Cybersecurity and Cybercrime: Dynamic Application versus Norm-Development

Antonio Segura-Serrano*
University of Granada, Granada, Spain
asegura@ugr.es

Abstract

The earliest approach by international lawyers to the question of cybersecurity was focused on collective security. Regarding this issue, there is consensus on the evolutionary and dynamic application, difficult in any case, of the basic rules concerning the prohibition of the threat and the use of force that already exists in the international order. However, cybersecurity does not only concern peace and security, as it is considered a problematic issue that poses various challenges from other international legal perspectives. This paper aims to analyse cybersecurity from this more holistic approach, pointing out the shortcomings of this evolutionary application as well as the

* Associate Professor (Senior Lecturer) of Public International law and EU Law at the University of Granada.

DOI 10.17104/0044-2348-2021-3-701 ZaöRV 81 (2021), 701-731

efforts that have been carried out so far in order to promote international cooperation in this field so as to achieve norm-development.

Keywords

cybersecurity – cyberattacks – cybercrime – international responsibility – jurisdiction – norm-development

I. Introduction

The earliest approach by international lawyers to the question of cybersecurity was focused on collective security. Regarding this issue, there is consensus on the evolutionary and dynamic application, difficult in any case, of the basic rules concerning the prohibition of the threat and the use of force that already exists in the international order. However, cybersecurity does not only concern peace and security, as it is considered a problematic issue that poses various challenges from other international legal perspectives. This paper aims to analyse cybersecurity from this more holistic approach, pointing out the shortcomings of this evolutionary application as well as the efforts that have been carried out so far in order to promote international cooperation in this field so as to achieve norm-development.

The goal of this paper consists of evaluating the background norms and the legal avenues that are proposed in extant international law in order to address cyberattacks, generally speaking. The central argument posed is that those avenues have important weaknesses and, therefore fall short of what is needed if international law is to be relevant in reacting against those cyberattacks within a rule-based international order. Thus, the norm-development avenue is analysed as the alternative option and the best way forward. However, the paper will be very critical of the efforts recently made in this realm, as they have produced only limited results. The test case of cybercrime will be used to show how far international law is from solving the problems posed by cyberattacks.

This paper will start by assuming that cyberattacks are a growing and, perhaps, the most persistent problem that the international community is in need of addressing in cyberspace. For example, the ransomware virus known as WannaCry, which put half the world in check in 2017, was still one of the most aggressive viruses in late 2019.[1] Likewise, the NotPeya cyber operation

[1] Naked Security, 'WannaCry – the Worm that Just Won't Die', 18 September 2019, <https://nakedsecurity.sophos.com>.

 DOI 10.17104/0044-2348-2021-3-701

has been termed as the most devastating cyber-attack in history, with at least $10 billion in total damages.[2] Cyberattacks can be attributed to State or non-State actors. In the first case, they fall within the scope of the use of force, as set by the 'scale and effects' standard,[3] prohibited by international law within the framework of the United Nations (UN) Charter. However, if those cyberattacks do not reach the use of force's threshold, then international responsibility and countermeasures may be invoked, but only if there is an international wrongful act. Many of the cyber operations like the two mentioned previously do not constitute a violation of international law, unless we consider that territorial sovereignty is the infringed rule.[4] In the case of cyberattacks attributed to non-State actors, various international legal cooperation mechanisms may be used, particularly the Budapest Convention on Cybercrime.

Section II will address the background issues that need to be solved if international law is to properly fulfil its functions and govern State relations regarding cyberspace in the face of cyberattacks. After a quick reference to the legal nature of cyberspace, this section will review how adaptive application of international law fares when it comes to basic rules such as those relating to international responsibility, which are of utmost importance for the discipline to be up to the task. Section III will be devoted to the alternative route, i. e., norm-development as the way out to achieve the international regulation needed for the most pressing cybersecurity issues. The UN efforts at the global level, and the specific endeavour to introduce new rules in the cybercrime realm mainly, but not only, at the regional level, will form the bulk of this section. Section IV will conclude this assessment with some final remarks.

II. Dynamic Application and Its Limits

The option consisting of the dynamic application of extant international law rules to cyberspace has been that held by the US and its Western allies. The cybersecurity strategies of these countries are very explicit in this regard,

2 Andy Greenberg, 'The Untold Story of NotPeya, the Most Devastating Cyberattack in History', 22 August 2018, <https://www.wired.com>.

3 ICJ, *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), Judgment, 27 June 1986, ICJ Reports 1986, 14 (para. 195).

4 Przemysław Roguski, 'Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace', 6 March 2020, <https://www.justsecurity.org>; François Delerue, *Cyber Operations and International Law* (Cambridge: Cambridge University Press 2020), 231; *Contra*: Gary P. Corn and Robert Taylor, 'Sovereignty in the Age of Cyber', AJIL Unbound 111 (2017), 207-212 (207 f.).

DOI 10.17104/0044-2348-2021-3-701

as are the French,[5] German[6] or Spanish[7] strategies. However, few States, e. g., France and The Netherlands,[8] have fully delved into the specifics of this difficult legal interpretation. Among the cross-cutting issues that need to be solved in order to provide stability and security in cyberspace are those relating to responsibility. Firstly, because these are principal problems from the perspective of the discipline of public international law, in order for it to properly fulfil its functions in this new environment. Second, because, although these issues have been debated for some time in their application to cyberspace, they are very hot areas on international agendas and have certainly not been definitively unravelled as of today in the face of cyberattacks.

This section seeks to reflect on the above-mentioned issues on the basis of the few existing reference documents on the subject. The aim is to comment, mainly, on the rules set out in the Tallinn Manual 2.0, published in 2017, the first edition of which was published in 2013,[9] and which is intended to reflect the *lex lata*. In addition, the reports of the Groups of Governmental Experts (GGE) which have been prepared to date within the framework of the UN will be reported, chiefly those corresponding to 2013 and 2015.[10] Also, the paper will consider the recent Open-Ended Working Group (OEWG) Report of 2021, which will be followed by the work of a new OEWG 2021-2025.[11] Likewise, the scarce State practice, mainly in the form of State views on the application of international law to cyberspace will be taken into account. Although this paper does not attempt to definitively elucidate the question of the legal status of these documents, the GGE reports and the

5 Prime Minister, French Republic, *French National Digital Security Strategy*, adopted in 2011 and updated in 2015, <https://www.ssi.gouv>.

6 Federal Ministry of the Interior, *Cyber Security Strategy for Germany*, adopted in 2011 and updated in 2016, <https://www.enisa.europa.eu>.

7 Prime Minister, Spanish Government, *National Cybersecurity Strategy*, adopted in 2013 and updated in 2019, <https://www.dsn.gob.es>.

8 Government of The Netherlands, *Letter to the Parliament on the International Legal Order in Cyberspace*, 5 July 2019, <https://www.government.nl>; Ministère des Armées, République Française, *Droit internationale appliqué aux opérations dans le cyberspace*, 2019.

9 Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press 2017), 2-3; Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press 2013).

10 UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 24 May 2013, A/68/98; UNGA, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, of 22 September 2015, A/70/174.

11 UNGA, Final Substantive Report, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security of 10 March 2021, A/AC.290/2021/CRP.2.

 DOI 10.17104/0044-2348-2021-3-701

OEWG Report have obviously more legal import, as they substantiate the collective opinion of UN Member States. However, those reports do not allow for an exhaustive legal critique, as they are very general texts which embody a global consensus on the applicability of extant customary law but are devoid of detailed rules. Conversely, the Tallinn Manual is more problematic, as it elaborates on very specific rules allegedly representing the *lex lata*, even if some previous analyses have already endeavoured to assess whether this Manual is actually followed by States.[12] Although the Tallinn Manual is the result of the work of a group of experts and therefore may be considered only as a private endeavour, it is also evident that as a North Atlantic Treaty Organization (NATO) supported project it also provides the legal arguments and the mainstream position mostly held by Western governments, i. e. that extant international law rules are sufficient to govern international relations in cyberspace. This is the reason why the Tallinn Manual is analysed more extensively in this paper, although reference is also made to UN reports and State views where they offer some guidance.

1. Legal Nature

Now that the first libertarian demands[13] have been forgotten, there is still some debate as to the legal nature of cyberspace. On the one hand, there are those who consider it to be part of the global commons, along with a varied group of international spaces.[14] However, given that the Internet infrastructure is currently both public and private, and that the rules that apply to it are both national and international, some authors opt for the concept of the 'imperfect' or pseudo-commons.[15] This type of characterisation suggests that an internationalised legal regime for the basic resources of cyberspace could

12 Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallin Manual 2.0 on Cyber-operations and Subsequent State Practice', AJIL 112 (2018), 583-657, (653), who are critical of the Tallinn Manual, as they believe that it is not being followed by States in their most recent practice, given the wait-and-see strategy that these States have adopted. However, this remark does not go as far as to conclude that the Tallinn Manual's rules are rejected outright by States or do not represent their views at all.

13 John P. Barlow, 'A Declaration of the Independence of Cyberspace', 8. February 1996, <https://www.eff.org>.

14 US Department of Defense, *Strategy for Homeland Defense and Civil Support*, 2005, 12; Government of Canada, *Canada's Cyber Security Strategy: For a Stronger and more Prosperous Canada*, 2010, 2.

15 Joseph S. Nye, *Cyber Power*, (Cambridge: Harvard Kennedy School 2010), 15; Scott J. Shackelford, 'Toward Cyberpeace: Managing Cyberattacks through Polycentric Governance', American University Law Review 62 (2013), 1273-1364 (1292).

be achieved in the future, following the contours of the concept of the common heritage of mankind (CHM).[16] Even if cyberspace is not a perfect commons, Internet governance following the contours of the CHM concept is an innovative proposal that may be added to the discussion with some success. The CHM's principles of non-appropriation, common management, peaceful use, and preservation seem to create a better legal framework to be applicable to Internet governance than the present multistakeholder approach, as represented by the Internet Corporation for Assigned Names and Numbers (ICANN), where big commercial interests linked to the United States (US) are the leading force.[17]

2. International Responsibility

One of the main difficulties in relation to international responsibility in cyberspace is that of attribution, due to the prevalence of anonymity on the Net. This anonymity can be achieved in various ways, through virtual private networks (VPNs), proxy servers, onion routing, etc. In fact, the 2013 and 2015 UN GGE reports have included a prohibition on the use of third parties by States to commit internationally illicit acts through (Information and Communication Technologies) ICTs. However, leaving aside the widespread practice of States consisting of the use of intermediaries to carry out clandestine acts on the web,[18] the operation of attribution itself is complicated by the diversity of actors present in cyberspace.[19]

a) Attribution: Rules and Problems

The Tallinn Manual raises as its most immediate concern the difficulty, both technical and legal,[20] of the question of attribution for a State seeking to

16 Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law', Max Planck UNYB 10 (2006), 191-272 (231).

17 Antonio Segura-Serrano, 'Cyberspace and the Common Heritage of Mankind' in: Daniele Amoroso et al. (eds) *Global Public Goods, Global Commons and Fundamental Values: The Responses of International Law*, 2017 ESIL Annual Conference, (Oxford: Oxford University Press 2021), 189-208.

18 Tim Maurer, '"Proxies" and Cyberspace', Journal of Conflict & Security Law 21 (2016), 383-403.

19 Michael N. Schmitt and Liis Vihul, 'Proxy Wars in Cyber Space: The Evolving International Law of Attribution', Fletcher Security Review 1 (2014), 55-73.

20 Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution', Journal of Conflict & Security Law 17 (2012), 229-244 (233).

make use of unilateral reaction measures. Indeed, the *ex ante* determination of the attribution of a cyber-operation as a preliminary step to a unilateral response may be subject to considerable uncertainty in cyberspace, in the absence of sufficient information. Given the extant situation, the Tallinn Manual considers that the unilateral reaction of the State must be subject to the criterion of reasonableness, according to the context in each case, which in turn is in line with the US and United Kingdom's (UK) views[21] on the matter.[22] However, consistent with the International Court of Justice (ICJ) case-law, the Tallinn Manual adds another decisive factor to this equation, namely the seriousness of the infringement, so that the more serious the infringement committed, the more confidence must be placed in the evidence put forward by the reacting State,[23] although the seriousness of the response must also be considered.[24] However, when a State takes countermeasures against the cyberactivities of another State it always does so at its own risk, so that if an error in attribution is subsequently found the State will have committed an international wrongful act with its response.

Another problematic issue raised by the Tallinn Manual is that of the publicity of the evidence on which the attribution of a cyber-operation to another State is based. The Manual understands that, although it could be positive, there is currently not enough practice or *opinio juris* to affirm this obligation. The United States has argued through the State Department's Legal Adviser that there is no international obligation to disclose the evidence before taking response action,[25] a position also expressed by the United Kingdom through its Attorney General,[26] by France,[27] and by The Netherlands.[28] On the contrary, the UN GGE has stated that 'the accusations of

21 Brian J. Egan, 'International Law and Stability in Cyberspace', Berkeley J. Int'l L. 35 (2017), 169-180 (177); Jeremy Wright, 'Cyber and International Law in the 21st Century', 23 May 2018, <https://www.gov.uk>.

22 Przemysław Roguski, 'Application of International Law to Cyber Operations: A Comparative Analysis of States' Views', The Hague Program for Cyber Norms Policy Brief, March 2020, 15, arguing that this reasonableness should be interpreted as a standard of evidence but not as a duty of care when making the attribution, as the US and UK views seem to convey.

23 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia-Herzegovina v. Serbia and Montenegro), Judgment of 26 February 2007, ICJ Reports 2007, 129, (paras 208-209).

24 Lorraine Finlay and Christian Payne, 'The Attribution Problem and Cyber Armed Attacks', AJIL Unbound 113 (2019), 202-206 (206), proposing a system of gradation in the standards of attribution, depending on the response to be adopted by the State that is the victim of a cyber-attack.

25 Egan (n. 21), 177.

26 Wright (n. 21).

27 Ministère des Armées (n. 8), 11.

28 Government of The Netherlands (n. 8).

organising and implementing wrongful acts brought against States should be substantiated',[29] in accordance with ICJ case law on evidence.[30] A recent analysis of practice has shown that difficulties relating to attribution are leading States to a strategy of caution in which, because of this impossibility of establishing attribution with certainty,[31] it is preferred not to invoke the illegality of certain cyber-activities, which in turn promotes impunity.[32] If we take the example of the Wannacry cyber-attack in 2017, where attribution to North Korea was readily made by private firms within few days,[33] it took several months for the US and the UK to publicly attribute this cyber-attack to North Korea,[34] and no public sanction followed. Likewise, the 2019 Georgia cyber-attack attributed to Russia four months after its occurrence is interesting in that an increased number of States publicly made an official attribution of the cyber incident to Russia (more than 20), but failed to indicate the specific international law rules that were breached by this cyber-attack, in what has been termed as a missed opportunity to strengthen the international rules-based order.[35] Therefore, there is much to be done in the field of public attribution of cyber-attacks from the point of view of State practice, as States are still balancing from the application of international law to strategic and political considerations.

A particular difficulty arises in relation to the taking of control and use of the cyber infrastructure, governmental or private, of another State to carry out malicious operations. The UN GGE has specifically addressed the situation regarding the illegal use of another State's cyber infrastructure. Thus, the 2015 Report states that a determination that a cyber activity has originated in the territory or infrastructure of a State is not sufficient to attribute that activity to that State.[36] However, for the Tallinn Manual this use could be an indication that the State is associated with the operation, although this presumption would be less convincing if the cyber infrastructure used was

29 UNGA, 2015 GGE Report (n. 10), para. 28 f.

30 Marco Roscini, 'Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations', Tex. Int'l L. J. 50 (2015), 233-275 (243).

31 Yuval Shany and Michael N. Schmitt, 'An International Attribution Mechanism for Hostile Cyber Operations', International Law Studies 96 (2020), 196-222 (217), arguing that major States have the capacity to make attribution, but are sceptical about the very push for legal accountability in the face of those States that do not share the commitment to the 'rule of law'.

32 Efrony and Shany (n. 12), 633-634.

33 Alex L. Johnson, 'WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group', 22 May 2017, <https://community.broadcom.com>.

34 BBC News, 'Cyber-Attack: US and UK Blame North Korea for WannaCry', 19 December 2017, <https://www.bbc.com>.

35 Roguski (n. 4).

36 UNGA, 2015 GGE Report (n. 10), para. 28 f.

private, rather than governmental. Cases of spoofing, through techniques such as impersonating other organisations, or through the use of their IP addresses, are very difficult to resolve, and the Manual proposes a case-by-case assessment, depending on the context of each case. Therefore, also on this point, legal certainty is difficult to be affirmed beforehand, and end-result that is not desirable from a legal point of view.

With regard to the attribution of international responsibility in the case of cyber operations carried out by non-State actors, the Tallinn Manual as well as the OEWG Chair's Summary[37] endorses the criterion of 'effective control' that the ICJ has expressed in the *Nicaragua* and *Genocide* cases.[38] As is well known, 'global control' or indirect control would not be sufficient to produce such attribution to the State.[39] However, some authors have already asserted the criterion of global control as more appropriate for cyberspace,[40] basically because it makes the operation of attribution easier.[41] Moreover, in the case of cyber-attacks that reach the threshold of armed attacks, some literature does not hesitate to reject the criterion of effective control out of hand and accept the much more lax criterion of tolerance or reluctance to act against such non-State actors, and end up attributing the act in question to the State from which the attacks originate.[42] Some authors, in a scarcely reasoned argument, have even put forward a criterion of 'virtual' control through which the burden of proof would be reversed.[43]

A final issue that connects with the question of attribution is that envisaged in the UN GGE 2013 and 2015 Reports. According to these reports, States must ensure that their territories are not used by non-State actors to commit internationally wrongful acts. On this basis, an intense debate has

37 UNGA Chair's Summary, Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 10 March 2021, A/AC.290/2021/CPR.3, para. 14.

38 ICJ, *Nicaragua* (n. 3), para. 115; ICJ, *Genocide* (n. 23), para. 400.

39 ILC, 'Articles on the Responsibility of States for Internationally Wrongful Acts with Commentaries', ILCYB, Vol. II, Part Two, (2001), 31, Art. 8, para. 5.

40 Kubo Mačák, 'Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors', Journal of Conflict & Security Law 21 (2016), 405-428 (423).

41 Scott J. Shackelford, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' in: Christian Czosseck and Karli Podins (eds), *Conference on Cyber Conflict Proceedings 2010* (Tallinn: CCD COE 2010), 197-208.

42 Tsagourias (n. 20), 242.

43 Peter Margulies, 'Sovereignty and Cyberattacks: Technology's Challenge to the Law of State Responsibility', Melbourne Journal of International Law 14 (2013), 496-519 (514), arguing that a State that has previously funded or assisted non-State actors who are perpetrators of malicious online activities should demonstrate its innocence in relation to such activities.

taken place around the due diligence obligation of States. This obligation is set out in Rules 6 and 7 of the Tallinn Manual and will be assessed later on.

Therefore, this paper is of the view that attribution is a crucial cybersecurity issue which extant international law is incapable of clarifying. To overcome this problem, part of the literature promotes attribution by non-State actors,[44] while other commentators support the setting up of a centralised international attribution mechanism,[45] though difficult to implement in the short run,[46] or propose a revision of the attribution determinants as stated by Article 8 of the International Law Commission (ILC) Draft Articles.[47] This kind of solution is in line with other proposals to internationalise the process of attribution, as those made by Microsoft[48] and RAND.[49] Hence, any of the mentioned ways forward entail the development of new rules of international law on this topic.

b) Countermeasures

The emphasis in the Tallinn Manual on countermeasures, to which a very extensive analysis is devoted, must be stressed. Perhaps this emphasis can be explained by the Tallinn Manual's undisguised interest in finding a formula for States to respond when self-defence against cyber-attacks is not legally justified in the specific case. This view is shared by those Western States that have expressed their opinion on the matter, e. g. the US, UK, France, and The Netherlands,[50] although the UN Reports by the GGE/OEWG do not refer to this possibility. However, a recent analysis of practice shows the States'

44 Kristen E. Eichensehr, 'Decentralized Cyberattack Attribution', AJIL Unbound 113 (2019), 213-217 (217).

45 Henning Lahmann, *Unilateral Remedies to Cyber Operations – Self-Defence, Countermeasures, Necessity, and the Question of Attribution*, (Cambridge: Cambridge University Press 2020), 279.

46 Shany and Schmitt (n. 31), 196 f., arguing that this mechanism would be of help in three contexts: for States facing capacity issues, for those interested in collective attribution, and in case of extant cyber-related sanctions regimes.

47 Nicholas Tsagourias and Michael Farrell, 'Cyber Attribution: Technical and Legal Approaches and Challenges', EJIL 31 (2020), 941-967, (941 f.)

48 Shaun Waterman, 'Microsoft Calls for UN-type Body to Attribute Big Cyberattacks', 23 June 2016, <https://www.fedscoop.com>.

49 Benjamin Boudreaux, Jonathan W. Welburn, John S. Davis (II) and Cordaye Ogletree, 'Stateless Attribution, Toward International Accountability in Cyberspace', RAND (2017), 25 ff., calling for a Global Consortium for Cyber Attribution.

50 Egan (n. 21), 169, 178; Wright (n. 21); Ministère des Armées (n. 8), 8; Government of The Netherlands (n. 8), 7.

reluctance to publicly claim their right to apply countermeasures for the time being regarding specific cyber-attacks.[51] The reason why countermeasures as active defences against a cyberattack (hack-back) have not been widely used yet is related to the difficulty of timely attribution, which in turn gives countermeasures a more prominent *ex post facto* role in the near future.[52] Indeed, the literature that is less inclined to make extensive use of self-defence, and therefore the use of force, in cyberspace considers that countermeasures have been given little consideration regarding this role, when in fact they may be the best recourse to be used, particularly since claims of malicious activity will ultimately have to be redirected to requests for financial compensation.[53]

As for the object of a countermeasure, it must always be a State. Therefore, it is not possible to take countermeasures against non-State actors, unless the State has failed to fulfil its due diligence obligation, as will be seen later. In other words, non-State actors are not subject to States' own international legal obligations and, for that reason, cannot be the object of countermeasures against a previous wrongful act. For the Tallinn Manual, the alternative response to actions by non-State actors would be two measures that preclude wrongfulness, namely self-defence and state of necessity. However, with respect to self-defence, the problem is that this alternative response presupposes that non-State actors may violate the principle of prohibition of the use of force, and that the State against which the defensive action is directed is not the object of an international wrong when its consent is not present.[54] In this sense, some literature asserts that it is currently possible for non-State actors to infringe the principle of prohibition of the use of force, thus allowing self-defence against them. In turn, self-defence as a ground for precluding wrongfulness provided for in Article 21 of the ILC Draft Articles would justify the violation of the territorial sovereignty of the State where these non-State actors, who are the object of self-defence, are located.[55] However, this position does not reflect customary international law, nor is it supported by ICJ jurisprudence.[56] With respect to state of necessity, as

51 Efrony and Shany (n. 12), 646.

52 Lahmann (n. 45), 200.

53 Mary E. O'Connell, 'Cyber Security without Cyber War', Journal of Conflict & Security Law 17 (2012), 187-209 (204-205).

54 Federica I. Paddeau, 'Use of Force against Non-state Actors and the Circumstance Precluding Wrongfulness of Self-Defence', LJIL 30 (2017), 93-115 (106-107).

55 Nicholas Tsagourias, 'Self-Defence against Non-state Actors: The Interaction between Self-Defence as a Primary Rule and Self-Defence as a Secondary Rule', LJIL 29 (2016), 801-825 (801 f.).

56 Monika Hakimi, 'Defensive Force against Non-State Actors: The State of Play', International Law Studies 91 (2015), 1-31 (1 f.).

DOI 10.17104/0044-2348-2021-3-701

opposed to countermeasures, its application does not require a prior international wrongful act, but the existence of a grave and imminent peril to an essential interest of the State, which makes the state of necessity very interesting so as to be applied to non-State actors. Yet, this situation is unusual in practice.[57]

In any case, and despite the difficulty of the attribution referred to above, the Tallinn Manual agrees with the ILC in considering that States adopting countermeasures do so at their own risk and must answer for the legality of such measures. Therefore, a State which adopts a countermeasure which subsequently does not pass the legitimacy test will be liable for the unlawfulness involved. This conclusion in the context of the adoption of countermeasures has a restrictive function, since otherwise there could be a certain risk of escalation which must be avoided,[58] particularly in cyberspace, the intrinsic speed of which may run counter to a careful consideration of the situation at hand. However, the Tallinn Manual understands that this risk of escalation is mitigated by the requirement of prior notification, although, surprisingly, the effectiveness of this requirement is negated by the considerations later made in the Manual, as will be seen.

As regards the aim of countermeasures, namely to induce the offending State to comply with its international obligations, the Tallinn Manual considers that countermeasures in cyberspace are of a reactive, not prospective, nature, as a consequence of the first requirement called for by the ICJ in the *Gabčíkovo-Nagymaros* case,[59] namely the existence of a previous international wrongful act. The Tallinn Manual therefore maintains that there can be no countermeasures equivalent to anticipatory self-defence against imminent armed attack, nor is there room for preventive countermeasures. However, the requirement of reversibility of countermeasures, which was confirmed by the ILC, is understood by the Tallinn Manual as a requirement in the broad sense, it should not be absolute, nor should the State be required to choose the option that is most easily reversible. The Tallinn Manual gives as an example a denial of service attack (DDoS) which, when used as a countermeasure, has very limited reversibility, since the cyber-activities that are prevented can no longer be carried out.

A particularly difficult issue in the context of countermeasures arises in relation to the obligation of prior notification, as it is said this requirement

57 ILC, ARSIWA (n. 39), Art. 25, para. 2.

58 Michael N. Schmitt, '"Below" the Threshold Cyber Operations: The Countermeasures Response Option and International Law', Va. J. Int'l L. 54 (2014), 697-732 (715).

59 ICJ, *Gabčíkovo-Nagymaros Project* (Hungary v. Slovakia), ICJ Reports 1997, Judgment of 25 September 1997, 7 (83).

could make countermeasures 'unrealistic' in cyberspace.[60] This is also the position taken by Western States, e. g. the US, UK, France, and the Netherlands, although it is not clear whether the absence of prior notification is limited to those cases of covert cyber intrusion (UK and France), or it is to be based on urgency of the action (The Netherlands).[61] Because of this unrealistic reason, the Tallinn Manual considers this requirement as non-categorical, in what has been called a pragmatic approach.[62] Firstly, because the perpetrator of a malicious online operation may be masked. Secondly, because of the speed present in that medium, the reaction may be considered urgent,[63] in which case the requirement for prior notification should lapse. Lastly, prior notification may mean that the countermeasure to be taken is rendered ineffective and it would therefore be pointless to require compliance. However, this paper considers that the unveiled intention to dispense with this prerequisite of notification is worrying because it makes the approach of the Tallinn Manual and the mentioned States' views clearly punitive.

Furthermore, the Tallinn Manual opts for the absence of an obligation to negotiate prior to the adoption of countermeasures, which departs from the rule reflected in the Commentary to the ILC Draft Articles on International Responsibility.[64] Indeed, the Tallinn Manual, in line with the position expressed by the United States on the Draft Articles, understands that a State may take countermeasures in cyberspace before entering into negotiations and even during negotiations, as otherwise the offending State would have control over the duration and impact of its breach.

c) State of Necessity

Rule 26 of the Tallinn Manual is devoted to state of necessity, which the Manual considers to be a controversial circumstance, even if it does attribute a customary character to it.[65] Although the Manual acknowledges that the threshold for invoking the plea of necessity is extremely high, the positive

60 William Banks, 'State Responsibility and Attribution of Cyber Intrusions After *Tallinn 2.0*', Tex. L. Rev. 95 (2017), 1487-1513 (1502).

61 Egan (n. 21), 178; Wright (n. 21); Ministère des Armées (n. 8), 8; Government of The Netherlands (n. 8), 7.

62 Eric T. Jensen, 'The Tallinn Manual 2.0: Highlights and Insights', Geo. J. Int'l L. 48 (2017), 735-778 (754).

63 ILC, ARSIWA (n. 39), Art. 52, para. 6.

64 ILC, ARSIWA (n. 39), Art. 52, para. 5.

65 *Contra*: Sarah Heathcote, 'Est-ce que l'État de nécessité est un principe de droit international coutumier?', RBDI 40 (2007), 53-89.

approach to this circumstance is surprising, given that the ILC had framed it in negative terms.[66] This circumstance precluding wrongfulness can therefore be invoked only in exceptional cases, that is, where the essential interests of the State are seriously compromised.

Although the consideration of what is essential depends very much on each State and is therefore basically contextual, the Tallinn Manual endorses the tendency of some States to classify certain State infrastructures as critical, including cyber-infrastructure, which may highlight their essential nature. Examples of critical infrastructure could be the national banking system, the air navigation system, etc.,[67] as The Netherlands has stated.[68] An unresolved issue in the Manual is whether an essential interest of the international community can be used by a State to take unlawful but legitimate action on the basis of the plea of necessity. Besides, as the ILC's Draft Articles points out, the existence of an essential interest is not sufficient and the danger generated by a cyber operation must be grave and imminent, which basically means the destruction of a certain essential interest or its fundamental impairment, so that it becomes dysfunctional. This would be the case of the aforementioned basic infrastructure and its destruction or alteration with severe negative consequences for the State's security, economy, health system, or environment.[69]

For the Tallinn Manual, the state of necessity can be used even if the response to the grave danger involves the infringement of the rights of other, non-responsible third States, as follows *a contrario* from Article 25(1)(b) of the ILC Draft Articles. Indeed, an objective limit is found in this provision, as a State could adopt a cyber-operation on the basis of necessity if it violates an international obligation, but could not do so if it seriously affects the essential interest of another State or the international community.[70] The Tallinn Manual chooses an example, which does not seem accidental, to explain this situation. In the case of cyber operations by non-State actors, where no State is responsible, the victim State can respond on the basis of state of necessity if this protects its essential interests, even if it thereby causes a breach in a non-responsible third State. However, if the response affects an essential interest of the third State, then the plea of necessity would not cover the response.

66 Karine Bannelier and Théodore Christakis, *Cyber-Attacks. Prevention-Reactions: The Role of States and Private Actors* (Paris: Les Cahiers de la Revue Défense National 2017), 38-39.

67 Antonio Segura Serrano, 'Cybersecurity: Towards a Global Standard in the Protection of Critical Information iIfrastructures', European Journal of Law and Technology 6 (2015), 1-24 (1 f.)

68 Government of The Netherlands (n. 8), 8.

69 Schmitt, 2017 (n. 9) 136-137.

70 James Crawford, *State Responsibility – The General Part* (Cambridge: Cambridge University Press 2013), 312.

Another problematic issue is whether the state of necessity also provides justification for reactions in cyber operations of unknown origin. The Tallinn Manual is inclined to consider that the state of necessity could cover responses that can take the form, for example, of a computer shutdown of another's infrastructure, or even counter-hacking. Furthermore, this type of response can be anticipated, as it is sufficient that the danger is imminent, as stipulated in Article 25(1)(a) of the ILC Draft Articles, without having to wait until it has actually taken place. The Netherlands concurs with the Tallinn Manual on both points.[71]

In short, the state of necessity offers a series of advantages, from the legal point of view, which have attracted a certain part of the literature and particular countries, e. g. The Netherlands, especially at the present time when the normative process has made little progress in relation to cyberspace, as we will see. First, the application of the plea of necessity does not depend on the prior attribution to a State of a wrongful act, so it is particularly interesting when acting against non-State actors. Furthermore, the plea of necessity can be activated even in the absolute absence of a previous international wrongful act. For these two reasons, the state of necessity has been considered the most appropriate instrument for reacting to the cyber-activities of non-State actors. However, this is a theoretical possibility rather than a legal certainty, since the very restrictive conditions for invoking the plea of necessity, in particular the fact that it is the 'only way for the State to safeguard an essential interest', make it very difficult to apply this plea in practice.[72] In addition, if the state of necessity was to be used by States on a regular basis, the normalisation of this exception would lead to a 'slow erosion of the rule of law'.[73] Therefore, this paper considers the state of necessity an option that will not be available to States in their day-to-day cyberspace business, as it entails an evolutionary interpretation of the international law customary rules that runs counter the limited scope this plea of necessity received by the ILC.

3. Due Diligence Obligation

One way for overcoming the problems of attribution in international responsibility is that proposed by the Tallinn Manual in Rules 6 and 7 on the

71 Government of The Netherlands (n. 8), 8.

72 Bannelier and Christakis (n. 66), 36-39; Michael N. Schmitt, 'In Defense of Due Diligence in Cyberspace', The Yale Law Journal Forum 125 (2015-2016), 68-81 (78).

73 Lahmann (n. 45), 265.

DOI 10.17104/0044-2348-2021-3-701

obligation of due diligence. It is understood that this obligation is based on the *Corfu Channel* case,[74] in particular on the principle of avoidance of damage, which is often applied in international environmental law.[75] Such due diligence would obviate the question of attribution, holding the State from which the cyber activities originated responsible on the basis of its inaction to prevent or avoid such harmful activities. The core elements of the due diligence obligation are not perfectly outlined in international law.[76] However, this obligation comprises at least two elements, the duty of prevention and the duty of knowledge,[77] whose more or less wide interpretation determines a more or less demanding obligation in relation to the State to which it applies.

Some authors argue that due diligence is required not only for cyber activities that the State is aware of, but also for those that it should have been aware of. This criterion is called constructive knowledge and the Tallinn Manual concedes that it is controversial in international law. There are certain factors that help determine whether the State should have known, such as whether the State's governmental cyber infrastructure was used, or whether the malicious activities consisted of denial of service (DDoS) attacks, which imply extensive use of bandwidth, etc.

With regard to the damage, the Manual understands that this rule applies to all cyber operations that are 'contrary to the rights' of the States concerned (to use the wording of the *Corfu Channel* case) under international law, and that involve serious adverse consequences. However, the threshold to be reached by the damage is an unresolved issue, although the Manual is inclined to consider that damage to things or injury to persons is not essential[78] as, for example, interference with critical infrastructure or a serious impact on the economy would be sufficient.

With regard to the element of prevention, some literature advocates that it includes the rule of reasonableness together with the duty of the State to adopt the necessary legislation to prevent.[79] However, the Tallinn Manual is

74 ICJ, *Corfu Channel* case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ Reports 1949, 22.

75 Jovan Kurbalija, 'State Responsibility in Digital Space', Swiss Review of International and European Law 26 (2016), 307-326.

76 International Law Association, Study Group on Due Diligence in International Law, Second Report, 2016, 7.

77 Russel Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm', Journal of Conflict & Security Law 21 (2016), 429-453, framing these elements in the form of an obligation of result (to have sufficient legislation and administrative apparatus) and an obligation of conduct (to use that capacity diligently).

78 Government of The Netherlands (n. 8), 5.

79 Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low Intensity Cyber Operations?', Baltic Yearbook of International Law 14 (2014), 23-39.

more conservative and upholds that the duty of care, first, requires States to effectively stop malicious cyber operations, both those that are occurring and those that are in preparation and are warned. Secondly, however, the Manual considers that there is no general obligation of prevention in cyberspace beyond the best efforts test, since this is an obligation of conduct, not result. In this sense, the State is not obliged to monitor activity in networks, which can lead to the violation of internationally protected human rights,[80] nor is it obliged to adopt institutional or legal measures to comply with this obligation.

As can be seen, the Tallinn Manual has analysed in detail the ins and outs of the due diligence obligation, and the editor himself, Prof. Schmitt, has endeavoured to highlight the advantages of its application in cyberspace. The main advantage of due diligence is that it can be invoked against malicious activities by non-State actors. In the case of activities of non-State origin, no countermeasures can be applied, as countermeasures can only be taken if the unlawful acts can be attributed to a State. Nor is it easy to invoke a plea of necessity, whose threshold for application is high because, as is well known, an essential interest and a grave peril must be present. On the contrary, due diligence would allow the attacked State to respond with a cyber-countermeasure against non-State actors. This response, which would initially infringe the sovereignty of the State targeted by the countermeasure, would nevertheless find legitimacy in the unlawfulness consisting of the prior breach of due diligence. Yet, the proportionality of the countermeasure in this case would have to be determined, not in relation to the seriousness of the malicious acts committed by the non-State actors, but in relation to the seriousness of the omission committed by the State which infringed the due diligence.

However, some authors have criticised the formulation of the due diligence obligation in the Tallinn Manual. Indeed, firstly, it has been pointed out that due diligence can lead to a destabilisation of international relations as a result of a proliferation of cybernetic countermeasures.[81] Likewise, as France has warned, there is a certain risk that the due diligence obligation be used as an excuse to legally resort to the use of force.[82] Secondly, and to the contrary, another part of the literature has stressed that the Tallinn Manual sets an

80 Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', Harv. Int'l L. J. 56 (2015), 81-146.

81 Eric T. Jensen and Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?', Tex. L. Rev. 95 (2017), 1555 -1577. These authors are members of the international group of experts of the Tallinn Manual 2.0.

82 Ministère des Armées (n. 8), 10, where France is cautioning that «(L)e non-respect de l'obligation de diligence requise par un État tiers ne suffit pas à fonder le droit de recourir à la force à son encontre dans le cadre de cyberattaques perpétrées depuis son territoire».

unclear standard, the application of which is uncertain, as States that are victims of a cyberattack carried out by non-State actors from the territory of a third State are going to encounter many legal difficulties in articulating a right of response.[83] Despite this, the latter literature also stresses that recent practice seems to be moving towards a less demanding standard of due diligence.

In this vein, some States have expressed their opposition to this due diligence, or have remained silent, such as the US and the UK,[84] because of the scope of obligations it may create to them, especially for these States which are more connected to the network and which could bear the heaviest burden.[85] According to this, the 2013 and 2015 GGE Reports simply note that 'States […] should seek to ensure that their territory is not used by non-State actors to commit [internationally wrongful acts]'.[86] Indeed, this formulation has been included in the UN GGE Report 2015 not as rule of international law, but as a voluntary and non-binding norm, which in turn anticipates the legal weight UN Member States are willing to attribute to it. The OEWG Report 2021 has not even mentioned the due diligence obligation.

As can be seen, the current customary formulation of the due diligence obligation is much less demanding than the one adopted in the Tallinn Manual. In other words, the Tallinn Manual has set up a standard of due diligence that States are unwilling to assume at this time, as demonstrated by the practice of using proxies,[87] as well as by the widespread refusal to conduct ongoing monitoring of activities taking place in cyberspace.[88] Therefore, the due diligence obligation must not be taken as panacea, as there are important limitations to its dynamic applicability in this field of cyberspace. The challenge of cybersecurity needs to be met but this kind of wide formulation of international law rules may be counterproductive compared to other avenues, even if in the long run, like norm-development.

III. Cybercrime as a Test Case of Norm-Development

From a holistic approach, international cooperation to tackle cybercrime should be a priority for international lawyers, thereby going beyond the

83 Efrony and Shany (n. 12), 592-593.
84 Egan (n. 21), 169; Wright (n. 21).
85 Schmitt (n. 72), 78.
86 UNGA, 2013 GGE Report (n. 10), para. 23; UNGA, 2015 GGE Report (n. 10), para. 28 (e).
87 Maurer (n. 18), 383 f.
88 Eric T. Jensen, 'Cyber Sovereignty: The Way Ahead', Tex. Int'l L. J. 50 (2015), 275 (299).

 DOI 10.17104/0044-2348-2021-3-701

traditional contours of peace and security with the aim of globally addressing the issue of cyberattacks. In this vein, it is true that cyber-attacks attributable to non-State actors are to be dealt by State authorities through the application of domestic law. Yet, international law's jurisdictional rules may be insufficient in order to solve the new issues posed by cyberspace. Therefore, norm-development efforts have been crucial in this field, with the Budapest Convention on Cybercrime as the main test case to be analysed.

1. Jurisdictional Issues

States can exercise their jurisdiction, and in fact are doing so, over cybernetic activity that is oriented towards a specific territory and has a local effect, bypassing the instrument used (Internet).[89] Yet, this paper claims that the exercise of State jurisdiction should be improved so as to allow for more coordination in this field. Indeed, State jurisdiction may be facilitated in the future if there is international consensus, as the example of the Budapest Convention on Cybercrime shows, even if in turn this Convention should be upgraded to achieve its goals.

Certainly, the bases of territory and nationality are being used normally in the exercise of State jurisdiction over cyberspace, as derived from Article 22 (1) of the 2001 Budapest Convention on Cybercrime, drawn up in the framework of the Council of Europe. These bases are sufficient to ensure the connection between acts of cybercrime and at least one State.

a) Territorial Jurisdiction

The exercise of territorial competence is full in relation to persons and objects located in the State territory, as warned in the Reports of the Groups of Governmental Experts of 2013 and 2015, which expressly refer to ICT infrastructures.[90] However, the Tallinn Manual also extends this territorial competence to data located on State territory. In addition, the Tallinn Manual considers that States that are intermediaries in a transnational cyber activity can also exercise their territorial jurisdiction if their infrastructure is used in

89 Édouard Treppoz, 'Jurisdiction in the Cyberspace', Swiss Review of International and European Law 26 (2016), 273 (275).

90 UNGA, 2013 GGE Report (n. 10), para. 20; UNGA, 2015 GGE Report (n. 10), paras 27 and 28.a.

that activity. In contrast, the experts who have prepared this Manual have not reached agreement on whether the States used for data transit can exercise the same territorial jurisdiction, given that in this case the connection with this infrastructure is minimal.[91]

The Tallinn Manual also reflects the *Lotus*[92] doctrine of subjective and objective territorial jurisdiction, i. e. cyber-activities that respectively originate or are completed on the territory of the State are subject to its jurisdiction. In other words, it is the jurisdiction that may be exercised by a State which happens to be the place of distribution or the place of reception of information circulating in cyberspace.[93] Subjective territorial jurisdiction is not appropriate in cyberspace because of the limitation it implies for the protection of the values and public policy options of the territorial State, making forum shopping by online operators very easy.[94] On the contrary, objective territorial jurisdiction, which is defined as that exercised by the State when none of the constituent elements of the crime occurs on the territory of the State exercising jurisdiction, tends to be too inclusive, which creates problems of overlap between jurisdictions.

Finally, the Tallinn Manual also echoes the effects doctrine, to which it attributes the status of customary law. This type of exercise of territorial jurisdiction is prevalent in cyberspace, since the latter allows the implementation of activities that cause effects in States in whose territory they do not originate or are not completed. In fact, malicious activities in cyberspace often seek precisely to affect a multitude of States simultaneously. However, this effects doctrine is problematic because it creates legal uncertainty by allowing a large number of States to claim the exercise of jurisdiction simultaneously. On the basis of the *Lotus* case, the effects doctrine has been applied in cyberspace with great laxity by States. Thus, mere accessibility has been used as a criterion to subject an activity to the jurisdiction of the territorial State from which a content is accessible, as happened in the *Yahoo!* case.[95] There have been efforts to refine the effects doctrine through the targeting principle. In the framework of this new rule of reason, an activity that has effects on and is oriented towards a specific territory is subject to State jurisdiction, as was the case in the *Google Spain* judgment decided by the

91 Schmitt, 2017 (n. 9), 55.

92 PCIJ, *S.S. Lotus* (France v. Turkey.), 7 September 1927 P. C. I. J. (ser. A) No. 10, 23.

93 Sean Kanuck, 'Sovereign Discourse on Cyber Conflict Under International Law', Tex L. Rev. 88 (2010), 1571 (1573).

94 Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface', EJIL 19 (2008), 799 (811).

95 Segura-Serrano (n. 16), 202, analysing the procedural path followed by this case in France and the United States.

Court of Justice of the European Union (CJEU).[96] This targeting principle appears to be the best balance between, on the one hand, *de facto* universal jurisdiction, to which the broad version of the effects principle (and, also, objective territoriality[97]) leads, and, on the other hand, the approach based on the principle of origin (or exclusive subjective territoriality), which would prevent States from exercising their regulatory autonomy over their territories in relation to the online activities to which they are subject.

b) Extraterritorial Jurisdiction

The previous analysis serves us to evaluate the risks posed by the rules proposed to be applied extraterritorially. Regarding extraterritorial jurisdiction, enforcement is the most pressing issue in the field of cyberspace. Rule 11 of the Tallinn Manual is framed as meaning that extraterritorial enforcement jurisdiction is justified only where there is a specific international law qualification, or there is consent by the territorial State, as in the *Lotus* case, a rule which is considered too rigid for cyberspace. In other words, the extraterritorial executive competence of the State is much more limited than legislative or judicial competence, which in cyberspace generates an obvious result of an executive or enforcement gap that has, however, been filled through measures such as voluntary compliance or local blocking of online content.[98] As a result, one State, for example, cannot hack into servers located in another State to obtain evidence. However, the Manual's assertion that evidence may well be obtained without violating international law when it cannot be determined with certainty in advance in which particular country such digital evidence is located is highly problematic. Similarly, the Manual states that it would be lawful to obtain data, now in the exercise of territorial jurisdiction, when accessing public content, although it is available on servers located in another country. Even if this content is not publicly available, but protected by passwords or otherwise, but ultimately intended to be available. This extensive reading of extant international law rules should be criticised, as it would offer technological powerful States an advantage to overreach

96 ECJ, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, judgement of 13 May 2014, Case no. C-131/12, ECLI:EU:C:2014:317.

97 Uta Kohl, 'Who Has the Right to Govern Online Activity? A Criminal and Civil Point of View, International Review of Law', Computers & Technology 18 (2004), 387 (401).

98 Uta Kohl, 'Jurisdiction in Cyberspace' in: Nicholas Tsagourias and Russel Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar 2015), 30, 53.

from a jurisdictional point of view. Finally, the Manual's group of specialists could not agree on whether contacting private storage service providers, located abroad, to request the voluntary provision of information is contrary to the exclusive executive jurisdiction of the territorial State.[99] As we will see, normative efforts are being developed nowadays in order to achieve this result, as the US Cloud Act and the proposed E-evidence Directive show.[100] However, this is an issue that is in need of elucidation from a legal point of view, as it may create uncertainties and potential conflicts between States in favour and against such a rule. Therefore, norm-development efforts to improve international cooperation in the cybercrime realm are much needed, at the regional and global level alike.

2. Cybercrime

a) Preliminary Remarks Regarding Norm-Development

The UN's activity has been very prolific in terms of cybersecurity and has to a large extent endorsed the option consisting of the application of international law rules to this field of cyberspace. It is the Groups of Governmental Experts established within the framework of the United Nations General Assembly (UNGA) First Committee that have attracted the most attention. If the first Group in 2004 was unable to prepare a final report due to a lack of consensus[101] (Russia wanted to advance in setting new rules and the United States objected that the current ones are sufficient), the second Group did reach in 2010 the consensus necessary to establish areas of cooperation in responsible State behaviour, as well as capacity-building and confidence-building measures (reiterated in subsequent reports).[102]

In the 2013 GGE Report, an agreement was reached regarding the applicability to cyberspace of existing international law, specifically, the UN Charter, human rights, as well as the basic rules on international responsibility.[103] Similarly, the 2015 GGE Report insisted on the applicability in cyberspace of

99 Schmitt, 2017 (n. 9), 68-70.

100 See Section III.2. on cybercrime.

101 UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 5 August 2005, A/60/202, 2.

102 UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 30 July 2010, A/65/201, 2-9.

103 UNGA, 2013 GGE Report (n. 10).

some principles of international humanitarian law (such as proportionality or distinction), as well as of the obligation of due diligence.[104] Some important private initiatives have supported this option, such as the Tallinn Manual, promoted by NATO, and which makes an exhaustive analysis of this evolutionary application as *lex lata*,[105] as we have seen.

By contrast, the second option, consisting of the elaboration of new international rules, has been championed by Russia, China, and other countries, which have made several proposals over the years such as the 2011 Code of Conduct for Information Security, updated in 2015.[106]

The contrast between these two options has been highlighted in the 2017 GGE Report, which has been deemed a failure.[107] Indeed, issues such as the recourse to self-defence, countermeasures, or the explicit recognition of certain norms of international humanitarian law have been rejected by countries such as Russia, China, or Cuba, on the grounds that Western countries are pursuing the militarisation of cyberspace. This failure may lead to think that the multilateral route is closed and that States are going to resort to the unilateral or regional route.

However, at the end of 2018, two working groups have been created within the framework of UNGA.[108] On the one hand, a new GGE sponsored by the US, with 25 government representatives, has been launched (UNGA Resolution 73/266) and, on the other hand, an Open-ended Working Group promoted by Russia has been created (UNGA Resolution 73/27). The latest group is not incompatible with the former and purportedly more inclusive, as it may incorporate all members of the UN. These two parallel tracks have been recently confirmed,[109] despite the efforts made in order to merge both

104 UNGA, 2015 GGE Report (n. 10).

105 Schmitt, 2017 (n. 9), 2-3.

106 UNGA, Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General of 14 September 2011, A/66/359; UNGA, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary General of 13 January 2015, A/69/723.

107 Stefan Soesanto and Fosca D'Incau, 'The UN GGE is dead: Time to Fall forward', 15 August 2017, <https://www.ecfr.eu>.

108 UNODA, *Developments in the Field of Information and Telecommunications in the Context of International Security*, <https://www.un.org/>, introducing a good account of both processes.

109 UNGA, First Committee, Resolution on Advancing responsible State behaviour in cyberspace in the context of international security, 5 October 2020, A/C.1/75/L.4 (sponsored by the U.S.); UNGA, First Committee, Resolution on Developments in the field of information and telecommunications in the context of international security, 26 October 2020, A/C.1/75/L.8/Rev.1 (sponsored by Russia).

initiatives, e. g. through the Programme of Action.[110] The OEWG has already produced its first Report,[111] though its work will continue with the setting up of a 2021-2025 OEWG (UNGA Resolution 75/240). The most recent development in this field has been the adoption of a GGE Report on 28 May 2021 (not officially published yet), which insists on the applicability of IHL to cyber operations during an armed conflict, together with the due diligence as a voluntary norm. This outcome shows a new, more pro-normative attitude among the UN member States, although it may be at the cost of a slower and more complex process. This pro-normative activity may also be a kind of government reaction to the various private efforts that are taking place recently. Indeed, in addition to the so-called Hague process, in which the 2017 Tallinn II Manual is to be placed, the initiative regarding the Digital Geneva Convention, promoted by Microsoft since 2017,[112] has a prominent role.

b) The Budapest Convention on Cybercrime

If this is what happens at the level of general international regulation regarding cybersecurity, in the most limited area of cybercrime there has been a particular evolution worth of analysis. From the holistic approach towards cybersecurity taken in this paper, we consider cybercrime as a test case where some progress has been achieved regarding the fight against cyber-attacks. This advancement in the cybercrime realm has also been encouraged by the pervasiveness of cyberattacks of private origin, which creates an increasing cost, above $800 billion annually, according to a 2018 report.[113] Therefore, the advanced international cooperation achieved in this field makes it appropriate to focus our attention on this process.

In the field of cybercrime, the Budapest Convention was already adopted in 2001 within the framework of the Council of Europe. It is a convention that very early exemplified the possibilities of successful international cooperation. This convention involves a minimum harmonisation in jurisdictional matters and, specifically, on issues regarding access to digital evidence. Unilateral transborder searches are provided in very limited cases: where the data is publicly available (Art. 32(a)) or disclosed on a voluntary basis (Art. 32

110 <https://front.un-arm.org>.

111 UNGA, 2021 OEWG Report (n. 11).

112 Brad Smith, 'The Need for a Digital Geneva Convention', 14 February 2017, <https://blogs.microsoft.com>.

113 Paul Dreyer *et al.*, 'Estimating the Global Cost of Cyber Risk, Methodology and Examples', RAND, (2018), <https://www.rand.org>.

(b)). However, as in other instances of international legal cooperation, this convention is weighed down by a significant slowness in assistance between Party States (requests take months to be answered), which leads many States to alternatively resort to bilateral instruments known as Mutual Legal Assistance Treaties (MLATs).[114] From a different perspective, it has also been pointed out by NGOs that this Convention allows States to circumvent national safeguards protecting human rights.[115]

As a consequence of the limited effectiveness of the international legal cooperation implemented through the Budapest Convention,[116] States have begun to resort to unilateral mechanisms to deal with the phenomenon of cybercrime of a transnational nature. One of those unilateral avenues is through cross-border hacking. So far, no State has formally charged other States of this type of practice. However, the certainty about the existence of this sort of capabilities indicates that their use has already been carried out in particular situations.[117] On the other hand, there is another unilateral way to access digital evidence, such as the one that involves obtaining direct collaboration from foreign service providers. The advantage of this option is that it makes the intervention of the authorities from the destination or territorial State unnecessary for the requesting State to have access to electronic evidence. This possibility is provided by the 2018 US Cloud Act[118] and it is also envisaged in the proposed E-evidence Directive, which includes a European Production Order.[119]

Precisely, the Council of Europe is trying to address the current underutilisation of the Budapest Convention, so it has started the negotiations leading to the adoption of a new Protocol to the 2001 Convention. This new Protocol aims to introduce simplification in the process of legal assistance between Party States, thus improving the cooperation obtained to date in this regard. The end-result that the Protocol intends to reach would allow the

114 Miriam F. Miquelson-Weismann, 'The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?', John Marshall Journal of Computer & Information Law 23 (2005), 329 ff.

115 Anne Peters, 'Russia and China Are Trying to Set the UN's Rules on Cybercrime', 16 September 2019, <https://foreignpolicy.com>.

116 UNODC, *Comprehensive Study on Cybercrime*, 2013, 201 <https://www.unodc.org/>, according to which, in transnational cybercrime cases, 'only in 25 per cent of cases were international and regional instruments cited as the legal basis'.

117 Philippe Jougleux, Tatiana E. Synodinou and Lilian Mitrou, 'Criminalization of Attacks against Information Systems' in: Ioannis Iglezakis (ed.), *The Legal Regulation of Cyber Attacks* (Alphen aan den Rijn: Kluwer Law International 2020), 116.

118 EPIC, 'The Cloud Act', <https://epic.org>.

119 European Council, 'E-evidence Package: Council Agrees its Position on Rules to Appoint Legal Representatives for the Gathering of Evidence', 8 March 2019, <https://www.consilium.europa.eu>.

DOI 10.17104/0044-2348-2021-3-701

State of origin to make prevail its applicable rules on the matter as a consequence of the exercise of its jurisdiction to prosecute the cybercrime in question. In the meantime, the Council of Europe (CoE) Cybercrime Convention Committee has produced a 2017 Guidance Note on Production Orders, with the aim to address the issue of the storage of data outside the investigating State's territory. Yet, this Guidance has been criticised as a unilateralist transborder access to electronic evidence promoted via soft law.[120]

However, several NGOs have condemned this attempt to elaborate a new Protocol, since they consider that it will surely entail an erosion of the applicable legal standards in the destination State.[121] Taking into account that not only is there no harmonisation of criminal laws among the States of the Council of Europe, but that the national legal systems are very diverse, the areas that could be most affected would be those related to human rights protected in the territorial State, among which must be highlighted the right to privacy and the protection of personal data, as well as the procedural safeguards applicable in that destination State.

c) Developments at the UN Level

Within the United Nations, a proposal by Russia for a Convention on Cybercrime was rejected as early as 2010.[122] In 2011, the Commission on Crime Prevention and Criminal Justice (CCPCJ) created an Expert Group, at the request of the General Assembly, to carry out an exhaustive study on cybercrime, in order to prepare legal or otherwise, national or international responses, to confront this phenomenon.[123]

This comprehensive study on cybercrime was commissioned from the UN Office on Drugs and Crime (UNODC) and completed in 2013.[124] The work of the Group of Experts will continue until 2021 when it is scheduled to complete its task. However, there is disagreement within the UN on how to tackle the scourge of cybercrime. On the one hand, the US and its allies

120 Paul de Hert, Cihan Parlar and Juraj Sajfert, 'The Cybercrime Convention Committee's 2017 Guidance Note on Production Orders: Unilateralist Transborder Access to Electronic Evidence Promoted via Soft Law', Computer Law & Security Review 34 (2018), 327 ff.

121 EDRI, 'New Protocol on Cybercrime: a Recipe for Human Rights Abuse?', 25 July 2018, <https://edri.org>; Katitza Rodríguez, 'The Cybercrime Convention's New Protocol Needs to Uphold Human Rights', 18 September 2017, <https://www.eff.org>.

122 ITProPortal, 'UN Rejects Russian Cyber-Crime Treaty', 21 April 2010, <https://www.itproportal.com/>.

123 UNODC, 'Global Program on Cybercrime', <https://www.unodc.org/>.

124 UNODC (n. 116).

understand that the Budapest Convention is the most adequate ongoing effort to fight cybercrime. Furthermore, the work of the Group of Experts is nearing completion, so that at present it is most convenient to wait to evaluate the results of that work, according to them. On the other hand, Russia and other States have stated that they prefer the elaboration of a new universal text that conveys a global consensus, therefore, a consensus that is not limited to the States party to the Council of Europe. Furthermore, in their opinion, certain mechanisms of the Budapest Convention, such as Article 32(b), constitute an attack on the sovereignty and the jurisdictional authority of the territorial State, since it implies the possibility of evading the prior authorisation of said State on the occasion of obtaining electronic evidence.[125]

In this context, some Western countries were shocked as a Proposal for a Convention on Cybercrime has been recently approved by the UNGA at the end of 2019. Indeed, the majority reached to adopt Resolution 74/247 has shown a divisive vote (79-60-30), but this time in favour of the normative proposal. The projected convention is based on a draft submitted by Russia in 2017.[126] This draft comprised a list of prosecutable cybercrimes (including hacking), the various options for legal cooperation between States, as well as the setting-up of an International Technical Commission. In order to move forward the proposal approved by the UN in 2019, the creation of an open-ended ad hoc intergovernmental committee of experts has been envisaged.

However, this UN proposal has been criticised by Non-Governmental Organizations (NGOs). In an open letter to the UNGA,[127] 36 human rights groups consider that, Russia being its main promoter, the proposal can only lead to greater criminalisation of conduct on the Internet, in line with the larger State control that nations such as Russia or China promote on the Internet. In their opinion, this proposal seeks to go beyond the provisions set forth in the Budapest Convention, so that the possibility of rejecting requests for assistance by the host State is diminished. Furthermore, according to them, the CCPCJ's Group of Experts should be allowed to finish its work in 2021.

125 Summer Walker, 'Cyber-Insecurities? A Guide to the UN Cybercrime Debate', *The Global Initiative against Transnational Organized Crime*, (2019), 5-6.

126 UNGA, Letter dated 11 October 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General of 16 October 2017, A/C.3/72/12.

127 APC, 'Open letter to UN General Assembly: Proposed International Convention on Cybercrime Poses a Threat to Human Rights Online', 6 November 2019, <https://www.apc.org/>.

The proposal for a new UN Convention on Cybercrime is an example of the new, more pro-normative attitude that seems to be consolidating today. Indeed, on the one hand, the Budapest Convention gathers an experience of two decades, with ample approval among States, as there are 65 Party States and many of them have integrated it into their national legislation. In particular, it has been the subject of a Statement in Support from the EU, which, together with the US, rejects the UN proposal.[128]

On the other hand, Russia, China and many developing countries argue that the Budapest Convention represents a limited club of States, far from the global consensus that can be reached at the UN.[129] In fact, this option for a new convention has been gaining weight among UN Member States, either because the foreign policy balances have been changing (there are State Parties to the Budapest Convention, including the Council of Europe, who have voted in favour of the proposal), or because there is a growing appeal around a new Global Treaty on this matter and the resulting reinforcement of State sovereignty that it may entail.

From a legal point of view, it should be borne in mind the consequences derived from the adoption of a new Convention on Cybercrime, which, like the Budapest Convention, seeks to attain global implementation. If there were two conventions on the same subject, it will be necessary to resort to Article 30 of the Vienna Convention on the Law of Treaties in the event of a concrete application. Regardless of the solution to be adopted in each case, by way of a sort of bilateralisation, the truth is that the existence of two general legal frameworks on the same subject is not going to help simplify legal assistance between States. However, as in the case of Human Rights, it may very well be the case that the existence of various self-contained regimes on this subject-matter do not run counter the objective sought, but to the contrary make it more probable the occurrence of international cooperation being achieved in the instance.

IV. Final Remarks

From the point of view of international law, there remain many issues to be solved regarding cybersecurity, either through evolutionary application or norm-development processes.

128 EEAS, 'EU Statement in Support of the Council of Europe Convention on Cybercrime', 15 January 2020, <http://eeas.europa.eu>.

129 UNGA, Official Records, 52nd Meeting of 19 December 2019, A/74/PV.52 (36).

 DOI 10.17104/0044-2348-2021-3-701

As we have seen, dynamic application of international law in cyberspace is not panacea,[130] specifically when relating to the enforcement of international responsibility rules for wrongful acts committed in cyberspace. The UN GGE Reports of 2013 and 2015, as well as the Tallinn Manual, generally take a conservative position on the rules of international law applicable in cyberspace. Not surprisingly, both documents claim to reflect customary law as it applies in this area, although the Tallinn Manual goes much further in its ambition to provide detailed regulation on the subject.

However, it can also be inferred from the analysis above that the Tallinn Manual and some States are inclined to flexibly interpret very particular legal issues, specifically regarding a strong unilateral State's right of reply in case of infringement of international obligations. In particular, it is to be highlighted the main role ascribed to countermeasures and the due diligence obligation, until now very limited to certain special regimes, as a way of ensuring a State's ability to respond to malicious actions carried out on the Net by non-State actors, an aim which, considered in itself, is obviously laudable.

Nevertheless, this kind of reformulation of the due diligence obligation and its use as a means of justifying the implementation of legitimate countermeasures could alter contemporary international relations if States entered into a dynamic of normalisation around their adoption. Indeed, the risk of escalation in such an event exists and should not be underestimated. Fortunately, however, as mentioned earlier, this practice is not being generally observed as States follow an overall strategy of 'wait and see'. Even so, this proposal, which encourages the somewhat exponential use of perfectly legitimate international legal instruments, is preferable to other proposals that seek precisely the opposite, that is, to undermine international legal rules to make way for the law of the strongest. Indeed, some authors seek to lighten the normative 'burden' arising from the existence of certain international legal norms, for example, that relating to State sovereignty, which would enable States to take a more proactive action in cyberspace, on the basis of the greater technological capacity that some enjoy.[131]

Likewise, norm-development is nowadays a very complex and slow process regarding cybersecurity. There is an absence of normative consensus in the international arena, which in turn reveals the confrontation between the position of the US and Western countries, on the one hand, and that of Russia, China, and many DCs, on the other hand. The former countries

130 *Contra*, François Delerue, 'The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?', ESIL Reflections (2018), 4.

131 Corn and Taylor (n. 4).

advocate an evolutionary application of existing standards to cyberspace, while the latter prefer the development of new international rules, as expressed by the OEWG Chair's Summary.[132] The root causes of this lack of consensus are both political, in terms of an open Internet and protection of human rights versus a closed Internet, together with greater State control; and strategic, in terms of the protection of the current technological advantage some enjoy versus the modification of the *status quo*.

This absence of consensus is dangerous for the stability of international relations, as well as for the ability to stop cyberattacks, in addition to the abandonment of State functions that it implies and that explains the proliferation of private regulatory initiatives. Moreover, in the most specific area of cybercrime, a certain paradox is emerging. Perceptions about the defence of State sovereignty at all costs, for whatever reason, prevent progress in terms of norm-development. However, greater cooperation in this field would lead to more effective protection of State interests since, in the current situation, unilateral whims remain frequent.

Even if there are objective reasons to call for either specific primary norms or specific norms of attribution,[133] the lack of agreement among big powers is hindering in the short to medium term any norm-development effort, undertaken by the United Nations or otherwise. Only regional initiatives (European Union [EU], CoE) seem to have success, if geographically limited, which in turn may make it more difficult to achieve any advancement from the point of view of general international law. Yet, this outcome is not the only possible one, as witnessed in the Human Rights realm, where self-contained regimes and general international law have evolved on parallel with positive results.

Truly, there is an impasse situation regarding cybersecurity. On the one hand, evolutionary application has been useful to a certain extent until now, but some proposals have important limits when flexibility in interpreting international law rules may lead to destabilising international relations. On the other hand, norm-development which is much wanted to complete the gaps left by interpretation of existing international law is nowadays very slow and very difficult to achieve. However, improving cybersecurity is a public good that is in need of a solid fostering effort. Therefore, the central argument advanced in this paper was that international cooperation needs to be enhanced if we want international law to be relevant in the near future in addressing cyberattacks, both attributable and non-attributable to States.

132 UNGA, 2021 OEWG Chair's Summary (n. 37), para. 16.

133 Andreas Zimmermann, 'International Law and "Cyber Space"', ESIL Reflections (2014), 3.

 DOI 10.17104/0044-2348-2021-3-701

Hence this paper serves as a legal critique of the mainstream position expressed by many Western governments and scholars.

Firstly, this paper supports as a way forward the enhancement of the international cooperation needed to set up a centralised mechanism for attribution, through the establishment of an international council or otherwise, that helps in the task of making public attributions of wrongful cyber operations through a process of impartial fact-finding. This way, the allocation of international responsibility would achieve the legitimacy needed in this field, where we find very advanced technological States together with other States that do not have the same technological capabilities. This improvement would open the door to the adoption of more legitimate countermeasures, or even public sanctions (e. g., the EU Cyber Diplomacy Toolbox), diminishing the need to resort to bilateral countermeasures where attribution is not well proved, countermeasures instrumented through the due diligence obligation, or the difficult-to-justify state of necessity. The application of existing international law rules would be facilitated, instead of unnecessarily stretched, this way reinforcing the rules-based international order.

Second, the OEWG seems to be gaining ground as the central forum to accomplish the cybersecurity goal and the most convenient avenue to foster legal engagement among the main players. This is not to say that the GGE will not help to finally reach a much-needed agreement. However, even if the interests at stake are very much in opposition from the start, the OEWG deserves to be considered as a convenient setting where cybersecurity must be built up from a legal point of view. Likewise, in the more limited realm of cybercrime, a new majority within the UNGA points towards a growing consensus on a UN Convention on this topic. As we have seen, the issue of access to digital evidence is crucial in order to fight against cybercrime but it is a particularly delicate problem when jurisdictional overreach is perceived as infringing State sovereignty. The UN legal avenue is worth of exploring, as the work developed regarding jurisdictional cooperation in this field may also help advance the task of developing norms in other cybersecurity-related areas.

DOI 10.17104/0044-2348-2021-3-701