doi:10.1017/ajil.2018.86

A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice

*By Dan Efrony and Yuval Shany**

Abstract

This article evaluates acceptance of the Tallinn Rules by states on the basis of eleven case studies involving cyberoperations, all occurring after the first Tallinn Manual was published in 2013. Our principal findings are that (1) it is unclear whether states are ready to accept the Tallinn Rules; (2) states show uneven interest in promoting legal certainty in cyberspace; and (3) a growing need for coordinated response to cyberattacks may induce states to consider more favorably the Tallinn Rules.

I. Introduction

The Tallinn Manuals represent a notable attempt by prominent international lawyers to facilitate the regulation of cyberoperations by international law.[1] This attempt constitutes part of a longstanding tradition of legal scholars and practitioners laboring to adapt existing law to new circumstances, opting to extend the law by way of interpretation and analogy rather than by developing a brand-new legal paradigm.

The approach taken in the Manuals toward the regulation of cyberattacks and other cyberoperations is based on several factual and normative premises, which underlie their attempt to

* General (ret.) Dan Efrony served as the IDF MAG between 2011–2015. He is currently a research fellow at the CyberLaw Program of the Hebrew University Cyber Security Research Center. Professor Yuval Shany is the Hersch Lauterpacht Chair in Public International Law at the Hebrew University of Jerusalem, the Academic Director of the Hebrew University's CyberLaw Program and a Vice President for Research at the Israel Democracy Institute. The authors thank participants in the international workshop on the Tallinn Manuals and Customary International Law held in Jerusalem on December 10, 2017, and in particular Professor Michael N. Schmitt and Nimrod Karin, for their useful comments provided in relation to an earlier draft. Thanks is also due to our research assistants Sima Granovsky, Ya'ara Mordecai, and Yael Oppenheim for their assistance, and to the four anonymous reviewers of the *Journal*. Responsibility for any errors remains with us.

[1] Tallinn Manual on the International Law Applicable to Cyber Warfare (Michael N. Schmitt ed., 2013) [hereinafter Tallinn Manual 1.0]; Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2017) [hereinafter Tallinn Manual 2.0]. A "cyber operation" is defined in Tallinn Manual 2.0 as "the employment of cyber capabilities to achieve objectives in or through cyberspace." Tallinn Manual 2.0, at 564. The term "cyber operation" is narrower from the term "cyber activity," which the Manual defines as "any activity that involves the use of cyber infrastructure or employs cyber means to affect the operation of such infrastructure." *Id.*

reinterpret international law through the drawing of analogies between kinetic (physical) and cybernetic domains.[2] These premises include the following:

- Cyberattacks have features that are comparable to kinetic attacks, including, at times, similar consequences, such as harm to life, bodily integrity, and destruction of property.
- The cross-border aspects of cyberoperations render them amenable to regulation by international law, the only global body of law capable of comprehensively governing cross-border activity, and there is nothing in international law that would exclude its application to cyberattacks and other cyberoperations.[3]
- One can draw an analogy between state sovereignty or state control over land, sea, and airspace to state sovereignty or state control over parts of the infrastructure that comprises cyberspace, which is physically present inside or passes through state territory.
- An attack from computers located in one country against computers located in another country can be regarded, under certain conditions, as an armed attack under international law, and is subject to international laws regulating the use of force.
- In the same vein, the international law of state responsibility can and should govern the attribution of responsibility to states over cyberoperations undertaken by state officials, as well as for failing to diligently address acts and omissions undertaken by private actors (individuals and non-state actors) in those areas of cyberspace over which states exercise sovereign power or effective control.

On the basis of these basic assumptions, Tallinn Manual 2.0 offers a comprehensive regulatory scheme (154 rules), laying out the general legal principles governing cyberoperations and their interaction with specialized international law regimes, such as human rights law, diplomatic law, space law, and telecommunication law. Most of the Tallinn Rules focus, however, on the interplay between cyberoperations and the use of force (addressing both *jus ad bellum* and *jus in bello*).

Both editions of the Tallinn Manual have generated considerable reaction by scholars, policymakers, and bloggers. These reactions range between indications of support, praising the initiative and its contribution to the reduction of legal uncertainty in cyberspace, to more critical comments, questioning key aspects of the Manuals, the premises on which they were constructed and even the adequacy of the drafting process itself. Reactions by states to the Tallinn Manuals also appear to be mixed. Many states seem inclined to take a "wait and see" approach toward the manner in which cyberspace ought to be regulated, maintaining, in effect, a policy of silence and ambiguity. A few states, however, publicly articulated national security doctrines or strategies applicable to cyberspace,[4] incorporating certain

[2] A "cyber-attack" is defined in Tallinn Manual 2.0 as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." TALLINN MANUAL 2.0, *supra* note 1, at 415 (Rule 92). The U.S. Director of National Intelligence (DNI) defines "cyber-attack" more broadly as "a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data." *See* Statement for the Record Worldwide Threat Assessment of the U.S. Intelligence Community Senate Select Committee on Intelligence, at 1, Mar. 12, 2013, *available at* https://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf.

[3] Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed,* 54 HARV. INT'L L.J. 13, 36 (2012).

[4] *See, e.g.*, *The White House International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World* (May 2011), *available at* https://obamawhitehouse.archives.gov/sites/default/files/

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

customary international law principles that are included in the Tallinn Manuals, while avoiding explicit references to other parts of the Manuals and, at times, rejecting some of the specific rules articulated in the Manuals.[5]

In this article, we attempt to evaluate the degree to which state conduct is consistent with acceptance on their part of the Tallinn Rules as an international legal framework describing their rights and obligations in relation to cyberoperations. This evaluation is based on mapping the principal reactions to the Tallinn Rules found in the professional legal discourse (including reactions by state representatives), and on investigating a number of incidents occurring since the first Tallinn Manual was published, which appeared to invite the application of international law norms by states that fell victim to harmful cyberoperations launched from other states. Arguably, the way in which attacking and victim states actually conducted themselves throughout such incidents, overtly and covertly, may allow us to make some initial observations on state practice and *opinio juris* in relation to cyberoperations and on the extent to which they accept the Tallinn Rules as a normative point of reference. Furthermore, the literature survey and case studies enable us to assess the degree to which the relevant epistemic communities—academics and practitioners working in the field—regard international law, as it currently stands, as a generally acceptable framework for shaping interstate activities in cyberspace.

Our principal findings are that there appears to be limited support in state practice for certain key Rules of the Tallinn Manuals, and that it is difficult to ascertain whether states accept the Tallinn Rules and wish them to become authoritative articulations of international law governing cyberoperations. Our research also shows that several states that are heavily engaged in cyberoperations appear at this point in time to have a limited interest in promoting legal certainty regarding the regulation of cyberspace. These findings put into question the degree to which the Tallinn Rules are universally regarded as an acceptable basis for articulating the norms of international law governing cyberoperations.

The legal framework established by the Tallinn Manuals, which has been criticized by some academics as too loose (for not going far enough in limiting unilateral cyberoperations), has been criticized by some state officials as too strict (arguably for going too far in denying victim states the ability to effectively deter and respond to aggressive cyberoperations). Some states have even gone further by challenging the very applicability of international law principles found in the UN Charter and elaborated in the Tallinn Manuals to cyberoperations.[6]

rss_viewer/international_strategy_for_cyberspace.pdf; *The DoD Cyber Strategy* (Apr. 2015), *available at* https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf; *China's International Strategy of Cooperation on Cyberspace* (Mar. 2017), *available at* http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm; *Secrétariat Général de la Défense et de la Sécurité Nationale, Strategic Review of Cyber Defense* (Feb. 2018), *available at* http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf; *The National Cyber Security Strategy 2016 to 2021* (Nov. 1, 2016), *available at* https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

[5] *See, e.g.*, Jeremy Wright, the UK Attorney General, Speech Delivered at Chatham House, London: Cyber and International Law in the 21st Century (May 23, 2018), *available at* https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. *See also* Harold H. Koh, Legal Adviser, U.S. Dep't of State, Speech delivered at USCYBERCOM Inter-Agency Legal Conference at Fort Meade, Maryland: International Law in Cyberspace (Sept. 18, 2012), *available at* http://www.harvardilj.org/wp-content/uploads/2012/12/Koh-Speech-to-Publish1.pdf.

[6] Ann Väljataga, *Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly*, INCYDER NEWS (Sept. 1, 2017), *at* https://ccdcoe.org/back-square-one-fifth-un-gge-fails-submit-conclusive-report-un-general-assembly.html.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

The gap we identify between state practice and some key Tallinn Rules is partly explained by the controversy surrounding the contents of the Rules and, at times, suggests doubts about the normative premises from which they developed.

More significantly, however, the case studies suggest that some states tend to go out of their way to avoid relying publicly and explicitly on specific rules of international law (i.e., *jus ad bellum* and *jus in bello*) in connection with cyberoperations, and opt instead for a policy of silence and ambiguity. Hence, some victim states do not acknowledge that they were attacked; when acknowledging that they were attacked, states do not tend to attribute responsibility to other states; and when attributing responsibility, most states do not explicitly invoke the right to engage in countermeasures, which the Tallinn Rules provide. In not a single case we review has a state overtly resorted to kinetic or cybernetic force in response to a cyberattack. These findings cast more doubt on whether states regard international law—not just the Tallinn Rules—as a desirable framework for regulating or justifying their cyberoperations.

It should be noted, however, that the trends identified in this article may not be fixed in time, and that, in fact, recent collective attribution claims and reactive measures resorted to by multiple states in 2017–2018 may signify a shift in the attitude of states to the role that international law can and should play to ensure stability and order in cyberspace. As will be shown below, this shift appears to be aimed at generating greater accountability through reinforcing interstate cooperation in attributing offensive cyberoperations, producing a coordinated reaction to certain cyberoperations and sanctioning the offender states. The growing interest in resorting to international law as a focal point for coordinating interstate responses to cyberoperations and for legitimizing such operations may induce states to adopt a more favorable attitude toward the Tallinn Rules, as representing a comprehensive, specific and plausible articulation of a ready-made international law framework.

At a more abstract level, the findings of our research raise interesting questions about the manner in which states operate under conditions, such as those prevalent in cyberspace, where there exists significant normative uncertainty and where effective enforcement mechanisms are absent. Our case studies reveal three interrelated strategies employed by states under such conditions: (1) *Optionality*—regarding the framework described in the Tallinn Manuals as optional, in the sense that the states have a choice about whether or not to invoke international law rights and obligations applicable to cyberspace; (2) *Parallel Tracks*—state practice in the field of cyberoperations appears to develop along two parallel tracks, acknowledged and unacknowledged, resulting in the emergence of two sets of "rules of the game"—international law rules and softer informal rules, which also limit state power. This development challenges the power of traditional sources of international law to explain and predict state conduct in cyberspace; and (3) *Gradations in law enforcement*—states seem to develop with regard to cyberoperations a nuanced understanding of law enforcement, distinguishing between violations likely to lead to some form of response and those unlikely to do so.

Arguably, all these strategies can be found in some form or another in other fields of international law as well, but their convergence in cyberspace, due to the prevailing conditions of secrecy and deniability, accentuates the limits of legal regulation in this particular field of interstate activity. Still, the recent interest shown by several states in moving away from the policy of silence and ambiguity—through making collective attribution claims, articulating a legal doctrine relating to cyberoperations, and publicly sanctioning wrongdoers—may

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

suggest a need for greater clarity in the application of international law to cyberoperations. We believe that this development may not only render the Tallinn Manuals more relevant than before, it may also create greater interest in the establishment of an international attribution agency to improve collective enforcement prospects.

Part II of the article briefly introduces the Tallinn manuals and reviews the academic controversy surrounding their authority and contents, laying the ground for assessing the attitude of states toward the Tallinn Rules. Part III reviews eleven cyberoperations, potentially covered by the Tallinn Rules because of their interstate attributes, political context, seriousness of the harm caused, and, at times, the framing of the operation by the victim state as a violation of its rights under international law. This part considers how, if at all, the involved states reacted, whether they attributed responsibility to the attacking states, and whether their reactions, in acts and statements, were compatible with the Tallinn Rules. Part IV discusses the implications of the case studies for ascertaining the status of key Tallinn Rules under international law and for ascertaining the role of international law in national security policy in cyberspace. Part V concludes.

II. The Academic Controversy Surrounding the Tallinn Manuals

The Tallinn Manuals were prepared by an international group of experts convened in Tallinn, Estonia at the invitation of the NATO Cooperative Cyber Defense Center of Excellence (CCDCoE). The original group consisted of twenty-three experts (including four observers) from academia and practice, and their work was reviewed by another group of thirteen experts. This led to the publication in 2013 of the first Tallinn Manual, which focused on the laws of war (*jus ad bellum* and *jus in bello*). In response to criticisms of the limited diversity of the participating experts (the group was dominated by professionals from the Anglo-American world and by past and present ICRC officers),[7] and the group's overreliance on Western legal sources,[8] a second, more diverse group, was convened in Tallinn to revise and expand the first Manual. This time, the group consisted of twenty-one experts (including one observer) and fifty-nine reviewers (each reviewer being assigned with a part of the Manual). Both groups were led by Professor Michael Schmitt from the U.S. Naval War Academy and Exeter University Law School.

Unlike the first Tallinn Manual, the Manual 2.0 covers not only "above the threshold" cyberoperations—that is cyberoperations whose scale and effect may constitute a prohibited use of force,[9] or which are executed in the context of an existing armed conflict[10]—but also "below the threshold," i.e., cyberoperations that might violate international law norms other

[7] Dieter Fleck, *Searching for International Rules Applicable to Cyber Warfare—A Critical First Assessment of the New Tallinn Manual*, 18 J. Conflict & Security L. 331, 335 (2013); Ashley Deeks, *Tallinn 2.0 and a Chinese View on the Tallinn Process*, Lawfare (May 31, 2015), at https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process; Ido Kilovaty, *Cyber Warfare and the* Jus ad Bellum *Challenges: Evaluation in the Light of the Tallinn Manual on International Law Applicable to Cyber Warfare*, 5 Nat'l Security L. Brief 91, 108 (2014).

[8] Kirsten E. Eichensehr, *Book Review: Tallinn Manual on the International Law Applicable to Cyber Warfare*, 108 AJIL 585, 588 (2014).

[9] Tallinn Manual 2.0, *supra* note 1, at 330 (Rule 69) ("A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.").

[10] *Id.* at 375 (Rule 80) ("Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict.").

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

than the prohibition on the use of force or international humanitarian law. Such operations may cause physical damage to, or through, computerized systems, entail their loss of functionality,[11] or result in interference with or usurping of inherent government functions.[12] The limited attention such operations received in the first iteration of the Manual was perceived by some as one of its main shortcomings.[13]

Although expert-driven,[14] the process of formulating the Tallinn Rules involved extensive consultations with states, providing them with the opportunity to have an active role in shaping the law codification process. Toward this end, the Dutch government launched, together with the CCDCoE, "The Hague Process"—a series of meetings held in The Hague with legal advisors from fifty states to discuss under "Chatham House Rules" the draft Tallinn Rules. Still, as subsequent parts of this article show, a number of states, involved in cyberoperations, maintained throughout The Hague Process and beyond a policy of silence and ambiguity in relation to their legal positions on the regulation of cyberoperations, with a view to preserving high levels of operational flexibility through adopting a "wait and see" approach. The reluctance by some states to take a public position on the contents of the applicable law during the drafting of Tallinn Manual 2.0 may explain the controversy that unexpectedly broke out *after* the issuance of the Manual, concerning the designation of the prohibition against infringement of sovereignty as a specific rule of international law.[15] Furthermore, as is shown below, the Rules' impact on state practice and whether they consider the Rules as an acceptable basis for governing cyberoperations remains unclear due to the persistent policy of silence and ambiguity relied on by many states, as well as because of practical problems relating to the application of international law to cyberspace and ongoing challenges to the contents and authority of the Tallinn Rule.

The remainder of this part describes the academic controversy around the Tallinn Rules, which partly derives from difficulties in ascertaining state practice and *opinio juris* in the field because of said policy of silence and ambiguity. In turn, the criticism leveled against certain aspects of the Rules partly explains the "wait and see" approach some states have adopted vis-à-vis them after their publication. It is against the backdrop of this academic controversy that state practice is discussed in Part III and key Tallinn Rules are reevaluated in Part IV.

A. The Process of Formulating the Rules

The literature on the Tallinn Manuals is extensive, notwithstanding the short time that had passed since the publication of the first Manual in 2013 (and *a fortiori* since the publication of Tallinn 2.0 in 2017). It includes multiple book chapters, articles, and blog entries. This is probably indicative both of the interest and controversy surrounding the Rules and of the importance attributed to the regulation of cyberoperations in the eyes of multiple observers.

[11] *Id.* at 20.

[12] *Id.* at 21.

[13] *See, e.g.*, Adam Segal, *Axiom and the Deepening Divide in US – China Cyber Relations*, NET POL. - COUNCIL FOR. REL. BLOG (Oct. 29, 2014), *at* https://www.cfr.org/blog/axiom-and-deepening-divide-us-china-cyber-relations.

[14] Michael Schmitt, *Tallinn Manual 2.0 on the International Law of Cyber Operations: What It Is and Isn't*, JUST SECURITY (Feb. 9, 2017), *at* https://www.justsecurity.org/37559/tallinn-manual-2-0-international-law-cyber-operations.

[15] *See infra* Part IV.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

One preliminary issue raised by a number of critics relates to the authority of the Manual, i.e., whether it is reflective of existing international law, or merely the articulation of the views of international group of experts on how international law *should* be applied to cyberoperations (including, at times, both consensus and dissension views).[16] Some critics have noted, in this regard, the dearth of state practice, the secrecy enveloping some of the practice that does exist,[17] the vagueness and diversity of state positions on the topic,[18] and the fact that the development of cyberoperations is still in a state of flux, as factors that put into question the ripeness of the field for codification.[19]

Other critics expressed concern over the extensive reliance by the international group of experts on open-ended principles and contextual factors, which create significant uncertainty in their application.[20] More specifically, it was claimed that the international group of experts assigned limited space and minimalist contents to international human rights law (IHRL) in cyberspace, when compared to the treatment given to the laws of war (*jus in bello and jus ad bellum)*.[21]

Finally, a number of critics have questioned the very suitability of international law as the principal normative framework for regulating cyberoperations, noting the "incongruity of the basic structure, design and operating protocols of the internet with traditional notions of Westphalian geography."[22] As we show below, the concerns about the authority, contents, and adequacy of Tallinn Rules may explain the decision of some states to reserve judgment on them, as well as on the degree to which contemporary international law does and should regulate cyberoperations.

B. Discussions About Specific Rules

A significant number of writers have addressed specific aspects of the Tallinn Rules. A recurring concern raised by critics of the Tallinn Rules relates to the "use of force" threshold endorsed by the international group of experts. According to Rule 69: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations

[16] Terence Check, *Book Review: Analyzing the Effectiveness of the Tallinn Manual's* Jus ad Bellum *Doctrine on Cyber-conflict: A NATO-centric Approach*, 63 Clev. St. L. Rev. 495, 511 (2015); Gary Corn, *Tallinn Manual 2.0 – Advancing the Conversation*, Just Security (Feb. 15, 2017), *at* https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation; Lianne JM Boer, *Restating the Law "As It Is": On the Tallinn Manual and the Use of Force in Cyberspace*, 5 Amsterdam L. Forum 4, 6 (2013).

[17] *See* Nominations of Gen. Paul J. Selva, USAF, for reappointment to the Grade of General and to be Commander, U.S. Transportation Command; and VADM Michael S. Rogers, USN, to be Admiral and Director, National Security Agency/Chief, Central Security Services/Commander, U.S. Cyber Command: Hearing Before the Armed Services Committee of the United States Senate, 113th Cong. 506 (2014), *available at* https://www.congress.gov/113/chrg/shrg93919/CHRG-113shrg93919.pdf (Rogers asserts that criteria used for assessing cyberspace events are classified).

[18] *Id.* at 507 (Rogers: "It is likely that other nations will assert and apply different definitions and thresholds for what constitutes a use a force in cyberspace, and will continue to do so for the foreseeable future.").

[19] Corn, *supra* note 16; *see also* Michael N. Schmitt & Sean Watts, *The Decline of International Humanitarian Law* Opinio Juris *and the Law of Cyber Warfare*, 50 Tex. Int'l L.J. 189, 223, 230 (2014).

[20] Oliver Kessler & Wouter Werner, *Expertise, Uncertainty and International Law: A Study of the Tallinn Manual on Cyberwarfare*, 26 Leiden J. Int'l L. 793, 809 (2013).

[21] Rebecca Ingber, *Interpretation Catalysts in Cyberspace*, 95 Tex. L. Rev. 1531, 1534–35 (2017); Dinah PoKempner, *Squinting Through the Pinhole: A Dim View of Human Rights from Tallinn 2.0*, 95 Tex. L. Rev. 1599, 1602 (2017).

[22] Corn, *supra* note 16.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

rising to the level of a use of force."[23] The experts reached consensus that operations having consequences in the physical world[24] (including harm to computer hardware)[25] can be regarded as potentially comparable in scale and effects to kinetic operations, but could not agree to treat operations lacking physical consequences also as potential use of force.[26] The lack of consensus on the qualification under *jus ad bellum* of cyberoperations without physical consequences, but which nonetheless lead to temporary suspension of operational functionality,[27] result in alteration and destruction of data or code,[28] or involve "psychological operation" and "cyber espionage,"[29] has been identified as one of the major shortcoming of the Tallinn Rules.[30]

Arguably, the narrow definition of "use of force" adopted in the Tallinn Rules leads to a counterintuitive outcome, according to which certain serious intentional non-physical harms with a major disruptive potential might not be effectively prohibited, whereas other, less serious harms of a physical nature may qualify as a prohibited "use of force," and even as an "armed attack,"[31] giving rise to self-defense action (kinetic or cybernetic).[32] Certain authors have particularly criticized the ambiguity of the consequential standard allegedly preferred by the international group of experts. They have noted the considerable difficulties of attributing multi-causal consequences to cyberoperations[33] and challenged the pedigree of exclusive or almost exclusive reliance on a consequence-based gravity test in *jus ad bellum*.[34]

[23] TALLINN MANUAL 2.0, *supra* note 1, at 330 (Rule 69).

[24] Ido Kilovaty, *Virtual Violence – Disruptive Cyberspace Operations as "Attacks" Under International Humanitarian Law*, 23 MICH. TELECOMM. & TECH. L. REV. 113, 146 (2016); Heather A. Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Military Objectives*, 48 ISR. L. REV. 39, 54 (2015); Adm. James Stavridis, *Incoming: What is Cyber Attack*, SIGNAL (Jan. 1, 2015), *available at* https://www.afcea.org/content/?q=node/13832. *But see* Deeks, *supra* note 7 (reporting on a speech by Prof. Huang ZhiXiong from Wuhan University, China, who criticized the Rules for introducing too low of a threshold).

[25] Ido Kilovaty, *Violence in Cyberspace: Are Disruptive Cyberspace Operations Legal Under International Humanitarian Law*?, JUST SECURITY (Mar. 3, 2017), *at* https://www.justsecurity.org/38291/violence-cyberspace-disruptive-cyberspace-operations-legal-international-humanitarian-law.

[26] *See* Fleck, *supra* note 7, at 336; Kilovaty, *supra* note 7. at 116.

[27] TALLINN MANUAL 2.0, *supra* note 1, at 21; Schmitt, *supra* note 3, at 20.

[28] Mačák Kubo, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law*, 48 ISR. L. REV. 55, 78 (2015); Dinniss, *supra note* 24, at 54.

[29] Kilovaty, *supra* note 25. For further information on psychological cyber warfare, see MARCO ROSCINI, CYBER OPERATIONS AND THE USE OF FORCE IN INTERNATIONAL LAW 240–42 (2014).

[30] A parallel concern arising under IHL involved the imprecise definition under the rules of what constitutes collateral harm to cyberattacks. Kilovaty, *supra* note 24, at 146 (criticizing Rule 113).

[31] Note, however, that some commentators and governments dispute the distinction offered by the International Court of Justice (ICJ) in the Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 ICJ Rep. 14 (June 27) [hereinafter *Military and Paramilitary Activities*], between "use of force" and "armed attack" (pursuant to which, according to the Court, only the latter, aggravated forms of the use of force, would justify self-defense action). *See* Collin Allan, *Was the Cyber Attack on a Dam in New York an Armed Attack?*, JUST SECURITY (Jan. 8, 2016), *at* https://www.justsecurity.org/28720/cyber-attack-dam-armed-attack.

[32] Kilovaty, *supra* note 7, at 115. *But see* Peter Pascucci & Kurt Sanger, *Why a Broad Definition of "Violence" in Cyber Conflict Is Unwise and Legally Unsound*, JUST SECURITY (Mar. 8, 2017), *at* https://www.justsecurity.org/38536/broad-definition-violence-cyber-conflict-unwise-legally-unsound.

[33] Sharon Afek, *Cyber-attacks – Legal Contours: Application of International Law Rules to Cyber Wars*, 5 ESHTONONT – NAT'L SECURITY C. RES. CTR. 17 (2013) (Hebrew), *available at* http://maarachot.idf.il/PDF/FILES/4/113504.pdf.

[34] Kilovaty, *supra* note 7, at 111.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Exacerbating concerns about what seems to be a narrow prohibition against the use of cybernetic force are concerns about the narrowness of the self-help remedies available to victim states under the Tallinn Rules—self-defense and countermeasures.[35] Under Rule 71, "[a] State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense."[36] Self-defense would only be applicable, however, to operations qualifying as uses of force, which, because of their significant scale and effect, constitute an armed attack.[37] The narrow consensus definition of what constitutes "use of force" implies necessarily an even narrower right to exercise self-defense in the face of an armed attack. True, a broader right to take responsive action is found under Rule 20, which provides that "[a] State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that is owed by another State."[38] Such measures are subject however to a variety of conditions, including notification and proportionality,[39] and cannot involve measures themselves amounting to a use of force.

The narrow construction of the right to exercise self-defense or undertake countermeasures under the Tallinn Rules might have derived from fears of the international group of experts that a broader construction might escalate cyberconflicts. The narrow authorization to conduct unilateral operations that generate effects in the territory of other states may also reflect the strong pro-sovereignty bias of the Rules.[40] Both of these considerations militate against a liberal self-help regime. It may be noted in this regard that although the international group of experts accepted the permissibility of preemptive cyberattacks (as a form of anticipatory self-defense), the utility of this approach has also been questioned given the practical difficulties of identifying preparations before the impending launch of cyberattacks.[41]

With regard to operations falling below the use of force threshold, Tallinn Manual 2.0 posits that they may violate, under certain conditions, other rules of international law. In particular, Rule 4 stipulates that "[a] State must not conduct cyberoperations that violate the sovereignty of another State,"[42] and the international group of experts took the view that such violations involve physical damage, loss of functionality, or interference with inherent government functions.[43] Shortly before the publication of Tallinn Manual 2.0, a U.S. official expressed doubts about the notion that sovereignty constitutes a legal *rule*, which

[35] *See, e.g.*, Troy Anderson, *Fitting a Virtual Peg into a Round Hole: Why Existing International Law Fails to Govern Cyber Reprisals*, 34 ARIZ. J. INT'L & COMP. L. 135 (2017).

[36] TALLINN MANUAL 2.0, *supra* note 1, at 339 (Rule 71) ("A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defense. Whether a cyber operation constitutes an armed attack depends on its scale and effects.").

[37] The experts were, for example, divided on whether the 2010 Stuxnet operation met the required scale and effect to warrant self-defense. *Id.* at 342.

[38] TALLINN MANUAL 2.0, *supra* note 1, at 111 (Rule 20).

[39] *Id.* at 120, 127.

[40] Corn, *supra* note 16.

[41] Eichensehr, *supra* note 8, at 587 (noting that the very notion of anticipatory self-defense in international law remains controversial).

[42] TALLINN MANUAL 2.0, *supra* note 1, at 17 (Rule 4).

[43] *Id.* at 20. The experts were divided as to whether harmful operations falling short of permanent non-functionality, such as introduction of malware, destruction of data, creation of open doors, and temporary loss of functionality (e.g., distributed denial of service attacks), violate sovereignty per se. *Id.* at 21. Most, though not all, experts were also willing to extend the sovereignty rule to operations calculated to disrupt essential government service, which occurred or manifested themselves outside the victim state's territory. *Id.* at 23.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

cyberoperations may violate.[44] Similar skepticism on the matter was recently expressed by the UK attorney general.[45] Instead, it has been proposed that sovereignty is a legal *principle*, which justifies and imbues the contents of other, specific legal rules, such as the prohibition against the use of force or non-intervention. According to this latter position, cyberoperations executed in the territory of another state, which do not violate any of these specific rules, do not violate international law just because of their incompatibility with abstract notions of sovereignty.[46] In concrete terms, the two sides of the debate disagree on whether or not low-scale operations directed against specific targets in other states involving, for example, temporary loss of functionality of hardware or software or tampering with data, are prohibited under international law.

Another difficult issue flagged by the literature on the Tallinn Manuals is the unclear standard for placing responsibility on host states for cyberoperations originating from their territory. The "due diligence" Rule (Rule 7), "requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and *produce serious adverse consequences for, other States*."[47] The application of this Rule is, however, uncertain with regard to the duty of host states to prevent prospective attacks, the parallel duties of routing states (i.e., the states through which territory the operation passes), and with regard to how any "constructive knowledge" test applies to host or routing states (i.e., whether the states should have known about the operation).[48] Note however, that the due diligence rule does not impose on host states a general duty to monitor cyberactivities in their territory with a view to preventing all transboundary harm originating from it (a position informed, inter alia, by privacy concerns).[49]

[44] See Memorandum from Jennifer M. O'Connor, Gen. Counsel of the Dep't of Def., International Law Framework for Employing Cyber Capabilities in Military Operations (Jan. 19, 2017), discussed in Sean Watts & Theodore Richard, *Baseline Territorial Sovereignty and Cyberspace*, 22 LEWIS & CLARK L. REV. 803, 859–63 (2018). The approach taken in the 2017 Memorandum stands in tension with the traditional approach of the United States to cyberattacks as potentially constituting a violation of sovereignty. U.S. Dep't of Def., Office of Gen. Counsel, *An Assessment of International Legal Issues in Information Operations* 19 (2d ed. 1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf. The document presented the pillars of the Department of Defense (DoD) legal policy regarding what it then called a computer network attack (CNA) or information operations and nowadays, "cyberwarfare" and "cyber-attacks." For instance, it provided that "any unauthorized intrusion into a nation's computer systems would justify that nation at least in taking self-help actions to expel the intruder and to secure the system against reentry. An unauthorized electronic intrusion into another nation's computer systems may very well end up being regarded as a violation of the victim's sovereignty. It may even be regarded as equivalent to a physical trespass into a nation's territory . . . ."

[45] Wright, *supra* note 5. For a discussion of the implications of the speech, see Gary Corn & Eric Jensen, *The Technicolor Zone of Cyberspace – Part I*, JUST SECURITY (May 30, 2018), *at* https://www.justsecurity.org/57217/technicolor-zone-cyberspace-part; Gary Corn & Eric Jensen, *The Technicolor Zone of Cyberspace – Part II*, JUST SECURITY (June 8, 2018), *at* https://www.justsecurity.org/57545/technicolor-zone-cyberspace-part-2.

[46] Corn, *supra* note 16. *See also* Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AJIL UNBOUND 207 (2017) (presenting the sovereignty as a principle approach). See the responding article by Michael N. Schmitt & Liis Vihul, *Respect for Sovereignty in Cyberspace*, 95 TEX. L. REV. 1639 (2017) (describing the evolution in the legal position of the DoD, and presenting support in state practice and *opinio juris* for sovereignty as a rule). *See also* Phil Spector, *In Defense of Sovereignty, in the Wake of Tallinn 2.0*, 111 AJIL UNBOUND 219 (2017).

[47] TALLINN MANUAL 2.0, *supra* note 1, at 43 (Rule 7) ("The principle of due diligence requires a State to take all measures that are feasible in the circumstances to put an end to cyber operations that affect a right of, and produce serious adverse consequences for, other States.").

[48] Fleck, *supra* note 7, at 338.

[49] TALLINN MANUAL 2.0 *supra* note 1, at 44–45; Eichensehr, *supra* note 8, at 586.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

The open-ended nature of the obligation of the host state under the Tallinn Rules to suppress attacks against other states by non-state actors renders it difficult for the victim state to establish a right to respond to operations originating from non-state actors. This difficulty confronting victim states is further complicated by their lack of legal authority to conduct investigations in the host states or to unilaterally engage in operations against non-state actors situated in such states (unless it can be established that the host state itself breached an international obligation owed to the victim state).[50] Consequently, it has been claimed that the Tallinn Rules provide victim states with limited guidance on how to react to certain cyberoperations and leave them with relatively few legal options.[51]

A final realm of uncertainty relating to the Tallinn Manuals can be found in the division of labor between different states that could have prevented cyberoperations and mitigated their consequences. The involvement of multiple states, including a number of states from whose territory the operation might have originated, the routing states, and several victim states raises difficult questions of allocating state responsibility, addressing conflict of laws (relating to criminal and civil liability), and applying the laws governing the use of force (e.g., whether one should evaluate cumulatively the scale and effect of the harm caused to different states in order to reach the threshold of harm giving rise to self-defense).[52]

Proponents of the Tallinn Rules, including Professor Schmitt, have responded to most of these criticisms by way of emphasizing the distinction found in the Tallinn Manuals between *lex lata* and *lex ferenda,* and explaining that the stated aim of the international group of experts was to reflect the former and not the latter. Thus, even if the Rules elaborated in the Manuals are flawed, uncertain or excessively restrictive (or, in the eyes of some, excessively permissive), they represent the current imperfect state of the law.[53] Indeed, Schmitt himself believes that the law will gradually develop in the direction identified by some of the critics, including through encompassing data and other non-physical targets of consequential importance in the list of objectives protected by *jus ad bellum* and *jus in bello*.[54]

The next part of this article looks into state practice (and, where relevant, also into manifestations of *opinio juris*). It explores whether *lex lata* as identified by the international group of experts coincides with the ways in which states actually conduct themselves in connection with cyberoperations, and whether the Tallinn Rules are regarded by them, explicitly or implicitly as an acceptable basis for regulating cyberoperations or even as relevant normative points of reference. Our discussion of state practice, the gaps we identify between the Rules and state needs, interests and expectations, and the policy of silence and ambiguity adopted by some states vis-à-vis the legal regulation of cyberoperations, lays the groundwork for our

[50] TALLINN MANUAL 2.0, *supra* note 1, at 111 (Rule 20) ("A State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State."); *see also id*. at 113.

[51] Corn, *supra* note 16; Kilovaty, *supra* note 7, at 119–20. For a defense of the position of the Manuals in this regard, see Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. FORUM 68 (2015).

[52] Andrew Keane Woods, *The Tallinn Manual 2.0, Sovereignty 1.0*, LAWFARE (Feb. 8, 2017), *at* https://www.lawfareblog.com/tallinn-manual-20-sovereignty-10.

[53] Michael N. Schmitt, *The Notion of "Objects" During Cyber Operations: A Riposte in Defiance of Interpretive and Applicative Precision*, 48 ISR. L. REV. 81, 82 (2015).

[54] *Id*. at 108. *See also* Michael N. Schmitt, *The Law of Cyber Warfare:* Quo Vadis?, 25 STAN. L. & POL'Y REV. 269–99 (2014); Kilovaty, *supra* note 7 at 115 (calling in this regard for reexamination of the exclusion of political and economic coercion from the scope of use of force prohibited by Article 2(4) of the UN Charter).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

discussion in Part IV of the direction in which international law norms and institutions governing cyberoperations are likely to develop in light of the uncertain position of states toward the Tallinn Rules.

III. The Case Studies

A. Case Selection Criteria

Countless cyberoperations took place in cyberspace after March 2013, when Tallinn Manual 1.0 was published, and countless more have taken place since February 2017 when Tallinn Manual 2.0 was issued.[55] The vast majority of these operations are of little interest to the present article, which focuses on the regulation of cyberoperations carried out in an interstate context, and which would have likely attracted the attention of senior policymakers and their consideration of an adequate response. This is not the case with most cyberoperations undertaken in recent years whose source and context is unknown, or which appear to have been of a private criminal nature or involve some form of "hacktivism" not tied to any specific state or to a specific national security or political agenda. Such cyberoperations are typically dealt with by law enforcement agencies and procedures. While law enforcement responses to private cyberoperations raise complicated question of jurisdiction under domestic and international law, as well as questions relating to international coordination and enforcement capacity, those questions are beyond the scope of this article.[56]

The eleven case studies discussed below (and summarized in a table in the Appendix) involve cyberoperations that possibly originate from states or state-sponsored groups or individuals (including groups or individuals who seem to operate with state acquiescence). They sometimes involve operations directed against public targets in the victim states, such as official databases, national infrastructure, and computer systems serving governmental agencies. Although the operations discussed in the case studies were all conducted in a clandestine manner, a political motive related to preexisting international conflicts or tensions can be deduced with respect to most of them on the basis of publicly available materials. Significantly, however, not a single state assumed responsibility for launching any of the cyberattacks or operations discussed in the case studies—a practice that may reflect the preference of attacking states to operate "below the radar," as well as doubts about the ability to justify their own actions under existing international law norms.

The evidence in the case studies suggests that states targeted by cyberoperations appear to focus their response on detecting, containing, and eliminating cybersecurity breaches, while being inclined to give little publicity to the operations launched against them and to downplay their adverse effects. The tendency of victim states to minimize the publicity given to cyberoperations is probably related to fears that advertising security breaches may inspire new attackers, including "copycat" cyberattackers, and provide them with useful information on the national cyberdefense apparatus. Furthermore, drawing attention to past attacks might undermine public confidence in the government's ability to provide cybersecurity; it may also

[55] *Cf.* Mark T. Peters, Cashing in on Cyberpower: How Interdependent Actors Seek Economic Outcomes in a Digital World 87 (2008) (claiming that millions of potential cyberattacks occur on a daily basis).

[56] *See, e.g.*, Ahmed Ghappour, *Tallinn, Hacking, and Customary International Law*, 111 AJIL Unbound 224 (2017).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

generate public pressures on governments to retaliate, even though such a retaliation might induce more aggressive cyberoperations in response, and generate significant legal or diplomatic costs.

The lack of transparency in the field—underreporting of cyberoperations and limited attribution claims—makes it difficult to identify relevant state practice. This constitutes a methodological constraint on our research, which relies exclusively on publicly available materials. Some of the data we used comes from primary sources such as press releases, official publications issued by governmental agencies, and cyber security firms' analyses or investigative reports. Other parts of the data come from secondary sources such as press reports, which sometimes contain unofficial allegations and speculations. We do not claim to present below a full factual picture regarding the reviewed case studies; nor can we claim that they represent all major cyberoperations that have occurred since 2013. To the contrary, they are probably just the very tip of the iceberg.

In selecting case studies, we have used a two-stage process. First, we conducted an extensive web-search designed to identify cyberoperations, which appear to meet the inclusion criteria enumerated below. In this part of the research we were aided by a professional web-search company named Buzzilla (which also scans social media). We then compared the list of cases arising from our own findings with the lists found in two well-regarded depositories of known cyber incidents: the Center for Security and Intelligence Studies' (CSIS) "list of incidents," and the U.S. Council on Foreign Relations' (CFR) Cyber Operations Tracker.[57] The CSIC list codes the significance of incidents on the basis of their relationship to states and the level of financial loss they caused. The Tracker list focuses primarily on operations potentially attributable to states. From this database, we selected eleven cyberoperations (some actually comprising a series of cyberoperations), which conformed to the following inclusion and exclusion criteria, and which contained relevant information about state practice or *opinio juris* in relation to cyberoperations:

- *Inclusion –*
    - Cyberoperations alleged to have been (1) politically motivated and (2) presumably initiated or supported by a foreign state (that is, by official state entities or by proxies such as state-sponsored groups), and which (3) caused significant damage in the physical world or to strategic government assets (including, erasing or intentionally altering data in the attacked computer or database, or leaking large quantities of sensitive government data). Particular attention was given, in this regard, to cyberoperations, whose direct or indirect consequences are comparable to those of kinetic operations and that might conceivably fall under the scope of application of traditional rules of *jus ad bellum* or *jus in bello*,[58] and to cyberoperations that generated responsive acts or statements by victim states suggesting that they

[57] The CSIS and the CFR are among the world's leading think tanks in the field of defense and national security studies. James G. McGann, 2017 Global Go To Think Tank Index Report, at 96 (University of Pennsylvania Scholarly Commons, 2018). *See Significant Cyber Incidents Since 2006*, CSIS, *at* https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity (The full list includes incidents since 2006, focusing on cyberattacks on government agencies, defense and high-tech companies or economic crimes, entailing losses of more than a million dollars.). *See also Cyber Operations Tracker*, CFR, *at* https://www.cfr.org/interactive/cyber-operations.

[58] TALLINN MANUAL 2.0, *supra* note 1, at 330–38 (Rules 69–70).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

consider the operations conducted against them to have violated the laws of war or infringed their national sovereignty.
- Cyberoperations that took place during 2013 or thereafter, and which therefore allow us to explore whether the conduct of implicated states suggests that they accept and follow the 2013 or 2017 Tallinn Rules.

- *Exclusion –*

  - Operations aimed exclusively at cyberespionage, given the understanding of the international group of experts that international law does not clearly prohibit espionage activities during armed conflict and in peacetime, unless they generate significant "collateral harm."[59] Such excluded cyberoperations typically consist of intrusions aimed at gaining military, political, commercial, or industrial intelligence, and which did not prompt an overt response by the victim state.
  - Operations appearing to constitute cybercrimes undertaken for financial gain, such as data thefts and ransom demands, unless they are perceived to be politically motivated and linked to a government.
  - Events preceding 2013, because those events do not assist us in evaluating the degree to which the Tallinn Rules have been accepted by states and whether they refer to the Rules and follow them in their actual practices. To that end, we have excluded from the list famous cyberoperations, which would otherwise qualify as prominent case studies, such as cyberattacks in Estonia (2007)[60] and Georgia (2008),[61] and the Olympic Games operation (the Stuxnet attack) (2009–2010).[62]

The case studies are grouped into six categories, according to the identity of the victim state—a categorization that helps us to establish the consistent practice of such states. Five of the cases reviewed relate to attacks against the United States. This is perhaps reflective of the many international political grievances held against it by other states as well as nonstate actors, and its relative vulnerability to cyberoperations due to its high level of dependence on digital technology. The availability of information about cyberattacks against the

[59] TALLINN MANUAL 2.0, *supra* note 1, at 168–74 (Rule 32). *See also* Darien Pun, *Rethinking Espionage in the Modern Era*, 18 CHI. J. INT'L L. 353, 359–68 (2017) (presenting the conflicting approaches regarding the legality of espionage activity under international law); Jens David Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?*, 95 TEX. L. REV. 1579 (2017).

[60] Gadi Evron, *Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War*, 9 GEO. J. INT'L AFF. 121 (2008); Stephen Herzog, *Revisiting the Estonian Cyberattacks: Digital Threats and Multinational Responses*, 4 J. STRATEGIC SECURITY 49 (2011); Ian Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, GUARDIAN (May 17, 2007), *at* https://www.theguardian.com/world/2007/may/17/topstories3.russia; Peter Finn, *Cyber Assaults on Estonia Typify a New Battle Tactic*, WASH. POST (May 19, 2007), *at* http://www.washingtonpost.com/wp-dyn/content/article/2007/05/18/AR2007051802122.html.

[61] John Markoff, *Before the Gunfire, Cyberattacks*, N.Y. TIMES (Aug. 12, 2008), *at* http://www.nytimes.com/2008/08/13/technology/13cyber.html; Noah Shachtman, *Top Georgian Official: Moscow Cyberattacked Us – We Just Can't Prove It*, WIRED (Nov. 3, 2009), *at* https://www.wired.com/2009/03/georgia-blames; Stephen W. Korns & Joshua E. Kastenberg, *Georgia's Cyber Left Hook*, 38 PARAMETERS 60 (2009); Eneken Tikk, Kadri Kaska, Kristel Rünnimeri, Mari Kert, Anna-Maria Talihärm & Liis Vihul, *Cyber-attacks Against Georgia: Legal Lessons Identified* (NATO Cooperative Cyber Defense Centre of Excellence, 2008).

[62] James P. Farwell & Rafal Rohozinski, *Stuxnet and the Future of Cyber War*, 53 SURVIVAL 23 (2011); Sean Collins & Stephen McCombie, *Stuxnet: The Emergence of a New Cyber Weapon and its Implications*, 7 J. POLICING, INTELLIGENCE & COUNTER TERRORISM 80 (2012); Kim Zetter, *An Unprecedented Look at Stuxnet, the World's First Digital Weapon*, WIRED (Mar. 11, 2014), *at* https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

United States may also stem from its relatively high degree of transparency in security matters, and the relative openness of government officials to discuss (at times, under condition of anonymity) cyberattacks and responses thereto. The five U.S. case studies include: (1) attacks against multiple targets in New York State resulting in serious disruption of financial services and, in one case, a potential sabotage of a water dam; (2) the stealing of exceptionally large volumes of national security data from the Office of Personnel Management (OPM), referred to by U.S. commentators as a "Cyber Pearl Harbor"; (3) destruction of multiple computers owned by the Sands Casino; (4) the stealing of data and destruction of computers owned by Sony Pictures Entertainment; and (5) multiple operations aimed at influencing the U.S. presidential election.

Other case studies reviewed in this part include a hacking of the Bundestag network, which was part of an attempt to interfere in Germany's internal affairs and prompted consideration of countermeasures and changes in the organization of the German security forces; destructive attacks against oil companies and infrastructure in Iran and in Saudi Arabia and Qatar; the downing of the Ukrainian electric grid; and two particularly destructive global cyberoperations—WannaCry and NotPetya—that have been attributed to specific source states (North Korea and Russia).

Our review does not focus on whether the attacks themselves are lawful under the Tallinn Rules (or other plausible interpretations of international law)—although many of them clearly appear to be illegal, and no state has assumed responsibility for them or attempted to publicly justify them. Instead, we focus on the reactions of victim states and consider whether they have referred to their legal rights and obligations under international law, as reflected in the Tallinn Rules, or instead maintained silence and ambiguity vis-à-vis the cyberoperations directed against them. State reactions or the absence thereof are arguably indications of state practice and/or *opinio juris*, which helps us identify emerging rules of customary international law, as well as evidence relating to the manner in which existing treaties should be interpreted and applied. They are also valuable indications of the extent to which the Tallinn Rules are actually regarded by states as an acceptable legal framework for regulating cyberoperations.

In assessing the legal significance of state reactions, we have followed the most recent International Law Commission (ILC) draft conclusions on the identification of customary international law, which include among indications of practice "operational conduct 'on the ground,"[63] and among indications of *opinio juris* "public statements made on behalf of [the] State."[64] It is notable in this regard that the ILC draft conclusions provide that "[f]ailure to react over time to a practice may serve as evidence of acceptance as law (*opinio juris*), provided that states were in a position to react and the circumstances called for some reaction."[65] Although the conclusions are silent on the question of secret practice, it is difficult to see how covert action, which other states have little opportunity to react to, can meaningfully serve as the basis of customary international law.[66]

[63] International Law Commission, Identification of Customary International Law, Conclusion 6(2), UN Doc. A/CN.4/L.908 (2018) (text of the draft conclusions as adopted by the Drafting Committee on second reading).

[64] *Id.*, Conclusion 10(2).

[65] *Id.*, Conclusion 10(3).

[66] *See, e.g.*, Michael Byers, Custom, Power and the Power of Rules: International Relations and Customary International Law 156 (1999); Tullio Treves, *Customary International Law*, *in* Max Planck Encyclopedia of Public International Law, para. 79 (2006).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

To the extent that states invoke in statements accompanying their practice any international treaty or rely implicitly thereupon, such practice may amount to subsequent practice in the application of the treaty that could establish, over time, the parties' agreement regarding its interpretation.[67] In none of the case studies discussed below, however, did states invoke rights under specific treaties, and only in one case (hacks relating to the presidential elections) did a state rely implicitly (and covertly) on international law doctrine.

B. Cyberoperations Against the United States

1. A sequence of cyberoperations against civilian targets in New York (2011–2013)[68]

a. Principal facts

Distributed denial of service (DDoS) operations targeting the financial sector in New York (known also as the "Ababil" or Swallows operation) were conducted between late 2011 to late 2013, reaching a cumulative total of 176 days of attacks.[69] The attackers—belonging to a group named "Izz ad-Din al-Qassam Fighters"—identified themselves as Arab Muslim youth hackers. The operations were designed to crash the commercial websites of forty-six U.S. financial sector institutions, such as the Bank of America, Wells Fargo, the Nasdaq composite index, the New York Stock Exchange, AT&T, and many others.[70] The harm sustained by the American financial institutions targeted by the Ababil operation ran into tens of millions of dollars as a result of severe interruptions of the business activities of the financial institutions. Additional damage was caused to hundreds of thousands of customers denied online access to their accounts. In August and September of 2013, the same hackers also obtained unauthorized access into the Supervisory Control and Data Acquisition (SCADA) systems of the Bowman Dam, located in Rye, New York.[71]

b. Attribution

The declared motive of "Izz ad-Din al-Qassam Fighters" was ideological: they demanded that YouTube remove from its website a video insulting the Prophet Muhamad. The American media and cyber experts pointed the finger at Iran, although no official American statement explicitly attributed to it responsibility for the operation. According to media speculations, Iran was seeking to retaliate for the Stuxnet cyberattack that had been

[67] *See* Vienna Convention on the Law of Treaties, Art. 31(3)(b), May 23, 1969, 1155 UNTS 331.

[68] Adam Samson & Matt Egan, *Chase, NYSE Websites Targeted in Cyber Attacks*, FOX BUSINESS (Sept. 19, 2012), *at* https://www.foxbusiness.com/features/chase-nyse-websites-targeted-in-cyber-attacks; Nicole Perlroth & Quentin Hardy, *Bank Hacking Was the Work of Iranians, Officials Say*, N.Y. TIMES (Jan. 8, 2013), *at* http://www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say.html.

[69] Sealed Indictment, United States v. Fathi, 16 Cr. 48 (S.D.N.Y. Jan. 21, 2016), *available at* https://www.justice.gov/usao-sdny/file/835061/download.

[70] U.S. Dep't of Justice Press Release, 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 Entities (Mar. 24, 2016), *at* https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-seven-iranians-conducting-coordinated.

[71] *Id.*; *see also* Indictment (U.S. v. Fathi), *supra* note 69.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

conducted against its nuclear facilities by the United States and Israel,[72] as well as to establish its power of deterrence by demonstrating significant operational capabilities in the cyber domain.

The Head of FETA (Iran's cyber police), Brigadier General Seyed Kamal Hadianfar, denied reports that accused Iran of masterminding the Ababil operations,[73] and called on the United States to provide Iran, via the Interpol, with any information on the alleged Iranian involvement in the attacks. He promised to investigate such a complaint as Iran had already done in 2011 in connection with a DDoS attack against Citibank. On that occasion, the investigative authorities found no genuine connection between the attack and Iran or Iranian nationals. (The only Iranians nationals involved in the 2011 incident were users whose computers were overtaken by third parties and used as "zombie" or "slave" computers.)[74]

In 2016, three years after the end of the Ababil operation, the FBI succeeded in gathering enough evidence to bring charges against seven Iranian hackers.[75] The indictments, submitted in March 2016, revealed,[76] inter alia, the following facts:

- The hackers were employees of two private computer security companies based in Iran that performed work on behalf of the Iranian government, including the Islamic Revolutionary Guard Corps. The two companies were involved in a myriad of national security operations, including in the field of military intelligence.
- One of the defendants received credit from the Iranian Government for his computer intrusion work toward completion of his mandatory military service in Iran.
- For three weeks (Aug. 28, 2013–Sept. 18, 2013), one of the defendants repeatedly obtained unauthorized remote access to the SCADA system of the Bowman Dam, allowing him to gather information regarding the water level, flow rate, and status of the sluice gate (responsible for controlling water levels and flow rates). Luckily, at the time of the actual intrusion, the sluice gate had been manually disconnected for maintenance.

Besides the firm statements made by senior law enforcement officials at the occasion of announcing the charges,[77] no official statement has ever been made by U.S. officials articulating the implications of linking the Ababil operation to an Iranian government agency or assigning legal responsibility to Iran for them.

[72] Mark Thompson, *Iranian Cyber Attack on New York Dam Shows Future of War*, TIME (Mar. 24, 2016), *at* http://time.com/4270728/iran-cyber-attack-dam-fbi. *See also* Perlroth & Hardy, *supra* note 68.

[73] *Iran Cyber Police Uncovers Hacking of US Bank*, MEHR NEWS AGENCY (Jan. 20, 2013), *available at* http://www.payvand.com/news/13/jan/1182.html.

[74] *Id.*

[75] U.S. Dep't of Justice Press Release, *supra* note 70.

[76] *See* Indictment (U.S. v. Fathi), *supra* note 69.

[77] U.S. Dep't of Justice Press Release, *supra* note 70. The U.S. attorney general stated: "[W]e will not allow any individual, group, or nation to sabotage American financial institutions. . . ." The assistant U.S. attorney for Manhattan added: "These were no ordinary crimes, but calculated attacks by groups with ties to Iran's Islamic Revolutionary Guard and designed specifically to harm America and its people." The head of the FBI promised that: "By calling out the individuals and nations who use cyber-attacks to threaten American enterprise, as we have done in this indictment, we will change behavior."

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

c. Response

As far as we know, the Obama administration handled the Ababil operation in a cautious, mostly defensive matter. It had been reported in the press that a counteroperation was considered and rejected, since it would have caused "unintended consequences," which "could invite escalatory attacks that might paralyze the networks of American businesses."[78] Even a proposal by the then National Security Agency (NSA) Director, Keith Alexander, to shut down the computer process in Iran responsible for the DDoS attacks by a covert cyber operation seems to have been rejected because the decisionmakers "were unsure that the action could be so precise and expressed concern that affecting a server in Iran—even if in self-defense—would represent a violation of its sovereignty"[79] and cause escalation. The option of using diplomatic back-channels was also put off the table, since it was assessed that doing so might prompt the Iranians to intensify their attacks.[80] A former U.S. official was cited in this connection as commenting that they "knew that Iran had the potential to do harm . . . and if [the Iranians] had chosen at various moment to aim all their capabilities down a narrow pipe, they would have succeeded in bringing the [American] networks down."[81] Apparently, the administration's policy to refrain from an immediate and firm response to stop the operation frustrated the defenseless victim-institutions, which led them to seriously discuss self-help options such as hacking back the attackers' servers.[82]

Ultimately, it looks as if the U.S. administration decided to respond in a manner that combined diplomacy with technology:[83] The State Department appealed to its counterparts in 120 countries to enable CERT-to-CERT connections, aimed at removing malicious computer code from servers used as springboards for the Ababil operation. Eventually, the operation concluded toward the end of 2013 as a result of a decision taken by the Iranian authorities, probably due to progress in the multilateral nuclear talks and the prospects of lifting economic sanctions against Iran. As indicated above, the United States supplemented its formal response to the Ababil operation by charging *in absentia*, in 2016, seven Iranian nationals accused of perpetrating illegal cyber activities,[84] thus indicating that the United States is aware of precisely what happened, and who was behind the operation.[85]

[78] Ellen Nakashima, *US Rallied Multinational Response to 2012 Cyberattack on American Banks*, WASH. POST (Apr. 11, 2014), *at* https://www.washingtonpost.com/world/national-security/us-rallied-multi-nation-response-to-2012-cyberattack-on-american-banks/2014/04/11/7c1fbb12-b45c-11e3-8cb6-284052554d74_story.html?utm_term=.ba23ea798108.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] Michael Riley & Jordan Robertson, *FBI Probes if Banks Hacked Back as Firms Mull Offensives*, BLOOMBERG NEWS (Dec. 30, 2014), *at* https://www.bloomberg.com/news/articles/2014-12-30/fbi-probes-if-banks-hacked-back-as-firms-mull-offensives (reporting on ongoing FBI investigation to find out if someone from the targeted banks hacked back Iranian servers). See also the follow-up report of Eric Chabrow, *The Case Against "Hack-Back,"* BANK INFO SECURITY (Jan. 6, 2015), *at* https://www.bankinfosecurity.com/case-against-hack-back-a-7759 (presenting the main arguments against hacking back by private victims); Nicholas Schmidle, *The Digital Vigilantes Who Hack Back*, NEW YORKER (May 7, 2018), *at* https://www.newyorker.com/magazine/2018/05/07/the-digital-vigilantes-who-hack-back (reporting that at least one of the targeted banks resorted to hacking back).

[83] Nakashima, *supra* note 78.

[84] Thompson, *supra* note 72.

[85] Mike Masnick, *DOJ's Tone Deaf Criminal Charges Against Chinese Hackers Helps No One, Opens US Officials Up To Similar Charges*, TECHDIRT (May 20, 2014), *at* https://www.techdirt.com/articles/20140520/

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

2. *Hacking the Office of Personnel Management (2014–2015)*[86]

a. *Principal facts*

In March 2014, the Department of Homeland Security (DHS) alerted the OPM that its security had been breached and that data was stolen. Since then, DHS and the OPM have monitored the attacker's activity. Despite such monitoring, another attacker succeeded in May 2014 in accessing the system as an employee of an OPM contractor (apparently in full coordination with the March attacker). Between May 2014 and June 2015, large quantities of personnel data of applicants and former and current government employees had been stolen, including their security clearance backgrounds and biometric data.[87]

The motive for this cyber operation could not be determined with a high degree of certainty, although it seems that it was, at least partly, aimed to facilitate intelligence gathering. There is no doubt, however, about the seriousness of the consequences of the operation, which went farther than any previous act of cyberespionage. This led some commentators to dub the operation as a "Cyber Pearl Harbor,"[88] and "one of the most devastating breaches of U.S. government data in history."[89] It also caused severe harm to the privacy of millions of Americans, whose personal data was included in the stolen files.

The then head of the FBI, James Comey, described it as a "very big deal from national security perspective and from a counterintelligence perspective. It's a treasure trove of information about everybody who has worked for, tried to work for, or works for the United States Government."[90] Most likely, the operation had short-term adverse consequences for counterintelligence activities, and compromised the safety of American intelligence agents operating abroad.

b. *Attribution*

Identified as a politically motivated operation, likely to have been undertaken by a foreign nation, the immediate suspects were China, North Korea, and Russia. The United States has not officially blamed any of these nations for the operation, but American media and some senior U.S. politicians identified China as the major suspect.[91] Cristopher Painter, the coordinator for

05303727288/dojs-tone-deaf-cri (criticizing the DOJ's decision to file charges against Chinese hackers, and predicting that the United States would never put its hands on the defendants).

[86] Committee on Oversight and Government Reform, The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation? (2016), *available at* https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[87] The stolen data included personal files of 4.2 million former and current employees, security clearance investigation information on 22.1 million individuals, and biometric data of 5.6 million individuals.

[88] Ian Tuttle, *Cyber Disaster: How the Government Compromised Our Security*, Nat'l Rev. (Sept. 9, 2016), *at* http://www.nationalreview.com/article/439869/opm-hack-house-oversight-committee-report.

[89] Ellen Nakashima, *Chinese Government Has Arrested Hackers it Says Breached OPM Database*, Wash. Post (Dec. 2, 2015), *at* https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-breaching-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html?utm_term=.65fd5ee72a90.

[90] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People*, Wash. Post (July 9, 2015), *at* https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/?utm_term=.655600c9d982.

[91] David Boyer, *Obama Says US Must Boost Cyber Defenses, Stops Short of Blaming China for Hacking*, Wash. Times (June 8, 2015), *at* http://www.washingtontimes.com/news/2015/jun/8/obama-says-us-must-boost-cyber-defenses.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

cyber issues at the U.S. Department of State, stated in Congressional testimony in May 2016, that this "kind of intrusion is just too big to ignore and too disruptive and it is a real concern."[92] James Clapper, the then head of the Office of the Director of National Intelligence (ODNI), was the only senior official in the Obama adminsitration who pointed the finger at China by stating publicly that: "you have to kind of salute the Chinese for what they did."[93] This may have been, however, a slip of a tongue, as no other statements were made to that effect by U.S. officials in the Obama administration.[94] Yet the information gathered by American security agencies over time strengthened the assessment that the attackers were Chinese,[95] and President Obama considered imposing sanctions against individuals or groups engaged in that operation.[96]

China has repeatedly insisted that its government played no role in the OPM hack, and its Foreign Ministry spokesman described the unofficial accusations as "irresponsible and unscientific."[97] Still, on December 2, 2015, it was reported that the Chinese authorities had arrested Chinese hacktivists suspected for the OPM hack, and that they would be investigated and prosecuted. The arrests took place in September 2015, a few days before a summit meeting between the leaders of the United States and China.[98] The Americans were informed about the arrests, but nothing has been published about the results of the Chinese investigation, including information on the identity of the attackers, their motives, and what became of the stolen data.

[92] Hearing Before the Subcommittee on East Asia, the Pacific, and International Cyber Security Policy of the Committee on Foreign Relations – United States Senate, International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms, at 15, 114th Congress, 2d Sess., May 25, 2016, *available at* https://www.govinfo.gov/content/pkg/CHRG-114shrg28853/pdf/CHRG-114shrg28853.pdf.

[93] David Welna, *In Data Breach, Reluctance to Point the Finger at China*, NPR (July 2, 2015), *at* http://www.npr.org/sections/parallels/2015/07/02/419458637/in-data-breach-reluctance-to-point-the-finger-at-china.

[94] Boyer, *supra* note 91. President Obama, when asked about the OPM hack in a press conference, refrained from leveling specific accusations against any specific actor, and presented his general view on current cyberoperations: "[B]oth State and non-state actors are sending everything they've got at trying to breach these [U.S.] systems. In some cases, it's non-state (actors) engaging in criminal activity and potential theft. In the case of state actors, they're probing for intelligence or, in some cases, trying to bring down systems in pursuit of their various foreign-policy objectives."

[95] Brendan I. Koerner, *Inside the Cyber-Attack that Shocked the US Government*, WIRED (Oct. 23, 2016), *at* https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government (referring to a wealth of evidence, ranging from IP addresses to telltale email accounts and a remote-access tool commonly deployed by Chinese-speaking hacking units on computers used by foes of China's government. Those footprints indicate that the hackers were tied to China, and that, in addition, the operation does not have any financial or commercial motive, but rather appears to serve the needs of intelligence services. Finally, the hack required professional human resources at a scale only governmental authorities are likely to have.).

[96] Michael D. Shear & Scott Shane, *White House Weighs Sanctions After Second Breach of a Computer System*, N.Y. TIMES (June 12, 2015), *at* https://www.nytimes.com/2015/06/13/us/white-house-weighs-sanctions-after-second-breach-of-a-computer-system.html. *See also* TIM MAURER, CYBER MERCENARIES: THE STATE, HACKERS, AND POWER 56 (2018).

[97] Ellen Nakashima, *Chinese Hack of Federal Personnel Files Included Security-Clearance Database*, WASH. POST (June 12, 2015), *at* https://www.washingtonpost.com/world/national-security/chinese-hack-of-government-network-compromises-security-clearance-files/2015/06/12/9f91f146-1135-11e5-9726-49d6fa26a8c6_story.html?utm_term=.9ea58a001b11.

[98] Nakashima, *supra* note 89. Interestingly, President Trump informally attributed the OPM hack to China during a phone interview to the *New York Times* in January 2017, in which he said: "China, relatively recently, hacked 20 million government names. How come nobody even talks about that?" This statement might relate to Trump's efforts to minimize the significance of Russian cyber operations, which allegedly influenced the presidential election. *See* Michael D. Shear & David E. Sanger, *Putin Led a Complex Cyberattack Scheme to Aid Trump, Report Finds,* N.Y. TIMES (Jan. 6, 2017), *at* https://www.nytimes.com/2017/01/06/us/politics/donald-trump-wall-hack-russia.html?_r=0.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

The incident was handled through bilateral diplomacy and professional channels as if it was a criminal act or an act of "hacktivism," not a state-sponsored operation. However, this official framing of the OPM hack is improbable. In the view of William Evanina, the director of the National Counterintelligence and Security Center,[99] the prospect that another country has the stolen data in its possession is higher than the alternative (i.e., that the information is held by criminal hackers, motivated by financial profit). The director observed that those who hold the data have not yet shared it. That made him more confident "that a foreign government did take it and, from an intelligence perspective, I know they'll keep it close hold."[100] Still, Evanina maintained the official line of refraining from publicly attributing responsibility to China.

c. Response

According to press reports, U.S. officials, including NSA director Admiral Rogers, and James Clapper, proposed taking response actions against China, such as covert cybermeasures or punitive economic sanctions, in order to deter future cyberattacks.[101] This suggests that at least two senior U.S. officials were inclined to view the operation as unacceptable—either as a violation of international law governing cyberspace or as a lawful, but exceptionally unfriendly act that violates informal rules of conduct in cyberspace—and that an overt or covert response measure was justified and even necessary for promoting deterrence against future operations. Others warned, however, against retaliating in response to what was actually an espionage operation, implying that the United States might be engaged in comparable operations.[102] Eventually, the administration did not retaliate; nor did it contest China's claim that it had opened a criminal investigation against private hackers.

In light of Evanina's statements,[103] it is highly likely that the U.S. administration took a deliberate decision to handle the OPM hack as an espionage operation and not to assign direct or indirect responsibility for it to China. Once qualified as an act of espionage, the operation is not considered under the Tallinn Rules as unlawful per se.[104] Such an act of qualification, if it indeed occurred, also limited the scope of legally permissible responses by the United States. And indeed, it appears that the U.S. response mostly constituted of undertaking necessary steps to improve defensive capacities and to reduce the adverse ramifications of the operation.

Notwithstanding the ultimate treatment of the OPM hack as a cyberespionage operation, the case was included within our list of case studies for several reasons. First, the operation appears to have had a major disruptive effect on government activities in the field of national security, including delays in the issuance of security contracts requiring background checks and undermining of trust in the ability of the United States to protect sensitive

[99] Chris Strohm, *Hacked OPM Data Hasn't Been Shared or Sold, Top Spy-Catcher Says*, BLOOMBERG POL. (Sept. 28, 2017), *at* https://www.bloomberg.com/news/articles/2017-09-28/hacked-opm-data-hasn-t-been-shared-or-sold-top-spy-catcher-says.

[100] *Id.*

[101] David E. Sanger, *US Decides to Retaliate Against China's Hacking*, N.Y. TIMES (July 31, 2015), *at* https://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?mcubz=0.

[102] Nakashima, *supra note* 90, (citing, inter alia, Rep. Adam Schiff stating that if the United States blurs the line between economic spying and foreign intelligence spying, "we risk undermining the fight against economic theft").

[103] Strohm, *supra* note 99.

[104] TALLINN MANUAL 2.0, *supra* note 1, Rules 32, 89. *See also* Pun, *supra* note 59.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

information.[105] Such operational and reputational harm exceed the scope of damage caused by "normal" interstate espionage operations. Indeed, the operation was regarded by some U. S. policymakers as tantamount to an armed attack ("Cyber Pearl Harbor") or as a possible violation of international norms of conduct justifying response measures (e.g., economic sanctions). The case study therefore illustrates the claim that we develop later in the article that due to the uncertain and ambiguous state of international law governing cyberoperations, states exercise significant discretion in applying or dis-applying the relevant international law rules (including a choice whether or not to rely on the Tallinn Rules). What appears to be a conscious decision by U.S. officials to qualify the OPM hack as an "acceptable" act of espionage, and not as an unlawful cyberoperation, may underscore the existence of such a choice.

Second, the OPM hack has been handled by the administration and the House of Representatives with a relatively high level of transparency, as a test case for American policy toward harmful cyberoperations. This allows us to distinguish between, on the one hand, forms of response to cyberoperations that were considered at the time by U.S. decisionmakers to be within the boundaries of accepted norms of international law or other, informal, norms governing interstate relations, and, on the other hand, forms of response which were considered excessive or counterproductive. The availability of two "parallel tracks" of regulation of cyberoperations, involving formal and informal rules of conduct, and the existence of gradations in law enforcement, resulting in the treatment of certain rules of international law as virtually non-enforceable, are further discussed in Part IV of this article.

It may be observed that had the OPM data been stolen entirely, without the option of restoring it, a question could have been raised as to whether the operation should be still regarded as a mere act of espionage. At least according to some commentators, altering or permanently erasing sensitive data should be considered as an operation with a use of force or sovereignty infringement dimensions.[106]

3. Cyberoperation against the Sands Casino (2014)[107]

a. Principal facts

On February 10, 2014, the computer systems of the Sands Casino in Bethlehem, Pennsylvania were hacked, and major communication and computer system functions became paralyzed, adversely affecting the company's operation in a significant and long-

[105] Dianna Cahn, *Effects of OPM Data Breach Are Far-Reaching*, GOV'T TECH. (July 13, 2015), *at* http://www.govtech.com/security/Effects-of-OPM-Data-Breach-Are-Far-Reaching.html; Joseph Marks, *Greatest Damage from OPM Breach Was to Government's Reputation*, NEXTGOV (Apr. 10, 2017), *at* https://www.nextgov.com/cybersecurity/2017/04/greatest-damage-opm-breach-was-governments-reputation/136902; Michael Adams, *Why the OPM Hack Is Far Worse Than You Imagine*, LAWFARE (Mar. 11, 2016), *at* https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine; Kristin Finklea, Michelle D. Christensen, Eric A. Fischer, Susan V. Lawrence & Catherine A. Theohary, *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*, CONG. RES. SERV. REP. (2015), *available* at https://digitalcommons.ilr.cornell.edu/key_workplace/1440; Ian Brown, *Imaging A Cyber Surprise: How Might China Use Stolen OPM Records to Target Trust?*, WAR ON THE ROCKS (May 22, 2018), at https://warontherocks.com/2018/05/imagining-a-cyber-surprise-how-might-china-use-stolen-opm-records-to-target-trust.

[106] *See, e.g.*, Stavridis, *supra* note 24.

[107] *FBI and Secret Service Investigating Las Vegas Casino*, HACKER5 MAGAZINE (Feb. 28, 2014); *Las Vegas Sands Sites Hacked as Posts Criticize CEO Sheldon Adelson's Politics*, POSTMEDIA (Feb. 12, 2014).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

term manner. Moreover, hard drives were wiped, and a huge quantity of essential data was permanently erased. Experts assessed that such a cyberoperation required a high level of technological capacity, most likely possessed by a state or a state-sponsored group of hackers.[108]

The attackers took control of all of the Sands Casino's websites and posted on them an image of the world's map with flames coming out from the Sands Casino's worldwide locations, a snapshot of Sheldon Adelson, the majority owner of the Sands Corporation, with the Israeli prime minister, and a message condemning the use of weapons of mass destruction.

b. Attribution

The cyberoperation directed against the Sands Casino appears to have been made in response to Adelson's suggestion, offered in October 2013, to drop a small nuclear bomb on the Iranian desert in order to demonstrate U.S. strength and deter Iran from pursuing its nuclear ambitions. Only one year later, on February 2, 2015, a seemingly spontaneous comment was made by the then U.S. Director of National Intelligence, James Clapper, relating to the Sands Casino operation. During a meeting with the U.S. Senate Armed Services Committee, Clapper noted that the operation was the first destructive cyberattack launched by a foreign state, in that case Iran, aimed at an American private company on U.S. soil.[109]

c. Response

The incident was reported to the FBI, which began to investigate it in conjunction with the local state police. No further action has been reported; nor were any further details about the investigation and its findings ever released.

4. Hacking Sony Pictures Entertainment[110]

a. Principal facts

"The Interview" is a Sony Pictures Entertainment (SPE) comedy film, which describes a plot to assassinate the North Korean dictator, Kim Jong-un. The movie's premier was scheduled for December 18, 2014, with wider release scheduled for Christmas Day 2014. Six months earlier, the North Korean regime tried to stop the distribution of the film by taking measures such as sending an official letter sent to the UN secretary-general, labeling the movie the most "undisguised sponsoring of terrorism, as well as an act of war,"[111] and threatening to act with "decisive and merciless countermeasure (if) the US administration tacitly approves or supports" the release of the film. The North Korean minister of foreign affairs further

[108] Tony Capaccio, David Lerman & Chris Strohm, *Iran Behind Cyber-attack on Adelson's Sands Corp., Clapper Says,* BLOOMBERG (Feb. 26, 2015), *at* https://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says.

[109] Jose Pagliery, *Iran Hacked an American Casino, US Says*, CNN TECH (Feb. 27, 2015), *at* http://money.cnn.com/2015/02/27/technology/security/iran-hack-casino/index.html.

[110] Gary Leupp, *A Chronology of the Sony Hacking Incident*, COUNTERPUNCH (Dec. 29, 2014), *at* http://www.counterpunch.org/2014/12/29/a-chronology-of-the-Sony-hacking-incident.

[111] *Id.*

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

published a statement objecting to the release of the movie, using expressions such as "terrorism," and "a war action" and threatening "decisive and merciless countermeasure."[112]

On November 24, 2014, a hacking group, identifying itself as the "Guardians of Peace" (GoP), exfiltrated confidential data from SPE's servers. It then gradually released stolen data, over a period of three weeks. The stolen data included, inter alia, information about new film productions that had not yet been released, and a huge quantity of personal information relating to the company's executives, including emails and confidential correspondence among themselves and with celebrities in the movie industry. Following consultations with government officials and private consultants, SPE decided to release the original version of the film as planned.[113] Although the first GoP emails to SPE management and employees included a general demand for monetary compensation, the real motive of the operation appears to have been an attempt to prevent the film's global distribution as well as an attempt to deter SPE and other studios from insulting the North Korean regime.

On December 16, 2014, the GoP released a written message threatening to commit terror attacks against theaters screening the movie. The message included reference to the terror attacks of 9/11: "The world will be full of fear. Remember the 11th of September 2001. We recommend you to keep yourself distant from the places at that time (If your house is nearby, you'd better leave)."[114]

The cyberoperation directed against SPE did not confine itself solely to data theft, but also comprised destructive malware that caused serious harm to SPE's computer infrastructure. More than 70 percent of its computers were melted down by malware and the company had to invest tens of millions of dollars in IT infrastructure repairs. Additionally, the hack exposed SPE to legal risks due to allegations of negligence in securing its data, and to loss of anticipated income for leaked unreleased films.

b. Attribution

The initial tendency of U.S. officials was to attribute the SPE operation to a foreign state, and the immediate suspect was North Korea. Later, suspicions were also raised vis-à-vis China or Russia and toward groups of hackers sponsored by these states.[115] Not surprisingly, no state assumed responsibility for the attack; to the contrary, each suspected nation denied

[112] Choe Sang-Hun, *North Korea Warns US Over Film Mocking Its Leader*, N.Y. TIMES (June 25, 2014), *at* https://www.nytimes.com/2014/06/26/world/asia/north-korea-warns-us-over-film-parody.html?mtrref=www.google.co.il&gwh=B3B3453BC13185E0E57B63F83177166B&gwt=pay&assetType=nyt_now.

[113] It turned out that, early in June 2014, SPE's CEO consulted with Bruce Bennett, a senior defense analyst in Washington DC, asking his advice on whether or not to preserve the movie's final scene, in which the head of the North Korean leader is blown up by U.S. CIA agents. Although cutting or changing the final scene might have eased the North Koreans' fury, Bennett's recommendation was to keep the film as it was, hoping that a movie "about the removal of the Kim family regime and the creation of a new government by the North Korean people" would "start a real thinking" among South and North Koreans who would watch it. That recommendation was supported by "very senior" U.S. government officials. *See id.*; Leupp, *supra* note 110; William Boot, *Exclusive: Sony Emails Say State Department Blessed Kim Jong-un Assassination in "The Interview,"* DAILY BEAST (Dec. 17, 2014), *at* http://www.thedailybeast.com/exclusive-sony-emails-say-state-department-blessed-kim-jong-un-assassination-in-the-interview.

[114] Boot, *supra* note 113.

[115] *A Breakdown and Analysis of the December, 2014 Sony Hack*, RBS (Dec. 5, 2014), *at* https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack. *See also* Alex Altman & Zeke J. Miller, *State Department Insists North Korea Behind Sony Hack*, TIME (Dec. 31, 2014), *at* http://time.com/3651171/sony-hack-north-korea-fbi/?xid=time_readnext.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

any involvement therein. Cybersecurity experts were divided as to whether North Korea was indeed the culprit as the FBI has insisted, or whether another state, or a group of private hackers did it.[116] Some have even raised the possibility that the hack was carried out by a company insider.[117]

The FBI, which led the investigation in conjunction with other law enforcement and intelligence agencies, had concluded that the Sony hack was attributable to North Korea. This conclusion was based on classified intelligence that could not be disclosed, and on circumstantial evidence, such as the technical similarity of the tools, methods, and infrastructure used in the Sony hack and other cyberoperations linked to North Korean actors that were directed, mainly, against South Korean sites.[118] On January 2, 2015, the U.S. administration officially announced that it holds North Korea responsible for the Sony hack.[119] Another U.S. senior official stated that North Korea crossed a threshold from "website defacement and digital graffiti" to an attack on computer infrastructure.[120]

It is worth noting that an investigation conducted jointly by Kaspersky Labs and AlienVault Labs also concluded that the SPE hackers were linked to hackers who have undertaken similar cyberactivities during 2015–2016, mostly against South Korean targets (including a South Korean nuclear power plant operator and Samsung).[121] Similar findings can also be found in the "Blockbuster Report" issued by another private cybersecurity company, Novetta.[122] Those technical findings support the FBI's conclusion attributing the operation to North Korea.

c. Response

The immediate response of SPE to the operation directed against it was the cancellation of the planned premier screening and distribution of the movie. This response was criticized publicly for incentivizing future cyber attackers, and for allowing foreign entities to impose their political agenda and to harm the application of the First Amendment on U.S. soil.[123]

Secretary of State John Kerry condemned North Korea for the Sony hack, stating that "these lawless acts of intimidation demonstrate North Korea's flagrant disregard for

[116] David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea After Sony Case*, N.Y. TIMES (Jan. 2, 2015), *at* https://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html (questioning the speediness of the FBI conclusions). *See also A Breakdown and Analysis*, *supra* note 115 (questioning attribution of the breach by the FBI to North Korea).

[117] Leupp, *supra* note 110 (arguing that North Korea does not have the advanced technological capability required to conduct such a destructive hack). *See also* Paul, *New Clues in Sony Hack Point to Insiders, Away from DPRK*, SECURITY LEDGER (Dec. 28, 2014), *at* https://securityledger.com/2014/12/new-clues-in-sony-hack-point-to-insiders-away-from-dprk.

[118] *Operation Blockbuster: Unraveling the Long Thread of the Sony Attack*, NOVETTA (Feb. 2016), *available at* https://www.operationblockbuster.com/wp-content/uploads/2016/02/Operation-Blockbuster-Report.pdf.

[119] White House Press Release, Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea" (Jan. 2, 2015), *available at* https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s.

[120] Sanger & Schmidt, *supra* note 116.

[121] Kim Zetter, *Evidence Suggests the Sony Hackers Are Alive and Well and Still Hacking*, WIRED (Dec. 2, 2016), *at* https://www.wired.com/2016/02/evidence-suggests-the-sony-hackers-are-alive-and-well-and-still-hacking.

[122] *Operation Blockbuster*, *supra* note 118.

[123] Oliver Laughland & Dominic Rushe, *Sony Pulling* The Interview *Was "a Mistake" Says Obama*, GUARDIAN (Dec. 20, 2014), *available at* https://www.theguardian.com/us-news/2014/dec/19/obama-sony-the-interview-mistake-north-korea.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

international norms."[124] When President Obama was asked in an interview whether the Sony hack was an act of war, he responded: "No, it was an act of cyber vandalism that was very costly." He added: "We will respond proportionally, and we'll respond in a place and time and manner that we choose."[125] He also indicated that he would review whether to put North Korea back on the state-sponsored terror list, mentioning this as one of the potential responses to be discussed and decided upon. Senator John McCain criticized the president's timid approach, claiming that the president failed to understand that this is "a manifestation of a new form of warfare."[126]

On January 2, 2015, the U.S. administration announced the imposition of new sanctions with respect to North Korea as the "first aspect of the (American) response" for creating "destructive financial effects on a US company and . . . [threatening] artists and other individuals with the goal of restricting their right to free expression."[127] The sanctions were imposed on ten individuals and three entities associated with the North Korean government. In addition, their entry into the United States and dealings with American entities were prohibited. The presidential order also included the seizing of property held by those individuals and entities in the United States. It has been remarked, however, that the seizure was mostly symbolic because few, if any, assets of targeted individuals or entities were likely to be located inside the United States.[128] It is not clear what specific evidence the U.S. administration had to connect the ten sanctioned individuals and entities to the Sony hack.

On December 24, 2014, North Korea's internet network was shut down for nine hours and connectivity became intermittent for the next two days. The disruption of internet service has been assumed be a covert response to the Sony hack,[129] based on the Obama

[124] *See* U.S. Dep't of State Press Release, Condemning Cyber-Attacks by North Korea (Dec. 19, 2014), *at* https://2009-2017.state.gov/secretary/remarks/2014/12/235444.htm.

[125] White House Press Release, Remarks by the President in Year-End Press Conference (Dec. 19, 2014), *available at* https://obamawhitehouse.archives.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference. *See also* Sean Sullivan, *Obama: North Korea Hack "Cyber-vandalism," Not "Act of War,"* WASH. POST (Dec. 21, 2014), *at* https://www.washingtonpost.com/news/post-politics/wp/2014/12/21/obama-north-korea-hack-cyber-vandalism-not-act-of-war/?utm_term=.a295316b9b98.

[126] *Id*. *See also* Michael B. Kelley & Armin Rosen, *The US Needs to Stop Pretending the Sony Hack Is Anything Less Than an Act of War*, BUSINESS INSIDER (Dec. 15, 2014), *at* http://www.businessinsider.com/sony-hack-should-be-considered-an-act-of-war-2014-12. The *Business Insider* story cited David Aitel, a former NSA research scientist, who opined that cyberattacks should be considered an act of war even when they do not meet the required threshold which might justify a military response and that once it has become known which nation should be held accountable, the United States must respond, at least with a firm diplomatic reaction, while considering additional measure in cyberspace, such as attacking targets of the adversary or shutting down the Internet for a while).

[127] White House Press Release, *supra* note 119.

[128] Sanger & Schmidt, *supra* note 116; *Sony Cyber-attack: North Korea Faces New US Sanctions*, BBC NEWS (Jan. 3, 2015), *at* http://www.bbc.com/news/world-us-canada-30661973. On September 6, 2018, the Department of Justice unsealed an indictment against Park Jin-Hyok, a North Korean citizen, charged with conspiracy to conduct multiple cyber operations, including the Sony hack. U.S. Dep't of Justice, Office of Public Affairs Press Release, North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions (Sept. 6, 2018), *at* https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[129] Chris Strohm, *North Korea Web Outage Response to Sony Hack, Lawmaker Says*, BLOOMBERG POL. (Mar. 17, 2015), *at* https://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sony-hack-lawmaker-says. *See also* Francesca Chambers, Lucy Crossley & Alexandra Klausner, *North Korea's Internet Is Shut Down AGAIN After Losing Connectivity for Nine Hours Yesterday*, DAILY MAIL (Dec. 23, 2014), *at* http://www.dailymail.co.uk/news/article-2885359/North-Korea-s-internet-shut-losing-connectivity-nine-hours-yesterday.html.

administration's strategy, which included covert actions as part of the U.S. response to hostile cyberoperations.

It is interesting to note that Admiral Rogers, the NSA director at the time, noted that he advised the president to strike back against North Korea, and stressed the need for "creating costs" for hackers in order to build up deterrence.[130] This is consistent with the position he expressed in connection with the OPM hack, according to which it is essential to adopt measures of deterrence against the escalating risk of cyberattacks.

5. The U.S. presidential campaign/Democratic National Committee hack (2016)[131]

a. Principal facts

In May 2016, six months before U.S. election day, the Democratic National Committee (DNC) invited a cyber security firm (CrowdStrike) to investigate a suspected breach of its network. The investigation team identified intrusions by two well-known hacking actors in cyberspace, the "Cozy Bear" (also referred to as Cozy Duke or APT 29) and the "Fancy Bear" (also known as Fancy Duke, Sofacy or APT 28). Both "Bears" had already established a reputation for being "some of the best adversaries out of all the numerous nation-state, criminal, and hacktivist/terrorist groups . . . ."[132] Cozy Bear intruded into the DNC computer system in the summer of 2015, and Fancy Bear had breached the system in April 2016. The investigation team did not find collaboration between the two intruders, or even mutual awareness of each other's activities.

On July 22, 2016, large quantities of written materials were published by WikiLeaks (almost 20,000 emails and 8,000 attachments written by key staff members of the DNC, dating to the period between January 2015 and May 2016). WikiLeaks did not reveal its source of data; still, a new hacker dubbed "Guccifer 2.0" claimed responsibility for the exfiltration (and denied any link to the Russian government). In parallel, the Gmail account of John Podesta, chairman of Clinton's campaign, was breached in March 2016 and thousands of emails were stolen from him. That exfiltration has also been investigated by cybersecurity experts, and "Fancy Bear" was identified as the offender. The stolen data was released gradually by WikiLeaks, from October 2016 until election Day (November 9, 2016).

The DNC hack had the essential components of an "influence cyberoperation" intended to modify attitudes and shape opinions through the dissemination of information and messages.[133] No significant harm was caused to any computer system (perhaps because

[130] Sanger, *supra* note 101.

[131] The facts described below are partial and subject to ongoing investigations by the Senate Select Committee on Intelligence (SSCI) and by Robert Mueller, a special counsel appointed by the deputy attorney general to investigate the Russian interference in the presidential election and related matters. The information presented here about the DNC hack is based mainly on Dmitri Alperovitch's blog. Alperovitch is the CTO of CrowdStrike. *See* Dmitri Alperovitch, *Bears in the Midst: Intrusion into the Democratic National Committee*, CROWDSTRIKE (June 15, 2016), *at* https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee. It should be noted that there are other narratives of the incident, such as the theory reported by Patrick Lawrence, *A New Report Raises Big Questions About Last Year's DNC Hack*, NATION (Aug. 9, 2017), *at* https://www.thenation.com/article/a-new-report-raises-big-questions-about-last-years-dnc-hack.

[132] *See* Alperovitch, *supra* note 131.

[133] *See* Pascal Brangetto & Matthijs A. Veenendaal, *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*, *in* CYBER POWER 113, 114 (N. Pissanidis, H. Rõigas & M. Veenendaal eds., 2016), *available at* https://ccdcoe.org/cycon/2016/proceedings/08_brangetto_veenendaal.pdf.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

indications of harm could lead to early detection of the data theft).[134] Still, the Obama administration regarded the operation as a serious provocation, with considerable national security implications. This assessment of the gravity of the operation was further compounded by revelations that parts of the operation sought to manipulate the election process itself, with a view to influencing the final tally.[135]

Indeed, a highly classified intelligence report dated May 5, 2017, which was obtained recently by the Intercept (an online news site),[136] sheds further light on key cyberactivities conducted at the final stage of the election campaign, aimed at influencing the results of the election. The report claims that Russian Military Intelligence executed a cyberoperation against at least one U.S. voting software supplier and sent spear-phishing emails to more than one hundred local election officials in thirty-nine states, between October 27 to November 1, 2016 (shortly before Election Day).

Jeanette Manffra, the head of cybersecurity at the Department of Homeland Security, confirmed that the Russians' cyber penetration efforts during the 2016 presidential campaign targeted twenty-one states and that an "exceptionally small number of them were actually successfully penetrated."[137] In the same vein, Michael Daniel, the former White House Cyber Security Coordinator, told a Senate Intelligence Committee hearing held on June 20, 2018, that since June 2016 it was understood that a Russian cyberoperation has been underway with the aim of influencing the elections, inter alia, through targeting the electoral infrastructure.[138] Daniel opined that it is highly likely the Russians scanned the electoral facilities in all fifty states, and that "it was more likely that we hadn't detected it than it didn't occur."[139]

The information revealed about the scope of the cyberoperation, the nature of the political data that was exfiltrated, and the way and the timing in which such data was exploited did not leave much room for speculation as to the political motives underlying the operation: to harm the Democratic campaign and reduce Hillary Clinton's chances of being elected. This conclusion was explicitly endorsed in a U.S. Intelligence Community Assessment Report (ICA)[140] submitted to the president and president-elect, on January 6, 2017 and reaffirmed

[134] Matthew Cole, Richard Esposito, Sam Biddle & Ryan Grim, *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, INTERCEPT (June 5, 2017), *at* https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election.

[135] Intelligence Community Assessment (ICA), Background to *"Assessing Russian Activities and Intentions in Recent US Elections": The Analytical Process and Cyber Incident Attribution* (Jan. 6, 2017), *available at* https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

[136] Cole, Esposito, Biddle & Grim, *supra* note 134; see the authentic document dated May 5, 2017, *available at* https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1.

[137] Cynthia Mcfadden, William Arkin & Kevin Monahan, *Russians Penetrated US Voter Systems, Top US Official Says*, NBC NEWS POL. (Feb. 8, 2018), *at* https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721.

[138] Michael Isikoff, *Obama Cyber Chief Confirms "Stand Down" Order Against Russian Cyberattacks in Summer 2016*, YAHOO NEWS (June 20, 2018), *at* https://www.yahoo.com/news/obama-cyber-chief-confirms-stand-order-russian-cyberattacks-summer-2016-204935758.html. *See also Russia Election Interference*, C-SPAN, (Senate Intelligence Committee Hearing, June 20, 2018), *at* https://www.c-span.org/video/?447328-1/obama-administration-officials-testify-russia-election-interference.

[139] Andrew Blake, *Russian Hackers Likely Scanned Election Systems in all 50 States During 2016 Race: Obama Cyber Czar*, WASH. TIMES (June 21, 2018), *at* https://www.washingtontimes.com/news/2018/jun/21/russian-hackers-likely-scanned-election-systems-al.

[140] ICA, *supra* note 135.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

in the initial findings published by the Senate Select Committee on Intelligence (SSCI) on July 3, 2018.[141] The question whether the cyberoperation has actually had any impact on the election results is still a hotly disputed issue in the United States political system.[142]

b. Attribution

An investigative team commissioned by CrowdStrike at the request of the DNC to investigate the breach concluded that the "Bears" have engaged in extensive cyberespionage operations, targeting defense, energy, finance, government, and media sectors, mostly in the United States, but also in other countries around the world.[143] The team also considered the lack of collaboration between the Bears alongside with the responsibility claimed by Guccifer 2.0, but did not find it sufficient to negate the overwhelming indications suggesting Russian responsibility for the intrusions. It explained that such disorder is typical in the Russian Intelligence Community (RIC).[144] According to this line of thinking, Guccifer 2.0's claim of responsibility was false, and was induced by elements related to RIC in order to deflect responsibility away from Russia. Ultimately, the team concluded that Russia was behind the DNC hack through its proxies, the "Bears," who "are believed to be closely linked to the Russian government's powerful and highly capable intelligence services."[145] Other research cybersecurity firms such as Mandiant and ThreatConnect reached the same conclusions.[146] Based on sources affiliated with the FBI and Robert Mueller's special counsel investigation, the Daily Beast recently reported that Guccifer 2.0 slipped up and inadvertently exposed itself as an officer of the Russian military intelligence agency (GRU), working out of the agency's headquarters in Moscow.[147]

On October 7, 2016, the U.S. Intelligence Community (USIC) published a Joint Statement[148] expressing its confidence that "the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations . . . ." On December 9, 2016, President Obama directed the USIC to conduct a full review and produce a comprehensive intelligence report assessing Russian activities and intentions in recent U.S. elections. A report was prepared and submitted to the president and the

[141] Senate Select Committee on Intelligence (SSCI), Initial Findings (July 3, 2018), *available at* https://www.burr.senate.gov/imo/media/doc/SSCI%20ICA%20ASSESSMENT_FINALJULY3.pdf.

[142] *Id.* Following the DNC Hack, the then DHS Secretary Jeh Johnson decided in January 2017 to designate the nation's electoral systems as federally protected critical infrastructure.

[143] *See* Alperovitch, *supra* note 131.

[144] The claim of "typical disorder" appears to us as somewhat implausible. It is more likely that intentional disorder was created in order to obfuscate the situation and divert suspicions from Russian Intelligence.

[145] Alperovitch, *supra* note 131.

[146] Ellen Nakashima, *Cyber Researchers Confirm Russian Government Hack of Democratic National Committee*, WASH. POST (June 20, 2016), *at* https://www.washingtonpost.com/world/national-security/cyber-researchers-confirm-russian-government-hack-of-democratic-national-committee/2016/06/20/e7375bc0-3719-11e6-9ccd-d6005beac8b3_story.html?utm_term=.4d8ae7360f6c. *See also* Sam Thielma, *DNC Email Leak: Russian Hackers Cozy Bear and Fancy Bear Behind Breach*, GUARDIAN (July 26, 2016), *at* https://www.theguardian.com/technology/2016/jul/26/dnc-email-leak-russian-hack-guccifer-2.

[147] Kevin Poulsen & Spencer Ackerman, *EXCLUSIVE: "Lone DNC Hacker" Guccifer 2.0 Slipped Up and Revealed He Was a Russian Intelligence Officer*, DAILY BEAST (Mar. 22, 2018), *at* https://www.thedailybeast.com/exclusive-lone-dnc-hacker-guccifer-20-slipped-up-and-revealed-he-was-a-russian-intelligence-officer.

[148] U.S. Dep't of Homeland Security Press Release, Joint Statement, the Department of Homeland Security & Office of the Director of National Intelligence on Election Security (Oct. 7, 2016), *at* https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national.

president-elect separately, and a declassified version of it was published on January 6, 2017.[149] The key finding of the report was that President Putin himself ordered a Russian multifaceted influence campaign to "undermine public faith in the US democratic process."[150]

Two specific points are particularly noteworthy in this regard: First, the USIC identified and analyzed the technical footprints found in the specific hacks in question and reached unanimous conclusions. As indicated before, this outcome conforms to the findings and conclusions of numerous private cybersecurity firms that investigated the same intrusions. Second, the ICA did not include classified evidence that would clearly attribute responsibility to Russia for the cyberoperation. Still, despite this, the USIC was able to attribute responsibility for the operation, explicitly and with a high degree of confidence, to Russian intelligence services.

Russia has regularly denied any involvement in the presidential campaign hacks and has challenged the United States to publicly present evidence establishing its involvement and responsibility. In a news interview published shortly before the elections, President Putin expressed the Russian position emphasizing that: (1) Russian officials did not have enough of an understanding of American politics to successfully compromise the election even if they wished to; (2) "[O]n a State level Russia has never done this," and this is probably the work of private hackers, who may have deliberately left marks of others in order to camouflage their activities; and (3) "The important thing is the content that was given to the public . . . . There's no need to distract the public's attention from the essence of the problem by raising some minor issues connected with the search for who did it."[151]

c. Response

The first leak of emails through WikiLeaks occurred on July 22, 2016, and the first official attribution of the intrusions to Russia was made in the Joint Statement of the USIC on October 7, 2016.[152] Both occurred during the election campaign, inflaming tensions between the different political camps. Given the concern that the election infrastructure itself, i.e., the voting system, would be targeted,[153] it was reported that a senior advisor to Obama urged him to send an ultimatum to Putin containing the following message: "Mess with the vote and we will consider it an act of war."[154] According to the same report, the president did not want to inflame an already tense situation. Therefore, in September 2016, when Obama met Putin during the G20 summit in China, he did not use the term "act of war." Instead, he warned the Russian leader "to cut it out," and that there were going to be "serious consequences if he didn't."[155] In fact, it is alleged that there was no subsequent tampering with

[149] *See* ICA, *supra* note 135.

[150] *Id.* at 1.

[151] Nick Gass, *Putin on DNC Leak: "Does it Even Matter Who Hacked this Data?,"* POLITICO (Sept. 2, 2016), *at* http://www.politico.com/story/2016/09/putin-interview-dnc-hack-227668.

[152] *See* Joint Statement, *supra* note 148.

[153] Louis Nelson, *Obama Says He Told Putin to "Cut It Out" on Russia Hacking*, POLITICO (Dec. 16, 2016), *at* http://www.politico.com/story/2016/12/obama-putin-232754 (What Obama was concerned about was the potential of "hamper[ing] the vote counting [an]d affect[ing] the actual election process itself.").

[154] William M. Arkin, Ken Dilanian & Cynthia McFadden, *What Obama Said to Putin on the Red Phone About the Election Hack*, NBC NEWS (Dec. 20, 2016), *available at* https://perma.cc/5CKG-G5XC.

[155] Nelson, *supra* note 153.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

the election process.[156] Obama explained later that by sending out a warning, he prevented Russian hacking into the election infrastructure that could compromise the integrity of the voting process.

In retrospect, it appears that even if President Obama's warning in September 2016 prevented a disruption of the voting process itself, it had little impact on the broader Russian influence campaign. First, the "Bears" ended their intrusive activities at least four or five months prior to Election Day, and the director of Homeland Security "assesse[d] that the types of systems [they] targeted or compromised were not involved in vote tallying."[157] Second, the leakage of information and resort to other means designed to influence the election outcomes continued even more intensively as Election Day approached despite American warnings.[158]

It has been reported that the White House asked the CIA in October 2016 to prepare options for a covert cyberoperation designed to harass and embarrass the Russian leadership. Vice President Biden reportedly expressed support for such a counteroperation, designed to send "a message" to Putin, hinting that "it will be at the time of our choosing, and under the circumstances that will have the greatest impact."[159] Arguably, the vice president implied that a clandestine operation was being considered or is underway.[160] It has been alleged, in this regard, that Admiral (ret.) James Stavridis, the former NATO supreme allied commander Europe, called for a proportional covert response in cyberspace, such as interfering with Russia's ability to censor internal internet traffic and exposing Putin's financial dealings, with a view to embarrassing the Russian leadership and influencing Russian public opinion.[161] In his view, if the United States were not to respond to the Russian cyberoperation, it would lose its power of deterrence and suffer from more serious cyberattacks in the future.

Still, some policy advisers to the White House reportedly opposed the idea of a covert response, preferring instead the use of more conventional responsive measures, such as economic sanctions. For example, an unnamed former senior CIA official was quoted as being critical of engaging in covert cyber counteroperations: "anything the U.S. can do[,] . . . the Russian can do in response."[162] Michael Morell, the former CIA deputy director, noted that covert attacks on computer networks initiated by the United States would set a bad precedent for other countries who may seek to imitate it, including when operating against the United States.[163]

[156] *Id.*

[157] *See* ICA, *supra* note 135, at 3.

[158] *Russia Election Interference*, *supra* note 138, at 36:17–37:00 (testimony by Ambassador Victoria Nulland, former assistant secretary of state for European and Eurasian affairs).

[159] William M. Arkin, Ken Dilanian & Cynthia McFadden, *CIA Prepping for Possible Cyber Strike Against Russia*, NBC NEWS (Oct. 14, 2016), *at* www.nbcnews.com/news/us-news/cia-prepping-possible-cyber-strike-against-russia-n666636.

[160] President Obama himself adopted similar language, saying: "I think there is no doubt that when any foreign government tries to impact the integrity of our elections . . . we need to take action. And we will—at a time and place of our own choosing. Some of it may be explicit and publicized; some of it may not be." Scott Detrow, *Obama on Russian Hacking: "We Need to Take Action. And We Will,"* NPR (Dec. 15, 2016), *at* http://www.npr.org/2016/12/15/505775550/obama-on-russian-hacking-we-needto-take-action-and-we-will.

[161] *See* Arkin, Dilanian & McFadden, *supra* note 159.

[162] *Id.*

[163] *Id.*

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Apparently, the internal debate ended on October 31, 2016, with the president's decision to use the "red phone" to stop Russian cyberactivities.[164] It was reported that Obama sent out an urgent, written warning emphasizing, inter alia, that "international law, including the law for armed conflict, applies to actions in cyberspace."[165] The practical meaning of the warning and its allusion to the law for armed conflict, appears to have been that if Russia would interfere in the American election process, by hacking the voting infrastructure or through other means, the United States might consider it as an armed attack and might exercise the right to defend itself. As explained below, such a warning, if indeed given, suggests that the United State was ready to adopt an interpretation of international law applicable to cyberoperations that goes beyond the provisions of the Tallinn Rules that insist on the occurrence of kinetic harm for triggering an armed conflict.

On December 15, 2016, when President Obama was asked about the policy he implemented to tackle the Russian cyber interference in the election process, he responded as follows:

> Our goal continues to be to send a clear message to Russia or others not to do this to us because we can do stuff to you. But it is also important for us to do that, in a thoughtful methodical way. Some of it we do publicly. Some of it we will do in a way that they know but not everybody will . . . . So at a point in time where we've taken certain actions that we can divulge publicly, we will do so. There are times when the message will be directly received by the Russians and not publicized.[166]

It is difficult to ascertain on the basis of open source intelligence whether and how the reported "red phone" warning affected the Russian cyberoperation. As noted above, there are some indications that there were continued cyberoperations directed against the U.S. election process, even after October 31, 2016, although there is a scarcity of information about their precise source.[167] There is also no publicly available information about any covert U.S. counteroperation against Russia.

On December 29, 2016, President Obama issued an Executive Order[168] assuming additional authority for responding to certain cyberactivities that seek to interfere with or undermine election processes and institutions.[169] Using this new source of authority, nine Russian entities were subject to economic sanctions, two Russian compounds in Maryland and New York that had been used by Russian personnel for intelligence-related purposes were shut down, and thirty-five Russian intelligence operatives were declared *persona non grata*.

[164] The "red phone" is a confidence-building measure for communication, upgraded by Obama and Putin in 2013. It is to be activated in urgent and very sensitive situations.

[165] *See* Arkin, Dilanian & McFadden, *supra* note 154.

[166] *See* Nelson, *supra* note 153.

[167] Erik Lipton, *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), *at* https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

[168] Exec. Order No. 13757, Dec. 28, 2016, "Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities," 82 CFR 1 (2016), *available at* https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/executive-order-taking-additional-steps-address-national-emergency.

[169] White House Press Release, Presidential Statement on Actions in Response to Russian Malicious Cyber Activity and Harassment (Dec. 29, 2016), *available at* https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

In addition, Homeland Security and the FBI released declassified technical information on the cyberactivities of various Russian civilian and military intelligence services, in order to assist cybersecurity experts in the United States and abroad to identify, detect, and disrupt Russia's global campaign of covert cyberoperations.

Obama ended his December 29 press release with the following statement:

> These actions are not the sum total of our response to Russia's aggressive activities. We will continue to take a variety of actions at a time and place of our choosing, some of which will not be publicized . . . [T]he United States and friends and allies around the world must work together to oppose Russia's efforts to undermine established international norms of behavior, and interfere with democratic governance.[170]

This statement appears to suggest that the United States may be open to regard influence campaigns as running contrary to international law governing cyberoperations, thus lending support for an expansive reading of the rule of non-intervention, or for accepting the position of the Tallinn Manuals that international law prohibits operations that violate state sovereignty. Such an interpretation of President Obama's statement would seem to support a move away from the United States' previous policy of legal ambiguity toward the contents of international law governing cyberoperations, as a first possible step toward imposing sanctions against Russia by the United States and its allies.

Alternatively, the allusion in the president's statement to "international norms of behavior" may suggest that the United States only took that the position that the Russians violated informal norms governing state conduct in cyberspace barring "interference with democratic governance," without expressing a view on whether specific international law norms were also violated. Under this alternative construction of the statement, the policy of ambiguity toward the contents of international law in cyberspace and the status of the Tallinn Rules was maintained after all.

On February 16, 2018, the U.S. Department of Justice (DOJ) announced that thirteen Russians and three Russian companies have been indicted by a grand jury for committing federal crimes

> while seeking to interfere in the United States political system, including the 2016 Presidential election.[171] The defendants allegedly conducted what they called "information warfare against the United States," with the stated goal of "spread[ing] distrust towards the candidates and the political system in general."[172]

[170] *Id. See also* Rebecca Crootof, *The DNC Hack Demonstrates the Need for Cyber-Specific Deterrents,* LAWFARE (Jan. 9, 2017), *at* https://www.lawfareblog.com/dnc-hack-demonstrates-need-cyber-specific-deterrents ("Despite this being the strongest public action the United States has ever taken in response to a cyberoperation, many are bemoaning its inadequacy. The U.S. actions have been derided as 'too little, too late,' 'confusing and weak,' and 'insufficient.' However, this seemingly insufficient reaction may have been informed by international law; the United States might have responded to the DNC hack as it did because international law did not permit it to do more.").

[171] U.S. Dep't of Justice Press Release, Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System (Feb. 16, 2018), *at* https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[172] *Id.*

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

According to the indictment,[173] the defendants conspired, from 2014 onward, to defraud the United States by "impairing, obstructing, and defeating the lawful functions of government . . . "[174] through interference with the American political and electoral processes. Their operation was facilitated by Internet Research Agency (IRA), a Russian company based in St. Petersburg, Russia, which employed twelve out of the thirteen defendants, and through two other Russian companies with many subsidiaries and affiliates, funded and controlled by their owner, Yevgeniy Prigozhin, a well-connected Russian billionaire, dubbed "the Kremlin's Chef." Prigozhin was included in July 2017 on the list of Russians sanctioned by the presidential executive order and was indicted in February 2018. He is presumed to be the person behind Russia's internet "troll factories."[175]

The IRA allegedly employed hundreds of people for online and offline activities and controlled an annual budget of millions of dollars to fund those activities. It established and operated—under covert American identities (stolen or fictitious)—hundreds of accounts within U.S. social networks such as Facebook, Instagram, and Twitter. These accounts were used to communicate with the American audience, to sow political discord, and to foster certain political activities. The deputy attorney general emphasized that none of the Americans cooperating with the indicted Russians did it with a mindset of promoting foreign interests and reiterated the position that the charges did not imply that Russian activities actually influenced the outcome of the elections.[176]

On July 13, 2018, the special counsel, Robert S. Mueller III, indicted twelve Russian GRU intelligence officers for hacking into Democratic Congressional Campaign Committee (DNCC) and DNC computers, stealing vast quantities of emails and documents, and staging their release with a view to influencing the U.S. presidential election.[177] The indictment alleges that the GRU officers were behind the leaks made by "DCLeaks" and "Guccifer 2.0." They were also charged with identity theft, and using cryptocurrencies for money laundering purposes. Two Russian officers were indicted for hacking computers charged with administering the 2016 elections, with a view to stealing voter data and other information. Indicting Russian nationals who acted directly and indirectly on behalf of the Russian government, knowing that they would, most probably, never be extradited, conforms to the U.S. policy of "naming and shaming" applied in other cyberoperation cases.

Finally, it is worth noting that in March and April 2018, the U.S. administration imposed sanctions on Russian government hackers known as "trolls," on Russian organizations such as the IRA, GRU, FSB (the successor of the KGB), and on seventeen senior Russian government officials from Putin's inner circle. Those measures were undertaken pursuant to the

[173] Indictment, United States v. Internet Research Agency LLC, Case No. 1:18-cr-00032-DLF (D.C. Cir., Feb. 18, 2018), *available at* https://www.justice.gov/opa/press-release/file/1035562/download.

[174] *Id.*, para.2.

[175] Jon Swaine & Marc Bennetts, *Robert Mueller Charges 13 Russians with Interfering in US Election to Help Trump*, GUARDIAN (Feb. 17, 2018), *at* https://www.theguardian.com/us-news/2018/feb/16/robert-mueller-russians-charged-election.

[176] *See* U.S. Dep't of Justice Press Release, *supra* note 171; Matt Apuzzo & Sharon LaFraniere, *13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign*, N.Y. TIMES (Feb. 16, 2018), *at* https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html.

[177] Indictment, United States v. Netyksho, Case No. 1:18-cr-00215-ABJ (D.C. Cir., July 13, 2018), *available at* https://int.nyt.com/data/documenthelper/80-netyksho-et-al-indictment/ba0521c1eef869deecbe/optimized/full.pdf?action=click&module=Intentional&pgtype=Article.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Countering America's Adversaries Through Sanctions Act (CAATSA) as retaliation for Russia's destabilizing activities, including the meddling with the 2016 US election, the NotPetya attack, and additional cyberoperations targeting U.S. critical infrastructure facilities and striving to destabilize Ukraine.[178]

C. Cyberoperations Against Germany

1. Hacking the Bundestag Network (2015)[179]

a. Principal facts

In May 2015, the Bundestag was reportedly hacked by the APT28 Russian hacking group ("Fancy Bear"/"Sofacy") linked to GRU. Over 20,000 accounts were breached, and much data having strategic importance was stolen. Following the attack, the internal Bundestag network was shut down for several days as a precaution against additional attacks. Other cyberattacks against German political and public targets have followed, including attacks against German lawmakers, ministers, the Christian Democratic Union party, and foundations (think-tanks) affiliated with Germany's ruling coalition parties.

The motive for these cyberoperations, which did not cause long-term physical damage, appears to have been political: the gathering of political data, including data on the personal life of senior officials, which could be used for influencing public opinion and/or delegitimizing the democratic processes.[180]

b. Attribution

Bruno Kahl, the head of Germany's Foreign Intelligence Service, did not attribute the responsibility directly to Russia. He stated, however, that while attributing an attack to "a State agent is technically difficult . . . there is some evidence that this is at least tolerated or desired by the State."[181] He also added that his office has indications that the attacks came from the Russian region.[182] By contrast to that cautious approach, Hans-Georg Maassen, the head of the Federal Office for the Protection of the Constitution (BfV—the

[178] U.S. Dep't of the Treasury Press Release, Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks (Mar. 15, 2018), *at* https://home.treasury.gov/news/press-releases/sm0312. *See also* Ellen Nakashima, *Trump Administration Hits Russian Spies, Trolls with Sanctions Over US Election Interference, Cyberattacks*, WASH. POST (Mar. 15, 2018), *at* https://www.washingtonpost.com/world/national-security/trump-administration-sanctions-russian-spies-trolls-over-us-election-interference-cyber-attacks/2018/03/15/3eaae186-284c-11e8-b79d-f3d931db7f68_story.html?noredirect=on&utm_term=.f8cf97eb19d5; Donna Borak, *US Imposes Sanctions Against Russian Oligarchs and Government Officials*, CNN (Apr. 6, 2018), *at* https://edition.cnn.com/2018/04/06/politics/russia-sanctions-oligarchs/index.html.

[179] Raimund, *Germany Blames Russia for Cyberattacks*, HACKED PRESS (May 5, 2017), *at* https://hacked.press/2017/05/05/germany-blames-russia-cyberattacks; Andrea Shalal, *Germany Challenges Russia Over Alleged Cyberattacks*, REUTERS (May 4, 2017), *at* http://www.reuters.com/article/us-germany-security-cyber-russia-idUSKBN1801CA.

[180] Kate Connolly, *German Spy Chief Says Russian Hackers Could Disrupt Elections,* GUARDIAN (Nov. 29, 2016), *at* https://www.theguardian.com/world/2016/nov/29/german-spy-chief-russian-hackers-could-disrupt-elections-bruno-kahl-cyber-attacks.

[181] *Id.*

[182] *Id.*

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

German equivalent to the FBI), attributed the hacking campaign to Russia,[183] accusing its intelligence agencies of involvement in obtaining the data and in acts of sabotage.[184] Reacting to cyberoperations, which took place after the Bundestag hack, he claimed that Russia had tried to conduct an influence campaign in Germany, comparable to the one it has undertaken in connection with the U.S. presidential elections.[185] The head of the BfV thus put the Bundestag hack in a strategic context—global Russian influence operations conducted in order to further Russian interests through interference in the internal affairs of another state. A similar view was recently expressed by Theresa May, the UK prime minister, who cited the Bundestag hack and other cyberattacks conducted in different European nations as examples of Russian influence campaigns against Western democracies,[186] and strongly criticized this Russian *modus operandi*.[187]

c. Response

Based on the views expressed by the heads of German security agencies, German Chancellor Angela Merkel stated that "such cyberattacks, or hybrid conflicts as they are known in Russian Doctrine, are now part of daily life and we must learn to cope with them."[188] Germany thereafter took several measures designed to strengthen its military capacity to thwart and respond to cyberoperations, including hacks into strategic assets, and to generate greater deterrence against attackers. A new military cyber command was established to strengthen German capabilities in cyberspace, including offensive capabilities. The German defense minister stated in this regard: "As soon as an attack endangers the functional and operational readiness of combat forces, we can respond with offensive measures."[189] Furthermore, legal changes have been discussed in Germany, including the authorization of "hack-backs"—allowing professional cyber units to hit back and remove or destroy attacking servers, if internet providers and server owners "are not ready to ensure

[183] *Russia "Was Behind German Parliament Hack,"* BBC NEWS (May 13, 2016), *at* http://www.bbc.com/news/technology-36284447.

[184] Samburaj Das, *Germany Blames Russia for Parliament Hack*, HACKED (May 14, 2016), *at* https://hacked.com/germany-blames-russia-parliament-hack.

[185] Connolly, *supra* note 180.

[186] Rowena Mason, *Theresa May Accuses Russia of Interfering in Elections and Fake News*, GUARDIAN (Nov. 14, 2017), *at* https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news.

[187] The UK Prime Minister's statement was issued in the wake of a significant increase in cyberoperations against UK media and telecommunication, and reports about hundreds of fake Twitter accounts and tens of thousands of other accounts tied to Russia, presumably used to influence the outcome of the referendum on the Brexit. *Brexit: Russian Twitter Accounts Tweeted 3,468 Times About EU Independence Referendum*, INDEPENDENT (Nov. 15, 2017), *at* http://www.independent.co.uk/news/uk/politics/brexit-latest-russian-twitter-accounts-eu-independence-referendum-tweets-influence-result-a8055746.html. Investigations into possible Russian interference in the British democratic process have been launched recently by the UK government and Parliament. Zach Marzouk, *The Intelligence and Security Committee Has Finally Reformed After the General Election*, ITPRO (Nov. 24, 2017), *at* http://www.itpro.co.uk/security/29963/parliaments-intelligence-committee-considering-russia-investigation.

[188] Melissa Eddy, *After a Cyberattack, Germany Fears Election Disruption*, N.Y. TIMES (Dec. 8, 2016), *at* https://www.nytimes.com/2016/12/08/world/europe/germany-russia-hacking.html.

[189] Andrea Shalal, *German Military Can Use "Offensive Measures" Against Cyber-attacks: Minister*, REUTERS (Apr. 5, 2017), *at* http://www.reuters.com/article/us-germany-cyber-idUSKBN1771MW.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

that they are not used to carry out attacks."[190] According to government officials, this method of operation would be utilized to respond to attacks on an electricity grid or future attacks on the Bundestag.[191]

Although the Bundestag hack might be viewed as an intelligence gathering operation, it was also regarded by senior German officials as part of a broader campaign of Russian cyber influence operations, which seeks to undermine democratic governments. It also resulted in the creation of new military structures with offensive and defensive capacities in cyberspace and in the consideration of far-reaching legal responses (hack-backs). It is for these reasons that we decided to include it in the list of the case studies as an example of a low-scale strategic operation that may nonetheless be regarded as sovereignty-infringing.

It is also worth noting in this regard that the UK prime minister stated in November 2017 that "Russian interference threatens to undermine the international order and Western institutions."[192] She also sent a strong message to Russia: "We know what you are doing. And you will not succeed. Because you underestimate the resilience of our democracies, the enduring attraction of free and open societies, and the commitment of western nations to the alliances that bind us. The UK will do what is necessary to protect ourselves, and work with our allies to do likewise."[193] Such a response coincides with the U.S. criminal investigations and economic sanctions imposed following the Russian influence operations during the 2016 presidential elections. These developments suggest that cyber influence operations are increasingly being viewed as unacceptable forms of external interference in internal affairs, which might run contrary to international law norms, or at least to informal norms of state conduct applicable to cyberspace.

D. Cyberoperations Against Iran

1. A string of fires and explosions in Iranian oil and gas facilities (2016)[194]

a. Principal facts

On July 6, 2016, fire broke out at the Bouali petrochemical plant in Northern Iran. It took three days to put out the fire. The fire and the toxic clouds of smoke it generated put at risk a population of several hundreds of thousands of people. No fatalities were registered, but the damage caused to the plant was estimated in the tens of millions of dollars. In the same week, a gas pipeline exploded in Marun Oil (in southwestern Iran), causing the death of a worker. At the end of the same month, another fire broke out in the Bisotoon petrochemical plant in the western Iranian city of Kermanshalah. A week later, on August 6, two more incidents occurred within hours of each other: The first was an explosion in a gas pipeline near

[190] *See* Shalal, *supra* note 179.

[191] Kate Brady, *Reports: German Government Plans Cyberattack "Hackback" Ahead of Election*, DEUTSCHE WELLE (Apr. 20, 2017), *at* http://www.dw.com/en/reports-german-government-plans-cyberattack-hackback-ahead-of-election/a-38506101.

[192] Mason, *supra* note 186. Prime Minister May echoed in her remarks the words of President Obama, who delivered a similar response in his 2016 Presidential Statement. White House Press Release, *supra* note 169.

[193] Mason, *supra* note 186.

[194] Kay Armin Serjoie, *Iran Investigates if Series of Oil Industry Accidents Were Caused by Cyber Attack*, TIME (Aug. 12, 2016), *at* http://time.com/4450433/iran-investigates-if-series-of-oil-industry-accidents-were-caused-by-cyber-attack.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Gonaveh (in southwest Iran), killing a worker and injuring three more; several hours later, another fire broke out in the Imam Khomeini petrochemical plant (situated near the Marun Oil facility). On September 14, 2016, a gas leak and fire broke at the Mobin Petrochemical Factory that services the South Pars gas field. Four workers were injured.[195]

The Iranian official response issued in July 2016 rejected the possibility that the incidents were caused by a cyberattack. The Iranian Oil Minister explained they were caused due to technical faults and human error. A week later, when the "errors" and "failures" seemed to be recurring with exceptionally high frequency, the Iranian Supreme National Cyberspace Council sent a special team to the sites to investigate the incidents.

b. Attribution

Brigadier General Gholam Reza Jalali, who heads an Iranian military unit in charge of combatting cyber sabotage, put the blame for the leaks, fires, and explosions on faulty equipment components imported into Iran and installed in the different gas production and conveyance facilities, denying that Iran was the subject of a cyberattack.[196] Indeed, it may be the case that the sanctions imposed on Iran by the international community limited its ability to acquire high-quality parts for industrial manufacturing from Western states, and this could explain some incidents. At the same time, the dependence of Iran on a small number of external equipment suppliers might have also been exploited for launching a cyberattack against its industrial facilities, using imported spare parts from a short list of suppliers for introducing malicious malware into targeted computer systems.

Notwithstanding the official position of the government of Iran, international media quoted a cybersecurity expert who pointed out similarities between the methods that may have been used in the 2016 attacks and in the Stuxnet operation and expressed his firm view that the incident were caused by a state-sponsored cyberoperation.[197]

c. Response

The Iranian regime has not changed its official approach, which denies being subject to a cyberoperation on a significant scale with serious effects. However, it is quite plausible that the Shamoon 3, Shamoon 4, and the Triton operations described below served as Iranian covert retaliation attacks against Saudi Arabia and its allies for their suspected involvement in cyberoperations against the Iranian oil and petrochemical facilities.

E. Cyberoperations Against Saudi Arabia and Qatar

1. The Shamoon cyberattacks (2012–2017) and the Triton attack (2017)

a. Principal facts

I. *Shamoon 1* – On August 15, 2012, a malware dubbed "Shamoon" attacked the computer hardware infrastructure of Saudi-Aramco, the world's largest oil company. An

[195] *Iran Oil Industry Fires, Blasts Raise Suspicions of Hacking*, FOX NEWS (Sept. 22, 2016), *at* http://www.foxnews.com/world/2016/09/22/iran-oil-industry-fires-blasts-raise-suspicions-hacking.html.
[196] *Id.*
[197] *Id.*

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

unknown group named "Cutting Sword of Justice" claimed responsibility for the attack, which it alleged was a "retaliation against the Al-Saud regime for the 'crimes and atrocities taking place in . . . Syria, Bahrain, Yemen, Lebanon [and] Egypt.'"[198] The malware was designed to replace data on hard drives with an image of a burning American flag, and more than 30,000 computers—three quarters of the workstations of the company—had their memory simultaneously wiped out. The network was put offline, and it took ten days to put it back to operation. Moreover, it took several months to complete replacing all infected computers. The economic harm caused by the attack was enormous, and the then U.S. Defense Secretary, Leon Panetta, described it as "the most destructive attack that the private sector has seen to date."[199]

II. *Shamoon 2* – Two weeks later, RasGas, the Qatari oil company, was attacked in a manner similar to the attack against Saudi-Aramco, compelling it to shut down its network and stop its online activities for several days.[200] The Qatari authorities did not confirm that they were attacked by the same malware as the Saudis (i.e., Shamoon malware), and they refrained from providing further information about the attack and the damage it caused. It was later reported that the attackers had indeed used the same Shamoon malware and that the attacks resulted in the destruction of computer and data belonging to RasGas.[201] It may be noted, that both Aramco and RasGas are joint ventures of local and American oil companies.

III. *Shamoon 3*[202] – On November 17, 2016, a version of Shamoon malware was used in an operation against crucial Saudi government agencies, including the transportation sector. Infected computers had their hard drives erased, and they displayed a photograph of the body of Alan Kurdi, the 3-year-old Syrian boy, who had drowned fleeing his country's civil war. Thousands of computers at the headquarters of the General Authority of the Civil Aviation were damaged, critical data was erased, and the operations of the Authority were halted for several days.[203] The Saudi authorities controlled the publication of information relating to the attack and declared that, although the operation was like Shamoon 1, its impact was "much smaller" and did not disrupt transportation or aviation services.[204]

IV. *Shamoon 4* – On January 23, 2017, a digital time bomb, set in advance to explode at a specific time, hit governmental and private institutions in the Saudi Kingdom, including the Labor Ministry and multiple petrochemical companies, such as the

[198] John Leyden, *Hack on Saudi Aramco Hit 30,000 Workstations, Oil Firm Admits*, REGISTER (Aug. 29, 2012), *at* www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis.

[199] Jon Gambrell, *Saudi Arabia Warns Destructive Computer Virus Has Returned*, US NEWS (Jan. 24, 2017), *at* https://www.usnews.com/news/business/articles/2017-01-24/saudi-arabia-warns-destructive-computer-virus-has-returned.

[200] Nicole Perlroth, *In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back*, N.Y. TIMES (Oct. 23, 2012), *at* http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?mcubz=0.

[201] Gambrell, *supra* note 199.

[202] Michael Riley, Glen Carey & John Fraher, *Destructive Hacks Strike Saudi Arabia, Posing Challenge to Trump*, BLOOMBERG TECH. (Dec. 1, 2016), *at* https://www.bloomberg.com/news/articles/2016-12-01/destructive-hacks-strike-saudi-arabia-posing-challenge-to-trump.

[203] Sewell Chan, *Cyberattacks Strike Saudi Arabia, Harming Aviation Agency*, N.Y. Times (Dec. 1, 2016), *at* http://www.nytimes.com/2016/12/01/world/middleeast/saudi-arabia-shamoon-attack.html?ref=technology.

[204] Mahmoud Habboush, Gwen Ackerman & Michael Riley, *Hack of Saudi Arabia Exposes Middle East Cybersecurity Flaws*, BLOOMBERG TECH. (Dec. 12, 2016), *at* https://www.bloomberg.com/news/articles/2016-12-12/hack-of-saudi-arabia-exposes-middle-east-cyber-security-flaws.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

National Industrialization Company, Tasnee, and the Sadara Chemical Company, a joint venture between Saudi Aramco and Dow Chemical (an American company).[205] Like in the case of Shamoon 3, the attacked computers displayed the photograph of the dead Alan Kurdi, after erasing their hard drives.[206] Recovery took months.

V. *The Triton attack* – A malware dubbed "Triton" or "Trisis" or "HatMan"[207] was designed to interact with Triconex Safety Instrumented System (SIS) Controllers, manufactured by Schneider Electric and commonly used in thousands of critical infrastructure plants around the globe, including nuclear, water, gas, oil, and chemical plants to ensure their safe operation. The operation was detected on August 29, 2017, when the controlling system in the attacked plant was shut down as an emergency protective procedure. Several private cybersecurity firms such as FireEye, Dragos, and Symantec along with the DHS, FBI, NSA, and the Pentagon's Defense Advanced Research Projects Agency have been investigating this particularly dangerous attack. No official information has been released about the victim company and the culprit. It was reported unofficially that the malware originated in computers outside Saudi Arabia and targeted a chemical plant in Saudi Arabia, and that it was designed not just to destroy data or shut down the plant but "to sabotage the firm's operations and trigger an explosion."[208] The goal has not been achieved due to a bug in the attackers' computer code that prematurely activated the protective measure for shutting down the plant's production systems.

b. Attribution

The prevailing theory among commentators is that the Shamoon operations were executed by a group of hackers sponsored by Iran.[209] Then U.S. Secretary of Defense Leon Panetta

[205] Nicole Perlroth & Clifford Krauss, *A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try*, N.Y. TIMES (Mar., 15, 2018), *at* https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html. *See also* Rebecca Cheetham & Sébastien Heon, *Triton Cyber-attack: Hackers Target the Safety Systems of Industrial Plants Score*, SCOR LIVE BLOG (Mar. 6, 2018), *at* https://www.scor.com/en/media/news-press-releases/triton-cyber-attack-hackers-target-safety-systems-industrial-plants. *See also* Blake Johnson, Dan Caban, Marina Krotofil, Dan Scali, Nathan Brubaker & Christopher Glyer, *Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure*, FIREEYE (Dec. 14, 2017), *at* https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html.

[206] Ed Clowes, *Destructive Computer Virus "Shamoon" Hits Saudi Arabia for Third Time*, GULF NEWS TECH. (Jan. 30, 2017), *at* http://gulfnews.com/business/sectors/technology/destructive-computer-virus-shamoon-hits-saudi-arabia-for-third-time-1.1970590.

[207] *Threat Analysis – Industrial Control System Technical Report* (Accenture Security, 2018), *available at* https://www.accenture.com/t20180123T095554Z__w__/us-en/_acnmedia/PDF-46/Accenture-Security-Triton-Trisis-Threat-Analysis.pdf.

[208] Perlroth & Krauss, *supra* note 205.

[209] The theory that Iran has been behind the Shamoon attacks developed incrementally. *See* Rob Rachwald, *The Significance of the Aramco Hack*, IMPERVA (Aug. 23, 2012), *at* https://www.imperva.com/blog/2012/08/the-significance-of-the-aramco-hack; Christopher Bronk & Eneken Tikk-Ringas, *The Cyber Attack on Saudi Aramco*, 55 SURVIVAL – GLOB. POL. & STRATEGY 81, 96 (2013), *at* https://doi.org/10.1080/00396338.2013.784468; David, E. Sanger & Nicole Perlroth, *Iran Is Raising Sophistication and Frequency of Cyberattacks, Study Says*, N.Y. TIMES (Apr. 15, 2015), *at* http://www.nytimes.com/2015/04/16/world/middleeast/iran-is-raising-sophistication-and-frequency-of-cyberattacks-study-says.html; Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community* (Feb. 13, 2018), *available at* https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—Unclassified-SSCI.pdf.

opined that the cyberattacks directed against Saudi Aramco and RasGas (Shamoon 1 + 2), required a technological capacity that only a few countries in the world had at the time.[210] The immediate suspect for these operations was Iran,[211] who may have had a particular interest in targeting U.S. joint ventures, as a form of retaliation for the alleged U.S./Israeli "Olympic Games" operation (aka Stuxnet) conducted against its nuclear facilities.[212] In addition, Iran may have had other political and ideological reasons to carry out cyberoperations against Saudi Arabia, as the two states are entangled in a religious and geopolitical conflict over hegemony in the Arabian/Persian Gulf, juxtaposing Shiite Muslim states, led by Iran, and rival Sunni Muslim states, led by Saudi Arabia (and supported by Qatar at the time).

The Shamoon operations were not officially and publicly attributed by Saudi Arabia to any state or state-sponsored group, but the prevailing opinion among experts is that Iran was behind these operations, and that the Shamoon 3 and 4 operations were acts of retaliation for the attacks on its gas and oil industry facilities, carried out a few months earlier.[213] It is notable that both operations were attributed to Iran by U.S. Director of National Intelligence Daniel R. Coates in his Worldwide Intelligence Assessment Report of the U.S. Intelligence Community, submitted to the House Intelligence Committee in February 2018.[214]

Although the Triton operation was more sophisticated and dangerous than previous cyberoperations in the region, and despite indications that it was launched by a state or a state-sponsored group of hackers, no attribution claim was made in this connection. Once again, Iran was named in the media as a possible culprit due to its capabilities in cyberspace and presumed motive to harm Saudi Arabia, with some observers suggesting that it may have cooperated in carrying out the attack with another state.[215] Interestingly, the Saudi foreign minister stated on February 18, 2018, on the sidelines of the Munich Security Conference, that: "Iran is the only country that has attacked us repeatedly and tried to attack us repeatedly. In fact, they tried to do it on a virtually weekly basis."[216]

[210] U.S. Dep't of Defense Press Release, Transcript Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security (Oct. 11, 2012), *available at* http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

[211] Perlroth, *supra* note 200.

[212] Gary D. Solis, *Cyber Warfare*, 219 MIL. L. REV. 1, 44–49 (2014) (describing the operation and analyzing its legal aspects); David Weissbrodt, *Cyber-Conflict, Cyber-Crime, and Cyber-Espionage*, 22 MINN. J. INT'L L. 347, 378–79 (2013). *See also* Michelle Nicholas, *Iran Says Terrorism Includes any Attack on Nuclear Facility*, REUTERS (Sept. 28, 2012), *at* https://www.reuters.com/article/us-un-assembly-nuclear-iran/iran-says-terrorism-includes-any-attack-on-nuclear-facility-idUSBRE88R13O20120928 (reporting on the Iranian Foreign Minister's speech during the UN summit stating that Iran places "special importance" on preventing nuclear terrorism targeted at is nationals and its nuclear facilities, adding that "any such act committed by a state, as certain countries continue to commit such crimes in my country, is a manifestation of nuclear terrorism and consequently a grave violation of the principles of U.N. Charter and international law").

[213] *Saudi Arabia Warns on Cyber Defense as Shamoon Resurfaces*, REUTERS (Jan. 23, 2017), *at* https://www.reuters.com/article/us-saudi-cyber/saudi-arabia-warns-on-cyber-defense-as-shamoon-resurfaces-idUSKBN1571ZR. *See also* Bill Gertz, *Iran Renews Destructive Cyber-attacks on Saudi Arabia*, WASH. FREE BEACON (Feb. 22, 2017), *at* http://freebeacon.com/national-security/iran-renews-destructive-cyber-attacks-saudi-arabia.

[214] Coats, *supra* note 209.

[215] Perlroth & Krauss, *supra* note 205.

[216] Natasha Turak & Hadley Gamble, *Saudi Foreign Minister Calls Iran Most Dangerous Nation for Cyberattacks*, CNBC (Feb. 18, 2018), *at* https://www.cnbc.com/2018/02/18/iran-most-dangerous-nation-for-cyber-attacks-says-saudi-foreign-minister.html.

c. Response

No specific attribution claim was made by Saudi Arabia in relation to the Shamoon 3 and 4 and Triton operations, and there are no reports of a response to any of these operations. This conforms to the tendency of both Iran and Saudi Arabia to refrain from attributing cyberoperations in what looks like an ongoing cyberconflict or a string of "tit for tat" operations. Instead, both states seem to opt for covert counteroperations. Hence, the 2016 cyberattacks on Iranian petrochemical facilities may have been acts of retaliation by Saudi Arabia or its allies for the Shamoon 1 and 2 operations (or for kinetic attacks on Saudi Arabia undertaken by Iranian proxies in Yemen),[217] and Shamoon 3 and 4 and the Triton operations might have been acts of retaliation for the Iranian petrochemical facilities attacks. The lack of reports about further responses may suggest that they took place in a completely covert manner, or that one or more of the parties to the cyberconflict made a policy decision to refrain from further reacting in order to de-escalate the situation.

F. Cyberoperations Against Ukraine

1. Cyberattacks against Ukraine power grid (2015–2016)

a. Principal Facts

Since the Russian invasion of the Crimean Peninsula in 2014, the armed conflict between Ukraine, Russia, and secessionist regions has spilled over to cyberspace where destructive cyberoperations have been undertaken by state-sponsored groups of hackers from both sides of the conflict.

I. *Black-Energy 1* – On December 23, 2015, the Ukraine power grid was attacked by hackers who interfered with the functioning of three distribution companies in the western regions of Ukraine. As a result, hundreds of thousands of people had their electricity cut off for several hours.[218] The hackers succeeded in infiltrating into the control centers of the three companies, replacing their original firmware with malicious malware—KillDisc—which wiped or overwrote data in essential system files. This caused the infiltrated computers to crash. Although electric supply was resumed by means of switching to manual control, it took several months to bring the control centers back to full operation. It was the first time a cyberoperation has been used to cause power outage in a large urban area.[219]
II. *Black-Energy 2* – A second outage took place between December 17–18, 2016. This time, a power distribution station near Kiev was switched off and the Northern part of the city was cut off electricity for an hour, reducing by about 20 percent the city's nighttime energy consumption. Senior researchers in two cybersecurity firms (ESET and Dragos Inc.) identified a malware dubbed "Industroyer" or "Crash

[217] For a discussion of the Iranian links to the war in Yemen, see Shaul Shay, *Saudi Arabia and the Houthi Missile Threat,* Israel Defense (Nov. 15, 2016), *at* http://www.israeldefense.co.il/en/node/27571.

[218] D. U. Case, *Analysis of the Cyber Attack on the Ukrainian Power Grid*, E-ISAC (Mar. 18, 2016), *available at* https://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf. *See also* Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, Wired (Mar. 3, 2016), *at* https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid.

[219] Elias Groll, *Did Russia Knock Out Ukraine's Power Grid?*, For. Pol'y (Jan. 8, 2016), *at* http://foreignpolicy.com/2016/01/08/did-russia-knock-out-ukraines-power-grid.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Override" as the cause of the blackout.[220] The malware, which was a variation of Stuxnet, was more sophisticated than the one used in the 2015 outage, because it featured a malicious code that could cause the blackout more quickly, on a greater scale, and with the involvement of far fewer attackers. Like Stuxnet, Industroyer/Crash Override could be programmed to run without operator control even in a network that is disconnected from the internet, i.e., it could be used as a "logic/time bomb" programmed to automatically detonate at a predetermined point in time. It could also destroy all files on systems infected to cover its tracks.

b. Attribution

The "Sandworm" hacker group,[221] also known as "Voodoo Bear" and "Telebots," was identified by cybersecurity experts as involved in both operations against the Ukrainian power grid.[222] The same group was identified by cybersecurity firms as responsible for numerous cyberoperations directed since 2015 against almost every sector of Ukrainian society, destroying hundreds of computers of media companies, deleting or encrypting terabytes of governmental data and paralyzing vital infrastructure.[223]

Ukrainian investigators, in conjunction with their U.S. counterparts from the FBI and DHS, concluded that the Black-Energy 1 operation started six months before the actual power outage, as a reconnaissance/espionage operation. Later on, it moved to the stage of weaponizing, i.e., setting the tools of action and getting prepared to launch a cyberoperation against the computer system controlling the electric grid. The investigators' other conclusion was that the attackers chose not to exhaust their destructive capabilities. Thus, the damage was deliberately limited in scope. Both conclusions led to a third one: the 2015 attack originated from a state or a state-sponsored group, and was primarily designed to send a warning, not to cause destruction on a large scale.

Naturally, Russia became the immediate suspect, as it had several reasons to send such a political message to Ukraine, and senior Ukrainian officials did not hesitate to blame it for the operations. For example, Petro Poroshenko, the Ukrainian president, stated that the 2016 outage (Black-Energy 2) was conducted with the "direct and indirect involvement of secret services of Russia which have unleashed a cyberwar against our country."[224] The Kremlin repeatedly denied these allegations.[225]

[220] Andy Greenberg, *"Crash Override": The Malware that Took Down a Power Grid*, WIRED (June 12, 2017), *at* https://www.wired.com/story/crash-override-malware.

[221] Andy Greenberg, *Your Guide to Russia's Infrastructure Hacking Teams*, WIRED (July 12, 2017), *at* https://www.wired.com/story/russian-hacking-teams-infrastructure. *See also* John Hultquist, *Sandworm Team and the Ukrainian Power Authority Attacks*, FIREEYE (Jan. 7, 2016), *at* https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html.

[222] Hultquist, *supra* note 221.

[223] *Id.*

[224] Andy Greenberg, *How an Entire Nation Became Russia's Test Lab for Cyberwar?*, WIRED (June 20, 2017), *at* https://www.wired.com/story/russian-hackers-attack-ukraine (citing the Ukrainian President's accusation). *See also* Pavel Polityuk, *Ukraine Points Finger at Russian Security Services in Recent Cyber-attack*, REUTERS (July 1, 2017), *at* https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P; Pavel Polityuk, *Ukraine Investigates Suspected Cyber-attack on Kiev Power Grid*, REUTERS (Dec. 20, 2016), *at* https://www.reuters.com/article/us-ukraine-crisis-cyber-attacks/ukraine-investigates-suspected-cyber-attack-on-kiev-power-grid-idUSKBN1491ZF.

[225] Jim Finkle, *Cyber Firms Warn of Malware that Could Cause Power Outages*, REUTERS (June 12, 2017), *at* https://www.reuters.com/article/us-cyber-attack-utilities-idUSKBN1931EG.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

c. Response

The operations directed against the Ukrainian power grid are considered to be the first cyberoperations conducted within the framework of an armed conflict and aimed at critical infrastructure. Ukraine along with cybersecurity experts from the United States and other NATO member states investigated the operations with a view to drawing the necessary lessons, including reinforcing cybersecurity in order to reduce the risk of recurrence.

As for retaliation, it appears that the parties to the conflict in Ukraine continue to embrace ambiguity and to deny any responsibility for concrete cyberoperations allegedly undertaken by hacktivists or "patriot hackers," Ukrainians, or Russians trying to retaliate for wrongs committed by the other party.

G. Cyberoperations with Global Effects

Since May 2017, two large-scale cyberoperations have been carried out using leaked NSA hacking tools that exploit vulnerabilities in existing computer networks. Those tools had been stolen and leaked online by a group called "Shadow Brokers," which is reportedly affiliated with Russia.[226]

1. WannaCry

a. Principal facts

On May 12, 2017, the WannaCry malware spread like wildfire, affecting hundreds of thousands of computers of companies, government agencies, and individuals in more than 150 countries, including Russia, the United States, China, Germany, Ukraine, and the UK (whose National Health Service was particularly affected). The WannaCry malware exploited a hole in the Windows Operating System identified in stolen NSA tools to infect the master boot record, encrypt the hard drive's file system table, and prevent Windows from booting. The affected computers had all data stored in them encrypted and displayed a message demanding payment of a ransom of $300 (later doubled to $600) in Bitcoins within three days in order to unlock the computer. Otherwise, access to the data would be permanently lost.[227] In August 2017 it was reported that 52.2 Bitcoins (at the time, around $143,000) were withdrawn from online wallets for depositing the ransom payments. It turned out, however, that paying the ransom did not ensure unlocking the computer.[228]

[226] *See* Michael B. Kelley, *"Very High Level of Confidence" Russia Used Kaspersky Software for Devastating NSA Leaks*, YAHOO FINANCE (Jan. 13, 2018), *at* https://finance.yahoo.com/news/experts-link-nsa-leaks-shadow-brokers-russia-kaspersky-144840962.html. *See also* Rohit Langde, *WannaCry Ransomware: A Detailed Analysis of the Attack*, TECHSPECTIVE (Sept. 26, 2017), *at* https://techspective.net/2017/09/26/wannacry-ransomware-detailed-analysis-attack (describing NSA tools such as EternalBlue and DoublePulsar, which exploit vulnerabilities in Microsoft-Windows operating system. Those tools were used in this operation, enabling the attacker to use the IP address of the computer to directly communicate with the Server Message Block (SMB) protocol and plant a backdoor to enable remote access and to facilitate control of systems by hackers who could easily install in them virus or malware.).

[227] Langde, *supra* note 226.

[228] Ryan Browne, *Hackers Have Cashed Out on $143,000 of Bitcoin from the Massive WannaCry Ransomware Attack*, CNBC (Aug. 3, 2017), *at* https://www.cnbc.com/2017/08/03/hackers-have-cashed-out-on-143000-of-bitcoin-from-the-massive-wannacry-ransomware-attack.html.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

The motivation of those behind the WannaCry operation remains unclear. Ostensibly, it looked like a large-scale criminal ransom operation intended to raise cash. Still, the global manner in which it was executed and the fact that computers remained locked even after the ransom was paid has raised doubts about the true nature of the perpetrators' motives. One possibility is that the operation was designed to draw attention to the NSA's stockpile of cyberweapons, which exploit undisclosed vulnerabilities in popular software.[229] Alternatively, it might just have been "meant to cause havoc and destruction" as Tom Bossert, a U.S. Homeland Security advisor put it recently.[230]

b. Attribution

Cybersecurity firms succeeded, within a few days, in identifying the technical footprints of the hackers group ("Lazarus"), which has been linked to North Korea.[231] A few weeks later it was published that the NSA assesses with "moderate confidence" that North Korea is responsible for the WannaCry operation.[232] The UK government was the first government to officially announce that North Korea is behind the WannaCry attack. The announcement was made by Ben Wallace, the minister of state for security and economic crime,[233] relying on the British intelligence community and other knowledgeable sources in the cybersecurity industry.[234] This assessment was endorsed by Microsoft's President, Brad Smith, stating in a press interview that "all observers in the know have concluded that WannaCry was caused by North Korea using cybertools or cyberweapons that were stolen from the National Security Agency in the United States."[235]

In late 2017, Tom Bossert, the U.S. Homeland Security advisor to the White House, attributed officially and publicly the WannaCry attack with high confidence to North

[229] Nicole Perlroth & David E. Sanger, *Hackers Hit Dozens of Countries Exploiting Stolen NSA's Tool*, N.Y. TIMES (May 12, 2017), *at* https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html?_r=0.

[230] U.S. Homeland Security Advisor, Thomas Bossert, Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea (Dec. 19, 2017), *available at* https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917.

[231] Olivia Solon, *WannaCry Ransomware Has Links to North Korea, Cybersecurity Experts Say*, GUARDIAN (May 15, 2017), *at* https://www.theguardian.com/technology/2017/may/15/wannacry-ransomware-north-korea-lazarus-group.

[232] Ellen Nakashima, *The NSA Has Linked the WannaCry Computer Worm to North Korea*, WASH. POST (June 14, 2017), *at* https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.9f6ef39a5856.

[233] Ryan Browne, *UK Government: North Korea Was Behind the WannaCry Cyber-attack that Crippled Health Service*, CNBC (Oct. 27, 2017), *at* https://www.cnbc.com/2017/10/27/uk-north-korea-behind-wannacry-cyber-attack-that-crippled-nhs.html.

[234] Symantec Security Response, *WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group*, SYMANTEC (May 22, 2017), *at* https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group (describing technical findings connecting WannaCry to the Lazarus group, which was also a key player in the Sony hack and in the theft of US$81 million from the Bangladesh Central Bank, emphasizing, however, that available technical information does not yet enable to attribute the attack to a specific state or non-state actor).

[235] Joel Hills, *North Korean Government Behind NHS Cyber-attack, Says Microsoft Boss*, ITV (Oct. 13, 2017), *at* http://www.itv.com/news/2017-10-13/hacking-threat-is-as-serious-as-terrorism-says-microsoft-boss. *See also* Brad Smith, *The Need for Urgent Collective Action to Keep People Safe Online: Lessons from Last Week's Cyberattack*, MICROSOFT BLOG (May 14, 2017), *at* https://blogs.microsoft.com/on-the-issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Korea.[236] The attribution was based on the investigation's findings and was endorsed by private cybersecurity firms and by five other governments: Australia, the UK,[237] Canada, New Zealand, and Japan. Bossert was asked about the long time it took to reach the conclusion and replied that time was needed to definitely attribute responsibility.[238]

c. Response

Notwithstanding the attribution of responsibility to North Korea by multiple states, no act of retaliation has been reported. The UK Security Minister merely called on Western nations to develop a "doctrine of deterrent" to prevent further cyberattacks.[239] Microsoft's president further called on governments "to come together as they did in Geneva in 1949 and adopt a new Digital Geneva Convention that makes clear that these cyberattacks against civilians, especially in times of peace, are off-limits and a violation of international law."[240]

The U.S. Homeland Security advisor stated that clear attribution is the first step toward holding North Korea accountable, although he did not point to a specific response measure that would actually impose accountability.[241] Simultaneously, in what seems to have been a coordinated statement, Lord Ahmad, the UK Foreign Office minister for cyber, stated that international law applies online as it does offline and that the UK is determined to respond and to impose costs on those who attack it in cyberspace.[242] He continued by emphasizing the UK's commitment to strengthening coordinated international efforts to uphold a secure cyberspace. UK officials also remained silent about any measures that were taken or would be taken against the attackers.

It may be noted, however, that Microsoft, Facebook, and other major tech companies did act independently against the North Korean hackers. They shut down the accounts used to launch attacks and remedied their own cyber vulnerabilities, which were exploited in the WannaCry operation.[243]

2. Petya/NotPetya[244]

a. Principal facts

"Petya," a ransomware program targeting Microsoft Windows operated computers, was first revealed in March 2016.[245] On June 27, 2017, a new variant of Petya malware—dubbed

[236] U.S. Homeland Security Advisor Press Briefing, *supra* note 230.

[237] Foreign and Commonwealth Office and Lord Ahmad of Wimbledon Press Release, Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks (Dec. 19, 2017), *available at* https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

[238] U.S. Homeland Security Advisor Press Briefing, *supra* note 230.

[239] Browne, *supra* note 233.

[240] Hills, *supra* note 235. *See also* Brad Smith, *The Need for a Digital Geneva Convention*, MICROSOFT BLOG (Feb. 14, 2017), *at* https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention.

[241] U.S. Homeland Security Advisor Press Briefing, *supra* note 230.

[242] Foreign and Commonwealth Office and Lord Ahmad of Wimbledon Press Release, *supra* note 237.

[243] U.S. Homeland Security Advisor Press Briefing, *supra* note 230.

[244] EY – Technical Intelligence Analysis, *Petya Wiper Malware Disguised as a Ransomware Attack* (June 2017), *available at* http://www.ey.com/Publication/vwLUAssets/ey-technical-intelligence-analysis-petya-wiper-disguised-as-ransomware-attack/$FILE/ey-technical-intelligence-analysis-petya-wiper-disguised-as-ransomware-attack.pdf.

[245] Lucian Constantin, *Petya Ransomware Is Now Double the Trouble*, NETWORKWORLD (May 13, 2016), *at* https://www.networkworld.com/article/3069990/petya-ransomware-is-now-double-the-trouble.html.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

"NotPetya" (to distinguish it from the first variant)—was launched against computer systems in Ukraine, using the leaked NSA tool that had already been exploited a month earlier in the WannaCry operation. The tool was employed, however, in a particularly sophisticated manner. NotPetya used an auto-update feature of specific software for tax calculation, which was required from any company operating in Ukraine, to infect many Ukrainian companies, institutions, and facilities, including banks, energy companies, governmental agencies, airports, metros, and even the radiation monitoring equipment within the Chernobyl nuclear power plant. The malware spread promptly and globally, and affected many companies, institutions, and facilities in more than sixty countries including, Russia, Poland, the United States, Germany, UK, Israel, Italy, Netherlands, and others. Almost 80 percent of affected companies were, however, Ukrainian. The malware encrypted all data on the infected systems and demanded a ransom of $300 in bitcoin for decrypting the files.

NotPetya turned out to be a wiper malware like the Stuxnet and Shamoon. Thus, the damage it caused was irreversible as it did not have the capacity to decrypt the files it had encrypted.[246] NotPetya caused the victim companies unprecedented losses—for instance, the U.S. pharmaceutical giant Merck reported a loss of over $310 million, the courier firm FedEx reported a loss of $300 million, and the shipping firm Maersk reported a loss of $200 million.[247]

b. Attribution

The tactics, techniques, and procedures (TTPs) of NotPetya operators, as analyzed by cybersecurity experts, lead with high confidence to the conclusion that Russia was behind this operation and that it was related to the ongoing armed conflict in Ukraine.[248] The fact that the operation was launched on the eve of the holiday marking Ukraine's adoption of its first constitution in 1996, and on the same day in which a top Ukrainian military intelligence officer was assassinated in Kiev, also does not seem to be a pure coincidence.[249] Indeed, Ukraine was the first state to point the finger at Russia for orchestrating the NotPetya operation. The Ukraine Security Service (SBU) stated that the operation was intended to destroy important data and to spread panic, and that it was conducted by the same hackers who attacked the power grid in December 2016.[250] Russia dismissed these statements as "unfounded blanket accusations."[251]

[246] EY– Technical Intelligence Analysis, *supra* note 244, at 3.

[247] Patrick Howell O'Neill, *NotPetya Ransomware Cost Merck More than $310 Million*, Cyber Scoop (Oct. 27, 2017), *at* https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million.

[248] Sam Jones, *Finger Points at Russian State Over Petya Hack Attack*, Fin. Times (June 30, 2017), *at* https://www.ft.com/content/f300ad84-5d9d-11e7-b553-e2df1b0c3220.

[249] Nolan Peterson, *Whose Cyberattack Brought Ukraine to a Shuddering Halt?*, Newsweek (July 1, 2017), *at* http://www.newsweek.com/nolan-peterson-whose-cyberattack-brought-ukraine-shuddering-halt-630500; Ben Dixon, *The Strange Failures of the Petya Ransomware Attack*, Daily Dot (July 1, 2017), *at* https://www.daily-dot.com/layer8/petya-ransomware-attack-hackers-motives-failures.

[250] *SBU Establishes Involvement of the RF Special Services into Petya.A Virus-Extorter Attack*, SBU Press-Center (July 1, 2017), *at* https://ssu.gov.ua/en/news/1/category/2/view/3660#.eXBAf7Sa.dpbs.

[251] *Ukraine State Security Service Blames Russia for the NotPetya Cyber-attack*, Firstpost (July 1, 2017), *at* http://www.firstpost.com/tech/news-analysis/ukraine-state-security-service-blames-russia-for-the-notpetya-cyber-attack-3835341.html.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

The fact that the malware spread out of Ukraine, harming companies, institutions and facilities in other states, including Russian targets, was explained by commentators through two alternative explanations. The attackers might have "underestimated the malware's spreading capabilities . . . [and it simply] went out of control."[252] Or, it may be that, although the hackers could have directed the operation only at victims using Ukrainian IP addresses or shielded from infection computers using Russian IP addresses, they refrained from doing so in order to complicate attribution efforts, and to convince global observers that the operation was a "regular" cybercrime, executed by criminal hackers and not by a foreign state or its proxies.[253]

Initially, no states affected by NotPetya (except Ukraine) came out with a clear, direct, and public attribution claim. Still, on February 15, 2018, the White House press secretary published a direct and official attribution, claiming that the Russian military launched NotPetya to destabilize Ukraine and it turned to be "the most destructive and costly cyberattack in history."[254] The statement depicted the attack as "reckless and indiscriminate," promising to "be met with international consequences."[255] Gavin Williamson, the UK defense minister, simultaneously made a similar attribution claim, blaming the Russian military for conducting an indiscriminate attack masqueraded as a criminal hack but targeting primarily Ukrainian financial, energy, and governmental targets, before spreading and affecting many others across the world. The British Minister added that: "Russia is ripping up the rulebook by undermining democracy . . . targeting critical infrastructure and weaponising information . . . . We must be primed and ready to tackle these stark and intensifying threats."[256] Australia joined the United States and the UK and published a similar statement, attributing to Russia the responsibility for the operation.[257]

c. Response

Some official statements made by senior politicians and practitioners in connection with the NotPetya operation are noteworthy. At the outset of the operation, the U.S. National Security Council stated that the United States is "determined to hold those responsible accountable."[258] It took eight months, however, for U.S. authorities to publicly attribute responsibility to the Russian government. It remains to be seen what might be the "international consequence" of holding Russia accountable for the attack.

[252] Anton Cherepanov, *TeleBots Are Back: Supply-Chain Attacks Against Ukraine*, WELIVESECURITY (June 30, 2017), *at* https://www.welivesecurity.com/2017/06/30/telebots-back-supply-chain-attacks-against-ukraine (concluding that the attack was directed against businesses in Ukraine, but the malware went out of control because its authors apparently underestimated the malware's spreading capabilities).

[253] Kimberly Zenz, *Is Russia or North Korea Behind Petya, the Latest Cyberattack?*, NEWSWEEK (July 7, 2017), *at* http://www.newsweek.com/russia-or-north-korea-behind-petya-latest-cyberattack-633410.

[254] White House Press Release, Statement from the Press Secretary (Feb. 15, 2018), *available at* https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25.

[255] *Id.*

[256] Sarah Marsh, *US Joins UK in Blaming Russia for NotPetya Cyber-attack*, GUARDIAN (Feb. 15, 2018), *at* https://www.theguardian.com/technology/2018/feb/15/uk-blames-russia-notpetya-cyber-attack-ukraine.

[257] Sarah Young & Denis Pinchuk, *Australia Joins UK, US to Blame Russia for NotPetya*, ITNEWS (Feb. 16, 2018), *at* https://www.itnews.com.au/news/australia-joins-uk-us-to-blame-russia-for-notpetya-485306.

[258] *Global Ransomware Attack Causes Turmoil*, BBC (June 18, 2017), *at* http://www.bbc.com/news/technology-40416611.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Jens Stoltenberg, the NATO secretary general, raised at the time of the NotPetya operation the possibility of direct involvement by NATO, and recalled that members of the Alliance agreed the previous year that a cyberattack could trigger Article 5 of the North Atlantic Treaty in the same way it can be triggered in the case of a conventional military assault, and promised more help to Ukraine to bolster its own cyber defenses.[259] In parallel, the then British defense secretary, Michael Fallon, publicly expressed his concern about the increasing militarization of cyberspace and emphasized British readiness to retaliate militarily if targeted by cyberattacks. "[260]

On March 14, 2018, the U.S. administration imposed sanctions on the FSB and GRU and six of its senior officials in response to the NotPetya attack.[261]

IV. Analyzing the Empirical Findings—Do States Accept the Tallinn Rules?

Before discussing our main findings and conclusions concerning the relationship between the Tallinn Rules and recent trends in state practice and relating to *opinio juris* it is worth reiterating three important caveats in our analysis. First, all of the information our research relies on is open source material. Thus, it encompasses only the small part of the perceptible "tip of the iceberg" that states have publicly acknowledged or that the media was able to uncover. We are not able to gauge undisclosed state practice or to fully understand the implications of overt acts and omissions, which are part of a broader set of covert acts and omissions.

Second, states often maintain silence with relation to their activities in cyberspace. This is because a high degree of transparency might expose their vulnerabilities, adversely affect their offensive or defensive capabilities, and weaken their power of deterrence. Thus, states tend to act in cyberspace, offensively or defensively, in a clandestine manner. Although lack of transparency or limited transparency is not exceptional in international law, especially in areas of activities involving proxies and intelligence agencies, the unique features of cyberoperations—e.g., limited or delayed impact in the kinetic world, the extensive use of private proxies, and technological masking capabilities—create exceptionally secretive conditions in relation to an ever-expanding area of interstate activity. As a result of these considerations, our findings and conclusions should be considered with caution, since they are premised on information that paints only a partial, and at times deliberately misleading, picture of reality.

Finally, we have encountered particular difficulties in ascertaining the principled position of states involved in cyberoperations. Considering the sensitivity of national security matters relating to cyberspace, internal discussions within governments and their agencies regarding their overall cyberstrategies and derivative policy choices for specific situations are mostly classified. Furthermore, given their doubts about the adequacy and workability of the existing international law framework, states tend to maintain ambiguity about the legal doctrine guiding their conduct in cyberspace. It is only a handful of public documents and occasional statements made by current or former senior officials that provide us with some opportunity to

[259] Roland Oliphant & Cara McGoogan, *NATO Warns Cyber-attacks "Could Trigger Article 5" as World Reels from Ukraine Hack*, Telegraph (June 28, 2017), *at* http://www.telegraph.co.uk/news/2017/06/28/nato-assisting-ukrainian-cyber-defences-ransom-ware-attack-cripples.

[260] *Id.*

[261] Nakashima, *supra* note 178.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

learn some (but not all) of the factors that actually guide policymakers and comprise part of their cyberstrategy.

A. The Attribution of State Responsibility

In the kinetic world, when an attack occurs for which no one has claimed responsibility, victim states are expected to try to establish, as soon as possible, international responsibility for the attack, so as to enable them to react against the responsible state, or to make demands from the state in whose territory the attack originated. Under the ILC Articles of State Responsibility, a state is responsible for every international wrongful act or omission that is attributable to it, and which constitutes a breach of its international obligations.[262] Wrongful omissions comprise situations in which a state had failed to act pursuant to obligations stemming from relevant norms of international law, including a due diligence obligation to prevent the use of its sovereign territory for launching attacks against other states.[263]

The unique characteristics of cyberspace, including the ability to act with full anonymity in ways that are difficult to discern across borders, make it difficult, and at times nearly impossible, to clearly attribute responsibility for unlawful cyberoperations. This is, especially the case when the attackers and their collaborators exploit those characteristics to mask their identity. Such difficulties are further compounded by the following features of cyberoperations:

- Unlike kinetic attacks that are typically noticed at the moment of impact (or before impact), permitting an immediate or almost immediate response, cyberoperations, especially those involving "logic/time bombs," "Trojan horses," and "trap doors" often take more time to detect.[264] Moreover, it may take a great deal of time (sometimes even years) to gather the forensic digital and non-digital information that might allow to attribute responsibility to any specific state. As a result, the attributing process very rarely ends promptly with a definite conclusion about attribution that can serve as the basis for timely responsive action.[265]
- The ability of hackers to infiltrate into cyberinfrastructure control systems and execute through them cyberoperations against third states, makes it even more difficult to reliably assign responsibility.
- Although cyberoperations leave trails in the form of TTPs (notwithstanding the attackers' efforts to mislead their potential trackers), such footprints are usually not sufficient in and of themselves to hold a state accountable for breaching its

[262] Articles on Responsibility of States for Internationally Wrongful Acts, in Int'l Law Comm'n Rep. on the Work of Its Fifty-Third Session, UN GAOR, 56th Sess., April 23–June 1 and July 2–August 10, 2001, UN Doc. A/56/10 [hereinafter ASR]. The ability to attribute wrongful acts or omissions to a state or to one of its agents—organs, entities, person, or group of persons—who in fact, acted "on the instruction of, or under the direction, or control of, that State in carrying out the conduct" (ASR, Art. 8), is essential for establishing state responsibility. According to the ICJ, a high threshold of "effective control" is required and mere acts of encouraging, financing, planning, and organizing do not meet that threshold. *Military and Paramilitary Activities*, *supra* note 31, at 64–65. At the same time, adopting the attack as one's own is sufficient to attribute the responsibility to the state. ASR, Art. 11.

[263] *See e.g.*, Corfu Channel (UK v. Alb.), Judgment, 1949 ICJ 4, 22 (Apr. 9).

[264] Peter Margulies, *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility,* 14 Melbourne J. Int'l L. 496, 500 (2013).

[265] William Banks, *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*, 95 Tex. L. Rev. 1486, 1493 (2017) (asserting that cyber attribution is challenging and often time-consuming when state responsibility is suspected and that "international law places States in an untenable posture in responding to cyber intrusions below the use of force level").

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

international obligations. This is because a separate process of legal attribution is needed in order to establish the requisite links between state officials and the attackers, or to show that the state failed to take reasonable measures to curb their operations.

- There is no established body of international law of evidence that clearly defines the legal criteria and standards of proof governing a determination of whether a given cyberoperation should be attributed to individuals, groups, or nations.[266] Although states are expected to adhere to a standard of reasonableness in attributing responsibility, and absolute certainty is not and cannot be required,[267] they are not compelled to present the intelligence they relied upon when making the attribution determination. Nor is there an internationally accepted mechanism for legally attributing cyberoperations that victim states can resort to. Thus, they often act as their own judge of the facts, based on loose legal criteria, with very limited oversight over their decisions.[268]
- While classified intelligence might enable the attribution of state responsibility with full, or almost full confidence, at times even rather quickly, national security interests, such as protecting intelligence sources or preserving the secrecy of technological capacities, might induce policymakers to refrain from making a public attribution claim or specifying its basis.[269] Note that both the United States and the UK have claimed in this regard that international law does not require full transparency as a precondition for attribution responsibility.[270]

All of these considerations encourage victim states and third states to adopt a cautious approach toward publicly attributing state responsibility, consisting of silence and ambiguity. Unfortunately, however, this may convey a message of impunity to other would-be cyberattackers. It may also result in victim states reacting in a clandestine manner—that is, responding to a cyberoperation without making public allegations against any specific state, or even without acknowledging that operation ever happened, so as to reduce any suspicion that could be directed against it for involvement in any future counterattack. Such dynamics push cyberoperations further "below the surface," using proxies and other unacknowledged operational methods, leading to a more polarized and less accountable threat environment.[271] These practical considerations reinforce the tendency of states to adopt a "wait and see"

[266] Marco Roscini, *Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations*, 50 TEX. INT'L L.J. 233 (2015) (describing and discussing the evidentiary aspects of attribution regarding state responsibility in cyber context).

[267] Brian Egan, *International Law and Stability in Cyberspace*, 35 BERK. J. INT'L L. 169, 177 (2017).

[268] *Id.*

[269] Roscini, *supra* note 266, at 272 (arguing that the standard of proof is not uniform for all rules applicable to cyberoperations. Whereas claims of self-defense against cyberoperations, like against kinetic attacks, must be proved with clear and convincing evidence, fully conclusive evidence is needed to prove that a litigant conducted cyberoperations amounting to international crimes, and a slightly less demanding standard seems to apply when what needs to be proved is that the state did not exercise due diligence to stop its cyber infrastructure from being used by others to commit international crimes). By contrast, see Egan, *supra* note 267, stating there is no legal obligation to present the evidence and the standard of proof used in specific incident, although political reasons might lead to greater transparency.

[270] Egan, *supra* note 267, at 177; Wright, *supra* note 5.

[271] MAURER, *supra* note 96, at 151–52 (suggesting three types of proxy relationships—*delegation*, under the state effective control; *orchestration*, looser relationship with the state, receiving funding but no specific instructions; and *sanctioning*, involving passive support from the state is aware and the turning of a blind eye on its part).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

approach toward the Tallinn Rules, as lack of ability to publicly and credibly attribute cyberoperations limits the utility of invoking rules that are premised on the ability to attribute responsibility for their violation.

The case studies discussed above flesh out the difficulties in attributing responsibility for cyberoperations. In almost half of the cases (five out of the eleven cases), no official attribution was made, although in several of the cases there were media reports, based mainly on investigations conducted by cybersecurity firm, that indicated at least the nationality of the attackers. In some of these cases, the findings appear to have been sufficient to attribute responsibility to a certain state, if not for its deliberate action, then for omission (violating the principle of due diligence)—that is, knowingly or unreasonably enabling the execution of cyberoperations in or from its sovereign territory. For example, although the U.S. administration appears to have had classified and declassified intelligence[272] that should have been sufficient to attribute responsibility for the Ababil operation against the New York financial sector and the Bowman Dam,[273] and the Sands Casino operation,[274] there has been no such official attribution claim. Such an outcome may simply reflect the absence of hard evidence tying the attacks to the Iranian regime, but it may also reflect a deliberate policy choice of silence and ambiguity and not publicly assigning responsibility to Iran.

A U.S. policy choice not to publicly attribute attacks to Iran may be explained through a number of possible considerations that illustrate the limited propensity to make attribution claims: there may have been geopolitical considerations, as attribution might have had immediate adverse impacts on the diplomatic efforts, including American efforts, to achieve an international agreement with Iran regarding its nuclear program. Attribution might also have put political pressure on the U.S. administration to overtly react against Iran, although such a course of action might have created legal difficulties in justifying any use of force (kinetic or cybernetic) in response to a cyberoperation that might be regarded as falling short of an armed attack.[275] Even if the retaliatory operation were to be executed covertly, it might nonetheless have resulted in an undesired escalation, exposing the United States to further and more harmful cyberattacks by Iran.[276] Public attribution might also have compromised the secrecy of American intelligence sources and revealed its technological capabilities vis-à-vis Iran. In the same vein, resort to American cyberweapons for a covert retaliation operation would have exposed them and rendered the technology accessible to everyone, including to America's adversaries. This is in fact what occurred with Stuxnet, whose success

[272] Note that criminal investigations provided sufficient evidence to file charges against seven Iranian hackers linked with the Iranian government in connection with the attacks, *see* Indictment and U.S. Dep't of Justice Press Release, *supra* notes 69-70.

[273] Regarding the standard of proof, see Roscini, *supra* note 266, at 248–54, and Egan, *supra* note 267, at 177. Regarding the countermeasures discussed by the administration against Iran, including destroying the attackers' server, see Nakashima, *supra* note 78. Such a discussion arguably suggests a high level of confidence in the possibility to attribute the operation, directly or indirectly, to Iran.

[274] The final results of the criminal investigation into this incident have not been published yet, but Clapper, the then director of national intelligence, had pointed the finger at Iran. *See* Capaccio, *supra* note 108.

[275] Nakashima, *supra* note 78.

[276] *Id. See also* Priyanka R. Dev, *"Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response*, 50 TEX. INT'L L.J. 379, 392 (2015) (arguing that the highly defensive strategy the United States adopted will do little to deter its adversaries and expose it to repeated attacks).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

has been emulated since 2012 by other destructive malwares, many of them used against American targets.[277] Furthermore, drawing more attention to the pattern of reciprocal cyberoperations in U.S.-Iran relations (the Ababil operation was considered by some to constitute an Iranian retaliation for the Stuxnet attacks), might have limited the United States' ability to deny its involvement in future covert operations against Iran.

Finally, making an explicit claim for attribution of state responsibility for a cyberoperation might limit the ability of the attributing state to maintain silence and ambiguity in respect of its legal policy and operational practices in cyberspace. Attribution claims constitute part of state practice, and they divulge, at times, *opinio juris.* Thus, they may generate international law that could restrict the ability of states to engage themselves in similar practices in the future. It may be speculated that considerations of such a nature may have led the United States to refrain from publicly attributing responsibility to Iran and China in the Ababil, Sands Casino, and OPM operations.

In most cases in which some form of attribution was made—the Sony hack, the DNC hack, the Bundestag hack, the Ukrainian power outages, and the WannaCry and NotPetya operations—claims of attribution were made after a significant delay. Only in four cases (Sony hack, DNC hack, WannaCry, and NotPetya), was the attribution made in a clear and official manner.[278] In two cases (Sony and DNC hacks), such attribution was followed by public sanctions, which might have been accompanied by covert cyber-counteroperations.[279] In some cases, such as the Bundestag and the OPM hacks, attribution was explicitly made to Russian and Chinese hackers, respectively, while avoiding the assignment of responsibility to the relevant government, despite the strong indications that the operations were state-sponsored.[280] Such a partial act of attribution may also stem from the interest of the relevant victim states in maintaining ambiguity about the precise content of international law regulating cyberoperations.

The attribution process in the case of WannaCry and NotPetya operations was unique in that it resulted in a public, direct, and official attribution by a group of affected states, albeit seven to eight months since the attacks were launched. This time gap was explained by the need of decisionmakers to reach a high level of confidence in the evidence before making attribution, even when based on undisclosed intelligence.[281] It can be presumed that the process of formulating a joint position on attribution was also time-consuming, and that the length of this process explains part of the delay. Only in the case of operations against Ukraine itself (the

[277] The first known imitation of the Stuxnet was the Shamoon malware deployed in August 2012, but there have been other copycat operations. Some are included in our case studies, for example, the Sony and Sands Casino hacks, Black-Energy 1+2, Shamoon 3+4, and NotPetya.

[278] In the DNC hack case, it seems that the president and directors of the U.S. intelligence community did not share the same approach. Whereas the USIC joint report of October 7, 2016 attributes responsibility to Russia and calls to back up American warnings with action, the president seemed to adopt a more cautious approach, focusing solely on preventing Russia from disrupting the election process. *See* Nelson, *supra* note 153.

[279] In the DNC hack case, the NSA released information about Russian cyber vulnerabilities to increase the risk of Russia being attacked by independent hacktivists and non-state actors, whereas in the Sony hack case the shutdown of the internet in North Korea for several hours was presumably a U.S. covert act of retaliation.

[280] See Evanina's remarks regarding the OPM hack, cited in Strohm's report, *supra* note 99. See also the head of the BfV's remarks regarding the Bundestag hack, *supra* notes 183–84.

[281] Browne, *supra* note 233; Hills, *supra* note 235; U.S. Homeland Security Advisor Press Briefing, *supra* note 230. *See also Pyongyang Denies Responsibility for WannaCry*, GLOB. TIMES (Dec. 21, 2017), *at* http://www.globaltimes.cn/content/1081511.shtml.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

attacks on its power grid and the NotPetya operation) was prompt and unambiguous attribution made by Ukrainian officials. This is, however, a non-surprising outcome given the armed conflict context in Ukraine, in which Russia is heavily involved. In this latter context, attribution may serve the need to expose violations of *jus in bello,* and to generate some accountability.[282] Still, it appears as if, in practice, the reliance on international law by Ukraine in both cases was minimal and that the process of attribution was largely perfunctory.

Ultimately, attribution is a prerequisite for invoking state responsibility under international law (as reflected, arguably, by the Tallinn Rules), and for justifying an overt reaction that is consistent with international law norms. Such a reaction may consist of acts of retorsion, countermeasures (in response to unlawful cyberoperations falling below the required scale and effect threshold which would constitute an armed attack), and even use of force in self-defense (in response to operations constituting an armed attack). However, technological difficulties typical to cyberspace—the ability to act with full anonymity or through proxies across international borders—and the lack of an internationally acceptable attribution mechanism, might limit the ability of the victim state to publicly make a successful and credible attribution claim that would permit it to undertake countermeasures or use force in self-defense. The practical difficulties of making attribution claims raise difficult questions regarding the requisite standard of proof under international law governing cyberspace, and about the extent to which information underlying attribution claims should be transparent. The international group of experts did not purport to resolve these questions, and they remain governed by general international law principles on evidence.[283] The legal uncertainty surrounding the attribution process may also tip the balance, at times, toward maintaining silence and ambiguity concerning cyberoperations.

Furthermore, the decision whether or not to assign responsibility or respond to a cyberoperation never relies exclusively on technical forensic findings or legal arguments. There are a variety of political and strategic considerations that decisionmakers are likely to consider prior to making the decision whether and how to react to cyberoperations. Such a decision-making process raises many practical challenges,[284] and has been characterized as "an art as well as a science,"[285] multi-layered and "more nuanced, more common, and more political."[286] In any event, political and strategic considerations may provide an additional explanation for the prevailing policy of silence and ambiguity.

Still, recent collective attribution claims and public measures taken in response to cyberoperations might indicate a shift in state approach to attribution of responsibility. For the first time ever, a group of states joined together to clearly assign responsibility for destructive cyberattacks (WannaCry and NotPetya) to specific nations (North Korea and Russia, respectively) and to

[282] William Banks, *Who Did It? Attribution of Cyber Intrusions and the* Jus in Bello, *in* THE IMPACT OF EMERGING TECHNOLOGIES ON THE LAW OF ARMED CONFLICT (forthcoming 2019), *available at* SSRN: https://ssrn.com/abstract=3191972.

[283] Egan, *supra* note 267, at 177 ("Absolute certainty is not—and cannot be—required[;] . . .there is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action."); Wright, *supra* note 5 (claiming, inter alia, that there is no legal obligation on states to disclose the information on which the decision to attribute is based).

[284] Banks, *supra* note 282, at 16–21; CLEMENT GUITTON, INSIDE THE ENEMY'S COMPUTER: IDENTIFYING CYBER ATTACKERS 5 (2017).

[285] Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 7 (2015).

[286] *Id.* at 6.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

carry out punitive measure (constituting acts of retorsion). This may signify the beginning of a coordinated Western effort to seriously address the threat to world order posed by global cyberoperations. The greater interest shown by some states in making attribution claims may encourage the development of new international norms on evidence relating to cyberoperations, as well as the creation of new international attribution mechanisms. It may also require states to reexamine their policy of silence and ambiguity vis-à-vis the Tallinn Rules.

Interestingly enough, the recent collective claims and measures largely coincided with the UK's retaliation against Russia for its use of a chemical weapon against a former Russian spy on British territory.[287] In the aftermath of the incident, more than 150 Russian diplomats were expelled from almost thirty states, including the United States, the UK, Germany, and France. Such an unprecedented response was undertaken collectively following a string of Russian provocations, viewed as aimed at destabilizing democratic nations. Consistent with the same proactive approach, the United States and the UK have also held Russia accountable for cyberoperations directed against British and American energy grids, as well as for hacking into global network infrastructure devices like routers and switches.[288] Once responsibility was assigned, U.S. authorities imposed an additional round of sanctions against Russia.

B. Use of Force

The use of force threshold is a key element of the *jus ad bellum* regulation of the response to cyberoperations by victim states, separating their right to resort to countermeasures falling short of the use of force from their right to resort to kinetic or cybernetic force used in self-defense.[289] As the literature survey above shows, this is one of the more controversial aspects of the Tallinn Rules, with the failure to clearly include DDoS attacks and destruction of data under the purview of use of force (and, by necessary implication, under the purview of armed attack) being subject to intense criticism.[290] In response, proponents of the Tallinn Manuals have claimed that the Rules merely represent the current legal situation (*lex lata*), and that the eight nonexclusive factors, which the Manuals list for the purpose of defining the use of force threshold best approximate the *jus ad bellum* criteria applicable in the kinetic domain.[291] Applying the Tallinn standards, it has been recently claimed by one author

[287] *See, e.g.*, Samuel Osborne, *Salisbury Nerve Agent Attack: Sergei Skripal and Daughter were Poisoned with Novichok on Their Front Door*, INDEPENDENT (Mar. 28, 2018), *at* https://www.independent.co.uk/news/uk/crime/sergei-skripal-salisbury-poison-nerve-agent-russia-daughter-attack-novichok-front-door-home-a8278631.html.

[288] U.S. Dep't of the Treasury Press Release, Treasury Sanctions Russian Federal Security Service Enablers (June 11, 2018), *available at* https://home.treasury.gov/news/press-releases/sm0410; Jim Finkle & Doina Chiacu, *U.S., Britain Blame Russia for Global Cyber Attack*, REUTERS (Apr. 16, 2018), *at* https://www.reuters.com/article/us-usa-britain-cyber/u-s-britain-blame-russia-for-global-cyber-attack-idUSKBN1HN2CK.

[289] TALLINN MANUAL 2.0, *supra* note 1, at 329 (Rule 68) ("A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."); *id.* at 330 (Rule 69) ("A cyber operation constitute a use of force when its scale and effects are comparable to non-cyber operations rising to level of a use of force.").

[290] *See* Nicolas Tsagourias, *The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II – The Use of Force*, 15 Y.B. INT'L HUMANITARIAN L. 22 (2013); Kilovaty, *supra* note 7, at 115–16; Ido Kilovaty, *Rethinking the Prohibition on the Use of Force in the Light of Economic Cyber Warfare: Towards a Broader Scope of Article 2(4) of the UN Charter*, 4 J. L. & CYBER WARFARE 210 (2015) (emphasizing the need to apply the prohibition on the threat or use of force to economic cyberattacks like kinetic cyberattacks). *See also* Kilovaty, *supra* notes 24–25; Fleck, *supra* note 7; Deeks, *supra* note 7.

[291] Schmitt, *supra* note 3, at 20; *see also* TALLINN MANUAL 2.0, *supra* note 1, at 331, paras. 2–3.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

that no cyberoperation has yet risen to the level of a use of force;[292] by contrast, the international group of experts that composed the Tallinn Manuals have identified the Stuxnet attack as meeting the required threshold of use of force, and some experts believed it even met the higher scale and effect threshold of an armed attack.[293]

The uncertainty and controversy surrounding the question of what constitutes a cyberoperation prohibited by Article 2(4) of the UN Charter seems to stem in part from the methodological limits of drawing analogies from kinetic and cybernetic domains, and accommodating the ever-growing role that cyberspace plays in the lives of individuals, groups and states.[294] They also reflect longstanding policy disagreements relating to the application of legal norms to new technology,[295] with some policymakers preferring, when applying law to new policy challenges, to err on the side of restraint (refraining from acknowledging new legal rights and obligations), and others preferring to err on the side of greater operational flexibility (rejecting old restrictions on the application of new capabilities).[296]

The eleven case studies examined above support the proposition that states have been so far more inclined to opt for a cautious approach toward the circumstances under which cyberoperations would qualify as a prohibited use of force. In no case has a victim state claimed publicly to have been the target of a prohibited use of force or an armed attack—an outcome that can only be partly explained through the difficulties of attribution of attacks to states or to the legal uncertainty as to whether Articles 2(4) and 51 of the UN Charter regulate the activities of non-state actors who may have launched some of the attacks in question.[297] Furthermore, the reluctance to make *jus ad bellum* claims appears to cut across the different definitions of use of force and armed attack discussed in the Tallinn Manuals. While it is

[292] Ian Yuying Liu, *State Responsibility and Cyberattacks: Defining Due Diligence Obligations*, 4 INDON. J. INT'L & COMP. L. 191, 195 (2017); Corn & Jensen, Part 1, *supra* note 45 ("the prevailing view is that most, if not all, documented cyber actions taken by states to date have fallen below the 'use of force' threshold").

[293] TALLINN MANUAL 2.0, *supra* note 1, Art. 71, at 342, para. 10 ("A case illustrating the unsettled nature of the armed attack threshold is that of the 2010 Stuxnet operation. In light of the damage they caused to Iranian centrifuges, some members of the International Group of Experts were of the view that the operations had reached the armed attack threshold (unless justifiable on the basis of anticipatory self-defense (Rule 73)."). *See also* Kilovaty, *supra* note 7, at 92.

[294] Margulies, *supra* note 264, at 514–18.

[295] For a debate over questions relating to the adaptability of law to cyberspace, see, e.g., David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Roger Brownsword, *So What Does the World Need Now? Reflections on Regulating Technologies*, *in* REGULATING TECHNOLOGIES: LEGAL FUTURES, REGULATORY FRAMES AND TECHNOLOGICAL FIXES 23 (Roger Brownsword & Karen Yeung eds., 2008); Mireille Hildebrandt, *Technology and the End of Law*, *in* FACING THE LIMITS OF THE LAW 443 (Erik Claus, Wouter Devroe & Bert Keirsbilck eds., 2009); Jack Goldsmith & Tim Wu, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

[296] *See* TALLINN MANUAL 2.0, *supra* note 1, Rule 69, as opposed to the flexible approach advocated by some authors. *Supra* note 290.

[297] TALLINN MANUAL 2.0, *supra* note 1, at 330, para. 5; Tsagourias, *supra* note 290, at 21 (opining that "non-state actors, or at least those showing some form of organization, should be viewed as direct addressees of the customary rule prohibiting the threat or use of force"); Kilovaty, *supra* note 7, at 119–20. For the state of general international law on the matter, see *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, 2004 ICJ 136, 194 (July 9); Sean Murphy, *Self-Defense and the Israeli Wall Advisory Opinion: An* Ipse Dixit *from the ICJ?*, 99 AJIL 62 (2005). *Cf.* Statement by the President George W. Bush in his Address to the American Nation (Sept. 11, 2001), *available at* https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html (declaring that the United States came under terrorist attack before attributing the attack to any particular entity).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

perhaps not surprising that no such claims were made with respect to cyberoperations clearly falling below the Tallinn Rules use of force threshold, it is remarkable that no *jus ad bellum* claims were made with respect to incidents that appear to have crossed this threshold (putting aside the question of whether or not they met or should have met a higher *Nicaragua* armed attack threshold in order to justify an act of self-defense).[298]

For example, no *jus ad bellum* claims were made in connection with the Ababil operation, which was designed to have a kinetic effect (interference with the Bowman Dam)[299] and also caused significant cybernetic harm to the financial industry, and with regard to the attacks on the petrochemical industry in Iran (which are the only known cyberattacks so far resulting in loss of life) and Saudi Arabia. Even the attacks on Ukraine, which had a direct kinetic effect on the local electric network, were not discussed in *jus ad bellum* terms, although this may be related to the fact that an armed conflict already existed in Ukraine at the time.

The case studies suggest that states do not denounce cyberoperations without physical consequences as running contrary to the prohibition on the use of force.[300] Yet, there is no indication that they treat very differently cyberoperations with actual or potential kinetic consequences. Nor do we have indications in the information before us supporting the proposition that a series of pin-prick attacks (such as the Ababil operation or Iranian petrochemical industry attacks), or attacks affecting multiple states (such as WannaCry and NotPetya) have been analyzed by states as crossing, cumulatively, the various gravity thresholds.[301] Here too, the dominant strategy resorted to by states appears to be silence and ambiguity, avoiding thereby the need to limit their concrete policy options in relation to cyberoperations that already occurred as well as to associate themselves with any particular interpretation of international law with regard to future cyberoperations.

Of course, the decision how to respond to any specific cyberoperation (including whether or not to respond to it diplomatically or militarily, in an overt or covert manner, using cybernetic or kinetic counterforce) is predominantly a political rather than legal decision, which factors in a variety of considerations, including the possible interest in maintaining legal ambiguity vis-à-vis the regulation of cyberspace. Thus, the fact that certain attacks have been met by victim states with silence as to whether or not they involve a violation of the prohibition against the use of force does not mean they could not treat them such in the future. Nor does it mean that states have actually decided to reject the Tallinn Rules on the use of force. Rather, our findings are consistent with the proposition that states maintain a "wait and see" approach toward the Tallinn Rules, and that their policy of silence of ambiguity may be one explanation for their limited reliance on the Rules in circumstances in which their *jus ad bellum* provisions could have been invoked.

[298] TALLINN MANUAL 2.0, *supra* note 1, at 331, 334. The Rules cite the *Nicaragua* "scale and effects" standard for categorizing a prohibited use of force as an armed attack. *See Military and Paramilitary Activities*, *supra* note 31, at 103–04.

[299] Allan, *supra* note 31. While it was unlikely that the attack on the dam could have resulted in much harm at the time of the attack (as it was closed for maintenance), obtaining through a cyberoperation the capacity to interfere with it in the future, might be regarded as the first step in an act of aggression.

[300] TALLINN MANUAL 2.0, *supra* note 1, at 333 (defining "use of force" as "acts that injure or kill persons or physically damage or destroy objects").

[301] For a rule reflecting the "pin-prick" theory, see TALLINN MANUAL 2.0, *supra* note 1, at 342, para. 11. *See also*, ROSCINI, *supra* note 29, at 108–10.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

C. *Sovereignty*

As indicated above in Part III, cyberoperations that do not qualify as a use of force or an armed attack may nonetheless violate other rules of international law. According to Tallinn Manual 2.0,[302] they might violate the sovereignty of another state if their consequences are significant enough (physical damage, loss of functionality, or other forms of infringement that interfere with inherent government functions).[303] Yet the notion that there actually exists a rule prohibiting a violation of sovereignty that applies over and beyond the specific legal rules that derive from the national sovereignty principle, such as the prohibition against the use of force and the non-intervention rule, has been challenged recently.[304] Specifically, it has been questioned whether international law bars cyberoperations other than those that reach the scale and effect of a use of force, or that coercively impinge on the inherent functions of other governments, thus violating the non-intervention rule.[305]

The eleven case studies reviewed above do not fully clarify this point of contention. The muted public response to the Ababil, Sands Casino, Shamoon, and Triton operations, as well as to the operations directed against the Iranian petrochemical facilities could either qualify as use of force or a violation of the victim states' sovereignty if attributable to another state, perhaps suggest a restrictive interpretation of the relevant legal framework consistent with the "sovereignty as principle" approach. On the other hand, the dire warning reportedly issued by President Obama to President Putin in connection with the DNC hack, the diplomatic and law enforcement reactions to the OPM hack, the relatively strong reaction to the Sony hack (which appears to have included a covert response), and the move to develop legislation authorizing "hack-backs" in response to the Bundestag hack, all responses to cyberoperations involving tampering with data, may be indicative of support for a broad application of the sovereignty rule in line with the more expansive views taken by some members of the international group of experts.[306]

It is also interesting to note that none of the attacking states that were allegedly behind the eleven cyberoperations that resulted in harm in the sovereign territory of another state has assumed responsibility for the operation, including when it resulted in relatively minor consequences. While there are obvious political and operational reasons for denying involvement in offensive cyberoperations, the denial of all forms of involvement is consistent with the legal proposition that states do not consider themselves as having a clear right to undertake cyberoperations with consequences in the territory of other states due to the conflict it generates vis-à-vis the sovereignty rule.

[302] TALLINN MANUAL 2.0, *supra* note 1, at 17 (Rule 4).

[303] *Id.* at 20. The experts were divided as to whether infringements falling short of non-functionality and which do not constitute interference in internal affairs violate sovereignty. *Id.* at 21.

[304] *See* Corn, *supra* note 16; Corn & Taylor, *supra* note 46, at 201–11. *See also* Schmitt & Vihul, *supra* note 46, at 1649 et seq.

[305] Eric Talbot Jensen, *The Tallinn Manual 2.0: Highlights and Insights*, 48 GEORGE. J. INT'L L. 735, 743 (2017) (discussing whether sovereignty is a binding norm and arguing that neither of the disputed approaches—sovereignty as a rule or a principle—is universally accepted, citing former Department of State Legal Advisor Brian Egan, opining that the international community is currently "faced with a relative vacuum of public State practice").

[306] TALLINN MANUAL 2.0, *supra* note 1, at 21

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Finally, it should be noted that the reactions following the operations directed against the Sands Casino, the Ukrainian electric grid, and the WannaCry and NotPetya operations are less telling about the status of sovereignty in cyberspace than the previous examples just discussed. The Sands Casino operation was directed against a purely private business and may be regarded for this reason to fall outside the scope of the sovereignty rule provided for in Tallinn Manual 2.0.[307] As explained before, the lack of attribution of responsibility to Iran for the operation, or for failing to exercise due diligence to stop it, may be explained by other policy considerations (e.g., U.S. interest in maintaining ambiguity about relevant due diligence standards and the nuclear disarmament negotiations). At the same time, the operations against Ukraine and the global cyberoperations could have been regarded as a clear violation of the non-intervention rule (and perhaps also of the prohibition on the use of force), which could have warranted a legal response under all approaches to sovereignty infringement. In any event, the statements attributing responsibility to North Korea and Russia for the WannaCry and NotPetya operations did not explicitly refer to infringements of sovereignty, or any specific rule derived thereof. Such statements are thus largely consistent with the policy of maintaining ambiguity vis-à-vis the regulation of cyberspace pursuant to the Tallinn Rules and the notion of sovereignty included therein.

D. Non-intervention

The non-intervention rule, which is derived from the sovereignty principle,[308] has been referred to in the Tallinn Manuals as part of customary international law.[309] Rule 66 reads: "A State may not intervene, including by cyber means, in the internal or external affairs of another State."[310] According to the International Court of Justice (ICJ) *Nicaragua* judgment, coercion is a requisite component of the non-intervention rule,[311] and the Tallinn Manual 2.0 stipulates that coercion is "an affirmative act designed to deprive another state of its freedom of choice, that is, to force that State to act in an involuntary manner or involuntarily refrain from acting in a particular way."[312]

Arguably, the coercive aspect of intervention is not confined to operations curbing governmental powers and policies, but also to the freedom of choice exercised by the people of a state.[313] Interventions in election campaigns or referenda (e.g., the U.S. 2016 presidential campaign, Brexit, and allegedly also in 2017 campaigns in France, Germany, and the

[307] *Id.* at 18.

[308] This is consistent with the approach regarding sovereignty as a principle, see Corn & Taylor, *supra* note 46 (non-intervention and due diligence might be considered rules which derived from the principle of sovereignty).

[309] *See, e.g.*, Declaration on Principles of International Law Concerning Friendly Relations and Co-operation Among States in Accordance with the Charter of the United Nations, Principle 3, UN Doc. A/RES/25/2625 (Oct. 24, 1970).

[310] TALLINN MANUAL 2.0, *supra* note 1, at 312 (Rule 66).

[311] *Military and Paramilitary Activities*, *supra* note 31, at 108.

[312] TALLINN MANUAL 2.0, *supra* note 1, at 317, paras. 17–18. Declaration on Principles of International Law, *supra* note 302, clarifies that: "No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State. . . . No State may use or encourage the use of economic political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind. . . ."

[313] Restricting freedom of choice in political affairs could further constitute a breach of the human rights of individuals within a state. International Covenant on Civil and Political Rights, Art. 25, Dec. 16, 1966, 999 UNTS 171: "Every citizen shall have the right and the opportunity, . . . (b) To vote and to be elected at genuine

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Netherlands)[314] might thus be regarded under certain conditions as unlawful coercive interventions. Such coercive intervention might be confined to remote altering of voting results or comparable acts, directly affecting the voting system and elections outcome. Such an operation appears to be proscribed under international law,[315] as suggested by President Obama's harsh warning to the Russians to refrain from tampering the election process.[316] Harold Koh and other scholars have taken a more expansive view, arguing that a foreign influence operation using covert activities such as spreading fake news and using social media networks to influence voters may also constitute illegal coercive intervention, which restricts the choice exercised by the voting population.[317] Still, the covert nature of such practices complicates the ability to identify, in real time, the true scale and coercive attributes of the operations in question.[318]

The non-intervention rule might be violated even in the absence of coercion when the activity in question usurps essential governmental functions.[319] Arguably, the election process implicates one of most important functions in a democracy. The U.S. Intelligence Community Assessment did not initially support the view that Russia usurped the U.S. election process by meddling with vote tallying,[320] but new data revealed in May 2017[321] and in February 2018[322] supports the claim that there may have been at least an attempt to usurp the process, and that such an attempt could qualify as contrary to the non-intervention rule even in the absence of coercion. The application of criminal indictments by the United States against Russian nationals involved in the influence operation, which came on top of diplomatic sanctions, and the recent public comments of the UK attorney general on manipulation of elections as a form of coercive intervention,[323] do seem to suggest a tendency to view such

periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free expression of the will of the electors."

[314] See *supra* note 187; Eric Auchard, *Macron Campaign Was Target of Cyber Attacks by Spy-Linked Group*, REUTERS (Apr. 24, 2017), *at* https://www.reuters.com/article/us-france-election-macron-cyber/macron-campaign-was-target-of-cyber-attacks-by-spy-linked-group-idUSKBN17Q200; Sumi Somaskanda, *The Cyber Threat To Germany's Elections Is Very Real*, ATLANTIC (Sept. 20, 2017), *at* https://www.theatlantic.com/international/archive/2017/09/germany-merkel-putin-elections-cyber-hacking/540162; Nick Allen, *Dutch Spies "Caught Russian Election Hackers on Camera,"* TELEGRAPH (Jan. 26, 2018), *at* https://www.telegraph.co.uk/news/2018/01/26/dutch-spies-caught-russian-election-hackers-camera.

[315] TALLINN MANUAL 2.0, *supra* note 1, at 312.

[316] *See* White House Press Release, *supra* note 169.

[317] Harold Hongju Koh, *The Trump Administration and International Law*, 56 WASHBURN L.J. 413, 450 (2017) ("even if the Russians did not actually manipulate polling results, illegal coercive interference in another country's electoral politics—including the deliberate spreading of false news—constitutes a blatant intervention in violation of international law"); Ohlin, *supra* note 59, 1595–98 (suggesting that influence operations could be considered as a violation of the self-determination rule); Egan, *supra* note 267, at 172.

[318] Ohlin, *supra* note 59, at 1592 (noting "there are substantial impediments to concluding that Russian hacking . . . constituted illegal coercion," but that it depends on factual elements). It may be noted that it took more than a year after the 2016 U.S. elections to uncover the relevant evidence needed to file criminal charges against Russian nationals and to attribute direct responsibility to Russia for their activities.

[319] *Id.* at 1594 n. 60 (citing Egan remarking that: "[A] cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention.").

[320] ICA, *supra* note 135.

[321] Cole, Esposito, Biddle & Grim, *supra* note 134.

[322] Mcfadden, Arkin & Monahan, *supra* note 137; Indictment (U.S. v. Internet Research Agency), *supra* note 173. *See also Russia Election Interference*, *supra* note 138.

[323] Wright, *supra* note 5.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

operations as violating both national and international law, and a move away from the policy of silence and ambiguity relating to the position of states on the status under international law of cyber influence operations. Such a move brings states closer to embracing the approach taken by the Tallinn Rules regarding the unlawfulness of cyberoperations that infringe state sovereignty. Still, it remains uncertain whether states accept in full the approach taken by the international group of experts relating to sovereignty as a direct source of a prohibition against certain cyberoperations.

Another possible approach to the non-intervention rule in the cyber domain is to encompass within it acts of interference aimed at seriously disrupting and affecting the internal affairs of a foreign state.[324] It is possible to regard the aforementioned U.S. and UK reactions to influence operations as glossing over the distinction between non-intervention and non-interference, which the Tallinn Manual 2.0 endorses,[325] thereby lending support to a broad reading of the non-intervention rule under international law.

It is noteworthy, however, that the United States is the only country that has so far undertaken acts qualifying acts of retorsion against foreign states implicated in influence operations. Since acts of retorsion do not necessarily presume that a violation of international law had occurred, they preserve a degree of ambiguity about the contents of international law that the offensive cyberoperation might have violated. Countries other than the United States have tended, instead, to invest in reinforcing cybersecurity perhaps out of fears that resorting to reactive steps might escalate the situation.

E. Due Diligence

Another important element in the normative edifice constructed by the Tallinn Manuals is the due diligence rule, which imposes positive obligations on states to prevent their territory from being exploited to affect the rights of other states in a manner that produces serious adverse consequences.[326] Although the threshold of "serious adverse consequences" is unclear,[327] it is safe to assume that operations that would comprise, were they to be directly undertaken by a state, "over the threshold" of international law rules on use of force and non-intervention that would entail state responsibility were they to be directly undertaken by a foreign state would also trigger the host state's rules obligations to prevent such activities undertaken by non-state actors operating from within its territory.

Recent developments suggest, however, that the positions of states on this point have been developing toward less stringent standards of legal obligation. For example, the 2015 report of the Group of Governmental Experts (UN GGE) provided that: "States must not use proxies to commit internationally wrongful acts using [Information and Communication

[324] Ido Kilovaty, *Doxfare – Politically Motivated Leaks and the Future of the Norm on Non-intervention in the Era of Weaponized Information,* 9 HARV. NAT'L SECURITY J. 149, 157–59, 174–77 (2018) (describing a disruption process of "doxfare," an operation undertaken by state-sponsored groups with a view to intruding networks and computers, gathering non-public data and leaking it at a chosen timing to influence the victim state's internal or external affairs).

[325] TALLINN MANUAL 2.0, *supra* note 1, at 313, para. 3.

[326] *Id.* at 30 (Rule 6) ("A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.").

[327] *Id.* at 36.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Technologies (ICTS)], and *should* seek to ensure that their territory is not used by non-State actors to commit such acts."[328] This has been perceived as falling short of the *must* exercise due diligence formulation used in Tallinn Manual 2.0.[329] Multiple reports about the continued use of proxies by states to conduct cyberoperations, including in the case studies discussed above, and the limited response taken by victim states against host states in this connection are further indications of the limited reliance on the due diligence rule by states in their actual practice.[330] Experts in the field also appear to have little appetite for construing the Tallinn Rules as requiring permanent monitoring of "national" areas of cyberspace.[331]

Indeed, the case studies discussed in this article illustrate the limited reliance of states on the due diligence rule in formulating their demands against the host states from which the operations emanated. For example, the phased-out nature of the Ababil operation (extending over more than a year), and its serious adverse consequences (damage in the millions of dollars and a risk to the operations of a water dam), could have clearly invited the application of the due diligence rule. This is especially the case after criminal charges were laid against private Iranian actors (albeit with links to the Iranian Revolutionary Guards). But despite the duration of the operation and indications that they emanated from Iranian nationals operating on Iranian territory, the U.S. administration did not overtly make a demand for the involvement of the Iranian authorities (who, at least after being out on notice, should have taken preventive measures that were "reasonably available and practicable").[332] In the same vein, other incidents ostensibly involving private actors, the OPM and Bundestag hacks, did not lead the victim states, the United States and Germany, to invoke publicly the due diligence against the putative host states (China and Russia). On the other hand, the DNC hack (which implicated two private groups of Russian hackers) and the Sony hack (which implicated North Korean group of hackers) were responded to, reportedly, at the interstate level. These latter examples can be regarded as an implicit endorsement of the due diligence rule, since the responses were carried out in the face of denials by the host states of direct involvement in the offensive cyberoperations.

The difficulty in assessing state practice in this field and their position vis-à-vis the relevant Tallinn Rules is intimately tied to the problem of attribution discussed above and to the prevailing policy of silence and ambiguity. The ability to claim state responsibility for lack of due diligence often requires that the violating state be confronted with evidence tying the operation in question to its territory, and, even more so, establishing, as a factual and legal matter, its actual or constructive knowledge thereof, and support or acquiescence.[333] Victim states

[328] Report of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, at para. 28(e), UN Doc. A/70/174 (2015) (emphasis added).

[329] Jensen, *supra* note 305, at 745 n.45.

[330] Tim Maurer, *"Proxies" and Cyberspace*, 21 J. CONFLICT & SECURITY L. 383 (2016).

[331] Eric Talbot Jensen, *Cyber Sovereignty: The Way Ahead*, 50(2) TEX. INT'L L.J. 275, 299 (2015) (asserting that the duty to monitor is controversial as it compromises potential human rights obligations). *See also* Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773, 810, 824 (2012) (citing President Obama stating: "Our pursuit of cybersecurity will not—I repeat, will not include—monitoring private sector networks or Internet traffic. We will preserve and protect the personal privacy and civil liberties . . . .").

[332] TALLINN MANUAL 2.0, *supra* note 1, at 43.

[333] The OPM hack and the Sony hack were launched from Chinese territory and the Bundestag hack was launched from Russian region. None of the three attacks was attributed to the host state, which might suggest some hesitation in relying on constructive knowledge as basis for claiming attribution.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

may be reluctant for a variety of reasons to break their silence and share such evidence with those states that may have been directly or indirectly involved in the operations against them. Making specific demands from the host states on the basis of their international law obligations might also require the victim state to move away from its policy of ambiguity and present a specific understanding of due diligence obligations relating to cyberoperations.

Finally, the availability of information tying the cyberoperation in question to the host state (i.e., establishing an attack by proxy) renders the due diligence rule largely irrelevant, since one would be dealing in such cases with direct state responsibility. Arguably, in the high-profile cases discussed above, deliberate use of proxies appears to have been the rule, not the exception. This reality renders those parts of the Tallinn Rules dealing with due diligence less relevant to state practice, regardless of whether or not they actually support the contents of the Rules comprising these parts.

F. Countermeasures

Countermeasures, involving reactive measures falling short of the use of force, play an important role in the Tallinn Manuals legal framework, as complementing the right to self-defense.[334] Victim states may resort to countermeasures falling short of the use of force even if by doing so they violate the non-intervention or sovereignty rule (to the extent that it can be recognized as a stand-alone rule), if the state from whose territory the operation originated was implicated in the first-in-time operation, directly or indirectly (through a breach of the due diligence rule). If it cannot be shown that the cyberoperation violated international law, then it seems that only acts of retorsion, which do not in themselves violate international law, including "under the threshold" cyberoperations (e.g., DDoS attacks entailing temporary loss of functionality with a limited disruptive effect), can be taken against the private actor that initiated the first-in-time operation and/or against the state from whose territory the operation originated.[335]

It is hard to deduce from the eleven case studies that state practice follows the provisions of Tallinn Manual 2.0 in connection with the application of countermeasures. There is no indication that the Ababil and Sands Casino operations and OPM and Bundestag hacks led to any countermeasures, overt or covert, despite their significant consequences. By contrast, the DNC hack did result in overt and covert threats of countermeasures or even a threat of use of force if the violations would not stop; it did eventually lead to the actual imposition of diplomatic sanctions. These steps must have been premised on the possibility of attributing the hack directly or indirectly to Russia and on qualifying the hack as a violation of a rule of international law (most probably, the non-intervention rule). Another case potentially featuring a resort to countermeasures is the Sony hack case, which allegedly led to the temporary

[334] It is noteworthy in that regard that most of the Tallinn experts were of the view that states may respond to an armed attack with an act of self-defense even if the attacker is a non-state actor. TALLINN MANUAL 2.0, *supra* note 1, at 345, paras. 18–19 (the majority of the IGE concluded it is state practice relying on the international community resolutions regarding the 9/11 attack). *See also* Nicolas Jupillat, *Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Laws of State Responsibility*, 92 U. DET. MERCY L. REV. 115, 122 (2015) (claiming that self-defense must remain an answer to armed attacks carried out by states only, but open to lowering the threshold of state responsibility to deter states hiding behind proxies).

[335] Colonel Gary Corn, a legal advisor of the U.S. Cyber Command, and Professor Eric Talbot Jensen have claimed that, so far, all U.S. reactions to cyberoperations directed against it were in the form of retorsions. Corn & Jensen Part 1, *supra* note 45.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

disruption of internet service in North Korea. Without a public statement on this matter, it is however difficult to deduce the precise legal position taken by the United States on the matter (especially since the Sony hack did not appear to violate the non-intervention rule and was at the low end of the scale for the purposes of finding a violation of sovereignty).

The cyberoperations directed against Saudi Arabia and Iran did not follow the rules of countermeasures and it looks as if both states have been engaged in a covert cyberconflict with one another, with little concern for the legal requirements attendant to the law of countermeasures. Finally, it is useful to mention in this regard the interest shown by German law enforcement authorities in passing a hack-back law following the Bundestag hack, which would allow for countermeasures against the direct source of the foreign cyberoperation. Such an initiative has not become, as of yet, official state policy.

The reluctance to publicly claim the right to apply countermeasures and to follow up thereon, may suggest that states are either not interested in clarifying the state of the law in the field or are uneasy about the stringent conditions associated with its application (including the need to notify the other state and to minimize collateral harm).[336] It is also likely the case that states rely on mostly non-legal policy considerations (such as fear of escalation or loss of an operational surprise effect) when shaping their reactions to cyberoperations. In the U.S.-Iran context, the cautious approach of the Obama administration, and the lack of a robust overt or covert response, which may relate to political and strategic considerations, has been nonetheless criticized in similar terms as eroding American deterrence.[337] The pursuance of criminal proceedings against the direct culprits (albeit with limited prospects of actually gaining custody over them) may have been designed to offset some of the concern of being regarded as "soft on cyber."

G. Distinction and Proportionality

Although our focus in discussing the case studies was on the regulation of the use of kinetic and cybernetic force in self-defense or the use of countermeasures in response to aggressive cyberoperations, they also raise serious questions regarding the compatibility of the measures taken with international humanitarian law, as applied to cyberspace.[338] The cyberattacks that have been conducted within the framework of an ongoing armed conflict in Ukraine failed to adhere to basic principles of distinction and proportionality. In the same vein, in the case of NotPetya, the attackers seem to have intentionally chosen an indiscriminate and disproportional method of operation (since they failed to confine the operation to specific IP addresses in Ukraine). Interestingly enough, public reactions to these operations have not focused

[336] According to the ASR, resort to countermeasures depends on several factors, including intent to induce compliance, prior notification, limits on application to fundamental international law norms, and proportionality. ASR, *supra* note 262, Arts. 49–54. Note that the UK attorney general has doubted whether there is a need to present a notification before engaging in cybernetic countermeasures. Wright, *supra* note 5 ("The one area where the UK departs from the excellent work of the International Law Commission on this issue is where the UK is responding to covert cyber intrusion with countermeasures. In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it.").

[337] Nakashima, *supra* note 78.

[338] Peter P. Pascucci, *Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution*, 26 MINN. J. INT'L L. 419 (2017) (discussing difficulties in implementing proportionality and distinction rules in cyberspace).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

largely on their indiscriminate and disproportionate nature, even though the White House depicted NotPetya in one statement as "reckless and indiscriminate," and "the most destructive and costly cyber-attack in history."[339]

In the same vein, it appears as if the operations directed against the petrochemical and oil industry in Iran and the Shamoon and Triton operations against Saudi Arabia were conducted in violation of both *jus ad bellum* and *jus in bello* rules, with little regard for the rights of uninvolved civilians. In both cases, silence on the part of the involved states does not allow for an adequate analysis of the way in which they interpret relevant *jus in bello* terms, such as what constitutes an "attack," "military object," or "collateral damage," or how to apply the proportionality rule in cyberspace. Nonetheless, the lack of acknowledgement and attribution of the operations and the serious effects they had on civilian populations and property might be indicative of a limited interest in upholding international humanitarian law principles, as reflected in the Tallinn Rules. This state of affairs may, in turn, also suggest that although the Tallinn Manuals contributed to closing the gap between international humanitarian law (IHL) and new forms of conduct of hostilities, the analogy to the kinetic world has its practical limits, and that, as a result of the limited fit between the law and its field of application and the tendency of states to opt for a policy of silence and ambiguity in respect of the norms of IHL too, the Tallinn Rules actually offer limited protection to civilians.[340]

H. General Implications for International Law

At a more abstract level, the findings of our research provide interesting insights about the manner in which international law develops and functions under conditions of significant normative uncertainty and in the absence of effective enforcement mechanisms. Such conditions are found in cyberspace, where the law on the books and its application in practice are unclear and where, because of the problem of attribution and other considerations that lead states to refrain from openly resorting to countermeasures and other response measures, international law is chronically underenforced. Still, while cyberspace may represent an extreme example of the application of law in circumstances of legal uncertainty, many of the dilemmas confronting states in this domain have also been encountered in other fields. Hence, our case studies may offer relevant lessons to all students of international law and invite further research into the implications of state conduct in cyberspace for general international law theory.

To be clear, even states skeptical of the Tallinn Rules do not regard cyberspace as a norm-free zone. Certain non-binding rules of conduct have emerged out of state practice and national strategy statements.[341] Some of them were broadly endorsed by the 2015 Report

[339] See White House Press Release, *supra* note 254.

[340] Pasucci, *supra* note 338, at 461 ("In cyberwar, the application of the principles of distinction and proportionality fail to adequately provide protection of the civilian population because the definitions and current application are based upon the historical application to kinetic warfare."). *See also* Duncan Hollis, *Re-thinking the Boundaries of Law in Cyberspace: A Duty to Hack?*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS 129 (J. Ohlin, Kevin Govern & Claire Finkelstein eds., 2015) (criticizing the insistence of relying on analogy while rejecting more appropriate non-analogous solutions); Rebecca Crootof, *Autonomous Weapon Systems and the Limits of Analogy*, 9 HARV. NAT'L. SECURITY J. 51 (2018) (emerging technologies create more and more situations where no analogy to other existing areas of law application will be appropriate).

[341] Egan, *supra* note 267, at 179–80.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

of the UN GGE,[342] and states have started to accept them through multilateral statements,[343] and international agreements regarding cybersecurity cooperation.[344] Over time, several of these non-binding rules are likely to consolidate into customary international law. Nevertheless, the case studies suggest that a significant normative gap exists in relation to the regulation of interstate cyberoperations. This is because the combination of silence and ambiguity in state practice and their reluctance to articulate their official policy in cyberspace prevents or, at least, slows the development of global norms of conduct.

The Tallinn Rules can play a potentially important role in this field as normative points of reference, around which customary international law and treaty interpretation can further coalesce.[345] Their existence inspires states and commentators to engage in a process of legal translation—a good faith effort to translate existing legal norms to the new circumstances of cyberspace.[346] Still, the process of establishing new rules of international law or accepting the applicability of existing rules requires a certain level of interstate communication and public diplomacy, which the aforementioned policy of silence and ambiguity undercut.[347]

I. Optionality

The reluctance of states to invoke the Tallinn Rules in relation to cyberoperations in which they find themselves involved as the attacking or victim state may stem not only from uncertainty as to whether the Tallinn Rules accurately reflect international law, but also from deeper doubts as to whether international law *should* govern all activities in cyberspace. Such doubts, in turn, may encourage states to develop a policy of *optionality* toward the application of international law, that is to adopt a deliberate strategy of treating the applicable international law framework as optional, in the sense that states may choose whether or not to invoke the legal discourse of international rights and obligations in their mutual interactions in cyberspace. Indeed, the case studies show that state tend to embrace a policy of silence and ambiguity, but that even when they acknowledge that they were victims of cyberoperations directed against them, the rhetoric they use to describe the operation and their planned reaction thereto tends not to include legal arguments or references to specific norms of international law.

Optionality is particularly relevant for those states that have the greatest capacity to operate covertly in cyberspace and to protect their national security interests outside the framework of

[342] Report of the UN Group of Governmental Experts, *supra* note 328.

[343] *See, e.g.*, G7 Declaration on Responsible States Behavior in Cyberspace, Apr. 11, 2017, *available at* https://www.mofa.go.jp/files/000246367.pdf. *See also* Mariarosaria Taddeo, *Deterrence by Norms to Stop Interstate Cyber Attacks*, 27 MINDS & MACHINES 387 (2017).

[344] *See, e.g.*, White House, Fact Sheet: President Xi Jinping's State Visit to the United States (Sept. 25, 2015), *available at* https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states (containing agreement on IP theft and cybersecurity).

[345] *See, e.g.*, Eric A. Posner & Jack Goldsmith, *Further Thoughts on Customary International Law,* 23 MICH. J. INT'L L. 191, 193 (2001).

[346] Koh, *supra* note 317, at 418.

[347] One may note in this regard that Brian Egan, the U.S. State Department's previous legal adviser, criticized the relative silence of states regarding cyberoperations, arguing that it increases uncertainty which "could give rise to misperceptions and miscalculations by States, potentially leading to escalation and, in the worst case, conflict." Egan, *supra* note 267, at 172.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

international law.[348] Paradoxically, the decision of states with advanced technological capacity to refrain from invoking international law in relation to the cyberoperations in which they are involved implies that their contribution to the development of customary international law norms in this field might be smaller in some respects than that of states with more limited capacity, which may have no choice but to conduct themselves within the existing legal framework.

One illustration of optionality can be found in President Obama's reaction to the Sony hack, which promised a U.S. response in the place and time and manner that it chooses,[349] and which manifested itself, probably, in an unacknowledged and possibly extralegal cyberoperation against the North Korean internet infrastructure. The same approach also characterized the Obama administration's reaction to the DNC hack, which similarly promised a clandestine response (though referring obliquely to "Russia's efforts to undermine established international norms of behavior, and interfere with democratic governance").[350] The lack of explicit reference to an international law framework when addressing the operations conducted against the United States and the anticipated response thereto, appears to reflect a deliberate policy choice to deal with the operation outside the four corners of the international law framework.

The choice of whether or not to invoke international law norms is even more apparent in those cases in which victim states did not acknowledge being attacked or refrained from attempting to attribute the attack to another states, thus consciously choosing not to facilitate the application of international law to the situation at hand. At the same time, the interest shown recently by multiple states in collectively attributing international responsibility for global cyberoperations, such as WannaCry and NotPetya, may reflect a conscious decision on their part to invoke an international law framework, with a view to facilitating a coordinated overt response, which could enjoy broad international legitimacy. We therefore seem to find ourselves in a critical juncture for the development of international law regulating cyberoperations in which national security considerations militating in favor of maintaining operational latitude through silence and ambiguity may be gradually giving way to the communicative and norm-consolidation imperatives of collective action and applying the pressures of public diplomacy, which seem to affect the policies even of these states with the most advanced capacity in cyberspace.

The availability of a choice as to whether or not to conduct certain international interactions pursuant to an international law framework is not unique to the field of cyberoperations. It can be found in other areas where states are ambivalent as to whether international law properly serves their interests, or whether they should clearly express themselves on its contents. For example, the failure of several states, including the United States, France, Turkey, and Israel, who have been involved in recent years in use of force action in and around Syria,[351] to enunciate a clear legal rationale for their activities, suggests a policy of optionality

[348] *Cf.* Matthew C. Waxman, *Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)*, 36 YALE J. INT'L L. 421, 424 (2011).

[349] Sullivan, *supra* note 125.

[350] White House Press Release, *supra* note 169 ; Egan, *supra* note 267, at 172.

[351] For a discussion of the legal implications of lack of a legal explanation for recent uses of forces in Syria, see Marko Milanović, *The Syria Strikes: Still Clearly Illegal*, EJIL: *TALK!* (Apr. 15, 2018), *at* https://www.ejiltalk.org/the-syria-strikes-still-clearly-illegal. The exception to the trend of not providing a legal explanation for recent

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

in this field as well. Such a policy can only succeed, however, if a significant number of states with international clout cooperate with it, and do not hold to account states operating outside the four corners of the law.

J. Parallel Tracks

A second feature of state practice in the field of cyberoperations, which the case studies seem to reveal, is the development of parallel tracks of interstate interaction, comprising acknowledged and unacknowledged practices, with each track governed by separate "rules of the game." Specifically, we believe that the fact that aggressive cyberoperations have resulted, up until now, in limited loss of life and injury, and the fact that the damage inflicted in cases such as the *Black-Energy* operations in Ukraine appears to have been contained by design, suggest that attacking states are actually adhering to certain restraining norms. In the same vein, one may find restraint in the measured nature of covert responses taken by victim states to cyberoperations. President Obama's allusion to proportionality in responding to the Sony hack,[352] while promising that some of the response will be covert, underscores the notion that operating outside the international law framework (through exercising a politically available option to do so) does not imply operating in a completely norm-free "track."

Here too, the situation in cyberspace finds analogies in the physical world. In fact, international law doctrine has long distinguished between usage—stable patterns of state conduct shaped by practice without the sense of a legal obligation—and custom, where practice is backed by *opinio juris*.[353] Arguably, norms of an extralegal nature govern the contents of non-legally binding usages. Furthermore, there are several important areas of international relations where interactions are governed by legitimate expectations of conduct, which are not directly regulated by international law, and that exist in parallel to international law frameworks. For example, the informal rules governing the work of regional groupings in international organizations are often adhered to far more scrupulously than the formal rules of the organization in which the members of the groupings participate.[354]

The preference of states to operate in a parallel track, subject to norms other than the rules of international law may even lead them, in certain contexts, to create by way of an international agreement a regulatory framework that operates as an alternative to existing international law frameworks. For example, the Final Act of the 1975 Helsinki Conference, which laid down important norms for the conduct of international relations, was explicitly formulated in a manner that would not ostensibly affect the rights and obligations of the parties to the Accords under international law.[355] The framing of the Joint Comprehensive Plan

interventions in Syria is the UK Prime Minister's Office, Syria Action – UK Government Legal Position (Apr. 14, 2018), *available at* https://www.gov.uk/government/publications/syria-action-uk-government-legal-position/syria-action-uk-government-legal-position.

[352] Sullivan, *supra* note 125.

[353] *See, e.g.*, HERSCH LAUTERPACHT, THE DEVELOPMENT OF INTERNATIONAL LAW BY THE INTERNATIONAL COURT 387 (1958, 1982 reprint).

[354] *See generally* Randall W. Stone, *Informal Governance in International Organizations*, 8 REV. INT'L ORG. 121 (2013).

[355] The Final Act of the Conference on Security and Cooperation in Europe, Aug. 1, 1975, Part X, 14 ILM 1292 (1975).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

of Action on Iran as comprising voluntary measures, not legal undertakings,[356] is also reflective of the utility in the eyes of certain states of creating a parallel, not strictly legal, track.

The institution of retorsion, which largely operates without an international law framework but nonetheless appears to be subject to notions of proportionality,[357] is another parallel track measure that supplements and even supplants international law-regulated countermeasures. This latter point is underscored by our case studies in which overt U.S. responses to cyberoperations were typically undertaken in the form of retorsions.[358] In fact, the resort to acts of retorsion may be reflective of the difficulty of states to choose between the conflicting policy imperatives of silence and ambiguity, on the one hand, and legal transparency, on the other hand. While public in nature, the application of retorsions, unlike countermeasures, does not depend upon the adoption of a clear position on the contents of international law and on the question whether it was violated.

What is exceptional about the "parallel track" of state conduct developed in connection with cyberoperations is its secretive nature, which complicates efforts to identify the norms governing it. The deniability of cyberoperations and counteroperations, and the attendant problem of attribution, adversely affects the power of all norms—formal international law norms and informal "parallel" norms—to guide and explain state conduct. Moreover, whereas adherence to informal rules cannot be normally relied upon to justify a violation of formal rules, in the "below the radar" world of cyberspace, the boundaries between formal and informal may not always be respected. It is this shadowy aspect of cyberoperations, which induces a comparison between such operations and espionage, another field of activity that appears to be operating primarily under informal rules.[359] Indeed, our findings suggest that one key dilemma confronting states in this field is whether or not to regard cyberoperations as a form of espionage. One can mention in this connection the debate within U.S. circles around the question of whether or not the OPM hack exceeded the expectations from a "normal" case of data theft for intelligence purposes.[360]

K. Gradations in Law Enforcement

Finally, it may be noted that the timid reaction of victim states to cyberoperations directed against them or against third states may suggest that even if the Tallinn Rules reflect in the eyes of states existing international law, they regard the Rules as a rather weak body of law, which do not lend themselves to robust enforcement measures. Such an approach may, in turn, stem from doubts about the utility of invoking international law in response to offensive cyberoperations, given the limited self-help tools it offers victim states and due to the aforementioned attribution challenges. Note that the latter difficulty is further compounded by the absence of an international attribution agency, which could enable states to obtain an internationally authoritative holding on the attribution of responsibility to state or non-

[356] Joint Comprehensive Plan of Action, at pmbl., July 14, 2015, *available at* https://www.state.gov/documents/organization/245317.pdf.

[357] Thomas Giegerich, *Retorsion*, *in* Max Planck Encyclopedia of Public International Law 983 (2011).

[358] Corn & Jensen Part 1, *supra* note 45.

[359] For a discussion of international law governing espionage, see Pun, *supra* note 57; Asaf Lubin, *Espionage as a Sovereign Right Under International Law and Its Limits*, 24 ILSA Q. 22 (2015–2016).

[360] *See supra* notes 101 and 102.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

state actors, and which could serve as a legitimate basis for collective sanctions against the law violating state.[361] Yet the limited nature of the responsive measures adopted by victim states may also reflect an interest on their part in maintaining legal ambiguity, which would allow them to engage in due course, if they so wish, in offensive cyberoperations, and to challenge at a subsequent point in time the contents of the Tallinn Rules.

The notion that the enforceability of some international law rules is gradated, that is, that some legal norms are subject to weaker enforcement action than others because of deep ambivalence of states about their utility and precise contents is, again, not unique to the field of cyberoperations. Situations indicative of little appetite to enforce certain international law norms may be found in fields as diverse as humanitarian intervention, where states exercising force in such controversial circumstances have been able to mostly avoid international censure and sanctions,[362] and the active duty to peacefully resolve disputes,[363] which is often honored in the breach without direct legal consequences. Chronic underenforcement in such fields may be indicative of the interest of states in maintaining flexibility in relation to the actual application of controversial international norms.

Although all three strategies—optionality, parallel track, and gradated enforcement—can be found in other fields of international law as well, their convergence in the law governing cyberoperations accentuates the particular challenge of regulating this particular field. It is the combination of contested rules and low enforcement prospects that renders cyberspace exceptionally difficult to regulate. As we have discussed above, the Tallinn Rules, which attempted to flesh out an existing regulatory framework, have been challenged as unfit to fully address the risks of cyberoperations, oblivious to important state interests, and non-reflective of the views held by all states. Furthermore, given the problem of attribution, the actual ability of states to effectively rely on international law in this field remains limited.

Hence, the regulation of cyberspace confronts a "perfect storm" of challenging circumstances, resulting in states choosing to operate outside legal frameworks, developing a non-transparent parallel regulatory track offering limited predictability and stability, and accepting chronic conditions of underenforcement. We are of the view that such difficult background conditions for promoting the rule of law in cyberspace put in question the long-term sustainability of the Tallinn Rules as an authoritative articulation of international law governing cyberoperations.

Still, recent developments and the elaboration of international law doctrines applicable to cyberoperations by some government officials suggest that under certain conditions states may be incentivized to apply international law to cyberoperations and to reduce the attendant legal ambiguity. This implies that the utility of enhanced coordination and increased legitimacy may tip the balance in favor of opting for reliance on international law (without necessarily rejecting other measures taken under "parallel tracks") and for moving to exact a price from the offending state by enforcing the law against it. The Tallinn Rules may play a useful role as a normative focal point for such reliance and enforcement attempts.

[361] For an exposition of the idea of establishing an international attribution agency, see Smith, *supra* note 240.

[362] For a discussion, see Ian Hurd, *Is Humanitarian Intervention Legal? The Rule of Law in an Incoherent World*, 25 ETHICS & INT'L AFF. 293 (2011).

[363] UN Charter Art. 2(3).

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

V. Conclusion

The criticism directed at the suitability of certain aspects of the Tallinn Rules, and the loose relationship between the Tallinn Rules and post-Tallinn state practice, invite an evaluation of the degree to which states have accepted, or are interested in accepting, the five premises of the Tallinn Rules noted in the introduction to this article, i.e., that harm caused by cyberoperations is comparable to that caused by kinetic attacks; that international law governs cyberoperations; that states exercise sovereignty or control over parts of cyberspace; that cyberattacks are regulated by analogous *jus ad bellum* and *jus in bello* rules to those applicable in the kinetic sphere; and that states may incur responsibility over private cyberoperators. The failure of the UN GGE to reaffirm in 2017 the applicability of international law to cyberspace underscores the "wait and see" approach adopted by several states involved in cyberoperations in respect of key aspects of the regulatory framework described in the Tallinn Manuals,[364] as does the tendency of some states to maintain a policy of silence and ambiguity vis-à-vis international law governing cyberoperations. Although the Tallinn Rules have been criticized by some commenters as not going far enough in limiting the ability of states to conduct cyberoperations in cyberspace, we are seeing some states claiming the opposite, and some going even farther than that by challenging the very suitability of *jus ad bellum* and *jus in bello* to cyberoperations.

At the bottom of these disagreements, we find deep uncertainty about the treatment of cyberspace as just another physical space, like land, air, or sea—over which states may exercise sovereignty or control. Such treatment is indeed controversial given the description of cyberspace as "virtual lands."[365] Interactions and communities formed in this virtual space are often deterritorialized,[366] and subject to greater regulatory control by global technological corporations, such as Google, Apple, Facebook, Amazon, and Microsoft, than by states.[367] Although the presence of physical infrastructures inside state territory does allow states to exercise some degree of control over end-users, routing stations, servers, data-flows, and the like, such control is hard to implement, and is rarely invoked in liberal democracies, since it is largely an anathema to basic human rights and to principles of privacy, freedom of expression and association, and free market economy.

Given the doubts that many state officials seem to have as to the contents of regulation that would best serve the interests of states who find themselves involved in cyberoperations, the uneven capacities of states in this field, and the lack of effective international institutions for attributing responsibility and applying international law norms, it is not surprising that efforts to regulate cyberspace through translating traditional concepts of statehood, including sovereignty, territorial integrity, and international responsibility meet some skepticism and resistance, and shape only to a limited degree state practice. Most significantly, our eleven case

[364] Väljataga, *supra* note 6.

[365] *See, e.g.*, Tim Jordan, Cyberpower: The Culture and Politics of Cyberspace and the Internet 1 (1999); Julian Raul Kücklich, *Virtual Worlds and their Discontents Precarious Sovereignty, Governmentality, and the Ideology of Play*, 4 Games & Culture 340 (2009).

[366] Jackson Adams & Mohamad Albakajai, *Cyberspace: A New Threat to the Sovereignty of the State*, 4 Mgmt. Stud. 256, 256–57 (2016) (depicting "the virtual nature of the cyberspace implies dematerialization (everything is paperless), detemporalization (instant communication), and deterritorialization (breaking the geographical boundaries and distances) of online activities and interactions").

[367] Charles Arthur, *Internet Regulation: Is It Time to Rein in the Tech Giants?*, Guardian (July 2, 2017), *at* https://www.theguardian.com/technology/2017/jul/02/is-it-time-to-rein-in-the-power-of-the-internet-regulation.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

studies do not show that states generally accept or rely on the normative categories used in the Tallinn Rules—armed attack, use of force, violations of sovereignty, and violations of due diligence obligations—to draw meaningful legal distinctions in their reactions to cyberoperations. Although states may decide for a variety of reasons not to invoke the rights due to them under international law and prefer instead to pursue a policy of selective reliance on international law (optionality), it is still remarkable that there is so little in the practice of victim states to indicate that they actually guide their conduct when confronted by cyberoperations pursuant to the Tallinn Rules. Statements by senior officials in the United States and the UK questioning some important elements of the regulatory scheme provided in Tallinn Manual 2.0, as well as the aforementioned failure by the UN GGE to agree on the applicability of international law to cyberspace, also cast doubt on whether such elements coincide with contemporary *opinio juris*.

The uneasy "fit" between traditional international law principles governing the exercise of state power inside and outside its territory, and the regulation of a deterritorialized cyberspace, provides one explanation for the preference given by some states involved in cyberoperations to retaining silence and maintaining ambiguity in relation to their legal position. Since they are not certain that the Tallinn Rules adequately protect their long-term interests, they may be reluctant to formally endorse them or push strongly for their enforcement. And even those states that may be interested in relying on the Tallinn Rules may not be able to publicly do so, in the absence of credible and effective processes for assigning international responsibility, such as an international attribution mechanism. The upshot is that, at this point in time, states seem to prefer to engage in cyberoperations and counteroperations "below the radar," and to retain, for the time being, some degree of stability in cyberspace by developing "parallel tracks" of restricted attacks, covert retaliation, and overt retorsion, subject to certain notions of proportionality.

This does not mean, however, that no international law regulation of cyberoperations is possible or desirable. For example, there appears to be no reason to allow under international law unprovoked cyberattacks by states against other states, or cyberoperations that deliberately harm civilians not involved in armed activities or criminal enterprises, to the extent that states are able to control the effects of such attacks. Furthermore, one cannot assume that the current policy of silence and ambiguity will remain a dominant strategy in state practice. In fact, recent developments relating to the need of certain states to join forces and respond collectively to cyberoperations and to utilize public diplomacy in this regard may render the Tallinn Rules more relevant than before and could create a greater interest in the establishment of an international attribution agency to improve collective enforcement capabilities.

Ultimately, the approach taken by the Tallinn Manuals represents, like in other fields of international law, a policy choice, which may reflect fully justified professional anxieties of international lawyers about addressing a new field of interaction not contemplated by past lawmakers. The approach taken by the Tallinn Rules drafters has the advantage of avoiding a regulatory void. However, it does expose the Rules, and subsequent attempts to regulate the field on their basis, to academic criticism, due to the imperfect analogy between the regulation of kinetic and cybernetic operations, and puts them under pressure the more states deviate from them or refrain from accepting them because of gaps between the contents of the Rules and what they consider to be their national security interests.

https://doi.org/10.1017/ajil.2018.86 Published online by Cambridge University Press

Appendix: Table of Case Studies

No.	Victim-State & Period	Incident	Damage	Possible Breaches of International Law	Attribution	Response
1.	U.S. 2012–2013	Ababil/ DDoS operations	Enormous financial harm; potential harm to dam's operational system	• Use of force • Infringement of sovereignty • Due diligence	No official attribution	• Criminal investigation leading to indictments in 2016 • Alleged self-help (hack-back) by at least one of the targeted banks
2.	U.S. Feb. 2014	Sands Casino	Severe physical harm to computer infrastructure	• Use of force • Infringement of sovereignty • Non-intervention • Due diligence	No official attribution	• Criminal investigation • No information whether investigation is still pending
3.	U.S. Dec. 2014	The Sony-Hack – Destructive Cyber Operation (DCA)	Severe physical damage to the computer infrastructure and leaking of data including new movies	• Use of force • Infringement of sovereignty • Non-intervention • Due diligence	Official attribution	• Sanctions • Indictment • Possible covert action (temporal blocking of internet service in North Korea)
4.	U.S. March 2014–June 2015	OPM Hack	Severe harm to U.S. national security and to the privacy of millions of Americans	• Infringement of sovereignty • Non-intervention • Due diligence	No official attribution	American diplomatic pressure led to Chinese announcement of the arrest of two suspected hackers
5.	U.S. 2016	DNC Hack/ Interference in U.S. Elections	Exfiltration of data (emails); potential tampering with voting process; influence campaign	• Infringement of sovereignty • Non-intervention • Due diligence	Official attribution for meddling with the U.S. election process	Diplomatic measures such as expelling Russian diplomats, economic sanctions, and criminal indictments

Continued

No.	Nation-State & Date	Incident	Damage	Probable Breaches of International Law	Attribution	Response
6a	Saudi Arabia and Qatar Aug. 2012	Shamoon 1 + 2 – DCA against Aramco (Saudi Arabia) and RasGas (Qatar)	Severe physical harm to the companies' computer infrastructure	• Use of force • Infringement of sovereignty • Due diligence	No official attribution	• No response reported • Covert retaliating attacks might have been carried out
6b	Saudi-Arabia Nov. 2016; Jan. 2017	Shamoon 3 + 4 – DCA against governmental agencies and critical infrastructure facilities	Harm to computers; disruption of operations of a government agency	• Use of force • Infringement of sovereignty • Non-intervention • Due diligence	No explicit and official attribution by the victim state; in Feb. 18, the US ODNI attributed the attacks to Iran	• No response reported • Covert retaliating attacks might have been carried out
6c	Saudi-Arabia Aug. 2017	Triton operation – DCA against a Saudi petrochemical critical facility	Potential explosion averted	• Use of force/ armed attack • Infringement of sovereignty • Due diligence	No explicit and official attribution	• No response reported
7.	Iran July–Sept. 2016	Six cyberattacks against Iran's oil and petrochemical industry.	Fires in petrochemical plants and two explosions of gas pipelines causing one death and seven injuries	• Use of force/ armed attack • Breach of sovereignty • Nonintervention • Due diligence	No official attribution	• No response reported • Covert retaliating attacks might have been carried out
8.	Germany 2015	The Bundestag Hack	Exfiltration of huge quantities of data; need to temporarily shutdown internal network; possible attempt of an influence campaign	• Infringement of sovereignty • Non-intervention • Due diligence	Statement by one official that the operation was launched from Russian territory, and by another that it was launched by Russia	• Move to adopt long term organizational and legal measures designed to enhance capacities for an effective response

No.	Nation-State & Date	Incident	Damage	Probable Breaches of International Law	Attribution	Response
9a	Ukraine Dec. 2015	Black Energy-1 – a DCA against power distribution companies	Electric power outage lasted six hours affecting a large populated area	• Use of force • Infringement of sovereignty • Non-intervention • Due diligence	Senior Ukrainian officials pointed the finger at Russia	• No response reported
9b	Ukraine Dec. 2016	Black Energy-2 – a DCA against a power distribution station	Electric power outage in Kiev for an hour, reducing by 20% the city's electric consumption	• Use of force • Infringement of sovereignty • Non-intervention • Due diligence	Senior Ukrainian officials blamed Russia	• No response reported
10.	Ukraine/ Global June 2017	NotPetya	Harm to computers in more than 60 states, causing economic harm in the billions of dollars and serious disruptions in public services and transportation systems	• Use of force • Infringement of sovereignty • Non-intervention • Due diligence	Clear attribution made by U.S., UK, Australia, and Ukraine	• Augmentation of the U.S. sanctions against Russia
11.	Global May 2017	WannaCry Data encrypted; cannot be decrypted in almost 150 nations.	Harm to computers in almost 150 states, resulting in serious economic harm and disruption of important services such as healthcare and transportation	• Use of force • Infringement of sovereignty • Non-intervention • Due diligence	Clear attribution to North Korea made by 11 nations including the five eyes	• No response reported