "beyond this inescapable subjectivity, international law is tainted by a degree of legal cynicism."[328] Several definitions of legal cynicism have been proposed in the literature.[329] Emily Ryo recites one definition by Robert Sampson and Dawn Bartusch, who state that it is "'a state of normlessness in which the rules of the dominant society [and hence the legal system]… are no longer binding in a community.'"[330] Ryo also puts forth an argument by David Kirk and Andrew Papachristos, who argue that legal cynicism refers to "a cultural orientation in which the law and the agents of its enforcement [such as the police and courts]…are viewed as illegitimate, unresponsive, and ill equipped to ensure public safety."[331] Ryo comes to the conclusion that these definitions all agree on a central premise that "legal cynicism relates to fundamental distrust 'in the basic intention of the laws' and legal authorities."[332] Sometimes, "legal cynicism" can result in international law – and LOAC particularly – bearing the weight of "perceptions of illegitimacy" of the law.[333] In areas where LOAC is ambiguous and unclear, its norms can be considered as worthless, as they can be interpreted in a variety of ways.[334] This "illegitimacy weakens the legal authority of international law and its potential to guide behaviour during armed conflicts."[335] For example, the gaps and unsettled issues described throughout this Article can contribute to the legal cynicism in the emerging cyber warfare regime, and hence trigger distrust in its legal validity. Additionally, the lack of "enforcement" and

326. *See, e.g.*, Schmitt, *supra* note 14, at 3, 20; Kilovaty *supra* note 1, at 108-09; Stephen Moore, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C. J. INT'L L. & COM. REG. 223, 241 (2013).

327. Krebs, *supra* note 18, at 237.

328. *Id.*

329. Emily Ryo, *Fostering Legal Cynicism through Immigration Detention*, 90 S. CAL. L. REV. 999, 1015 (2017).

330. *Id.* (citing Robert J. Sampson & Dawn Jeglum Bartusch, *Legal Cynicism and (Subcultural?) Tolerance of Deviance: The Neighborhood Context of Racial Differences*, 32 L. & SOC'Y REV. 777, 782 (1998)).

331. Ryo, *supra* note 329, at 1015 (citing David S. Kirk and Andrew V. Papachristos, *Cultural Mechanisms and the Persistence of Neighborhood Violence*, 116 AM. J. SOCIO. 1190, 1191 (2011)).

332. Ryo, *supra* note 329, at 1015.

333. Krebs, *supra* note 18, at 236.

334. *Id.* at 238.

335. *Id.* at 238.

"supreme judicial authority" leads to divergence in the application of LOAC norms to specific cases and to unresolved legal disputes.[336]

Another aspect of legal cynicism is the servitude to powerful states' interests and agendas.[337] For example, Jochen von Bernstorff argues that there has been a recurring trend in the development of LOAC to prohibit weapons during "future armed conflicts" that have lost their relevance and effectiveness.[338] Bernstorff also posits the example of suspending the use of weapons that "are not yet ready to be used for military purposes" or weapons that are no longer effective to use in warfare because of other military innovations.[339] Despite the fact that such restrictions have no appreciable humanitarian effects, powerful states may present them as a significant achievement.[340] In contrast, relevant weapons, such as those used for cyber operations, would have no restrictions imposed on them or only the governments that are unable to use them would limit them (similar to the nuclear weapons regime).[341]

To demonstrate this legal cynicism when adapting international law to cyberspace, this section focuses on the grey zone of *use of force* under *jus ad bellum*.[342] First, it is important to examine the legal perspectives of Israel, the United States, Australia, the Netherlands and France concerning the applicability of *use of force* to cyber operations.[343] The analysis of the positions of these states demonstrates two significant aspects of legal cynicism: (i) a degree of uncertainty concerning the legal rules, based on different interpretations of relevant countries in their application of the legal rules;[344] and (ii) expressions of legal interpretations that are consistent with, and reflecting of, states' political and military interests.[345]

---

336. *Id.*

337. *Id.* at 239, 253; Jochen von Bernstorff, *Is IHL a Sham? A Reply to Eyal Benvenisti and Doreen Lustig*, 31 EUR. J. INT'L L. 709, 715 (2020).

338. Bernstorff, *supra* note 337, at 715.

339. *Id.*

340. *Id.*

341. *Id.*

342. Schmitt, *supra* note 133, at 570.

343. Michael Schmitt, *The Defense Department's Measured Take on International Law in Cyberspace*, JUST SEC. (Mar. 11, 2020), https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/ (last visited Mar. 4, 2023) (citing French Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (2019), https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf; Government of the Netherlands, *Appendix: International law in cyberspace* (2019)); Roy Schondorf, *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, EJIL TALK! BLOG OF THE EUR. J. INT'L L. (Dec. 9, 2020), https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/.

344. Krebs, *supra* note 18, at 238.

345. Krebs, *supra* note 18, at 253; Bernstorff, *supra* note 337, at 715.

For the purpose of this Article, one relevant question, as examined by Michael Schmitt, within these positions is "[w]hen does a cyber operation constitute a wrongful 'use of force' in violation of Article 2(4) of the United Nations charter and customary international law?"[346] States disagree on this topic. While France and the Netherlands determined that "a use of force need not be destructive or injurious,"[347] the US, Israel, and Australia share the view that a cyber operation can be considered as use of force only if it results in physical harm.[348] This suggests cyber-capable countries, such as the United States, Israel and Australia, find that only the most serious cyber incidents – which rarely occur in practice – are uses of force and legitimize less serious cyber incidents, whose damage is not physical (which are much more common). This can be analysed as a cynical use of international law.

Further, these conflicting views strengthen the cynical perception of international law, as each state or international actor can legitimately interpret the law according to their national needs and interests. This flexibility of the legal rules turns international law into a tool that justifies states' actions, rather than providing clear guidance to states' behaviour.[349]

Second, the example of the Stuxnet cyber operation is useful in this context. Applying the "use of force" position of the US, Israel, and Australia, articulated above, this operation should have been classified as a clear incident of "use of force" considering the significant physical destruction caused to the nuclear centrifuges at Natanz.[350] In particular, as analysed by Andrew C. Foltz, the application of Schmitt's seven criteria[351] to the Stuxnet incident shows that "the worm was highly invasive, [and] caused direct and measurable physical damage."[352] Further, the Tallinn Group unanimously determined that Stuxnet should be considered as "use

346. Schmitt, *supra* note 133, at 570.

347. Schmitt, *supra* note 343 (citing French Ministry of the Armies, *International Law Applied to Operations in Cyberspace* (2019), https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf; Government of the Netherlands, *Appendix: International law in cyberspace* (2019)).

348. Schmitt, *supra* note 343 (citing Paul C. Ney Jr., General Counsel, Dept. of Defense, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, (Mar. 29, 2020)); Roy Schondorf, *Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operation*s, EJIL TALK! BLOG OF THE EUR. J. INT'L L., https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/(Dec. 9, 2020); AUSTRALIAN IMPLEMENTATION OF NORMS OF RESPONSIBLE STATE BEHAVIOUR IN CYBERSPACE (Australia's International Cyber Engagement Strategy 2020).

349. Krebs, *supra* note 18, at 235, 253.

350. *See, e.g.*, Andrew C. Foltz, *Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate*, 67 JOINT FORCE Q. 40, 45 (2012); Qureshi, *supra* note 6, at 22-23; Buchan, *supra* note 51, at 214; Ryan Jenkins, *Is Stuxnet Physical? Does It Matter?*, 12 J. MIL ETHICS 68 (2013).

351. Schmitt, *supra* note 133, at 575-77, 578; Foltz, *supra* note 310, at 42-43. The criteria that Schmitt lays out can help to determine if a cyber operation was a use of force despite a lack of physical damage; *See supra* note 130 and accompanying text.

352. Foltz, *supra* note 350, at 45.

of force."[353] Thus, when using these criteria to analyse the Stuxnet incident and considering the positions of states regarding use of force, it should have been expected that states – in particular those proposing "physical damage" as the main attribute of a cyberattack – would conclude that this operation crosses the level of use of force and violates "Article 2(4) of the UN Charter."[354] However, in practice, even after more than 10 years since that incident, states are disinclined to classify the Stuxnet attack as illegal use of force;[355] there is a complete silence regarding this issue as no state has condemned or supported this operation. Moreover, Iran's silence on the issue has also had an impact on states and the international community that ignored this core legal question.[356] This silence is highly significant, especially when comparing this operation to other international attacks which were directly condemned by the international community. For example, a recent physical attack by Iran on an Israeli ship, where two of the crew members were murdered, was severely condemned by the "G-7 Foreign Ministers," including "Canada, France, Germany, Italy, Japan, the United Kingdom and the United States" as well as by the European Union who condemned this attack a few days after it had happened.[357] As already shown above, a few States, including Israel and the United States (who were allegedly responsible for the Stuxnet operation),[358] share the "view that a cyber operation can amount to use of force if it is expected to cause physical damage, injury or death."[359] Especially since Harold Koh[360] remarked that "[c]yber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force" and added the example of "operations that trigger a nuclear plant meltdown."[361] This position is clearly inconsistent with the actions in the Stuxnet attack in which there was use of cyber capabilities to cause the very same damage. The failure of the international community to condemn the Stuxnet attack as a breach of

353. Schmitt, *supra* note 20, at 45.

354. Foltz, *supra* note 350, at 42-43, 47.

355. *Id.* at 47.

356. *Id.*

357. *Tanker attack: UK and US blame Iran for deadly ship attack*, BBC (Aug. 2, 2021), https://www.bbc.com/news/world-middle-east-58048007; *MV Mercer Street Attack: G7 Foreign Ministers' Statement*, EUROPEAN UNION EXTERNAL ACTION (Aug. 6, 2021), https://eeas.europa.eu/headquarters/headquarters-homepage_en/102860/MV%20Mercer%20Street%20attack:%20G7%20Foreign%20Ministers%27%20statement ("We condemn the unlawful attack committed on a merchant vessel off the coast of Oman on 29 July [2021], which killed a British and a Romanian national. This was a deliberate and targeted attack, and a clear violation of international law. All available evidence clearly points to Iran. There is no justification for this attack.").

358. Qureshi, *supra* note 6, at 2, 13, 22; Kilovaty, *supra* note 1, at 91.

359. Schondorf, *supra* note 343; Ney, *supra* note 348.

360. Legal advisor of the U.S. Dept. of State; Koh, *supra* note 108, at 1.

361. Harold Hongju Koh, Remarks at USCYBERCOM Inter-Agency Legal Conference (Sept. 18, 2012), https://2009-2017.state.gov/s/l/releases/remarks/197924.htm.

international law colors it in cynical elements. This example strengthens the claim that much like legal cynicism in domestic contexts, international "'law and the agents of its enforcement…are viewed as illegitimate, unresponsive, and ill equipped to ensure public safety.'"[362]

Finally, the issue of "use of force" also demonstrates how legal uncertainties can affect analysis of cyber cases, especially in borderline incidents, which do not constitute a clear case of "use of force" such as Stuxnet.[363] For example, the 2007 cyber operations against Estonia can show how multi-interpretation of one case can render the law cynical and even irrelevant as any state can rely on different interpretation to justify its actions.[364] While Michael Schmitt argues that the operations against Estonia "reached the use-of-force threshold" because they were severe and highly invasive, they had direct consequences which were difficult to quantify, there was immediate disruption, and the operation was not necessarily legitimate under international law,[365] others argue that these operations cannot be qualified as a "use of force" violating Article 2(4) of the UN Charter.[366] According to these commentators, like Reese Nguyen, these operations were not serious, took place without any physical invasion, their effects were not immediate, their "effects were indirect," and they were assumed to be legal under international law due to the fact that they "merely interrupted communications systems."[367] Also, there was no physical destruction done to Estonia's infrastructure.[368] Moreover, Russell Buchan argued that these operations violated Estonia's sovereignty and thus constitute an unlawful intervention, rather than use of force.[369] These conflicting viewpoints and various analyses of the same cyber operation emphasize the weakness of these criteria and show how readily they may be altered to serve the interests of different states.[370] Such criteria should be solid and not open for multi-interpretations. For example, whether a certain operation causes physical damage should not be arguable and subject to disagreements. The Estonia case is only one example of the legal uncertainties and disagreements which render international law a tool to justify – rather than guide – behaviour. Also, the fact that scholars and experts have come to opposite conclusions regarding the same case

362. Ryo, *supra* note 329, at 1015 (citing David S. Kirk and Andrew V. Papachristos, *Cultural Mechanisms and the Persistence of Neighborhood Violence*, 116 AM. J. SOCIO. 1190, 1191 (2011)).

363. Schmitt, *supra* note 20, at 45.

364. Nguyen, *supra* note 140, at 1124.

365. Schmitt, *supra* note 133, at 577.

366. Nguyen, *supra* note 140, at 1123-4; Buchan, *supra* note 51, at 219.

367. *Id.* at 1123-24 (citing U.N. Charter art. 41).

368. *Id.* at 1123; Buchan, *supra* note 51, at 219.

369. Buchan, *supra* note 51, at 226.

370. Nguyen, *supra* note 140, at 1124.

illustrates the ambiguity of international law and constructs it as non-juridical and cynical.

In summary, legal grey zones relating to cyber warfare intensify elements of legal cynicism in the law of armed conflict in several ways. First, conflicting interpretations and uncertainty about the legal rules allow states to behave according to their national strategies and interests and use international law to justify their actions.[371] Second, the weak enforcement mechanism characterizing international law enables states to act inconsistently with their own positions.[372] Finally, as long as the grey zones of cyberspace detailed above remain open and unclarified, states may continue to harness international law to their political agenda and security policies; they may prohibit, limit, or delegitimise actions or methods that they identify as less useful or necessary for their national interests and vice versa.[373]

In addition, it is important to discuss the grey zone of attribution as another aspect of cynicism; even when there is information available linking states to cyber operations, the high legal standard of control is used cynically to prevent attribution and shield states from responsibility.[374] Hence, the legal cynicism in cyberspace is derived from both uncertainties about facts and uncertainties about the actors conducting the operations (attribution). This legal cynicism harms the legitimacy of international law and hinders the development of an efficient legal regime regulating cyber warfare.

CONCLUSION

Despite many efforts, there is still no specialized, binding international regime tailored specifically for the unique challenges of cyber warfare.[375] Due to the constituent elements of cyberspace detailed above, applying existing international norms to cyber operations generates many unresolved grey zones.[376] While LOAC generally applies to cyber operations, during or outside armed conflict,[377] the existing uncertainties require clarification, either by the development of customary international law or by a specialized international convention or treaty designed to regulate cyber warfare.[378] This

371. Krebs, *supra* note 18, at 238, 253.

372. Ryo, *supra* note 329, at 1015.

373. Krebs, *supra* note 18, at 253; Bernstorff, *supra* note 337, at 715.

374. Schmitt and Vihul, *supra* note 295, at 56, 72.

375. Hathaway et al., *supra* note 4, at 821.

376. Schmitt, *supra* note 14, at 4-19.

377. *See, e.g.*, Schmitt, *supra* note 20; Kodar, *supra* note 45; Nyabuto, *supra* note 110; Voitasec, *supra* note 110; Döge, *supra* note 56; Ayalew, *supra* note 41; Brown, *supra* note 40; Droege, *supra* note 221.

378. *See, e.g.*, Hathaway et al., *supra* note 4, at 885; Epstein, *supra* note 114, at 299; Ayalew, *supra* note 41, at 221-22; Gary Brown & Keira Poellet, *The Customary International Law of Cyberspace*, 6 STRATEGIC STUD. Q. 126 (2012).

clarification is important not only because it might prevent confusion concerning the applicable rules and contribute to "deterrence in cyberspace" and to international stability,[379] but mainly because the very existence of such grey zones adds to the existing wave of cynicism and backlash against international law.[380] The solution to this problem is to identify the way to mitigate grey zones. Possible pathways to do so are to empirically examine states' positions concerning each of the identified grey zones, or to identify emerging agreements among states, which could lead to meaningful progresses in the development of the international law of cyber warfare.[381]

379. Schmitt, *supra* note 14, at 21.

380. Krebs, *supra* note 18, at 235.

381. In a separate article, I collect state positions on these grey zones, creating a dataset that identifies emerging agreements on the application of specific international law norms to cyber operations.

* * *