2017 9th International Conference on Cyber Conflict
Defending the Core
H. Rõigas, R. Jakschis, L. Lindström, T. Minárik (Eds.)

Control and Capabilities Test: Toward a New *Lex Specialis* Governing State Responsibility for Third Party Cyber Incidents*

Peter Z. Stockburger
Senior Managing Associate
Dentons
San Diego, California, US
peter.stockburger@dentons.com

Abstract: It is well accepted under international law that a State is generally responsible for the internationally wrongful acts of its *de jure* and *de facto* State organs. It is equally well accepted that a State is generally responsible for the internationally wrongful acts of non-State actors who are neither *de jure* nor *de facto* State organs if the State sufficiently directs and controls each element of the internationally wrongful act committed by the non-State actor. This general rule, known as the "effective control" test, is recognized as the *lex generalis* governing imputed State responsibility for the unlawful actions of non-State actors. As the *lex generalis*, this principle does not vary with the nature of the wrongful act in question unless there is a clearly expressed *lex specialis*. Based on a review of State practice since 2014, there is, in fact, a *lex specialis* forming that would allow for imputed State responsibility for the internationally wrongful cyber operations of non-State actors even in the absence of evidence demonstrating "effective control." Specifically, a review of State practice since 2014 reveals that States have attributed the unlawful cyber operations of non-State actors to States, publicly, even in the absence of evidence demonstrating clear State direction and control. States have instead applied what this paper calls the "control and capabilities" test, examining a multitude of factors to determine State responsibility, including: (1) the relationship between the non-State actor and the State, if any; (2) any apparent influence the State exercises over the non-State actor; (3) the methods used by the non-State actor; (4) the motivations of the two parties, if known; (5) whether the two parties use similar code; (6) technical capabilities; and (7) geographic location. This new attribution model, if risen to the level of customary international law as the *lex specialis*, would represent a dramatic shift in the law of State responsibility and would supplant the *lex generalis*

* The views and opinions stated herein belong to the author only, and are not reflective of Dentons or Dentons US LLP.

"effective control" test in the context of imputed State responsibility for the unlawful cyber operations of non-State actors.

Keywords: *state responsibility, lex specialis, effective control, customary international law, cyber attribution*

1. INTRODUCTION

State attribution for the internationally wrongful cyber operations of a non-State actor is an issue that lies at the heart of a complicated and dynamic public debate. As in all areas of State responsibility, attribution in cyberspace is critical when determining the rights and responsibilities of States. Without proper attribution, States are limited in their options to defend against unlawful cyber operations, both within the *jus ad bellum* and *jus in bello*. Attribution in cyberspace is also incredibly difficult to establish factually. Non-State actors often mask their identity, and State actors often hide their true intentions. The degree to which the rules of State responsibility apply in cyberspace is therefore a matter of great public importance.

It is well accepted under the law of State responsibility that a State is generally responsible for the internationally wrongful acts of its *de jure* and *de facto* State organs.[1] It is equally well accepted that a State is generally responsible for the internationally wrongful acts of non-State actors, who are neither *de jure* nor *de facto* State organs, if the non-State actor in question operates on the instructions of, or under the direction or control of the State.[2] This general rule, commonly referred to as the "effective control"[3] test, is recognized as the *lex generalis* governing imputed State responsibility for the internationally wrongful conduct of non-State actors. As the *lex generalis*, this rule does not vary "with the nature of the wrongful act in question" unless there is a "clearly expressed *lex specialis*."[4] Scholars agree this principle, as the *lex generalis*, applies in cyberspace.[5]

1 *Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosn. & Herz. v. Serb. & Mont.)*, 2007 I.C.J. Rep 43 at 210 (Feb. 26) *("Bosnia Genocide")*.

2 See International Law Commission, *Articles on the Responsibility of States for Internationally Wrongful Acts*, Report of the International Law Commission on the Work of its 53rd session, A/56/10, August 2001, UN GAOR, 56th Sess Supp No 10, UN Doc A/56/10(SUPP) (2001), art. 4(1) ("Articles on State Responsibility").

3 See *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S.)*, 1986 ICJ Rep 14 at 109, 115 (June 27) ("*Nicaragua*")*; Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)*, 2005 I.C.J. Rep 168 at 228 (Dec. 19) ("*Congo*")*; Bosnia Genocide*, note 1, at 209. There is a competing test known as the "overall control" test, which is discussed further herein. *Prosecutor v. Tadić*, Case No. IT-94-1-I, Appeal Judgment, ¶ 118 (Jul. 15, 1999) ("*Tadić*").

4 *Bosnia Genocide*, note 1, at 209; Articles on State Responsibility, note 2, at art. 55.

5 See *Intl'l Grp. of Experts at the Invitation of the NATO Coop. Cyber Def. Ctr. Of Excellence, Tallinn Manual on the International Law Applicable to Cyber Warfare* at 3 (Michael N. Schmitt ed., 2013) (hereinafter "*Tallinn Manual*") (recognizing it is well accepted that international norms apply in cyberspace); *Int'l Grp. of Experts at the Invitation of the NATO Coop. Cyber Def. Ctr. Of Excellence, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* at 3, 94-100 (Michael N. Schmitt ed., 2017) (hereinafter "*Tallinn Manual 2.0*") (same); NATO Coop. Cyber Def. Ctr. Of Excellence, International Cyber Norms: Legal, Policy & Industry Perspectives at 13-14 (Anna-Maria Osula and Henry Rõigas eds., 2016) (same); United Nations, General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/68/98 (24 June 2013) (same); Peter Z. Stockburger, *Known Unknowns: State Cyber Operations, Cyber Warfare, and the Jus Ad Bellum*, 31 Am. J. Int'l L. 545, 548-550 (2016) (same).

This paper posits that a new *lex specialis* is forming, which would, if risen to the level of customary international law, supplant the *lex generalis* "effective control" test and allow for imputed State responsibility for the internationally wrongful cyber operations of non-State actors even in the absence of evidence demonstrating express direction or control. Specifically, a review of the general practice of interested States since 2014 reveals that the internationally wrongful cyber operations of non-State actors have been attributed to States in the absence of evidence of State direction or control where a number of factors are considered, including: (1) the relationship between the non-State actor and the State, if any; (2) any apparent influence the State exercises over the non-State actor; (3) the methods used by the non-State actor; (4) the motivations of the two parties, if known; (5) whether the two parties use similar code and/or technology; (6) technical capabilities; and (7) geographic location. This developing *lex specialis*, referred to herein as the "control and capabilities" test, would, if elevated to the level of customary international law, supplant the *lex generalis* rule of "effective control" and mark a significant shift in the law relating to imputed State responsibility in cyberspace.[6]

2. STATE RESPONSBILITY STANDARDS

State responsibility is generally premised on two elements: (1) the act or omission that breaches the international obligation; and (2) attribution of that act or omission to the responsible State.[7] As a general rule, the acts or omissions of a private person or group are not attributable to the State.[8] There are, however, exceptions.

A. Direct State Responsibility – De Jure and De Facto State Organs

The first exception relates to the acts and/or omissions of *de jure* or *de facto* State organs. A "State is responsible only for its own conduct, that is to say the conduct of persons acting, on whatever basis, on its behalf".[9] This includes acts:

> carried out by [State] official organs, and also by persons or entities which are not formally recognized as official organs under internal law but which must nevertheless be equated with State organs because they are in a relationship of complete dependence on the State.[10]

These types of individuals and groups are commonly referred to as *de jure* and *de facto* State organs. Both are recognized under Articles 4-6 of the Articles on State Responsibility,[11] and it is widely accepted that the conduct of *de jure* and *de facto* State organs is generally attributable to the State.[12]

B. Imputed State Responsibility – Control and Direction

The conduct of a non-State actor that is neither a *de jure* nor *de facto* State organ may also be attributable to the State "if the [non-State actor] is in fact acting on the instructions of, or

6 *Nicaragua*, note 3, at 109, 115; *Congo*, note 3, at 228; *Bosnia Genocide*, note 1, at 168-211.
7 Articles on State Responsibility, note 2, at art. 2(a)-(b); Michael N. Schmitt & Liis Vihul, *Proxy Wars in Cyberspace: The Evolving International Law of Attribution*, Fletcher Security Review, Vol. I, Issue II at 57 (2014) ("Schmitt & Vihul").
8 Articles on State Responsibility, note 2, at art. 8, commentary (1).
9 *Bosnia Genocide*, note 1, at 210.
10 *Ibid.*; Articles on State Responsibility, note 2, at arts. 4-6.
11 Articles on State Responsibility, note 2, at arts. 4-6.
12 *Ibid.*; see *Bosnia Genocide*, note 1, at 210.

under the direction or control of, [the] State in carrying out the conduct[.]"[13] This direction and control test, known as the "effective control" test, reflects the *lex generalis* as it pertains to imputed State responsibility for the conduct of non-State actors.

1) Effective Control Test Background

The "effective control" test was first outlined by the International Court of Justice (ICJ) in its 1986 case concerning *Military and Paramilitary Activities in and against Nicaragua*. There, the Court examined whether US control over Nicaraguan *Contras* was sufficient to impute the actions of the *Contras* to the US under international law. In so doing, the Court made clear that although the actions of *de facto* State organs may be attributable to the State, the actions of non-State actors not totally dependent on the State, but who are nonetheless paid, financed and equipped by the State, would be attributed to the State only if it were established that the State "directed or enforced the perpetration" of the internationally wrongful act in question.[14] Under this "effective control" test, the Court determined that although the US was responsible for the general "planning, direction and support" given to the *Contra*s, the US was not internationally responsible for the internationally wrongful actions of the *Contras* because "there [was] no clear evidence of the US having actually exercised such a degree of control in all fields as to justify treating the [*Contras*] as acting on its behalf."[15] This "effective control" test, reflected in Article 8 of the Articles on State Responsibility,[16] was expressly endorsed by the International Group of Experts (IGE) in the recently published Tallinn Manual 2.0 as reflective of customary international law.[17]

2) Overall Control Test Introduced

Thirteen years later, in 1999, a competing test known as the "overall control" test was introduced by the Appeals Chamber of the United Nations International Criminal Tribunal for the Former Yugoslavia (ICTY) in its influential *Tadić* opinion. There, the tribunal rejected the "effective control" test, and instead applied an "overall control" test to determine the attribution of acts of hierarchically structured groups, such as a military unit or armed bands of irregulars or rebels under the *jus in bello*.[18] According to the tribunal, in such circumstances, the State will be internationally responsible for the wrongful acts of the non-State actor where the State exercises "overall control" over the non-State actor, and not the higher standard of "effective control." The tribunal adopted this approach with hierarchically structured groups because such groups are less likely to receive express direction and control from the State due to their "structure, a chain of command and a set of rules as well as the outward symbols of authority."[19] Instead, the State is more likely to exercise "overall control" over the unit. The tribunal's decision was also limited to the application of the doctrine within the *jus in bello* framework as it was determining the existence of an international armed conflict under the Fourth Geneva Convention of August

13 Articles on State Responsibility, note 2, at art. 8.
14 *Nicaragua*, note 3, at 61-64; Antonio Cassese, *The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia*, 18 Eurp. J. Int'l L. 649, 652 (2007) ("Cassese").
15 *Nicaragua*, note 3, at 51, 62, 64-65.
16 Articles on State Responsibility, note 2, at art. 8, commentary (7).
17 *Tallinn Manual 2.0*, note 5, at 97, Rule 17, commentary (5) ("The International Group of Experts agreed that the phrase 'effective control' employed by the International Court of Justice in the *Nicaragua* and *Genocide* judgments captures the scope of the concept" under Article 8 of the Articles on State Responsibility).
18 *Tadić*, note 3, at ¶ 120.
19 *Ibid*.

12, 1949.[20] The "overall control" test is discussed in the commentaries to Article 8 of the Articles on State Responsibility, and is generally seen as a lower standard of attribution than the "effective control" test.[21] Under the "overall control" test, the State need only have control over the group generally, and not have given specific direction for each alleged internationally wrongful act in order for there to be imputed State responsibility.

3) Effective Control Test Revisited

The ICJ revisited the "effective control" test in 2007 in the case concerning the *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*. There, the Court criticized the ICTY's "overall control" test as going beyond the ICTY's jurisdiction, and being unsupported in State practice. The Court reaffirmed the customary status of the "effective control" test, and announced that the actions of the Republika Srpska and certain paramilitary groups known as the Scorpions, Red Berets, Tigers and White Eagles were not attributable to the Federal Republic of Yugoslavia (FRY) because there was insufficient evidence demonstrating that State instruction and direction was given with regard to each operation in which the alleged violations occurred, and not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.[22] Consequently, and controversially, the Court determined that the FRY could not be internationally responsible for the acts committed by the non-State actors in question, most notably the massacres at Srebrenica.[23]

4) Safe Harbor / Duty to Prevent

There has been additional State practice endorsing a theory for imputed State responsibility wherein the State in question harbors and provides material support to those who cause harm in another State. After the September 11, 2001 attacks, the US invoked its right to self-defense pursuant to Article 51 of the United Nations Charter on the premise that the September 11 attacks constituted an "armed attack."[24] The US attributed those attacks to the Taliban regime in Afghanistan because they were:

> made possible by the decision of the Taliban regime to allow the parts of Afghanistan that it controls to be used by this organization as a base of operation. Despite every effort by the United States and the international community, the Taliban regime has refused to change its policy. From the territory of Afghanistan, the Al-Qaeda organization continues to train and support agents of terror who attack innocent people throughout the world and target United States nationals and interest in the United States and abroad.[25]

20 Art. 2 of the Statute of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991, S/RES/827 (1993) of 25 May 1993, Annex.

21 Articles on State Responsibility, note 2, at art. 8, commentary (5) (noting 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).

22 *Bosnia Genocide*, note 1, at 208.

23 *Id*. at 206-08.

24 UN Security Council, Letter Dated 7 October 2001 From the Permanent Representative of the United States of America to the United Nations Addressed to the President of the Security Council, UN Doc No S/2001/946 (2001).

25 *Ibid*.

The global community generally accepted the legality of this action.[26]

This "safe harbor" principle is distinct from the "effective" or "overall" control tests because it is premised upon a separate doctrine of international law – namely, the duty to prevent trans-boundary harm and the "due diligence" principle as articulated in the 1941 *Trial Smelter* arbitration,[27] the ICJ's *Corfu Channel* judgment,[28] the ICJ's Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*,[29] and the ICJ's *Case Concerning Gabčíkovo-Nagymaros Project* judgment.[30] The "due diligence" principle has been applied to many areas of international law, including international environmental law,[31] human rights law,[32] and State responsibility.[33] It is distinct from imputed State responsibility because due diligence is an "obligation of conduct rather than of result[.]"[34] The doctrine therefore imposes responsibility directly on the State for its own actions, and is not on the basis of imputed State responsibility. The degree to which a State must exercise "due diligence" under international law remains highly contextual.[35]

5) Articles on State Responsibility

The "effective control" test is articulated in Article 8 of the Articles on State Responsibility, which provides that 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 that conduct.[36]

The "overall" control test is discussed in the commentary to Article 8,[37] which also provides that it is:

26 See G.A. Res. 56/220, U.N. GAOR, 56th Sess., 91st mtg., U.N. Doc. A/RES/56/220 A-B (2001) (affirming the condemnation of the use of Afghan territory for terrorist activities); G.A. Res. 56/1, U.N. GAOR, 56th Sess., 1st mtg., Agenda Item 8, U.N. Doc. A/RES/56/1 (2001) (noting "those responsible for aiding, supporting or harbouring the perpetrators, organizers and sponsors of such acts will be held accountable"); S.C. Res. 1378, U.N. SCOR, 56th Sess., 4415th mtg., U.N. Doc. S/RES/1378 (2001) (condemning the Taliban "for allowing Afghanistan to be used as a base for Al-Quaida [sic]"); S.C. Res. 1373, U.N. SCOR, 56th Sess., 4385th mtg., U.N. Doc. S/RES/1373 (2001) (reaffirming principle that every State has "the duty to refrain from organizing, instigating, assisting or participating in terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts [.]").

27 *Trail Smelter (U.S. v. Can.)*, 3 R.I.A.A. 1905, 1965 (1941).

28 *Corfu Channel Case (U.K. v. Alb.)*, 1949 I.C.J. 4, 35 (Apr. 3).

29 *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 I.C.J. 226, 29 (July 8)

30 *Gabčíkovo-Nagymaros Project (Hung. V. Slovk.)*, 1997 I.C.J. 7, 53 (Sept. 25).

31 Report of the United Nations Conference on the Human Environment Held at Stockholm, 5-16 June 1971, Principle 21, at 7, U.N. Doc. A/CONF.48/14 (1972), reprinted in 11 I.L.M. 1416, 1420 (1972); *Trail Smelter*, note 27, at 1965.

32 See, e.g., Special Rapporteur on Violence against Women, its Causes and Consequences, *Report of the Special Rapporteur on violence against women, its causes and consequences*, Comm'n on Human Rights, U.N. Doc. A/HRC/23/49 (May 14, 2013) (by Rashida Majoo); *Velasquez Rodriguez Case*, 1988 Inter-Am. Ct. H.R. (ser. C) No. 4 (July 29) at ¶ 166; Compilation of General Comments and General Recommendations Adopted by Human Rights Treaty Bodies, U.N. Human Rights Comm'n, 44th Sess., Gen. Cmt. 20 art. 7 para. 13, at 32, U.N. Doc. HRI/GEN/1/Rev.1 (1994).

33 See Ian Brownlie, *Principles of Public International Law*, 7th ed., 2008, pp. 275-285 ("Brownlie").

34 David Freestone, *Advisory Opinion on the Seabed Disputes Chamber of the International Tribunal for the Law of the Sea on 'Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area*, 15 Amer. Soc. Int. L. (March 2011).

35 See *Makaratziz v. Greece*, (No. 50385/99), 2004 Eur. Ct. H.R. 694.

36 Articles on State Responsibility, note 2, at art. 8.

37 *Id*. at art. 8 commentary, (4).

> a matter of 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.[38]

Article 55 of the Articles of State Responsibility is entitled "Lex specialis" and provides that the Articles of State Responsibility "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."

6) Tallinn Manual Recognition

The authors of the Tallinn Manual have also concluded that the "effective control" test is the *lex generalis* controlling imputed State responsibility for the conduct of non-State actors. Although the IGE recognized the tension between the "effective" and "overall" control tests in the 2013 Tallinn Manual,[39] they appear to have discarded the "overall control" test in the revised 2017 Tallinn Manual 2.0 and instead focus on the "effective control" test as the test that applies in cyberspace.[40] Specifically, Rule 17 of the Tallinn Manual 2.0, reflecting Article 8 of the Articles on State Responsibility, provides that cyber operations conducted by a non-State actor are attributable to a State when "engaged in pursuant to its instruction or under its direction or control[.]"[41] By this standard, the IGE notes that a State may, either by specific directions or by exercising control over a group, in effect assume responsibility for their conduct, with each case dependent on its own facts.[42] Instructions within this context "refers most typically to situations in which a non-State actor functions as a State's auxiliary."[43] And a State is in "effective control" of a particular cyber operation by a non-State actor whenever it is the State that "determines the execution and course of the specific operation and the cyber activity engaged in by the non-State actor is an 'integral part of that operation.' Effective control includes both the ability to cause constituent activities of the operation to occur, as well as the ability to order the cessation of those that are underway."[44]

3. TOWARD A NEW *LEX SPECIALIS* – THE "CONTROL AND CAPABILITIES" TEST

Based on the foregoing, it is well accepted that the "effective control" test is the *lex generalis* governing the imputation of State responsibility for the internationally wrongful conduct of non-State actors. As the *lex generalis*, this test applies in all situations unless there is an express *lex specialis* providing otherwise.[45] As explained below, a review of State practice since 2014 reveals that a new *lex specialis* has, in fact, begun to form that would, if risen to the

38 *Id*. at art. 8 commentary, (5), citing the Iran-United States Claims Tribunal and the European Court of Human Rights as additional authority for the proposition that institutions have wrestled with the "problem of the degree of State control necessary for the purposes of attribution of conduct to the State[.]"

39 See *Tallinn Manual*, note 5, at 32 (suggesting that a State's responsibility for cyber attacks may become rather common under the "effective control" standard).

40 *Tallinn Manual 2.0*, note 5, at 4 (the rules adopted reflect customary international law as applied in the cyber context), 94-100 (applying "effective control" standard to imputed State responsibility for cyber operations of non-State actors).

41 *Id*. at 94, Rule 17.

42 *Id*. at 95, Rule 17, commentary 4.

43 *Ibid*.

44 *Id*. at 96, Rule 17, commentary 6, citing Articles on State Responsibility, art. 8, para. 3, commentary.

45 *Bosnia Genocide*, note 1, at 209; Articles on State Responsibility, note 2, at art. 55.

level of customary international law, supplant the *lex generalis* "effective control" test for the imputation of State responsibility for the internationally wrongful cyber operations of non-State actors. Specifically, States that have attributed the internationally wrongful cyber operations of non-State actors to States since 2014 have done so on the basis of a multitude of factors, including but not limited to geographic location, methods and motivations, capabilities and technical indicators. This State practice appears to deviate from the rigid focus on control and direction as outlined by the "effective control" test, and instead focuses on a multi-factored analysis to determine State responsibility for cyber operations perpetrated by non-State actors. This State practice is creating a new test under customary international law referred to herein as the "control and capabilities" test.

A. Development of Custom

Customary international law is defined as the general practice of States accepted as law.[46] This definition comes from Article 38(1)(b) of the ICJ's Statute, and encompasses two elements: (1) long-term, widespread practice by interested States;[47] and (2) *opinio juris*, or the requirement that "[S]tates must believe that conformance with the practice is not merely designed, but mandatory and required by international law."[48]

For State practice to become a binding norm of customary international law, it must be "extensive and representative."[49] It does not, however, need to be universal.[50] There is no "precise number or percentage" of States participating required for the formation of custom, because the question is not "how many States participate in the practice" but instead which States participate.[51] Where States with influence in a particular area impacted by the normative development adopt a practice, it is given more weight in the analysis of whether the particular State practice has risen to the level of customary international law. Therefore, whether a particular State practice has achieved a level of compliance necessary for normative effect is a question of fact, involving an analysis of both physical and verbal acts of States.[52] The requirement of *opinio juris* refers to the legal conviction that a particular practice is carried out as required by law.[53] It is usually not necessary to demonstrate separately the existence of an *opinio juris* because it is generally contained within a particular dense practice. That said, proving *opinio juris* is still critical when proving the establishment of custom.

B. General Overview of "Control and Capabilities" Test

A survey of State practice since 2014 reveals that States generally do not adhere strictly to the "effective control" test set forth under Article 8 of the Articles on State Responsibility or Rule 17 of the Tallinn Manual 2.0 when attributing the internationally wrongful cyber operations of non-State actors to the State. They instead apply the "control and capabilities" test, examining the methods and motivations of the non-State actor, their geographic location, and whether,

46 Statute of the International Court of Justice, art. 38(1)(b).

47 Lynn Loschin, *The Persistent Objector and Customary Human Rights Law: A Proposed Analytical Framework*, 2 U.C. Davis J. Int'l L. & Pol'y 147, 148 (1996) (quoting Ian Brownlie, Principles of Public International Law 6-7 (2d ed. 1973) who noted that elements of this part of custom are duration, uniformity and consistency of practice, and generality of practice) ("Loschin").

48 *Ibid*.

49 Loschin, note 47, at 148.

50 Stockburger, note 5, at 564.

51 *Ibid*.

52 *Ibid*.

53 See generally Lori F. Damrosch et al., *International Law Cases and Materials* 3 (4th ed. 2001); *Nicaragua*, note 3, at 126.

if at all, the State had similar technical capabilities. Below is a survey of that State practice, which this paper argues reflects the development of a *lex specialis* for the imputation of State responsibility for the unlawful cyber operations of non-State actors.

C. State Practice

1) Pre-2014 Private Attribution Based on Control and Capabilities

Prior to 2014, although public attribution of internationally wrongful cyber operations was virtually non-existent, private attribution began to follow the control and capabilities model. In 2007, after Estonia was hit with a wave of distributed denial of service ("DDoS") attacks after deciding to remove a Soviet-era bronze soldier monument from its location in central Tallinn, Estonia, a number of scholars and jurists privately attributed the attacks to Russia.[54] Evidence showed that the "hackers claimed to be Russian, the tools to hack and deface were contained in Russian websites and chatrooms, and the attacks picked a day of" significance to most Russians.[55] Moreover, although the botnets used included computers from different countries, at least some of the attacks "originated from Russian IP (internet protocol) addresses, including those of state institutions."[56] In 2008, a similar scenario played out with Russia being privately blamed for carrying out a DDoS attack during its 2008 conflict with Georgia[57] wherein fifty-four "web sites in Georgia related to communications, finance, and the government" were attacked[58] "immediately before and continu[ing] throughout the armed conflict between" the two States.[59] All signs pointed to a Russian hacker community as the responsible perpetrator,[60] including the fact that coordination for the attacks took place in the Russian language, and in Russian or Russia-related "fora."[61] Likewise, despite confirmation from State actors regarding the 2010 Stuxnet virus,[62] and although it has been reported that the Stuxnet virus was formally developed under former US administrations,[63] no formal attribution has been declared. And in 2013, the controversial Mandiant Report attributed APT1 attacks to the Chinese State based on the geographic location of the bad actors, the methods and capabilities of the actors in question, and the motivations of the Chinese State. The report followed the US Department of Defense's 2013 Report to Congress that indicated some of the 2012 cyber intrusions into US government computers appeared to be attributable directly to the Chinese State (without providing detail as to why that attribution was provided).

2) Sony - 2014

It was not until 2014 that a State first publicly attributed what appeared to be a non-State actor's unlawful cyber operations to a State, and stated the reasons publicly for the attribution. In 2014, Sony Pictures was hit with a highly publicized DDoS attack of unknown proportions after its

54 See Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, May 16, 2007, https://www.theguardian.com/world/2007/may17/topstories3.russia.

55 *Ibid*.

56 Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations", in *Cyber War: Law and Ethics for Virtual Conflicts* 216 (Jens David Ohlin et al. eds., 2015) ("Roscini").

57 David Hollis, "Cyberwar Case Study: Georgia 2008", Small Wars J., Jan. 6, 2011, at 1.

58 *Ibid*.

59 Roscini, note 56, at 216.

60 *Ibid*.

61 *Ibid*.

62 Katharina Ziolkowski, Stuxnet - *Legal Considerations* 3 (2012).

63 David P. Fidler, "Recent Developments and Revelations Concerning Cybersecurity and Cyberspace: Implications for International Law", Am. Soc'y Int'l L. Insights (June 20, 2012), available at https://www.asil.org/insights/volume/16/issue/22/recent-developments-and-revelations-concerning-cybersecurity-and.

computer systems were compromised by suspected North Korean tied hackers.[64] The attack surrounded the release of the movie "The Interview" about the fictional assassination of the North Korean leader, Kim Jong-un. Prior to the movie's release, the spokesperson for North Korea's Ministry of Foreign Affairs said in a statement "that the country would take 'a decisive and merciless countermeasure' if the United States' government permitted Sony to make its planned Christmas release of the comedy."[65] In November, Sony's computer systems were compromised, and embarrassing e-mail communications from its CEO were leaked online. A group calling itself the "Guardians of Peace" claimed responsibility for the attack.[66]

Unbeknownst to North Korea, years earlier US officials gained access to the North Korean cyber infrastructure and implanted malicious code to track North Korean operations, allowing them to identify certain IP addresses that were being used to send spear phishing e-mails from North Korea.[67] This capability allowed US officials to trace the origins of the Sony attack[68] and shortly thereafter, in December 2014, publicly attribute the attack to the "North Korean government[.]"[69]

The US Federal Bureau of Investigation (FBI) attributed the attack to the North Korean State not on the basis of direction or control, but instead on the methods and motivations of the attackers and the North Korean government, including: (1) data deletion malware used in the attack revealing links to other malware that the FBI knew North Korean actors previously developed, including "similarities" in specific lines of code, encryption algorithms, data deletion methods, and compromised networks; (2) a significant overlap between the "infrastructure" used in the attack and other malicious cyber activity the US government had previously linked directly to North Korea; (3) IP addresses associated with known North Korean infrastructure; and (4) tools used in the attack that had "similarities" to a cyber attack in March 2013 against South Korean banks and media outlets, "which was carried out by North Korea".[70] This information about methods and capabilities led the US to publicly attribute the attack to North Korea without mention of any direction or control by the North Korean government. In response, the US imposed economic sanctions on North Korea, further reflecting the attribution of the attack to the North Korean State. North Korea also reportedly suffered widespread Internet outages in December 2014, raising the possibility that countermeasures were taken. These countermeasures were likely taken on the basis that the US viewed North Korea's actions, through the non-State actor's cyber operations, as an internationally wrongful act under the law of State responsibility, thereby justifying the imposition of proportional countermeasures.

3) Iran - 2016

In 2016, the US Department of Justice (DOJ) publicly attributed the cyber operations of private

64 Michael Cieply & Brooks Barnes, "Sony Cyberattack, First a Nuisance, Swiftly Grew Into a Firestorm", *N.Y. Times* (Dec. 30, 2014), available at http://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html (asserting that Sony was slow to realize the magnitude of the public relations complexities, financial loss, and uniqueness of the cyber attack).

65 *Ibid*.

66 FBI, "Update on Sony Investigation", *Press Release* (Dec. 19, 2014), available at https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation.

67 David E. Sanger and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say", *N.Y. Times* (Jan. 18, 2015), available at http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=0.

68 *Ibid*.

69 FBI, note 66.

70 *Ibid*.

non-State actors to Iran based on a control and capabilities analysis.[71] In March 2016, a grand jury in the Southern District of New York criminally indicted seven Iranian individuals who were employed by two Iran-based computer companies, ITSecTeam and Mersad Company that "performed work on behalf of the Iranian Government, including the Islamic Revolutionary Guard Corps, on computer hacking charges related to their involvement in an extensive campaign of over 176 days of distributed denial of service (DDoS) attacks".[72] The seven individuals were alleged to have "launched DDoS attacks against 46 victims, primarily in the U.S. financial sector, between late 2011 and mid-2013."[73] These attacks purportedly disabled victim bank websites, prevented customers from accessing their accounts online, and cost tens of millions of dollars in damage.[74] One of the defendants was also charged with obtaining unauthorized access into the Supervisory Control and Data Acquisition systems of the Bowman Dam located in upstate New York in August and September 2013.[75] In releasing the indictment, the US stated:

> Like past nation state-sponsored hackers, these defendants and their backers believed that they could attack our critical infrastructure without consequence, from behind a veil of cyber anonymity[.] This indictment once against shows there is no such veil - we can and will expose malicious cyber hackers engaging in unlawful acts that threaten our public safety and national security.[76]

In the indictment, the US attributed the actions of the seven private individuals to the State of Iran because the individuals purportedly "performed work on behalf of" the Iranian Government, as evidenced by the scope and capabilities of their cyber operations.[77] In the press release accompanying the indictment, the US Department of Justice noted these individuals had "ties" to Iran's Islamic Revolutionary Guard.[78] And without explaining the instruction from the State involved, the indictment alleged Ahmad Fathi, as the leader of the defendants, was "responsible for managing computer intrusion and cyber projects being conducted on behalf of the Government of Iran."[79] The indictment also alleged that defendant Amin Shokohi received credit for his work from the Iranian Government towards completion of his mandatory military service in Iran.[80] These allegations did not discuss direction or control, and instead focused on means and methods, capabilities, and motivations of the perpetrators in effectuating State attribution.

4) Russia - 2016 / 2017

a) DNC / US Election

In June 2016, the private security firm CrowdStrike issued a report entitled "Bears in the Midst:

71 US Dep't of Just., "Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps - Sponsored Facilities", *Press Release* (Mar. 24, 2016), available at https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated ("Iran Press Release"); *U.S. v. Ahmad Fathi, et al., Case* No. 16 Cr. 48 (S.D.N.Y. Mar. 24. 2016) ("Iran Indictment").

72 Iran Press Release, note 71.

73 *Ibid*.

74 *Ibid*.

75 *Ibid*.

76 *Ibid*.

77 Iran Indictment, note 71, at ¶ 1.

78 Iran Press Release, note 71.

79 Iran Indictment, note 71, at ¶ 11.

80 *Id*. at ¶ 13.

Intrusion into the Democratic National Committee",[81] which described an investigation into the 2015 and 2016 cyber breaches of the Democratic National Committee's (DNC) computer systems.[82] In the report, CrowdStrike identified two "sophisticated adversaries on the network - COZY BEAR and FANCY BEAR."[83] CrowdStrike concluded these two adversaries were linked to the Russian State because of their "advanced methods consistent with nation-state level capabilities including deliberate targeting and 'access management' tradecraft[,]" and because both adversaries "engage in extensive political and economic espionage for the benefit of the government of the Russian Federation and are believed to be closely linked to the Russian government's powerful and highly capable intelligence services".[84] CrowdStrike determined that COZY BEAR had infiltrated the DNC's computer systems in the summer of 2015, and FANCY BEAR had breached the network in April 2016.[85]

In October 2016, the US Director of National Intelligence (DNI) issued a joint statement on behalf of the DNI and the US Department of Homeland Security (DHS) stating that the US Intelligence Community was "confident" that the "Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations."[86] The evidence to support this conclusion, however, was that the subsequent disclosures of "hacked e-mails" that followed the DNC intrusion were "consistent with the methods and motivations of Russian-directed efforts[.]"[87] Specifically, the DNI and DHS stated that such thefts and disclosures are reflective of past Russian efforts "across Europe and Eurasia" to "influence public opinion there."[88] Based on the "scope and sensitivity of these efforts," the DNI and DHS concluded that "only Russia's senior-most officials could have authorized these activities."[89]

Several months later, in January 2017, the DHS and the FBI issued a Joint Analysis Report entitled "GRIZZLY STEPPE - Russian Malicious Cyber Activity." In the report, the DHS and FBI expanded on the October 2016 Joint Statement issued by the DNI and DHS, and publicly attributed the DNC cyber intrusion to the Russian State based on a series of "technical indicators":

> Previous JARs have not attributed malicious cyber activity to specific countries or threat actors. However, public attribution of these activities to [Russian civilian and military intelligence Services] is supported by technical indicators from the U.S. Intelligence Community, DHS, FBI, the private sector, and other entities.[90]

81 Dmitri Alperovitch, "Bears in the Midst: Intrusion into the Democratic National Committee," *CrowdStrike Blog* (June 15, 2016), available at https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.
82 *Ibid*.
83 *Ibid*.
84 *Ibid*.
85 *Ibid*.
86 Director of National Intelligence, "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security," *Joint Statement* (Oct. 7, 2016), available here https://www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1423-joint-dhs-odni-election-security-statement.
87 *Ibid*.
88 *Ibid*.
89 *Ibid*.
90 DHS & FBI, "GRIZZLY STEPPE - Russian Malicious Cyber Activity", *Joint Analysis Report* (Dec. 29, 2016), available here https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.

According to the Joint Report, those "technical indicators" prove the threat actors are "likely associated" with the Russian State.[91]

The Joint Report was widely panned by industry experts for its purported failure to provide a "smoking gun" that showed Russian control or direction over the DNC intrusion, and for using false technical indicators linking the purported threat actors to the Russian State.[92] But the focus of the Joint Report was not on express direction or control. It instead focused on capabilities, methods, motivations and technical indicators, further reflecting the development of the control and capabilities test as the growing *lex specialis* for imputed State attribution for the unlawful cyber operations of non-State actors.

b) Yahoo Breach

In March 2017, the US DOJ announced the indictments of five individuals, including two Russian officials, for "computer hacking, economic espionage and other criminal offenses in connection with a conspiracy, beginning in January 2014, to access Yahoo's network and the contents of webmail accounts."[93] In the indictment, the DOJ alleged that "officers of the Russian Federal Security Service" and "intelligence and law enforcement agency of the Russian Federation" "conspired together and with each other to protect, direct, facilitate, and pay criminal hackers to collect information through computer intrusions in the United States and elsewhere."[94] The evidence cited to link the Russian officials to the "criminal hackers", however, was less than express direction and control. Instead, the evidence included: (1) that the criminal hackers obtained evidence of "information of predictable interest to the FSB", including access to "Russian journalists and politicians critical of the Russian government" (i.e., motivations); (2) the geographic location of the criminal hackers; (3) the ability of the Russian State to "arrest and prosecute" the criminal hackers and its failure to do so; and (4) threadbare allegations that the Russian officials provided direction to the criminal hackers.[95] The focus therefore was on motivations, capabilities and geographic proximity, in combination with conclusory allegations of State direction. The test applied was not the "effective control" test. The DOJ instead focused on a control and capabilities analysis.

91 *Ibid*.

92 See, e.g., Kelly Jackson Higgins, "DHS-FBI Report Shows Russian Attribution's A Bear", *Dark Reading* (Jan. 4, 2017), available at http://www.darkreading.com/threat-intelligence/dhs-fbi-report-shows-russian-attributions-a-bear/d/d-id/1327828; Justin Raimodo, "The Evidence That Russia Hacked The DNC Is Collapsing", *Zero Hedge* (Mar. 26, 2017), available at http://www.zerohedge.com/news/2017-03-25/; Shaun Waterman, "DHS slammed for report on Russian hackers", *Cyber Scoop* (Jan. 6, 2017), available at https://www.cyberscoop.com/dhs-election-hacking-grizzly-steppe-iocs/.

93 US Dep't of Justice, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts: FSB Officers Protected, Directed, Facilitated and Paid Criminal Hackers", *Press Release* (Mar. 15, 2017), available at https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions; Ellen Nakashima, "Justice Department charges Russian spies and criminal hackers in Yahoo intrusion", *The Washington Post* (Mar. 15, 2017) available at https://www.washingtonpost.com/world/national-security/justice-department-charging-russian-spies-and-criminal-hackers-for-yahoo-intrusion/2017/03/15/64b98e32-0911-11e7-93dc-00f9bdd74ed1_story.html?utm_term=.d0a7e78e2d2d.

94 *United States of America v. Dmitry Dokuchaev, et al*., No. CR17-103, Indictment at ¶ 1(N.D. Cal. Feb. 28, 2017), available at https://www.justice.gov/opa/press-release/file/948201/download.

95 *Id*. at ¶¶ 1-6, 34.

4. CONCLUSION

The foregoing examples of State practice support the conclusion that imputed State responsibility for the unlawful cyber operations of non-State actors who are neither *de jure* nor *de facto* State organs is being assigned without rigid adherence to the "effective control" test. State attribution is instead being assigned based on a control and capabilities test, examining motivations, geographic location, technical indicators, and relationship between the non-State actor and the State. In 2014, the US publicly attributed the Sony attack to North Korea based on similarities between the code and infrastructure used by the malicious actor and the North Korean State. In 2016, the US publicly attributed certain cyber attacks to Iran based on the relationship between the purported bad actors and the State. In 2016 and 2017, the US publicly attributed the cyber intrusion of the DNC computer system to the Russian State based on technical indicators and similarities in motivations between the malicious actors and the Russian State. And most recently, the US publicly linked the 2014 intrusion of Yahoo to Russian State officers based on the geographic and motivational similarities between the criminal hackers and the Russian intelligence officers involved. In none of these cases did the State apply a rigid effective control test to determine attribution.

These State examples, of course, are not conclusive. This paper does not argue that such limited examples of State practice, alone, constitute a binding principle of customary international law. This State practice does, however, indicate that a *lex specialis* is forming that, if risen to the level of customary international law, would supplant the *lex generalis* "effective control" test, endorsed in Article 8 of the Articles on State Responsibility and Rule 17 of the Tallinn Manual 2.0.

The "control and capabilities" test, as it is developing, is not without its drawbacks. Relying solely on digital forensics to establish attribution is rife with risk. Digital evidence is volatile and has a short life span.[96] And although digital evidence may lead to the identification of the computer or computer systems from which the cyber event was triggered, "it does not necessarily identify the individual(s) responsible for the cyber operation (as the computer may have been hijacked, or the IP spoofed)."[97] These are difficult policy discussions that go beyond the scope of this paper.

The purpose of this paper is to highlight the growing trend that State attribution for the unlawful cyber operations of non-State actors who are neither *de jure* nor *de facto* State organs is deviating from the "effective control" test, and is instead focusing on a multitude of factors, including control and capabilities. This shift in State practice is reflective of a developing *lex specialis*. With more State practice, this new *lex specialis* will help shape State response to cyber operations, and will generate additional, and hopefully positive attribution analysis regimes for operational use.

96 Marco Roscini, "Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations", 50 Tex. Int'l L.J. 233, 264 (2015).

97 *Ibid*.