Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors

Kubo Mačák[1]

Abstract

Cyber operations pose a set of novel challenges to the generally conservative body of the law of State responsibility. Central among them is the problem of attribution, which lies at the intersection of technology and law. This article reflects the recent developments in the States' technological capacity to identify the sources of cyber attacks from the perspective of international law. It revisits Article 8 of the International Law Commission's Articles on State Responsibility in order to 'decode' its contents vis-à-vis its drafting history and with an eye on its future application to the conduct in cyberspace. The article argues that there are three autonomous standards of attribution built into that provision: instructions, direction, and control. It then demonstrates the utility and limitations of each of them against the backdrop of actual and hypothetical cyber operations. The article concludes with suggestions for further development of the law in this area, focussing on the missing potential of the law to regulate instigation of wrongful cyber conduct and on the prohibitively strict test of control applicable *de lege lata*.

1. Introduction

Not uncommonly among other late-medieval timepieces and sundials, the magnificent astronomical clock in Exeter Cathedral bears the Latin inscription '*Pereunt et imputantur*'. They—meaning the hours—pass and are reckoned to our account.[2] This principle, supposed to apply to the medieval sinners and their actions in the physical world around them, should equally hold for modern actors straddling the divide between the offline and the online realms. The conduct in cyberspace surely is reckoned: but to whose account?

---

[1] Lecturer in Law at the University of Exeter, Exeter, UK. E-mail: k.macak@exeter.ac.uk. I would like to gratefully acknowledge the generous support of the Minerva Center for the Rule of Law under Extreme Conditions at the Faculty of Law and Department of Geography and Environmental Studies, University of Haifa, Israel and of the Israeli Ministry of Science, Technology and Space. Earlier versions of this article were presented at the conference on Non-State Actors and Responsibility in Cyberspace at the University of Sheffield on 18 September 2015 and at the Cyberspace Conference at Masaryk University in Brno, Czech Republic on 27 November 2015. I am grateful to the participants for their feedback and suggestions. I would like to especially thank Ana Beduschi, Rob Merkin, Aurel Sari, Mike Sanderson, Michael N. Schmitt, Chantal Stebbings, Nicholas Tsagourias, and Vassilis Tzevelekos for their helpful comments on earlier drafts of this article. The usual disclaimer applies.

[2] Despite its obvious religious meaning underlined by its location, this phrase originated in the satirical writings of the 1st century Roman poet Martial. For more on the context of the phrase and its English translation, see Peter Howell, *Martial* (Duckworth 2008) 19–20.

This article revisits the standards of attribution of private conduct under the law of State responsibility, which are an essential element of any effort to answer that very question. Today, initial doubts as to whether international law applies in cyberspace[3] have largely disappeared, replaced by consistent State practice confirming the applicability of this body of law to cyber operations.[4] Importantly, this includes the law of State responsibility as the paradigm regime of international responsibility under international law.[5] Yet, although we now know that cyberspace is not a lawless world, how precisely international legal rules apply within it is still far from settled.

One of the cornerstones of the law of State responsibility is the longstanding principle that States are normally not responsible for the acts of private or non-State actors.[6] On closer scrutiny, this requires some qualification. Indeed, who else is there to act for States—fictitious entities that they are—if not individual human beings, in other words, non-State actors? It is thus more accurate to say that each act of a State is 'nothing but the activity of individuals that the law imputes to the State'.[7] These imputable (attributable) types of conduct must include those that a State would not want to carry out directly through its own organs.[8] Otherwise States would be able to escape responsibility simply by outsourcing their 'lower work'[9] to private groups and individuals. Recent press reports carrying headlines such as 'Cyber Crime: States Use Hackers To Do Digital Dirty Work' illustrate that outsourcing of this kind has now become a recurrent feature of the online world, as well.[10]

Consequently, a breach of international law carried out through a private entity acting on behalf of a State may trigger the responsibility of that State. This much is recognized in Article 8 of the International Law Commission's Articles on State Responsibility:[11]

---

[3] See, eg, JP Barlow, 'A Declaration of the Independence of Cyberspace' (1995) <https://projects.eff.org/~barlow/Declaration-Final.html> (all internet resources were last accessed on 20 March 2016); DR Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367.

[4] UN Doc A/65/154 (2010), 15 (United Kingdom); UN Doc A/68/156/Add.1, 4 (Canada); ibid 12 (Iran); ibid 15 (Japan); ibid 16-17 (Netherlands); UN Doc A/66/152 (2011) 6 (Australia); ibid 18 (US); UN Doc A/68/156 (2013) 18 (United Kingdom); UN Doc A/69/112 (2014) 16 (Switzerland).

[5] Michael N Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (CUP 2013) ('*Tallinn Manual*') 29–41. For statements of State representatives, see, eg, HH Koh, 'International Law in Cyberspace' (2012) 54 Harvard International Law Journal Online 1, 6 (US position); UN Doc A/68/156/Add.1 (2013), 9 (Germany); UN Doc A/68/156/Add.1, 13 (Iran). In 2015, a group of governmental experts representing 20 States from all geographic regions of the world unanimously agreed to use the language of the law of State responsibility to the conduct in cyber space. See Report of the 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) 7–8 and 12–13.

[6] See, eg, Cedric Ryngaert, 'State Responsibility and Non-State Actors' in Math Noortmann, August Reinisch, and Cedric Ryngaert, *Non-State Actors in International Law* (Hart 2015) 163.

[7] Dionisio Anzilotti, *Cours de droit international* (1929, republished Editions Panthéon-Assas 1999) 469.

[8] Olivier de Frouville, 'Attribution of Conduct to the State: Private Individuals', in James Crawford, Alain Pellet, Simon Olleson (eds), *The Law of International Responsibility* (OUP 2010) 266.

[9] Paul Reuter, *Le développement de l'ordre juridique international: Ecrits de droit international* (Economica 1995) 377.

[10] Sam Jones, 'Cyber Crime: States Use Hackers To Do Digital Dirty Work', *Financial Times* (4 September 2015) <http://on.ft.com/1JHBuds>.

[11] International Law Commission (ILC), Articles on the Responsibility of States for Internationally Wrongful Acts, UN GA Res 56/83 annex, UN Doc A/RES/56/83 (12 December 2001) ('ASR').

> The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.[12]

This provision structurally belongs to chapter II of part 1 of the Articles, which codifies general international law standards of attribution[13] applicable in the absence of a special standard.[14] Article 8, as well as the majority of the document as a whole, is generally considered to reflect customary international law.[15]

Although it certainly is 'particularly relevant in the cyber context',[16] its application to cyber operations poses a number of significant challenges. First, as a precondition for any legal attribution, is it even technically possible to attribute online conduct to its true author? Second, which standard or standards of attribution should be read into Article 8 and how do these apply to cyber operations? Third, does the emergence of new technologies and the fact of inter-State clashes in the virtual world necessitate the development of the applicable law? This article examines each of these issues in turn and puts forward a nuanced and context-adjusted reading of Article 8. It concludes with suggestions for the further evolution of the relevant law with a particular focus on instigation of wrongful cyber conduct and on the applicable test of control.

Before discussing the applicable law, it should be noted that this article does not look further into evidentiary issues.[17] It is true that international law may be seen as lacking clarity as to the applicable standards of evidence in relation to the present matter. However, questions of evidence logically only become relevant once the rules of substance are properly understood. In other words, it is necessary to first understand how the relevant rules of the law of State responsibility apply to the facts at hand before considering the standard of proof to which the compliance with or the violation of those rules needs to be proven. This approach corresponds to the International Law Commission's general approach of maintaining a clear divide between substantive and evidentiary rules in its study of the law of State responsibility.[18]

2. Attribution problem

[12] Art 8 ASR.

[13] See art 4–11 ASR.

[14] See art 55 ASR.

[15] See, eg, ICJ, *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Bosnian Genocide)* (Judgment) [2007] ICJ Rep 91 [385] and [398] (re article 8); ICSID, *Noble Ventures v Romania*, Case No ARB/01/11 (12 October 2005) [69] (re entire document).

[16] *Tallinn Manual* (n 5) 32.

[17] [Cross-reference to article(s) on evidentiary aspects of cyber operations in the same issue]

[18] See, eg, ASR, commentary to ch III, para 4 ('Questions of evidence and proof of such a breach fall entirely outside the scope of the articles.'); ibid, commentary to art 19, para 8 ('Just as the articles do not deal with questions of the jurisdiction of courts or tribunals, so they do not deal with issues of evidence or the burden of proof.').

In the past, the problem of technical attribution in cyberspace was considered virtually unsolvable without either an unambiguous admission by the perpetrating State[19] or at least a clearly linked follow-up kinetic attack revealing the author of the cyber operation in question.[20] Accordingly, States refrained from making any pronouncements about the responsibility of their counterparts. As late as 2002, the United States (US) White House cyber security advisor Richard Clarke publicly admitted that the US had not yet had any evidence linking another State to a particular cyber attack.[21]

For a long time, even the most prominent of attacks, which have triggered waves of speculation in the media, had gone without official apportionment of the blame. For instance, although Iran paid a heavy price as a result of the Stuxnet virus, which reportedly caused the destruction of about 20% of Iran's nuclear centrifuges,[22] its representatives never issued an official statement in connection with the incidents.[23] One early exception to this general trend merits a mention. In the immediate aftermath of the 2007 cyber attacks against the Estonian government, the Estonian foreign minister wrote: 'The European Union is under attack, because *Russia is attacking Estonia*.'[24] However, this bold statement was soon mitigated by an admission of another government member that Estonia did not in fact have sufficient evidence linking the attacks to Russian authorities.[25]

States' reticence to formally attribute cyber operations used to prevail even when the origin of the attack was traced with a considerable degree of certainty. For instance, in the late 1990s, the US government suffered a large-scale network intrusion aimed at the exfiltration of vast amounts of data, referred to today as the 'Moonlight Maze breaches' after the eponymous FBI-led inquiry.[26] The US government investigators were able to conclude on the basis of digital forensic data as well as a combination of intelligence sources that these large-scale exfiltrations of US government data originated with the Russian government.[27] Despite that, no official statement attributing the attacks to Russia has ever been made.

---

[19] So far, this has not happened. Significantly, the UK became the first State to openly admit to building offensive cyber capabilities in September 2013. See UK, 'New cyber reserve unit created' (29 September 2013) <https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit>.

[20] Yoram Dinstein, 'Computer Network Attacks and Self-Defense' in Michael N Schmitt and Brian T O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College 2002) 112.

[21] Testimony of Richard Clarke, Special Advisor to the President for Cyberspace Security, Senate Judiciary Committee, Administrative Oversight and the Courts Subcommittee (13 February 2002) <http://www.techlawjournal.com/security/20020213.asp>.

[22] Michael B Kelley, 'The Stuxnet Attack on Iran's Nuclear Plant Was "Far More Dangerous" Than Previously Thought' *Business Insider* (20 November 2013) <http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11>.

[23] See, eg, Terry Pattar, 'Cyber Attacks in the Middle East' *Current Intelligence* (29 July 2013) <http://www.currentintelligence.net/analysis/2013/7/29/cyber-attacks-in-the-middle-east.html>.

[24] 'Statement by the Foreign Minister Urmas Paet' *Eesti Päevaleht* (1 May 2007) <http://epl.delfi.ee/news/eesti/statement-by-the-foreign-minister-urmas-paet?id=51085399> (emphasis added).

[25] 'Estonia Says Cyber-Assault May Involve the Kremlin' *The New York Times* (17 May 2007) <http://nyti.ms/1M7k8eD>; see also 'Estonia Has No Evidence of Kremlin Involvement in Cyber Attacks' *RIA Novosti* (6 September 2007) <http://sptnkne.ws/2QP>

[26] See further Adam Elkus, 'Moonlight Maze' in Jason Healey (ed), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (CCSA 2013) 152–163.

[27] Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks' (2014) 38 Journal of Strategic Studies 1, 9.

Yet, it appears that the tide has begun to turn. In 2012, the then US Defence Secretary Leon Panetta announced that the US had made major progress with respect to the problem of attribution, warning potential perpetrators that the US now had 'the capacity to locate them and to hold them accountable for their actions that may try to harm America'.[28] Although this purported US capacity has not gone unchallenged by other key players,[29] the increased confidence in the attribution potential has been echoed by other States[30] and has recently been reflected in the newly issued US Department of Defense (DoD) Cyber Strategy.[31] There is no doubt that attribution in cyberspace is still fraught with evidentiary difficulties, a challenge admitted even by the US as recently as in June 2015.[32] Nevertheless, since the ability to attribute at least some cyber operations to their source is now increasingly considered within the realm of the possible, it is essential to analyse the relevant rules.

3. Article 8 decoded

Article 8 of the Articles on State Responsibility is the central provision governing the attribution of the conduct of private or non-State entities to States. This is because, on the one hand, if the actual link between a State and a non-State actor falls short of the requirements stipulated by this provision, the State will not be responsible for the acts in question.[33] However, on the other hand, if the said relationship outgrows these requirements and becomes one of 'complete dependence' of the non-State actor on the State,[34] the former will be considered a *de facto* organ of the latter, thus removing the situation from the scope of Article 8 altogether and leaving the State responsible under Article 4.[35] Therefore, understanding the terms of Article 8 is crucial for the establishment of State responsibility for the conduct of non-State actors. This section aims to unravel the text of this provision and examine the origin and relationship of the legal standards contained therein.

As a starting point, the International Law Commission (ILC) commentaries seem to identify three autonomous criteria in Article 8: 'the three terms "instructions", "direction" and "control" are disjunctive; it is sufficient to establish any one of them.'[36] However, the remainder

---

[28] Zachary Fryer-Biggs, 'DoD's New Cyber Doctrine: Panetta Defines Deterrence, Preemption Strategy' *DefenseNews* (13 October 2012) <http://archive.defensenews.com/article/20121013/DEFREG02/310130001/DoD-8217-s-New-Cyber-Doctrine> (emphasis added).

[29] See, eg, Adam Segal, 'A Chinese Response to the Department of Defense's New Cyber Strategy' *Net Politics* (7 May 2015) <http://blogs.cfr.org/cyber/2015/05/07/a-chinese-response-to-the-department-of-defenses-new-cyber-strategy/>.

[30] See, eg, Canada, Statement by the Chief Information Officer for the Government of Canada (29 July 2014) <http://news.gc.ca/web/article-en.do?nid=871449>.

[31] US, Department of Defense, Cyber Strategy (2015) <http://www.dtic.mil/doctrine/doctrine/other/dod_cyber_2015.pdf> 10–12.

[32] US, Department of Defense, Law of War Manual (June 2015) <http://www.dod.mil/dodgc/images/law_war_manual15.pdf> para 16.3.3.4.

[33] ASR, commentary to art 8, para 1.

[34] See ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v US)* (Merits) [1986] ICJ Rep 14 [110]; *Bosnian Genocide* (n 15) [391]–[406].

[35] See art 4 ASR ('Conduct of organs of a State'); see further text corresponding to notes 106–110 below.

[36] ASR, commentary to art 8, para 7.

of the commentary is more ambiguous. To begin with, the very title of Article 8 omits a reference to the first of the criteria: 'Conduct directed or controlled by a State'.[37] Moreover, the commentary does not provide any definitions of the three key terms and, apart from the acknowledgement quoted above, it in fact treats 'direction' and 'control' as synonymous.[38]

The tendency to collapse the three criteria together is actually quite common. This should not be too surprising given that even in common parlance, the three terms are used interchangeably. For example, the respected Oxford English Dictionary uses 'instruction' to define 'direction'[39] and 'directing' to define 'control'.[40] Although many academic writers echo the ILC's description of the criteria as disjunctive,[41] on closer reading, this mostly amounts to little more than lip service.

In practice, commentators tend to conflate all or some of the criteria. Most often, this concerns 'direction' and 'control'. First and foremost, the ambiguous approach of the ILC has been reflected in Professor Crawford's academic writing, as well.[42] Interestingly, although his monograph on State responsibility justifies this conflation by noting that 'courts and tribunals have tended to interpret the words "direction or control" as imposing a single standard of attribution'", the text cites no cases to support this proposition.[43] Others have followed the same path of treating 'direction' and 'control' as synonymous or, more accurately, as providing a single criterion of attribution only.[44] In addition to Professor Crawford's position set out above, this view has at times been assumed tacitly without further explanation[45] or supported by the strictly

---

[37] Art 8 ASR.

[38] See ASR, commentary to art 8, paras 3 et seq.

[39] 'direction, n.' in *The Oxford English Dictionary Online* (OUP 2016) <http://www.oed.com/view/Entry/53301?redirectedFrom=direction> point 1(c) ('The action or function of directing … of instructing how to proceed or act aright; authoritative guidance, *instruction*.') (emphasis added).

[40] 'control, n.' in *The Oxford English Dictionary Online* (OUP 2016) <http://www.oed.com/view/Entry/53301?redirectedFrom=control> point 1(a) ('The fact of controlling, or of checking and *directing* action; the function or power of *directing* and regulating; domination, command, sway.') (two emphases added).

[41] See, eg, Avril McDonald, 'Ghosts in the Machine: Some Legal Issues Concerning US Military Contractors in Iraq' in Michael N Schmitt and Jelena Pejic (eds) International Law And Armed Conflict, Exploring the Faultlines (Martinus Nijhoff 2007) 396; Robert McCorquodale and Penelope Simons, 'Responsibility Beyond Borders: State Responsibility for Extraterritorial Violations by Corporations of International Human Rights Law' (2007) 70(4) Modern Law Review 598, 608 fn 71; Amanda Tarzwell, 'In Search of Accountability: Attributing the Conduct of Private Security Contractors to the United States Under the Doctrine of State Responsibility' (2009) 11 Oregon Review of International Law 179, 193; Brigitte Stern, 'The Elements of An Internationally Wrongful Act' in Crawford, Pellet, and Olleson (n 8) 206; James Crawford, *State Responsibility: The General Part* (CUP 2013) 146; Róisín Sarah Burke, *Sexual Exploitation and Abuse by UN Military Contingents* (Martinus Nijhoff 2014) 282; Robert Heinsch, 'Conflict Classification in Ukraine: The Return of the "Proxy War"?' (2015) 91 International Law Studies 323, 348; Helen Duffy, *The 'War on Terror' and the Framework of International Law* (2nd edn, CUP 2015) 108.

[42] See Crawford (n 41) 146 et seq.

[43] Crawford (n 41) 146 (text corresponding to fn 28). See also text corresponding to notes 87–90 below (noting the endorsement of the disjunctive approach by the ICJ in the *Bosnian Genocide* case).

[44] See, eg, André JJ de Hoogh. 'Articles 4 and 8 of the 2001 ILC Articles on State Responsibility, the *Tadić* Case and Attribution of Acts of Bosnian Serb Authorities to the Federal Republic of Yugoslavia' (2002) 72 British Year Book of International Law 255, 277–278; Tarzwell (n 41) 193; Hannah Tonkin, *State Control over Private Military and Security Companies in Armed Conflict* (CUP 2011) 58–59; Heinsch (n 41) 348.

[45] See, eg, Tonkin (n 44) 58–59.

grammatical interpretation that there is no 'comma before the "or"', and thus 'direction or control' ought to be seen as a single category.[46]

Less frequently, we can come across the tendency to conflate the first and second criteria. The central proponent of this interpretation was the late Professor Cassese, for whom the affinity between the two terms was in their 'rather specific' nature: 'the issuance of instructions or the fact of directing persons or groups of persons to do something involves ordering or commanding those persons to undertake a certain conduct'.[47] In contrast, he viewed the test of control as 'rather loose', justifying a layered approach to the required degree of control that he had spearheaded during his time at the International Criminal Tribunal for the former Yugoslavia (ICTY).[48]

Although these tendencies certainly indicate that many leading international law scholars consider the nuances between the three terms in Article 8 as miniscule or even non-existent, an examination of the historical provenance of the formulation of that provision shows that the ILC did in fact intend to differentiate them from one another. The history of Article 8 reveals that the present wording is actually the result of three evolutionary steps.

First, the ILC's Special Rapporteur Roberto Ago proposed what could be denoted as the original narrow wording. In his 1974 draft, the predecessor of today's Article 8 provided that the conduct of a person or group of persons would be attributable to a State if 'it is established that such person or group of persons was in fact *acting on behalf of* that State'.[49] The attached commentary clarified that for conduct to be seen as undertaken 'on behalf of' a State, it had to 'be genuinely proved that the person or group of persons were actually appointed by organs of the State to discharge a particular function or to carry out a particular duty, that they performed a given task at the instigation of those organs'.[50] In other words, the provision would have covered cases of 'actual agency' only but would not extend to less formalized and more fact-based types of State control.[51]

Secondly, after Professor Crawford assumed the position as the ILC's Special Rapporteur, he proposed to broaden Ago's original formulation and replace it with what could be called the intermediate semi-disjunctive wording. According to his proposal, the conduct of a non-State actor would also be attributed to a State if '[t]he person or group of persons was in fact acting on the instructions of, or under the *direction and control* of, that State in carrying out the conduct'.[52] This novel proposal was motivated[53] by a desire to bring the draft in line with the usage of the terms in ordinary language but also with the analysis by the International Court of Justice (ICJ) in

---

[46] Heinsch (n 41) 348.

[47] Antonio Cassese, 'The *Nicaragua* and *Tadić* Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia' (2007) 18(4) EJIL 649, 663.

[48] Ibid.

[49] ILC, Yearbook (1974) vol II(1) 283 (draft art 8(a)) (emphasis added).

[50] Ibid 284–285 (commentary to art 8, para 8); see also *Nicaragua* (n 34) sep op Judge Ago [16] (attribution requires a 'specific charge').

[51] ILC, Yearbook (1998) vol II(1) 40 [197].

[52] Ibid 56.

[53] See ibid 40–43.

the 1986 *Nicaragua* ruling.[54] This may appear somewhat surprising from today's vantage point as the judgment is perceived as embodying a rather strict standard of attribution.[55] Nonetheless, for Professor Crawford, the ruling permitted attribution even without a 'specific charge' and solely on the basis of 'the exercise of command and control in relation to a particular operation'.[56] He endorsed this interpretation as a step in the right direction, noting that 'in many operations, in particular those which would obviously be unlawful if attributable to the State, the existence of an express instruction will be very difficult to demonstrate'.[57] The formulation[58] he proposed on the basis of this reasoning is described as semi-disjunctive here, because it included a disjunction as between instructions on the one hand and direction and control on the other hand, while still using direction and control as a single joint standard of attribution.

In the third and final step, the ILC replaced the conjunction 'and' between 'direction and control' with the disjunctive 'or'.[59] The Drafting Committee of the ILC thus modified Special Rapporteur Crawford's version as it 'did not believe that the scope of article 8 should be restricted through a cumulative requirement in that regard.'[60] This formulation was retained in the text endorsed by the General Assembly in 2001 and may thus be called the final disjunctive wording.

Three salient features of this development should be noted. First, the formulation of Article 8 has evolved from the general and 'less than clear'[61] single criterion of acting on behalf of a State to the three specific categories of instructions, direction, and control. Second, the trend has been to move from a more restrictive to a more permissive wording, covering not only cases of actual agency, but also less formalized types of association between States and non-State actors.[62] Third, the replacement of 'and' for 'or' between 'direction' and 'control' has meant that the Commission included three autonomous criteria of attribution in the final text of Article 8.[63] The UN General Assembly endorsed the final text of the Articles and expressly commended it to all governments, giving it a more authoritative status in contrast to other ILC outputs.[64]

In the next section, we turn to the individual criteria set out in Article 8 and how they apply to cyber operations. Before analysing when any of these criteria will be met, it should be noted that some considerations are irrelevant for a finding of attribution in general. First, the association of private individuals with a State need not have any basis in the domestic law of that State.[65] Second, whether the group of individuals has any specific legal form or exists purely on a

---

[54] *Nicaragua* (n 34).

[55] See section 4.3 below.

[56] ILC, Yearbook (1998) vol II(1) 41 para 204.

[57] Ibid 43 para 212.

[58] See text corresponding to note 52 above.

[59] See ILC, Yearbook (1998) vol I, 289 para 79.

[60] Ibid.

[61] ILC, Yearbook (1998) vol II(1) 43 para. 212.

[62] See further text corresponding to notes 135–141 below.

[63] Accord de Frouville (n 8) 271.

[64] See UN GA Res 56/83, UN Doc A/RES/56/83 (12 December 2001) para 3.

[65] Luigi Condorelli and Claus Kress, 'The Rules of Attribution: General Considerations' in Crawford, Pellet, and Olleson (n 8) 230.

de facto basis is equally immaterial.[66] In this connection, writers have lamented the malleable and ever-changing identities characteristic of many online actors. For instance, Klimburg noted that a Chinese 'information-warfare militia unit' may 'be, *at the same time*, a university IT department, an online advertising agency, an online gaming clan, a patriot-hacker team, and a local cyber-crime syndicate engaged in software piracy'.[67] Nonetheless, from the perspective of international law, the type or even the lack of any domestic legal status of such groups is immaterial for attribution purposes.

4. Attribution criteria

4.1. Instructions

Under the first of the three criteria, a State issues instructions to a non-State actor, requesting it to engage in the conduct in question. The criterion of instructions is the post-2001 equivalent of Roberto Ago's 'specific charge' or James Crawford's 'actual agency'. These terms serve to denote that a State decides to engage in a particular act and instructs a non-State entity to do so on its behalf. Such an entity must not have been empowered by the domestic law to exercise elements of governmental authority, as then its conduct would fall within the scope of Article 5 of the Articles on State Responsibility.[68] In the physical world, examples of acting on instructions in the sense of Article 8 include individuals outside official State structures who are employed by the State as 'auxiliaries' or sent to third States as 'volunteers' charged with specific tasks.[69] In the context of cyber operations, if a State specifically instructed an IT department within a university to carry out a Distributed Denial of Service (DDoS) attack against a designated target, the resulting operation would be attributable to the State in question.

In order for this—arguably the most stringent—criterion to be met, the non-State entity must be factually subordinate to the State at the moment when the State decides to commit the acts in question.[70] This can be corroborated simply by the fact of accepting the instructions and then acting on them. However, a general 'rallying call' by the State encouraging likeminded but unspecified 'patriotic' hackers to engage in offensive action would not suffice for the purposes of attribution. As held by the ICJ in the *Bosnian Genocide* case, the instructions must be given specifically 'in respect of each operation in which the alleged violations occurred'.[71]

Similarly, the fact of a goal shared by the State and the private actor is insufficient without further evidence establishing the subordination between the two and the issuance of instructions by the former to the latter. For example, it has been noted that the targets of a non-State cyber entity Honker Group based in China have included Indonesia, Taiwan, and the US, Japanese

[66] ASR, commentary to art 8, para 9.

[67] Alexander Klimburg, 'Mobilising Cyber Power' (2011) 53 Survival 41, 47.

[68] ASR, commentary to art 5, para 7.

[69] ASR, commentary to art 8, para 2.

[70] Lindsey Cameron and Vincent Chetail, *Private Military and Security Companies under Public International Law* (CUP 2013) 205.

[71] *Bosnian Genocide* (n 15) [400].

institutions, and a Tibetan political dissident.[72] Although the choice of targets may suggest an alignment of goals between the Honker Group and the Republic of China,[73] it would be incorrect to draw the conclusion that the acts of the former are solely on that basis attributable to the latter in law. While shared goals may indicate political alignment and may thus suffice for the purposes of political attribution, the same cannot be said for the establishment of legal liability.

This conclusion applies equally to acts instigated or encouraged by a State. In the absence of a hierarchical relationship between the State and a non-State group, such encouragements may be morally reprehensible but do not suffice for the purposes of attribution under the present state of the law. By way of example, in the context of the Estonian incidents of 2007, speculations arose that Russian government agents used various chatrooms and other online fora to incite Russian patriotic hackers to strike against Estonian networks.[74] Interestingly, the goal 'to inculcate in the people patriotism and values' openly proclaimed in the Russian Information Security doctrine valid at the time may seem to support the veracity of these reports.[75] However, even that would not make Russia responsible for the eventual conduct of the private hackers frequenting these online groups.[76] Of course, Russia would remain responsible for the acts of its own agents given that these must be considered State organs.[77] However, there is no international law rule prohibiting incitement of wrongful conduct in general,[78] as opposed to specific rules prohibiting, for example, incitement to genocide[79] or discrimination.[80] Therefore, it can be concluded that similar State conduct, encouraging cyber attacks against other States, remains *praeter legem* for the time being.

Additionally, the resulting act must be traceable in its material components back to the instructing State. This does not mean that the State must specify exactly all the details of the act to be undertaken. On the contrary, if it issues intentionally vague instructions, it opens itself to the risk that these will be interpreted in a way giving rise to the State's responsibility for the

---

[72] Laura Saporito and James A Lewis, 'Cyber Incidents Attributed to China' *Center for Strategic and International Studies* (13 March 2014) <http://csis.org/files/publication/130314_Chinese_hacking.pdf> 4.

[73] See, eg, Mike Chapple and David Seidl, *Cyberwarfare: Information Operations in a Connected World* (Jones & Bartlett 2014) 155 ('The Honker Union [has] waged cyberwarfare against targets whose views and actions conflict with those of the Chinese government.').

[74] See, eg, James A Lewis, 'Cyber Attacks Explained' *Center for Strategic and International Studies* (15 June 2007) <http://csis.org/files/media/csis/pubs/070615_cyber_attacks.pdf>.

[75] Richard M Harrison, 'Getting on the same wavelength' *Washington Times* (8 July 2013) <http://www.washingtontimes.com/news/2013/jul/8/getting-on-the-same-wavelength/>.

[76] But see, eg, Scott Shackelford and Richard B Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2010) 42 Georgia Journal of International Law 971, 992–993 (arguing that 'if it were possible to prove Russian … incitement behind the cyber attacks' in question, this would suffice for the attribution of responsibility under the overall control standard).

[77] Art 4 ASR.

[78] ASR, commentary to art 15, para 9.

[79] Convention on the Prevention and Punishment of the Crime of Genocide (adopted 9 December 1948, entered into force 12 January 1951) 78 UNTS 277 ('Genocide Convention') art III.

[80] International Convention on the Elimination of All Forms of Racial Discrimination (adopted 7 March 1966, entered into force 4 January 1969) 660 UNTS 195 ('CERD') art 4; International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 ('ICCPR') art 20(2).

resulting course of conduct.[81] However, for the purposes of attribution the original instructions must manifest the will of the State to authorise the unlawful conduct, however broadly they may be phrased. For instance, in the context of the Iranian revolution of 1979, the Ayatollah Khomeini called on the youth of Iran 'to expand with all their might their attacks against the United States and Israel' in order to effectuate the return of the shah.[82] The ICJ later held in the *Tehran Hostages* case that this general call cannot be interpreted to have amounted to 'an authorization from the State to undertake the specific operation of invading and seizing the United States Embassy'.[83] The original statement of the Ayatollah, even if inflammatory, did not contain a manifestation of a specific desire on part of the State of Iran to occupy the embassy.

Likewise, a State will not incur responsibility for conduct that exceeds the express instructions by going beyond what is incidental to the authorized course of action.[84] Such behaviour would amount to conduct *ultra vires* and attributing it to the State would go against the general presumption against attribution of private conduct. By way of example, we may imagine that a State tasks a private company with a one-off risk and vulnerability assessment of its government networks. If the employees of the company go beyond this authorization and use their access to the networks to launch a cyber attack against another State, the instructing State would not bear the responsibility for the attack in question as it would clearly be *ultra vires* with respect to the original instructions.

4.2. Direction

The criterion of direction is possibly the least studied of the three standards of attribution contained in Article 8. As noted above, it is often conflated with one of the other two.[85] However, the examination of the historical development of this provision demonstrates that such conflation is inaccurate and that the term is meant to have an autonomous meaning.[86] What exactly this meaning entails remains unanswered in the literature and international jurisprudence. Accordingly, the following lines first advance a concrete conceptualization and then test it against one of the most prominent cyber operations, the Stuxnet virus attack.

One of very few international cases, in which the parties devoted any attention to the meaning of 'direction' in the context of Article 8, was the *Bosnian Genocide* case before the ICJ,[87] in which attribution of acts of non-State actors was one of the central issues.[88] In his oral pleadings, Professor Alain Pellet acting for Bosnia and Herzegovina, described 'direction' as 'a less rigorous term than "instructions"'.[89] This description was not challenged in the course of the proceedings. The Court eventually held that the criterion is met "where an organ of the State …

---

[81] Tonkin (n 44) 116; Crawford (n 41) 145; Cameron and Chetail (n 70) 207.

[82] ICJ, *United States Diplomatic and Consular Staff in Tehran (Tehran Hostages)* (Judgment) [1980] ICJ Rep 3 [59].

[83] Ibid.

[84] ASR, commentary to art 8, para 8.

[85] See text corresponding to notes 42–48 above.

[86] See analysis in section 3 above.

[87] *Bosnian Genocide* (n 15).

[88] Ibid [396]–[412].

[89] *Bosnian Genocide* (n 15) CR 2006/8 [62] (Pellet).

provided the direction pursuant to which the perpetrators of the wrongful act acted".[90] The wording used by the Court implies the need for a continuing relationship between the State and the non-State actor in question, one that goes beyond the simple issuance of instructions with no further follow-up.

Although Professor Crawford generally treated direction and control as a single standard,[91] in an exceptional footnote devoted solely to the former, he made a helpful suggestion not dissimilar from the ICJ's explanation reproduced above. He noted that "'[d]irection" implies a continuing period of instruction, or a relationship between the state and a non-state entity such that suggestion or innuendo may give rise to responsibility.'[92] The modal verb 'may' is apposite here as it is doubtful States would accept the attribution of responsibility *solely* on the basis of 'suggestion or innuendo' arising from State organs. As we have seen, instigation and encouragement are not sufficient grounds for attribution in the present state of the law. Logic then requires that suggestion or innuendo—as less demanding forms—would not suffice either. The key ingredient here is the requirement of a *relationship* between the State and the non-State actor. If a State nurtures a relationship of subordination with an individual or a group of individuals outside of formal State structures and guides the conduct of such private actors,[93] it may incur responsibility for their individual acts even in the absence of express instructions to commit those acts.

Evidence that a subordinate relationship of this kind exists may take a number of forms. In the *US-DRAMS* report, the WTO Appellate Body held that in most cases, 'direction of a private body' would be evidenced by 'some form of threat or inducement'.[94] It is submitted that this is a convincing approach, as it bases the existence of 'direction' in a legal sense on a subordinate relationship between the directing and the directed bodies, as confirmed by threats or inducements emanating from the former to the latter.

In the cyber context, the example of the Stuxnet worm is highly relevant in this connection. Admittedly, the authorship of the well-known virus still remains to be officially acknowledged. However, investigative reports, the choice of targets as well as the complex structure of the virus all indicate that the attack was designed and launched by nation States, with the greatest deal of suspicion falling on the US and Israel.[95] Indeed, this mainstream understanding has never been disputed by these States and has instead been given a tacit if indirect endorsement.[96] Still, an open question remains in relation to the exact legal mechanism

---

[90] *Bosnian Genocide* (n 15) [406].

[91] Crawford (n 41) 146 et seq.

[92] Ibid 146 fn 28.

[93] See also ILC, Yearbook (1998) vol I, 230 (stating that the direction must be related to the conduct in question; it is not enough that a State would exercise 'merely general control').

[94] *United States — Countervailing Duty Investigation on Dynamic Random Access Memory Semiconductors (DRAMS) from Korea*, Report of the Appellate Body, WT/DS296/AB/R (27 June 2005) [116].

[95] See, eg, David E Sanger, 'Obama Order Sped Up Wave of Cyberattacks Against Iran' *The New York Times* <http://nyti.ms/1DHQP8b> (1 June 2012).

[96] See, eg, William J Broad, John Markoff, and David E Sanger, 'Israeli Test on Worm Called Crucial in Iran Nuclear Delay' *The New York Times* (15 January 2011) <http://nyti.ms/19honmd> (reporting the US chief strategist for combating weapons of mass destruction, Gary Samore, as stating that 'I'm glad to hear they are having troubles with their centrifuge machines, and the U.S. and its allies are doing everything we can to make it more complicated.');

by which those States would incur responsibility for the aspects of the operation that might have amounted to internationally wrongful conduct.[97]

Crucially, the well-known virus was reportedly 'created in a modular fashion – programmed in "chunks" by teams that probably had no idea of the larger project'.[98] A considerable number of these programmers have likely not been in any official or formalised employment of the author States; instead, reports have suggested that parts of the project had been 'contracted out to a number of organisations involved in cyber crime'.[99] Guidance of the teams involved in such a long-term project was likely too continuous to qualify as 'instructions' and yet too detached to amount to 'control' in the sense analysed in the following section.[100]

Still, the management of the participating groups of programmers—to the extent that these were independent of the State apparatus—has likely utilised some forms of inducement, including of a pecuniary nature.[101] As such, it would have resulted in the creation of an ongoing relationship of subordination that can best be subsumed under the notion of 'direction' as conceptualized here. This conclusion may complement well the generally prevalent belief as to the responsibility for the operation and support it with a convincing legal analysis as to the specific mechanism of attribution of the purported acts that together resulted in the destructive effect on Iran's nuclear facility in Natanz.

4.3. Control

The final standard of attribution in Article 8 relates to situations in which non-State entities act under the 'control' of a State. The term 'control', as argued above, must have an autonomous meaning and it would be incorrect to equate it with either of the two preceding criteria. It is equally inaccurate to construe 'control' as being evidenced simply by the existence of 'instructions' and/or 'direction'; again, the utility of the concept of 'control' in Article 8 would be nullified if that was the case.[102]

The crucial question is the type and degree of control which the State must exercise in order for the conduct to be attributable to it. It is true that each State may be presumed to have 'some capacity to control private acts committed in its territory' simply as a corollary of its sovereign power over its own territory.[103] However, the fact of State control over its own

---

Chistopher Williams, 'Israeli security chief celebrates Stuxnet cyber attack' *The Daily Telegraph* (16 February 2011) <http://www.telegraph.co.uk/technology/news/8326274/Israeli-security-chief-celebrates-Stuxnet-cyber-attack.html> (reporting that a video played at the retirement party of the former IDF's chief of general staff, Gabi Ashkenazi, listed Stuxnet as one of his operational successes).

[97] cf Katharina Ziolkowski, 'Stuxnet: Legal Considerations' (2012) 25 Journal of International Law of Peace and Armed Conflict 139, 147 (suggesting that as a 'legal masterpiece', this operation did not breach any rules of international law).

[98] Klimburg (n 67) 43.

[99] Ibid.

[100] See section 4.3 below.

[101] cf Klimburg (n 67) 43.

[102] See also Cameron and Chetail (n 70) 211.

[103] Tonkin (n 44) 123

territory does not mean it must or even should know of each unlawful act perpetrated therein.[104] *A fortiori*, this potentiality of control arising from geographical proximity or location does not suffice for the purposes of attribution.[105] There must therefore be a relationship of actual control between the State and the non-State actor in question.

As held by the ICJ in *Bosnian Genocide*, if the degree of control is 'particularly great'[106]—more precisely, if the non-State actor acts 'in "complete dependence" on the State, of which they are merely the instrument'[107]—then the relationship in question will fall outside the remit of Article 8.[108] Instead, the non-State entity will be viewed as a *de facto* organ of the State in question.[109] That State will therefore be responsible for the conduct of such an entity under Article 4.[110]

For example, a State might put together a group of individuals drawn from State institutions and private cyber security firms to respond to a cyber emergency, while maintaining complete control over this group's operations. In such a situation, the group would be equated with an organ of that State for the purposes of State responsibility even without any recognition or authorization provided by domestic law.

As we can see, the issue of when a high degree of control transforms the relationship into one of 'complete dependence' is reasonably straightforward. However, the reverse question of the *minimum* degree of control necessary for attribution has proved to be much more problematic. It is often said that two competing tests of control have emerged in the international jurisprudence over the last three decades.

First, the ICJ formulated the test of 'effective control' in the *Nicaragua* case[111] and re-endorsed it in the *Bosnian Genocide* case.[112] Second, the Appeals Chamber of the ICTY proposed a supposedly competing test of 'overall control' in the *Tadić* case.[113] The two are therefore also sometimes referred to as the '*Nicaragua* test' and the '*Tadić* test', respectively. However, it is submitted that the supposed choice between the two tests is in fact a false dichotomy. Before setting out the reasons for this viewpoint, it is necessary to examine the elements of each of the two tests.

On the one hand, for the effective control test to be met, the State in question must go beyond merely supporting the relevant non-State actor, whether this takes the form of 'financing,

---

[104] ICJ, *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 18.

[105] Accord Michael N Schmitt, '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law' (2014) 54(3) Virginia Journal of International Law 697, 713; see also *Nicaragua* (n 34) [110] (the potential control constituted by the possibility that the US would cease its military aid to the *contras* did not by itself suffice for a finding of responsibility of the US for the acts of the *contras*).

[106] *Bosnian Genocide* (n 15) [393].

[107] Ibid [392].

[108] See ibid [406].

[109] Ibid [397].

[110] See ibid [385], [406].

[111] *Nicaragua* (n 34).

[112] *Bosnian Genocide* (n 15).

[113] ICTY, *Prosecutor v Tadić* (Appeal Judgement) IT-94-1-A (15 July 1999).

organizing, training, supplying [or] equipping' the latter.[114] The State must be involved in planning the operations, choosing the targets, and provision of operational support throughout.[115] In short, it 'must be able to control the beginning of the operation, the way it is carried out, and its end.'[116] This notably does not require control over each potentially wrongful act but only over a broader course of action within which such acts would have been committed.[117] Nonetheless, it is a very high bar even in the physical world, as evidenced by the fact that the two prominent cases in which the standard was applied by the ICJ have both resulted in a negative finding.[118]

In the cyber context, where evidence is notoriously difficult to gather, the use of this standard may in many cases lead to the same outcome. For example, the hacking and cyber crime group Russian Business Network (RBN) has reportedly benefited from long-term support of the Russian government in the form of patronage and special treatment by the authorities.[119] Similarly, China has provided government funding and training to universities allegedly involved in cyber attacks against its adversaries.[120] None of these forms of association with non-State entities, even if the facts as described were accurate, would have been sufficient in order to satisfy the test of effective control.

On the other hand, the test of overall control was proposed by the ICTY in the *Tadić* case expressly as a test requiring 'a lower degree of control'.[121] This test, as it evolved in the later case-law[122] culminating in the *Prlić* judgement,[123] requires the State in question (1) to provide the non-State entity with financial and training assistance, military equipment and/or operational support, and (2) to participate in the organization, co-ordination or planning of operations of the entity in question.[124] These two requirements—essentially, support and co-ordination—are decidedly less

---

[114] *Nicaragua* (n 34) [115]; see also *Bosnian Genocide* (n 15) CR 2006/16 [116] (Brownlie) ('Le financement, l'organisation, la formation, l'approvisionnement et l'équipement des contras ne constituaient pas un contrôle.'); ICJ, *Armed Activities on the Territory of the Congo (DRC v Uganda)* (Judgment) [2005] ICJ Rep 116 [160] ('training and military support' does not suffice for the finding of control).

[115] cf *Nicaragua* (n 34) [112] (holding that the existence of control 'may also be inferred from other factors … such as the organization, training and equipping of the force, the planning of operations, the choosing of targets and the operational support provided.').

[116] Stefan Talmon, 'The Responsibility of Outside Powers for Acts of Secessionist Entities' (2009) 58 ICLQ 493, 503.

[117] *Nicaragua* (n 34) [115] (requiring that the State control be exercised over 'the military or paramilitary operations *in the course of which* the alleged violations were committed') (emphasis added); *Bosnian Genocide* (n 15) [400] (requiring that the control be exercised 'in respect of each operation *in which* the alleged violations occurred') (emphasis added).

[118] *Nicaragua* (n 34); *Bosnian Genocide* (n 15). But see Cameron and Chetail (n 70) 213 (advancing a novel interpretation of the *Nicaragua* case, according to which the conduct of the UCLAs was in fact deemed by the court to have been under the effective control of the US).

[119] See 'A Walk on the Dark Side', *The Economist* (30 August 2007) <http://www.economist.com/node/9723768>.

[120] Saporito and Lewis (n 72) 2.

[121] *Tadić* (n 113) [124]. Antonio Cassese, one of the appellate judges in the *Tadić* case, described the *Nicaragua* test in his later extrajudicial writing as a 'very exacting' one; as setting a 'high threshold'; and as raising 'serious problems of evidence'. Cassese (n 47) 653, 654, and 666 (respectively).

[122] See, in particular, ICTY, *Prosecutor v Kordić and Čerkez* (Trial Judgement) IT-95-14/2-T (26 February 2001) [115]; ICTY, *Prosecutor v Kordić and Čerkez* (Appeal Judgement) IT-95-14/2-A (17 December 2004) [361]; ICTY, *Prosecutor v Naletilić and Martinović* (Trial Judgement) IT-98-34-T (31 March 2003) [198].

[123] ICTY, *Prosecutor v Prlić et al* (Trial Judgement) IT-04-74-T (29 May 2013).

[124] Ibid [86(a)].

demanding that the standard of effective control analysed above. For example, if a State provided malware that it had developed to a non-State group of hackers and co-ordinated the choice of targets with this group, its conduct would likely satisfy the test of overall control, although it would fall short of the standard of effective control.

However, it is submitted that the two tests do not in fact amount to two independent alternatives of the requisite standard of control for the purposes of attribution under Article 8. That is so for at least two primary reasons. First, the ICTY itself expressly limited the use of this test to organized armed groups only and it emphasized that—even under its more permissive approach—the test of effective control would still apply with respect to 'individuals or groups not organized into military structures'.[125] In the context of cyber operations, even if sometimes hackers do form groups, these typically differ markedly from organized armed groups. The latter are normally characterized by 'a structure, a chain of command and a set of rules as well as the outward symbols of authority',[126] while in the online world populated by loosely structured entities such as the Anonymous, the Honker Group, or CyberBerkut, such features would be very exceptional.[127]

Second, and much more importantly, although the ICTY Appeals Chamber ostensibly aimed to revise and replace the applicable standard of control for the purposes of attribution, it is actually doubtful that it needed to deal with the question of State responsibility at all. The issue that was properly before the Appeals Chamber in *Tadić* was the legal nature of the armed conflict in Bosnia at the time when the crimes alleged in the indictment had been committed. It considered that if an outside State controlled an armed group fighting on against another State on that State's territory, the conflict in question would become international in nature.[128] It further held that international humanitarian law (IHL) lacked unique criteria for determining whether a group of individuals is acting under the control of a State. Thus, because in its perception, the applicable *lex specialis* lacked applicable rules, it turned to the *lex generalis* comprised of the norms of State responsibility laid down in general international law.[129]

However, 'international humanitarian law is in no way *lex specialis* to the law of state responsibility'.[130] The ICTY's analysis is thus marred by a misunderstanding of the distinction between primary and secondary rules of international law.[131] While the nature of an armed conflict is determined by the primary rules of international law systematically belonging to the body of law known as IHL,[132] the question of State responsibility is determined by the secondary

---

[125] *Tadić* (n 113) [132]; see also Cassese (n 47) 657.

[126] *Tadić* (n 113) [120].

[127] Accord Marco Roscini, 'World Wide Warfare: *Jus ad bellum* and the Use of Cyber Force' (2010) 14 Max Planck Yearbook of United Nations Law 85, 100–101; Zhixiong Huang, 'The Attribution Rules in ILC's Articles on State Responsibility: A Preliminary Assessment on Their Application to Cyber Operations' (2014) 14 Baltic Yearbook of International Law 41, 49–50.

[128] *Tadić* (n 113) [97]

[129] Ibid [98]

[130] Marko Milanović, 'State Responsibility for Genocide' (2006) 17 EJIL 553, 587 (italics added).

[131] See also de Frouville (n 8) 270; Tonkin (n 44) 118–119; Crawford (n 41) 153.

[132] See Dapo Akande, 'Classification of Armed Conflicts: Relevant Legal Concepts' in Elizabeth Wilmshurst (ed), *International Law and the Classification of Conflicts* (OUP 2012) 59–60.

rules of international law, which govern whether international law obligations have been violated and the consequences of such violations.[133] It is therefore submitted that the ICTY's proposal of the 'overall control' test is unpersuasive insofar as the determination of the requisite degree of control under Article 8 is concerned. Broadly for these reasons, it was also rejected by the ICJ in the *Bosnian Genocide* case.[134]

Even if, as we have seen, the test of effective control is the correct standard for the purposes of the last criterion in Article 8, there are good reasons why this test may gradually be losing its relevance to modern challenges including those posed by the realities of cyberspace. In the first place, the general trajectory of the development of the law of State responsibility is towards more permissive rules of attribution.[135] This trend has been reflected in the maturation of Article 8 itself, which has expanded from Special Rapporteur Ago's narrow conception of a 'specific charge'[136] (i.e. actual instructions) to the current tripartite structure encompassing instructions, direction, and control.[137] It has been argued that this expansive trajectory has informed the evolution of specific areas of law, a prominent example being the antiterrorism regime.[138] According to this line of argument, this development has resulted in the emergence of looser standards of attribution such as 'harbouring' or 'supporting', as evidenced by the general endorsement of the US response to the 9/11 attacks.[139] Nonetheless, whatever the merits of this argument in relation to antiterrorism measures,[140] there is no corresponding State practice as of yet that would indicate that analogical looser standards have emerged in relation to operations in cyberspace.[141] The general trajectory towards permissiveness may thus inform the development of the law *de lege ferenda*, but does not justify lowering the bar *de lege lata*.

Secondly, the ILC's approach may plausibly be seen as allowing for a more liberal test under specific circumstances. In other words, while the effective control test might be the generally applicable standard of control, certain types of situations or contexts may warrant the use of a more lenient test. A close reading of the ILC commentary reveals indeed that the Commission did not insist on the use of the *Nicaragua* test without exception, nor did it reject the *Tadić* test altogether.[142] Instead, it allowed for context-based flexibility in an excruciatingly tautological wording at the end of the paragraph discussing the latter test, noting that 'it is a matter for appreciation in each case whether particular conduct was or was not carried out under the control of a State, to such an extent that the conduct controlled should be attributed to it.'[143]

---

133 ILC, Yearbook (1970) vol II, 306.

134 *Bosnian Genocide* (n 15) [403]–[406].

135 Condorelli and Kress (n 18) 227.

136 See *Nicaragua* (n 34) sep op Judge Ago [16].

137 See section 3 above.

138 Derek Jinks, 'State Responsibility for the Acts of Private Armed Groups' (2003) 4(1) Chicago Journal of International Law 83, 88–90.

139 Ibid 90.

140 Cf Ryngaert (n 6) 171.

141 Johann-Christoph Woltag, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law* (Intersentia 2014) 92.

142 ASR, commentary to art 8, paras 4–5.

143 ASR, commentary to art 8, para 5.

On this basis, it has been claimed that the strictness of the test 'depend[s] on the context'[144] or that it may be lowered 'in specific cases'.[145] While it is hard to argue against such broadly phrased qualifications, it is not clear that the 'context' or the 'specific cases' of cyber operations in and of themselves justify the lowering of the bar. So far, little evidence has been given of State practice supporting a more flexible or more lenient approach in respect of cyber operations.

It has further been suggested that Article 55 of the Articles on State Responsibility[146]—which acknowledges the existence of special regimes with their own rules on attribution—may bolster the case for flexibility.[147] However, the present state of the law does not seem to support this suggestion as far as cyber operations are concerned. The general law of State responsibility is residual in nature,[148] meaning States would need to specifically agree to adopt a modified rule for it to apply in a specific context.[149] This has, however, happened very rarely in practice.[150] In the current nascent phase of the law applying to cyber operations, it would therefore be premature to speculate about the existence of such specific rules in the sense required by Article 55. Therefore, it is still true that 'the same legal criteria apply [to the cyber domain] as with any other attribution of the conduct of private parties to a state'.[151]

Thirdly, it is possible to argue that the *Nicaragua* test, even if correctly decided at the time, should be seen through the historical prism of its origin, which was far removed from the modern reality of cyber attacks occurring in the virtual world. Accordingly, challenges posed by operations in cyberspace could not have been foreseen by the ICJ, which had completed its deliberations three years before Tim Berners Lee laid groundwork for the future World Wide Web.[152] This would mean that, although the *Nicaragua* test may be sound in the offline world, the notion of control needs to be re-examined in the cyber domain. Those that maintain this line of argument suggest that under the effective control test, 'it is far too easy for governments to hide

144 Nicholas Tsagourias, 'Cyber Attacks, Self-Defence and the Problem of Attribution' (2012) 17(2) JCSL 229, 238–239.

145 Tullio Treves, 'International Courts and Tribunals: Alternatives to Treaty Making' in Rüdiger Wolfrum and Volker Röben (eds), *Developments of International Law in Treaty Making* (Springer 2005) 600.

146 Art 55 ASR ('These articles do not apply where and to the extent that the conditions for the existence of an internationally wrongful act or the content or implementation of the international responsibility of a State are governed by special rules of international law.').

147 Tsagourias (n 144) 239.

148 ASR, general commentary, para 5; ibid, commentary to art 55, para 2.

149 ASR, commentary to art 55, para 1; see also *Bosnian Genocide* (n 15) [401] (rules on attribution 'do not vary with the nature of the wrongful act in question in the absence of a clearly expressed *lex specialis*').

150 See, eg, Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (signed 10 December 1984, entered into force 26 June 1987) 1460 UNTS 112, art 1(1) (providing a narrower rule of attribution for the purposes of the regime established by that treaty).

151 Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 International Review of the Red Cross 533, 545.

152 Tim Berners-Lee, 'Information Management: A Proposal', Internal Memo (CERN, March 1989), <http://cds.cern.ch/record/1405411/files/ARCH-WWW-4-010.pdf>.

their information warfare operations'.[153] Consequently, it has been argued, 'a more flexible approach similar to the overall control standard' would enhance cybersecurity.'[154]

The problem with this argument is that the flipside of making it harder for a government to disassociate itself from a specific cyber operation is the ease with which an unfounded accusation may be levelled at one's political adversary.[155] Such accusations may rapidly fuel escalation of cyber conflicts and result in further destabilisation of the situation, which would directly undermine international law's fundamental goal of preservation of peace and prevention of conflict.[156] Accordingly, the law of international responsibility is conservative in nature and tends to err on the side of non-attribution of responsibility for the conduct of private parties. This conservative tendency follows from the central assumption of this area of law, namely that only acts that are willed by an autonomous person may be attributed to it.[157] The maintenance of the *Nicaragua* standard is therefore not just a relic of a bygone offline era but also the reflection of values shared by States as primary international actors up until the modern days.[158]

5. Conclusion

Although Article 8 is rightly the first port of call for the assessment of State responsibility for the conduct of private actors, its content is often misunderstood and standards that it contains are frequently conflated. This is to the detriment of the clear and precise application of the law of State responsibility to many online activities that have come to define our time. The utility of all three standards of attribution contained in that provision needs to be understood and acknowledged. This article has confirmed the distinctive nature of these standards by reference to the drafting history underpinning Article 8 and by specific examples of modern-day cyber operations in relation to each of them.

A few cross-cutting remarks may be drawn out from the preceding analysis. First, unlike 'instructions', the standards of 'direction' and 'control' are both characterised by the continuity of the relationship between a State and a private actor. In contrast, the standard of 'instructions' permits the establishment of responsibility on the basis of a potentially singular State act of issuing a specific charge to the non-State actor in question. Second, the relationship of 'control'

---

[153] Shackelford and Andres (n 76).

[154] Scott Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations* (CUP 2014) 292.

[155] See also Roscini (n 127) 100 (arguing that the test of effective control prevents states from being frivolously accused of cyber attacks); Marco Roscini, *Cyber Operations and the Use of Force in International Law* (OUP 2014) 38; James A Green, 'The Regulation of Cyber Warfare under the Jus ad bellum' in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 113.

[156] See, eg, Russell Buchan, *International Law and the Construction of the Liberal Peace* (Hart 2013) 74 (arguing that the raison d'être of the international society is to create a regulatory framework which fosters the peaceful coexistence of States); ICJ, *Questions of Interpretation and Application of the 1971 Montreal Convention arising from the Aerial Incident at Lockerbie (Libya v UK)* (Provisional Measures: Order of 14 April 1992) [1992] ICJ Rep 3, 71 (Dissenting Opinion of Judge Weeramantry) (arguing that modern international law has been built up around the notion of peace and the prevention of conflict).

[157] de Frouville (n 8) 261.

[158] See also Michael N Schmitt and Liis Vihul, 'Proxy Wars in Cyberspace' (2014) 1(2) Fletcher Security Review 54, 72 (arguing that the high bar set by the effective control test aligns with State interests, because it creates a 'normative safe zone' for State-sponsored activities in cyberspace).

is characterised by a higher proximity of actors than the other two standards, as evidenced by the strict requirements of the applicable test of effective control developed and confirmed by international jurisprudence. Third, all three standards share the same conceptual underpinning, namely the need for the existence of a *subordinate* relationship between the State and the private actor. That means that horizontal forms of collusion such as training and support would not suffice for any of the Article 8 standards.[159]

This article has identified two principal areas with the potential for the development of the law as far as cyber operations are concerned. The first one relates to the phenomenon of government 'nudges' to private parties engaging in online activities. Just as States have outlawed incitement of specific conduct by primary rules prohibiting the incitement to genocide or discrimination,[160] it is well within their powers to do the same in relation to cyber attacks instigated by governments but performed by individuals or private groups. It is true that it may prove difficult to formulate a general rule outlawing encouragement of such kind, as noted already by Judge Ago in *Nicaragua*.[161] Nonetheless, first bilateral steps in that direction may have already been taken, as evidenced by the recent agreements concluded by the UK and China and the US and China, respectively.[162] Developing these steps on a multilateral plane might be one way of limiting the conduct of this sort in the future without a fundamental reshuffle of the rules of State responsibility.

The second area relates to the applicable test of control under Article 8. While the effective control test remains the correct one in law due to the dearth of State practice or *opinio juris* suggesting otherwise, it is acknowledged that it may be too strict in its application to particular scenarios online. Proposals to replace it with the overall control test[163] or another more lenient alternative[164] have thus far not been successful in generating any visible traction among the States. Nevertheless, the trajectory of the evolution of the law towards more permissiveness in attribution suggests that there might be scope for the development of an intermediate test that would lower the bar to allow for more flexibility while protecting the logic of the law of State responsibility. Until such time, a provisional solution is to fall back on the obligation of due diligence,[165] the violation of which essentially means that attribution problem is resolved by the

---

[159] *DRC v Uganda* (n 114) [160].

[160] Genocide Convention (n 79) art III; ICCPR (n 80) art 20(2); CERD (n 80) art 4.

[161] *Nicaragua* (n 34) sep op Judge Ago [19] fn 1.

[162] UK, FCO, 'UK-China Joint Statement 2015' (22 October 2015) <https://www.gov.uk/government/news/uk-china-joint-statement-2015> (recording the agreement of the parties not to conduct or support cyber attacks); US, White House, 'Fact Sheet: President Xi Jinping's State Visit to the United States' (25 September 2015) <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> (recording the agreement of the parties to mitigate malicious cyber activity emanating from their territory).

[163] Shackelford and Andres (n 76).

[164] See, eg, Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 Melbourne Journal of International Law 496 (proposing a novel test of 'virtual control' under which a State providing funding or other forms of support to a non-State entity would bear the burden of proof that it was *not* responsible for the latter's conduct).

[165] On the notion of due diligence, see further [cross-reference to Russell Buchan's article in the same issue].

imputing to the State not the private conduct as such but rather the consequences of such conduct.[166]

[166] Stern (n 41) 208.