The Law of Cyber Warfare: Restrictions, Opportunities and Loopholes

Nicholas Tsagourias*

Abstract

The article considers the applicability of existing international rules on the use of force to cyber attacks and assesses their effectiveness. The author's conclusion is that the current regime on the use of force fails to capture the particularities of cyber attacks and for this reason he makes some tentative proposals for enhancing security in this area.

I. INTRODUCTION

It is quite trite to say that cyberspace offers many opportunities to individuals, businesses, and states but it is also a source of significant threats.[1] The interconnected and indivisible nature of networks, the mobility and speed of cyber activities, the anonymity cyberspace affords, the low technical barriers and costs of entry, all these mean that states and non-state actors (individuals, groups, companies) can use cyberspace for malicious purposes as well. The most important threats arising in and from cyberspace are cyber terrorism, cyber espionage, cybercrime and war-like cyber attacks.[2] The latter are attacks against an adversary's physical or cyber infrastructure by using cyber tools and perpetrated through or in cyberspace.

As the United Nations Group of Governmental Experts recognized, cyber threats are "among the most serious challenges of the twenty-first century".[3] The importance placed by states in countering such threats is demonstrated by the fact that by 2013, 114 states had adopted national cyber security strategies with 47 states adopting cyber security strategies that give some role to the armed forces whereas 67 states have solely civilian strategies.[4]

---

* Professor of International Law, University of Sheffield (Nicholas.Tsagourias@Sheffield.ac.uk).

1 James R. Clapper, United States Office of the Director of National Intelligence, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Select Committee on Intelligence" (12 March 2013).

2 See e.g. Canada, Minister of Public Safety, "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada" (2010), online: < www.publicsafety.gc.ca >; United Kingdom, "The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world" (2011), online: < www.gov.uk >; United States, White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World" (2011), online: < obamawhitehouse.archives.gov >.

3 GA, 65th Sess., Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/65/201 (30 July 2010) at 6.

The immediate question is whether international law applies to cyberspace and in particular to military-like cyber attacks. Although in the early days of the internet it was claimed that cyberspace is not subject to legal regulation,[5] it is broadly accepted nowadays that international law applies to cyberspace and to cyber activities and, indeed, that the international law regime regulating the use of force applies to military-like cyber attacks.[6] The two main components of this regime are, first, the prohibition of the use of force and, secondly, the sanctioning of the defensive use of force in response to an armed attack. It should be noted that the use of force regime is an admixture of UN Charter law and of customary law.

In sections II to IV of this paper, I will consider the extent to which these rules apply to cyber attacks, whether new interpretations are needed, and whether there are gaps in legal regulation whereas in section V, I suggest alternative methods of enhancing security in cyberspace.

II. CYBER ATTACKS AND THE PROHIBITION OF THE USE OF FORCE (ARTICLE 2(4) OF THE UN CHARTER)

According to Article 2(4) of the UN Charte, states should not use force in their international relations against the territorial integrity, or political independence of other states or in any other manner inconsistent with the UN

---

4 UNIDIR, "The Cyber Index: International Security Trends and Realities", UNIDIR/2013/3 (2013).

5 John Perry Barlow, "A Declaration of Independence for Cyberspace", *Electronic Frontier Foundation* (8 February 1996), online: < projects.eff.org/~barlow/Declaration-Final.html > .

6 GA, 68th Sess., Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (24 June 2013) at para. 19: "International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment"; GA, 70th Sess., Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (22 July 2015) at paras 24-29. The Report mentions certain principles of the UN Charter and international law that apply to cyberspace and cyber activities such as the sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining 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; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States; White House, *supra* note 2; Harold Hongju Koh, "International Law in Cyberspace" (Remarks delivered at the USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD, 18 September 2012), (2012) 54 Harv Intl LJ; *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law and Cyberspace* (Cheltenham: Elgar, 2015).

Charter. The prohibition of the use of force is not only a Charter rule but also a rule of customary law.

The extent to which this article applies to cyber attacks depends on whether cyber attacks come under this Article's definitional thresholds.[7] The first question is whether a cyber attack can be a use of force. For example, is the manipulation of data or the destruction of data in a hospital's computer system a cyber use of force? The answer may differ depending on how force is defined; is it defined by the instrument used or by the consequences it produces irrespective of instrument? By instrument is meant by a weapon and indeed a military weapon but cyber weapons such as viruses and worms are not military weapons. By consequences is meant by the physical consequences of the action in the form of material destruction or loss of life. Applying these two interpretative lines to the example given above, if the manipulation causes damage to medical equipment or human loss because medical care cannot be provided, it will constitute a use of force according to the consequences-based approach but not according to the instrument-based approach.

The different legal implications of these approaches can be graphically demonstrated by the 2007 denial of services attacks (DDoS) on Estonia[8] and the 2010 Stuxnet attack on the Iranian nuclear reactors.[9]

In Estonia, governmental and banking sites were taken offline for a period lasting nearly three weeks following the denial of service attacks. The attacks would not, however, amount to a use of force according to the instrument-based or the consequences-based interpretation of force because no armed force was used and no physical destruction was caused.

Regarding the Stuxnet attack, centrifuges were damaged because of the change in rotation speed caused by the Stuxnet virus and, according to reports by the International Atomic Energy Association (IAEA), up to 1,000 centrifuges were replaced at the time that Stuxnet would have been in operation. The Stuxnet attack would thus amount to a use of force and a violation of Article 2(4) according to the consequences-based approach but not if the instrument-based approach is adopted.

At this juncture it should be noted that unless one takes a very formalistic view of Article 2(4), the differences between the instrument-based and the consequences-based approach are not irreparable since a weapon is something that causes harm or damage. In any case, the consequences-based approach is

---

7 For a general exposition, see Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014); Matthew C. Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)" (2011) 36 Yale J Intl L 421.

8 Eneken Tikk, Kadri Kaska & Liis Vihul, "International Cyber Incidents: Legal Considerations", Cooperative Cyber Defence Centre of Excellence (2010) at 14-35, online: < www.ccdcoe.org > .

9 Katharina Ziolkowski, "Stuxnet-Legal Considerations", Cooperative Cyber Defence Centre of Excellence (2010), online: < www.ccdcoe.org > .

currently broadly accepted.[10] As Harold Koh, former Legal Adviser of the US State Department, stated:

> In analyzing whether a cyber operation would constitute a use of force, most commentators focus on whether the direct physical injury and property damage resulting from the cyber event looks like that which would be considered a use of force if produced by kinetic weapons. Cyber activities that proximately result in death, injury, or significant destruction would likely be viewed as a use of force.[11]

Even if the consequences-based approach is widely accepted in the cyber context,[12] there are still questions that require further consideration. One such question concerns the consequences that should be taken into account when qualifying an attack as a use of force. Cyber attacks cause first, second and third order consequences and, furthermore, certain consequences are not immediately identifiable or quantifiable. In the example given above, the first order consequences are those affecting the computer system, for example the destruction of data; the second order consequences are perhaps the effects on medical equipment; and the third order effects are the deaths of those connected to that equipment. Another example is an attack on the Stock Exchange network which causes huge economic losses but also triggers an economic downturn which leads to human loss and property destruction because of riots, hunger or lack of medical care. Which of these consequences should be taken into account when assessing the nature of the attack? This raises questions of causality.[13] In the case of physical force, there is almost immediate and direct causation but in the case of cyber attacks there is a long line of causal effects. Moreover, the intention of the attacker is to cause the second and the third order effects than the first order effects which relate to the system. If a threshold of remote causality is adopted, the link between the attack and the produced consequences will fade away and there is a danger that less serious attacks with less serious immediate consequences may become serious by piling up consequences. For this reason, it is submitted here that in order to determine which consequences matter for Article 2(4) purposes, one needs to take into consideration the intention of the attacker and the consequences that are closely linked to the attack and are not the result of any intervening factor.

If the attacked state contributes through actions or negligence to the consequences, would that break the chain of causation or reduce the seriousness of the consequences? For example, would an attack on a state that failed to keep

---

[10] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, [1996] IJC Rep 226 at para. 39.

[11] See Harold Hongju Koh, *supra* note 6.

[12] *Tallinn Manual*, *supra* note 6, Rule 11.

[13] Jens David Ohlin, "Cyber-Causation" in Jens David Ohlin, Claire Finkelstein, and Kevin Govern, eds., *Cyber War Law and Ethics for Virtual Conflicts* (Oxford: Oxford University Press, 2015).

its network safe or to back-up critical services constitute a use of force on the basis of the consequences it causes which could have been prevented? As with physical force, the state's possible contribution is irrelevant in the qualification of the action as a use of force but will be taken into account in the calculation of reparations.

Another question is whether cyber attacks that produce no physical damage or human loss can constitute uses of force. The novelty of cyber weapons is that they may not produce any tangible and violent damage but they may cause significant disruption to a system or paralyze a system. This is particularly threatening when it involves critical state infrastructure such as defence, government, electricity, emergency services or transport, among others. Although views as to whether such a cyber attack should constitute a use of force differ, it is the author's view that cyber attacks that cause substantial disruption or cyber attacks that paralyze a system should be included in the prohibition of the use of force. This is because even if there is no destruction, the operability and the function of the system are removed and that affects a critical state function. Whether the denial of services attacks on Estonia in 2007 will amount to a use of force under this construction is debated. They caused disruption but was the disruption grave? This relates to another interpretative problem with Article 2(4) namely, whether a use of force needs to reach a certain threshold. Views are again divided. There are those who maintain that any use of force regardless of gravity is prohibited, whereas others opine that only the use of force of certain gravity is prohibited by Article 2(4). The former aspire to a total ban on the use of force whereas the latter accept that insignificant uses of force should not aggravate a situation. If disruption is accepted as constituting a use of force, then any disruption, even a minimal one, would constitute a use of force and consequently the disruption caused to Estonia is a use of force. To any reasonable person this would appear an exaggeration in view of the political and legal implications that such a qualification may produce and in view of the ease with which disruption can be caused. It is for this reason that in the opinion of the present author Article 2(4) should require a certain threshold of force even if that threshold cannot be quantified.

Should cyber attacks be categorized as uses of force also on the basis of the intent of the attacker? Intent is a subjective element and the law on the use of force dismissed intent because of difficulties in identifying and assessing a state's intent. Instead, it grounded the prohibition of the use of force on objective facts. However, intent might play a certain role in the cyber context because of the indistinguishable, intangible and transient nature of cyber operations. I have already mentioned the role it can play in establishing the causal link between action and effects. Intent is also important in distinguishing between different cyber operations because the techniques and tools used are often similar. For example, it is not always evident at first sight whether the emplacement of a virus on a system is for reconnaissance, spying, or for attack. Cyber operations may fall over a wide spectrum but, in order to establish what they are, they need to be

analyzed. Technical analysis may reveal the intention of the attacker but identifying the intention of the attacker is also a matter of information and intelligence analysis and, finally, a political determination. This reveals that intent is important but not easy to decipher.

Finally, the presence of non-state actors in cyberspace and their ability and willingness to attack not only individuals and businesses but also states presents a serious challenge to the use of force regime. This regime, but also international law, is state-centred. Article 2(4) of the UN Charter for example prohibits the use of force between states but not by non-state actors. Furthermore, although states have a due diligence obligation not to allow non-state actors to use force from their territory,[14] this is not an obligation of result that can abolish such uses of force. As a result, powerful non-state actors can attack states without violating any rule and, moreover, they can be legally protected from external action by international rules protecting the sovereignty of the state on whose territory they reside. It is true that the challenges posed by non-state actors to international law and to international peace and security are not confined to cyberspace as the case of terrorism shows but in cyberspace the problem is further aggravated by the proliferation of non-state actors due to the low entry and cost barriers that exist in cyberspace. How international law currently deals with non-state actors will be considered later but serious consideration should be given to proposals advocating the application of the prohibition of the use of force to organized non-state actors. Otherwise, the aim behind this rule which is to maintain international peace and security will be undermined.

III. CYBER ATTACKS AND SELF-DEFENCE

The second component of the use of force regime is that it permits the use of force by way of self defence against an armed attack. The self-defence norm is contained in Article 51 of the UN Charter and in customary law and applies equally to cyber attacks.[15] The immediate question is whether a cyber attack can be an armed attack for self-defence purposes. As the ICJ opined, an armed attack is a grave use of force in terms of scale and effects.[16] It follows then that only cyber attacks that produce serious physical damage or human loss will constitute armed attacks and trigger the right to self-defence. If the view that disruption can amount to a use of force is accepted, then grave cyber disruption or the paralysis of a state's network will equally constitute an armed attack.[17]

---

[14] UN Doc. A/70/174, *supra* note 6 at para. 28.

[15] *Tallinn Manual*, *supra* note 6, Rule 13.

[16] *Case Concerning Military and Paramilitary Activities in and against Nicaragua*, [1986] ICJ Rep 14 at paras 191-195 [''*Nicaragua Case*'']; *Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America)*, [2003] ICJ Rep 161 at para. 51; *Armed Activities on the Territory of the Congo* (*DRC v Uganda*), [2005] ICJ Rep 53; *Tallinn Manual*, *supra* note 6, Rule 13.

[17] Walter Gary Sharp, Sr., *Cyberspace and the Use of Force*, (Huntsville: Aegis Research

Even if gravity as a definitional element of an armed attack is well-established, still it gives rise to interpretative difficulties. For example, whereas the Court spoke of the scale and effects of the attack, cyber attacks may produce significant effects but have insignificant scale. Compare for example the "shock and awe" attacks on Iraq in 1991 and in 2003 with the destruction of data or the manipulation of a code. Even more critically, the Court did not identify the requisite threshold of gravity and no criteria were given to distinguish grave from less grave uses of force. For example, was the destruction of 1,000 centrifuges grave as for the Stuxnet attack to amount to an armed attack? If there is a spectrum of gravity — from a use of force to an armed attack — it is difficult to decide where the destruction of 1,000 centrifuges is placed. Of course, as was said above, other consequences should also be taken into account but, is the fact that the Stuxnet attack delayed Iran's nuclear programme by four years a consequence that adds to the gravity of the attack?[18]

Secondly, what happens when a state falls victim to a less grave (low-intensity) cyber attack or to a series of low intensity cyber attacks? This is a quite realistic scenario in cyberspace because non-state actors that are rather active in cyberspace may not have the technical know-how and capabilities to launch grave attacks against states.

One way of dealing with this issue is to follow the ICJ which said that states cannot use forcible responses but, instead, they can resort to proportional peaceful countermeasures. [19] However, the disparity between action and reaction in such cases is apparent: a forcible action is encountered by a non-forcible action. This is not fair to states and does not enhance their security. It becomes even more unrealistic when non-state actors are involved. What peaceful countermeasures can the victim state take against non-state actors and how such countermeasures can be effective? It is for this reason that certain states such as the U.S. treat any use of force regardless of gravity as an armed attack triggering the right to self-defence[20] but also arguments were put forward to the effect that in the case of low intensity cyber attacks proportional forcible countermeasures should be permitted. [21]

Corporation, 1999) at 129; Eric Talbot Jensen, "Computer Attacks on Critical State Infrastructure: A Use of Force Invoking the Right of Self-Defence" (2002) 38 Stan J Intl L 207 at 221-229.

[18] For different views on the 2007 Estonian incident and the 2010 Stuxnet attack, see Mary Ellen O'Connell, "'Cyber Security without Cyber War" (2012) 17 J Confl & Sec L187 at 189; Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited" (2011-2012) 56 Vill L Rev 569 at 569-71.

[19] *Nicaragua Case*, *supra* note 16 at para. 249; *Tallinn Manual*, *supra* note 6, Rule 11 at para. 11, Rule 13; ILC, 53rd Sess., Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10 (2001) ["Draft Articles"]; GAOR, 56th Sess., Supp. No. 10 (2001), art. 49(1). Also *Gabíkovo-Nagymaros Project (Hungary/Slovakia)*, [1997] ICJ Rep 7 at paras. 55-56.

[20] See Harold Hongju Koh, *supra* note 6.

The other approach is to qualify a series of low intensity cyber attacks as a cyber armed attack if their cumulative effects reach the requisite threshold of gravity. Indeed, certain states such as Israel adopt this view in relation to terrorist attacks[22] and, although this view is not overwhelmingly supported, it has also been proposed in relation to low intensity cyber attacks for the reasons explained above.[23] Still, the question that can be asked is on what basis will individual attacks become part of the same overall attack and, more specifically, what factual, subjective and circumstantial links are needed?

Another issue that causes legal and political controversy concerns the use of defensive force prior to an actual cyber attack. Because cyber attacks can produce instantaneous consequences, acting in anticipation of an attack is the only credible line of defence left to states.[24] However the critical question is at what point in time can a state act?

Although the legal status of anticipatory self-defence and its place in the post-Charter legal regime on the use of force have been debated by international layers, it is not far from the truth to say that, currently, there is broad consensus that self-defence can be exercised against an imminent attack if the *Caroline* criteria of imminence are satisfied namely, "instant, overwhelming, leaving no choice of means, and no moment for deliberation".[25] For example, if a state has credible information that another state is about to launch a cyber attack or if a cyber attack disables its air defence systems and the state has credible information that a physical attack will immediately follow, it can act in self-defence before the actual attack.

The *Caroline* criteria, however, interpret imminence in temporal terms which does not provide states with sufficient time to defend themselves against cyber attacks because of their instantaneous character. The question thus arises as to whether other factors should be taken into consideration when assessing the imminence of the attack. Indeed, the Chatham principles on the use of force in

---

21 *Case Concerning Oil Platforms (Islamic Republic of Iran v United States of America)*, [2003] IJC Rep 161 at paras. 14–15 (dissenting judgment by Justice Simma) ["*Oil Platforms*"]. Judge Kooijmans is rather noncommittal: *ibid* at paras. 52 and 62. Nicholas Tsagourias, "The Law Applicable to Countermeasures Against Low Intensity Cyber Operations" (2014) 14 Baltic YB Intl L 105.

22 Yoram Dinstein, *War, Aggression and Self-Defence* (Cambridge: Cambridge University Press, 2011) at paras. 547-549; Bruno Simma et al., eds., *The Charter of the United Nations* (Oxford: Oxford University Press, 2012) at 1409; Christopher Greenwood, "Self-Defence" in *Max Planck Encyclopedia of Public International Law* at para. 12, online: < opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e401?rskey = 2i36pK&result = 2&prd = EPIL > .

23 Nicholas Tsagourias, "Cyber Attacks, Self-Defence and the Problem of Attribution" (2012) 17 J Confl & Sec L 229; *Tallinn Manual*, *supra* note 6, Rule 13 at para. 8.

24 *Tallinn Manual*, *supra* note 6, Rule 15.

25 *The Caroline*, (1841) 29 British and Foreign State Papers at paras 1137-1138. *A More Secure Would: Our Shared Responsibility, Report of the High-Level Panel on Threats, Challenges and Change*, UNDPI, 2004, UN Doc A/59/565 at para. 18.

self-defence also include qualitative factors such as the gravity of the expected attack, the capabilities and determination of the attacker, the nature of the threat, the possibility of being warned that an attack is pending and the ability of the victim to defend itself.[26] Others reduce all relevant factors into the criterion of the "last window of opportunity" within which self-defence will be effective.[27]

These factors are not free from difficulties. For example, if gravity is a factor in the construction of imminence, is this different from the gravity needed in order to qualify a use of force as an armed attack? Put differently, is it more gravity, less gravity or equivalent gravity that is needed? Also, how can the gravity of the projected attack be quantified? Concerning the possibility of being warned of an impending attack, how would this apply to clandestine attacks in view of the fact that, in cyberspace, most attacks are clandestine and cyberspace is actually used by attackers because of the anonymity it affords? Assessing the determination of the attacker raises a different type of questions concerning intent and how it can be identified as discussed above. Finally, questions also arise concerning the target of the anticipatory self-defence action. If the anticipated attack is through a virus, what will be the target of the self-defence action?

Another issue relating to anticipatory self-defence concerns its proportionality. Proportionality is a condition in the exercise of self-defence[28] but the question is, against what should the proportionality of anticipatory self-defence be measured? Moreover, because of the interconnectedness of cyberspace, how can the spill over effects of the self-defence action be contained?

That notwithstanding, if imminence is assessed according to these factors, a state will be able to use defensive force well before an armed attack occurs and well beyond the narrow *Caroline* criteria. In this case anticipatory self-defence moves towards prevention which is frowned upon in international law.

IV. NON-STATE ACTORS AND THE USE OF FORCE IN CYBERSPACE

I have already mentioned the challenges that non-state actors pose to the use of force regime and that these challenges are magnified in cyberspace. How international law deals with non-state actors is critical for its credibility and legitimacy and for achieving its aims of maintaining peace and security. If international law continues to ignore non-state actors, a two-tier system will be created; one involving states where international law applies and the other involving non-state actors or states and non-state actors where no law applies. The consequences of this scenario are quite alarming.

---

[26] "The Chatham House Principles of International Law on the Use of Force in Self Defence" (2006) 55 ICLQ 963.

[27] *Tallinn Manual*, *supra* note 6, Rule 15 at para. 4.

[28] *Nicaragua Case*, *supra* note 16 at para. 176; *Oil Platforms*, *supra* note 21 at paras. 51, 73, 76-77; *Tallinn Manual*, *supra* note 6, Rule 15 at para. 5.

In this section I will examine how international law deals with non-state uses of force. As was said above, according to the currently prevailing doctrine, non-state actors are not bound by the rules on the use of force. International law deals with non-state uses of force indirectly, only if they are attributed to a state. Attribution is the mechanism of linking a non-state use of force to a state, triggering the application of the law on the use of force. This means that the use of force becomes a use of force by a state and thus international law maintains its state-centred character. It is not, however, every non-state force that is attributed to a state because the attribution criteria are quite strict and narrow and exclude more than what they include.

If a non-state actor that commits an attack is an organ or agent of a state[29] or performs governmental functions[30] or acts under the instructions, direction or effective control of a state[31] then its attack will be attributed to the referent state and become a state-armed attack. Yet these are quite strict criteria and mainly require dependence and subordination of the non-state actor to the state. It is quite interesting to note in this regard that the ICJ has not been able to attribute acts to a state on the basis of the effective control criterion. The situation is further exacerbated by the difficulties in tracing back cyber attacks and in identifying the culprits. The GGE in its 2015 report states that "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated"[32], but the question is how it can be substantiated and what evidence is needed. Even if technical attribution is successful, it cannot identify the person behind the computer or behind the attack and for that to happen intelligence information and analysis is needed.[33] For example, the Estonian DDoS attacks in 2007 involved almost 80,000 computers from 170 countries.[34] This shows that it is not only the legal but also the technical and political aspects of attribution that cause problems in cyberspace. Because of the problems with attribution, non-state actors have ample space to act with impunity and states to act through non-state actors with impunity.

---

[29] Draft Articles, *supra* note 19, art. 4; *Nicaragua Case*, *supra* note 16 at para. 109; *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* [2007] ICJ Rep 595 at para. 385 ["*Bosnia Genocide Case*"].

[30] Draft Articles, *supra* note 19, arts. 5, 6.

[31] Draft Articles, *supra* note 19, art. 8; *Nicaragua Case*, *supra* note 16 at paras. 116-117; *Bosnia Genocide Case*, *supra* note 29 at paras. 398, 402-406, 413-414.

[32] UN Doc. A/70/174, *supra* note 6 at para. 28.

[33] David D. Clark and Susan Landau, "Untangling Attribution" in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy* (Washington: National Academies Press, 2010) at 25.

[34] Tikk et al., *supra* note 8 at 20, 23.

In response to these problems, proposals have been made to relax the attribution criteria by including, for example, a criterion of "overall control"[35] or a criterion of toleration and acquiescence or a criterion of state complicity in the attack.[36] The legal status of these criteria is subject to debate and still they place the issue within a state-centred view of international law but there may exist non-state actors that are powerful enough to act independently from states. Unless international law recognizes non-state actors as the authors of a cyber attack and applies to them the full panoply of the law, there will be no closure. If that were to happen, a non-state actor that launched a cyber armed attack independently from states will be the direct target of self-defence action in contrast to the current position where the non-state armed attack will remain outside the law if it is not attributed somehow to a state.[37] Even if non-state actors are to be treated as autonomous subjects, the problems with attributing acts accurately to a state or to a non-state actor remain and all will depend on technical advancement and on accurate political assessments.

V. PROPOSALS FOR ENHANCING SECURITY

The preceding sections revealed the existence of competing interpretations of the rules on the use of force as well as gaps in the legal regulation of cyber attacks. More specifically, there are interpretative disagreements and gaps as to what constitutes a prohibited cyber force or a cyber armed attack; under what conditions cyber attacks can be attributed to states; whether states can resort to forcible countermeasures against low level cyber attacks and how non-state actors should be treated by international law. These problems, it should be stressed, are not specific to cyber attacks but the characteristics of cyberspace and the prominence of non-state actors aggravate them.

One might have expected the *Tallinn Manual on the International Law Applicable to Cyber Warfare* to resolve any interpretative controversies concerning the *jus ad bellum* rules instead of reflecting those same controversies in its text. Nonetheless, what is important is that by mentioning these controversies, the Manual highlights the mismatch between international rules and contemporary phenomena. Also, by airing these interpretative controversies and by integrating them in the narrative, they were presented as legitimate enquires. As a result, some incremental changes and clarifications may take place but the speed of developments in this area will continue to pose new

---

[35] *Prosecutor v Duko Tadi a/k/a "DULE"*, Appeal, [1999] ICTY-94-1-T at paras. 131, 137

[36] Michael N. Schmitt, "Bellum Americanum Revisited: US Security Strategy and the Jus Ad Bellum" (2003) 176 Mil L Rev 364.

[37] Nicholas Tsagourias, "Non-State Actors and the Use of Force" in Jean d'Aspremont, ed., *Participants in the International Legal System: Theoretical Perspectives*, (London: Routledge, 2011) at 327-328; Nicholas Tsagourias, "Self-Defence Against Non-State Actors: The Interaction Between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule" (2016) 29:3 Leiden J Intl L 801.

challenges to the law. Also, states have different interests, different approaches to security and different cyber capabilities which affect their position on the law. Other issues such as the place of non-state actors in international law raise more fundamental questions about the structure of the international order and are more difficult to tackle.

In my opinion, such interpretative penumbra is not necessarily bad to the extent that there is agreement on the basic use of force principles because it allows all actors irrespective of their particular position and interests to claim a stake in the rules. In any case, the development of international law in the absence of a world legislature is not a linear process but is the result of claims, counterclaims and contestations.

If that is the case and to the extent that cyberspace adds another layer of insecurity, there may be other means of assuaging states' fears and reducing the risk of conflict in cyberspace. For example, agreeing on confidence and trust building measures concerning the offensive and defensive use of cyber weapons, agreeing on rules of cyber behaviour, establishing cyber early warning systems, exchanging information, improving security standards of national critical information infrastructures to make them more resilient, improving civil preparedness for contingency planning, are some measures that can help in this regard. The need for such measures has also been recognized by states and international organizations. Indeed in 2010, the United Nations Group of Governmental Experts reached agreement on five general recommendations for future actions, among them ''Further dialogue among States to discuss norms pertaining to State use of ICTs [information and communications technologies], to reduce collective risk and protect critical national and international infrastructure, and, in particular, 'Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict'".[38] Its 2015 Report adopted by consensus identifies norms, rules, and principles for the responsible behaviour of states, confidence-building measures and reaffirms the application of international law to cyberspace.[39] According to the Report, states should not conduct or knowingly support ICT activity that intentionally damages critical infrastructure; states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions; states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams (CERT/CSIRTS) and should not use their own teams for malicious international activity; states should respect the UN resolutions that are linked to human rights on the internet and to the right to privacy in the digital age; states should cooperate to increase stability and security in the use of ICTs and to prevent harmful practices; states should consider all relevant information in case of ICT

---

[38] UN Doc. A/65/201, *supra*, note 3 at para. 18.

[39] UN Doc. A/70/174, *supra* note 6.

incidents; states should consider how best to cooperate to exchange information, to assist each other, and to prosecute terrorist and criminal use of ICTs; states should take appropriate measures to protect their critical infrastructure; states should respond to appropriate requests for assistance by other states whose critical infrastructure is subject to malicious ICT acts; states should encourage responsible reporting of ICT vulnerabilities and should share remedies to these. As for the confidence building measures, the report mentions points of contact on the policy and technical level; focal points of exchange of information concerning cyber incidents; sharing national legal and policy views as well as information on vulnerabilities; developing bi- or multilateral cooperation mechanisms to investigate ICT-related crime or terrorist activities.

As with international law norms and principles which encounter difficulties when their application is particularised, confidence and trust building measures present their own difficulties for example concerning monitoring and verification whereas defining cyber weapons is not an easy exercise because of their dual — military and civilian — nature and use. Yet, as with international rules and principles they provide a context where mutual security can be forged.

With regard to the fora where such measures can be discussed and agreed upon, international organizations such as the United Nations or regional organizations[40] are better places to facilitate the production of policies, norms, and strategies but also to oversee compliance and implementation. This is because of the interconnected nature of security in cyberspace which demands cooperation and coordination in order to increase confidence, security and to prevent conflict. As was seen, the UN is very active on this issue with the General Assembly taking the lead with the creation of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.

Such initiatives cannot be successful if they do not involve the private sector including the internet governance organizations, businesses as well as civil society. The difference between cyber security and other areas is that the private sector controls the internet. The involvement of the private sector which is critical would require different approaches to participation in norm creation as well as in norm implementation and enforcement.

Although such security-oriented measures may succeed in reducing insecurity and in building trust and confidence, they should not lead to unnecessary and disproportional limits on people's access to internet or to unjustified intrusion into their privacy. A balance between security and human rights is important but since states hold different views on the relationship between human rights and security, this may hinder the prospect of agreements.

---

[40] For the EU, see European Union External Action, "Foreign Affairs", online: <eeas.europa.eu>; for The Shanghai Cooperation Organization (SCO), see Info SCO, "SCO responds to cyber challenges", online: <www.infoshos.ru/en/?idn=8349>; for NATO, see NATO, "Cyber defence", online: <www.nato.int>.

If agreement on the issues mentioned above is reached, this may in time lead to agreement on legally binding norms about rules of cyber behaviour. Still, those norms will not substitute for the rules on the use of force which are part of the constitution of the international society, neither will they make the use of force impossible but they will provide another layer of preventing conflict.

VI. CONCLUSION

In order to conclude, the current regime on the use of force has been impacted by the rise of cyber actors and cyber activities with cyber security being at the forefront of international legal and political debates. Currently, there are competing views as to how international rules on the use of force apply to cyberspace as well as gaps in legal regulation. There is, however, recognition that international law applies and that developing norms, regulations and principles on rules of cyber behaviour and related issues will contribute to a safe and secure cyberspace and prevent conflicts. In order to achieve this, multilateral and multi-stakeholder processes are needed. We are still at the early stages of just acknowledging such a need and much work remains to be done.