WILL CYBER CONSEQUENCES DEEPEN DISAGREEMENT ON INTERNATIONAL LAW?

*Eneken Tikk**

ABSTRACT

Both the US and the European Union have declared a move towards unilateral and multilateral efforts to use international law to prevent, deter, and react to undesirable state behavior in cyberspace. Through this policy, States will draw new boundaries of acceptable and permissible behavior under existing international law that, ideally, will create further common understanding of the law. However, as State practice can be anticipated to advance interpretations that support their particular strategic interests and operational needs, this phase may also reveal differences on international law not just between the proponents of competing world orders but also between the generally like-minded states.

TABLE OF CONTENTS

I. INTRODUCTION 185
II. DIFFERING NATIONAL VIEWS ON INTERNATIONAL LAW 187
III. CYBER CONSEQUENCES WITHIN INTERNATIONAL LAW 189
A. *The Trend of Consequences* 189
B. *The Red Line Opportunities within Retorsion and Its Gaps* 192
C. *Will Consequences Lead to More Agreement and Understanding?* 194
IV. CONCLUSION 195

I. INTRODUCTION

The contestation known to arise from nuclear arms control, use of outer space, climate change, and many other past and recent issues relating to technological development is now retelling itself in the context of international cyber security. Differences over what cyberspace should be and how it should function are not limited to those between the leading cyber powers—the United States, Russia, and China. They have also become visible between the most and least technologically developed states, between agile technology adopters and technological laggards, and, most importantly for this paper, between like-minded states.

The inability of the fifth United Nations (U.N.) Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security to achieve a consensus report reveals how difficult it is to find common ground not only on the nuances of international law but also on its principles.[1] The international community should be aware that states continue

The genesis for the essays that comprise issue 32.2 of this Journal was a May 2017 workshop hosted at Temple University, and co-hosted with Leiden University. Under the theme "Influencing

making international law beyond the treaties they sign and ratify. As such, the out-of-step understanding on cyber affairs sends a clear signal that there is a significant gap between theory and practices of international law.

With the international dialogue on the applicability of international law in cyber affairs on a pause, states must resort to remedies at hand to respond to malicious and hostile activities mounted by the use of information and communications technologies (ICTs). State-on-state conflict is not the primary issue; even the U.N. GGE itself has framed this in hypotheticals.[2] However, as states are plagued by regular and blatant cyber incidents,[3] many of them would appreciate finding solid ground in international law to remedy the situation. Without satisfactory guidance and coordination, national conclusions about international law are likely to vary.

When reaching for international law, states favour rules that allow their preferred freedom of manoeuvre, while effectively constraining the problematic behaviour of others. Accordingly, while in their choice of remedies, states clarify international law in ways that have been impossible in international negotiations and political speech, they also likely reveal their different reading and understanding of it. States clarify international law by condemning certain behavior, or failure to act, as breaches of international law. Furthermore, their choice of responses, and how these are mounted, testify to what they believe are within the boundaries of the permissible under existing international law.

International Behavior in Cyberspace: Devising a Playbook of Consequences for Cyber Incidents," the workshop gathered a broad array of academic and governmental experts. Participants included representatives of the Estonian, Finnish, and U.S. governments (including officials from the Department of Defense, the State Department, and the U.S. Trade Representative). All government officials, however, participated in their personal capacity. As such, the views expressed in this special issue should not be attributed to any government or government agency.

* Lead of strategy and power studies at the Cyber Policy Institute (CPI) in Jyväskylä, Finland. Her work at CPI focuses on questions of strategic stability, cybersecurity governance, normative leadership and state behavior. Dr. Tikk also serves as senior adviser to the board of the ICT for Peace Foundation in Geneva, Switzerland advising governments, policy and decision makers on international peace and security issues in the context of ICTs. In 2018, she became the first female member of the board of the Estonian Defence League's Cyber Defence Unit. In her previous assignment, as Senior Fellow for Cyber Security at the International Institute for Strategic Studies (IISS), Eneken launched and coordinated a network of experts in support of the UK foreign cyber policy. She led the international law thread of the UK-China track 1.5 cyber security dialogue (2014–2017). At the invitation of the Estonian Ministry of Foreign Affairs (MFA), Eneken has been advising the Estonian expert in the U.N. First Committee Group of Governmental Experts on International Information Security (U.N. GGE) (2012–2013; 2014–2015; 2016–2017). Eneken was the first foreign national contractor at the MITRE Corporation (2012–2016), where her work focused on analyzing and advising national cyber security strategy processes and the U.S. cyber diplomacy.

1. For a detailed discussion of the U.N. GGE process and the 2016/2017 no-report outcome, *see* ENEKEN TIKK & MIKA KERTTUNEN, THE ALLEGED DEMISE OF THE UN GGE: AN AUTOPSY AND EULOGY (2017).

2. *See* LIISI ADAMSON, CENTER FOR INT'L GOVERNANCE INNOVATION, CUMULATIVE RECOMMENDATIONS IN THE UN GGE REPORTS (2010-2015) (2017).

3. *See, e.g.*, *Significant Cyber Incidents*, CTR. STRATEGIC & INT'L STUD., https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity (last visited Feb. 2, 2018).

II. DIFFERING NATIONAL VIEWS ON INTERNATIONAL LAW

That states have a different reading or understanding of international law in the context of international cyber security should not come as a surprise to anyone.[4] The Sino-Russo proposition for *lex specialis* on state development and use of ICTs is based upon the assertion that current international law does not contain adequate and sufficient remedies to violations of international information security. Even if we limit the discussion to international cyber security,[5] Moscow's and Beijing's basic proposition remains unaltered: existing international law does not offer a clear and convincing remedy. One may read it as a purely political stand, since, after all, it constitutes an attempt to curb the technological dominance of the United States. However, one must be mindful that the Sino-Russo reading of international law differs from that of Western schools.[6] The Sino-Russo reading follows a textualist approach, whereby all that is agreed is within the very text, and that nothing is agreed unless it is explicitly written down. This approach leads them to conclude that while the spirit of the U.N. Charter is the unquestionable basis covering international cyber security, the development and use of ICTs should be made subject to a specialized regime just like other technological advances in the past.

One does not have to limit the discussion to treaty-or-no-treaty to be able to detect significant differences in states' reading and implementation of international law. The status of the doctrine of countermeasures is contested in terms of whether it stems from an embrace of the International Law Commission (ILC) Draft Articles on Responsibility of States for Internationally Wrongful Acts.[7] For some states, the Draft Articles are fully reflective of customary international law, and therefore legally binding. Others refuse to regard this instrument as fully incorporating customary international law—choosing, rather, to rely on their own reading of customary international law.[8] The United States has persistently objected to the

4. Former State Department Legal Adviser Brian Egan notes that states will likely have divergent views on specific issues (of international law). This leads to the need for further discussion, clarification, and cooperation on issues of international law. Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 174 (2017); *see also* MATTHEW C. WAXMAN, CYBER STRATEGY AND POLICY: INTERNATIONAL LAW DIMENSIONS: TESTIMONY BEFORE THE SENATE ARMED SERVICES COMMITTEE (2017) (emphasizing that international law on international cyber security is not settled).

5. For the purposes of this paper, "international cyber security" refers to the Western reading of the discourse, wherein the question of information and content is left out of the scope of discussions.

6. *See* ANTHEA ROBERTS, IS INTERNATIONAL LAW INTERNATIONAL? (2017).

7. Int'l Law Comm'n, Draft Articles on Resp. of States for Internationally Wrongful Acts, Rep. On the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001).

8. *See* U.S. DEP'T OF STATE, OPINION LETTER ON DRAFT ARTICLES ON STATE RESPONSIBILITY: COMMENTS OF THE GOVERNMENT OF THE UNITED STATES OF AMERICA (Mar. 1, 2001) ("However, we believe that the particular provisions we have discussed continue to deviate from customary international law and state practice. To enhance prospects for broadest support of the Commission's work in this important area, we believe it critical that the Commission better align the provisions with customary international law in the areas discussed above."); *see also Statement by Mr. SHI Xiaobin of the Chinese Delegation at the 71st Session of the UN General Assembly on Responsibility of State for Internationally Wrongful Acts*, PERM. MISSION OF CHINA TO THE UN (Oct. 7, 2016), http://www.china-un.org/eng/gdxw/t1404593.htm (providing that

restrictions and requirements set out in ILC Draft Articles on taking countermeasures. In the view of the United States, the Draft Articles do not reflect customary international law or state practice, and potentially undermine efforts by states to peacefully settle disputes.[9]

Due diligence is another legal concept that invokes different national views on the binding nature and specific standards of international law. Some states do not believe there is sufficient support in state practice to conclude that due diligence is a binding concept of international law. Others derive the binding nature of the concept from the rulings of the International Court of Justice (ICJ). Some states, without taking an explicit stand on the binding nature of the concept itself, contest any particular standards of due diligence in the context of ICTs.[10]

In light of the Sino-Russo reading of sovereignty as the justification to stop almost anything that would impinge on their borders, Professor Waxman expressed doubt in testimony before the U.S. Senate Armed Services Committee on whether the United States could support the view that a breach of sovereignty would occur merely because some cyber activities take place within another state, or even have some effects on its cyber infrastructure.[11]

There are also the important potential lacunae projected in scholarly works on the subject. The Tallinn Manual[12], so far the most significant scholarly contribution to the discourse of international law and cyber operations, highlights potential areas of divergence and the limitations of law as it currently stands. Yet, some significant questions remain, including the categorization of data as an object, and whether it should be afforded protections like other civilian objects under the Law of Armed Conflict. Whereas the question of applicability of international humanitarian law (IHL) remains beyond the immediate context of countermeasures, this example highlights the basic issue at stake: if a norm of international law can be read in diametrically different ways, then states could also implement it in different directions.

An equally interesting discussion is unfolding around evidence as an element of attribution. Likely at the request of Russia, China, and developing countries, the 2015 U.N. GGE report underscored that accusations against a state must be substantiated.[13] On this issue, it appears that the United States has taken a textualist

although the Draft Articles seem mature, some clauses are still controversial—particularly "articles on 'serious breach by a State of an obligation arising under a peremptory norm of general international law,' the countermeasures, and 'measures taken by states other than an injured State,' [because] member states still have different understandings and various concerns, and consensus is not yet within reach.").

9. *See* Draft Articles on State Responsibility: Comments of the Government of the United States of America March 1, 2001, 2001 DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, ch. 7, §B(1) at 365; OFF. OF THE LEGAL ADVISER, U.S. DEP'T OF STATE, DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW 365 (Sally J. Cummins & David P. Stewart eds., 2001).

10. *See* Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace*, 125 YALE L.J. F. 68 (2015) (discussing due diligence in the context of cyber affairs).

11. WAXMAN, *supra* note 4.

12. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2nd ed. 2017).

13. U.N. Secretary-General, *Developments in the Field of Information and*

approach, as shown by former U.S. State Department Legal Adviser Brian Egan's assertion that "there is *no* international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action."[14]

Suffice it to say, neither states nor their advisers are in unanimous agreement about the content and scope of international law when it comes to uses of ICTs. Agreeing on the need to better respond to unlawful acts in cyberspace would constitute a clear step toward upholding international law. However, it remains to be seen whether state practice in identifying behavior that, in their view, does not correspond to international law, and reacting in ways that, in their view, does correspond to international law, will build more consensus on the matter or divide the international community even more.

III. CYBER CONSEQUENCES WITHIN INTERNATIONAL LAW

A. The Trend of Consequences

Evidence of a political push for a 'policy of consequences' can be found in both U.S. and European cyber policy. Both powers have made efforts to develop a political response framework for preventing and reacting to disruptive or destructive cyber incidents.[15]

Rhetoric from the White House and the U.S. Department of Defense has been clear on their intent to make use of international law to whatever extent possible.[16] On another contested issue involving the South China Sea, President Obama reiterated in early 2016 that "the United States will continue to fly, sail, and operate wherever international law allows, and we will support the right of all countries to do the same."[17]

Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015); *see* Adam Segal, *The 2015 GGE Report: Breaking New Ground, Ever So Slowly*, COUNCIL ON FOREIGN REL. (Sept. 8, 2015), https://www.cfr.org/blog/2015-gge-report-breaking-new-ground-ever-so-slowly (stating that "the text was inserted at the last minute at Russia's request, and it's unclear why," although "China, not Russia, is generally the most vocal about the need for evidence when publicly attributing malicious cyber activity.").

14. Egan, *supra* note 4, at 177 (emphasis original).

15. While the United States has not issued a written policy of consequences, the theme has been discussed by leading State Department officials. The U.S. administration is also working on an updated approach to deterrence, which is likely to include a cyber component.

16. *See, e.g.*, Alex Spillius, *US Could Respond to Cyber-Attack with Conventional Weapons*, TELEGRAPH (June 1, 2011), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/8550642/US-could-respond-to-cyber-attack-with-conventional-weapons.html (providing statement by White House on May 16, 2011: "We reserve the right to use all necessary means—diplomatic, informational, military, and economic—as appropriate and consistent with applicable international law, in order to defend our nation, our allies, our partners and our interests.").

17. OFF. OF THE PRESS SEC'Y, *Remarks at U.S.-ASEAN Press*, THE WHITE HOUSE (Feb. 16, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/16/remarks-president-obama-us-asean-press-conference (remarking on the need to lower tensions in the South China Sea, including ceasing, reclamation, construction, and militarization of disputed areas, in addition to ensuring continued freedom of nagivation and trade) (last visited Feb. 19, 2018).

Within the European Union, discussion of a joint response to cyber operations is ongoing. The draft Cyber Diplomacy Toolbox[18] is yet to be approved by the European Council, but it has received considerable support from member states in the process.[19] Viewed through the European Union lens, a policy of remedies is seen as an avenue of conflict prevention, a tool of mitigating cybersecurity threats, and a motor of greater stability in international relations.[20] In their approach, the E.U. emphasizes that malicious cyber activities might constitute wrongful acts under international law.[21] The policy is intended to uphold international law in cyberspace and emphasizes the E.U.'s commitment to the settlement of international disputes by peaceful means.[22]

Outlining potential and suitable measures, the E.U. emphasizes that any actions under the Toolbox "should encourage cooperation, facilitate mitigation of immediate and long-term threats, and influence the behavior of potential aggressors in a long term."[23] Underlying E.U. diplomatic action will be a respect for applicable international law and adherence to fundamental rights and freedoms.[24]

International law has a role in both U.S. and European thinking about remediation. So far, references to international law have been used primarily as highlights and margins of possible or preferred courses of action. However, a more systematic approach to consequences is likely to add substantively to the U.S. and E.U. understanding and interpretation of international law.

From a scholarly point of view, added clarity in this regard would be a welcome contribution. It is not common for states to publicly articulate their views on how international law applies to specific circumstances and situations. This does not, however, mean that states are agnostic to the issue. The question of international law is a high priority in national cyber security strategies, and is regarded as a strategic element in international cyber policy. As several commentators note, silence on international law is not the best strategy when it comes to cyber operations.[25]

18. *Id.*

19. *See* Patryk Pawlak, *A Wild Wild Web? Law, Norms, Crime and Politics in Cyberspace*, EU INST. SECURITY STUD. (July 2017), https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2023%20Cyber%20norms.pdf (providing that the Council Conclusions on Cyber Diplomacy to develop a Cyber Diplomacy Toolbox were endorsed by the EU Ministers of Foreign Affairs).

20. *Id.*

21. *Id.* at 4.

22. *Id.* at 1.

23. Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") (EC) No. 9916/17 of 7 June 2017, art. 5, 2017.

24. Erica Moret & Patryk Pawlak, *The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?*, 24 EUR. UNION INST. FOR SECURITY STUD. 2 (July 2017).

25. *See* Egan, *supra* note 4; Justin Dolly, *The Cyber Cold War: The Silent, but Persistent Threat to Nation States*, ITPROPORTAL (Apr. 19, 2017), https://www.itproportal.com/features/the-cyber-cold-war-the-silent-but-persistent-threat-to-nation-states/ ("Any effective cyber strategy will require like-minded countries to cooperate and abide by an internationally agreed legal framework. Failing to pool knowledge, resources and capabilities could bring a dystopian future closer in a world where the main aim of hackers and their taskmasters is to cause chaos and disruption.").

Specific cyber incidents provide states with opportunities to express their views and take a firm stand on how existing international law applies to state conduct in cyberspace.[26] States' "relative silence" on the account of international law has contributed "to unpredictability in the cyber realm, where states may be left guessing about each other's views on the applicable legal framework."[27]

However, the application of consequences may have a few political side effects. Waxman stresses the application of international law to cyber activities will "affect how the United States [or any state in question] may defend itself against cyber-attacks and what kinds of cyber-actions the United States [or a state in question] may itself take."[28] Waxman states that international law can be construed as a deterrent that inhibits undesirable action.[29] Seen from this perspective, consequences will be telling of national ambitions and capabilities, or at least perceived to be.

Furthermore, implementation of consequences would contribute to the analysis of state practice in the formation of norms and customary international law. After all, international law does not just apply itself; it *is applied*, by states, and state silence has come to sound too loud amidst obvious international cyber security issues.

Consequence implementation is an area of international cyber policy that would offer opportunities for states to establish themselves as leaders of certain interpretations and views on international law. Waxman recommends that the United States advance "interpretations that support its strategic interests, including its own operational needs."[30] This call for decisive national and international leadership is in line with the observation made earlier by another former U.S. State Department Legal Adviser, Harold Koh: "If we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we *do* take will earn enhanced legitimacy worldwide for their adherence to the rule of law."[31]

Furthermore, state practice is also likely to draw clearer lines between national and international emphasis of consequences. For instance, the U.S. cyber sanctions program goes beyond issues of international law.[32] The United States views certain prevalent and severe cyber-enabled activities as an unusual and extraordinary threat to national security, thus calling for a national emergency response.[33] As a result, the White House has authorized the imposition of sanctions against persons

26. Egan, *supra* note 4.

27. *Id.*

28. *Cyber Strategy & Policy: International Law Dimensions: Testimony Before the S. Armed Services Comm.*, 1 (Mar. 2, 2017) (statement of Mathew C. Waxman, Professor of Law, Columbia Law School).

29. *Id.*

30. *Id.*; *see also* 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, 434 (2011).

31. Harold H. Koh, *International Law in Cyberspace*, 54 HARV. INT'L L.J. 1, 11 (2012) (emphasis original).

32. Exec. Order No. 13694, 80 Fed. Reg. 60 (Apr. 1, 2015).

33. *Id.*

responsible for or complicit in, or to have engaged in, certain malicious cyber-enabled activities.[34]

Any consequences, either under national or international law, are essentially unilateral. While they might convene additional same-minded coalitions around issues of shared priority, they will also highlight the need for a wide margin of interpretation that individual states choose to apply to issues of cyber security.

B. The Red Line Opportunities within Retorsion and Its Gaps

A potentially dividing and unifying line is that of retorsion. Retorsion denotes a boundary between international law and no international law.[35] It is defined as unfriendly conduct, by the retaliating state, that is not otherwise inconsistent with any of its international obligations.[36] Therefore, acts that would breach a responding state's universal, multilateral or bilateral treaty arrangements or other sources of international law cannot, by definition, constitute retorsion.[37] Where states are not able to agree whether something is allowed or prohibited under existing international law, the domain of mere retorsion—or unfriendly nature of the affairs—will extend. Egan stresses that "a State can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other States."[38]

In *State Responsibility: The General Part*, Crawford notes that retorsion constitutes the "most common unilateral self-help measure in international practice."[39] This underscores the seamless functioning of international law—the minding by states, in their routine affairs, of their own acts and the acts of others. Crawford's observation manifests the lucrative nature of retorsion. Unlike countermeasures and self-defense—both of which have been discussed extensively in the context of ICTs—retorsion as a concept does not have any specific pre-conditions. It can be employed regardless of whether the targeted state's unwanted behavior violated international law or not.[40] In other words, states may employ retorsion in response to any unwelcomed or unfriendly act by the target state.[41] States can do so to achieve punitive or retributive ends, and they are not bound under retorsion to the sorts of temporal conditions or requirements of reversibility that limit the use of counter-measures.[42]

The lack of extensive pre-conditions for employing retorsion makes it an

34. *Id.* at 1(a)(i).

35. JAMES CRAWFORD, STATE RESPONSIBILITY: THE GENERAL PART, 676 (James Crawford & John S. Bell eds., 2013) (discussing states' rights to act freely when there is no clear international law prohibition).

36. *Id.*

37. *Id.* For example, if a state has a bilateral investment treaty that requires the provision of compensation at a specific level, it cannot expropriate another state's or its nationals' property as a retorsion without compensation.

38. Egan, *supra* note 4, at 177.

39. CRAWFORD, *supra* note 35, at 676.

40. *Id.* at 677.

41. *Id.*

42. *Id.*

attractive tool for states, even in cases where they might be legally entitled to use counter-measures.[43] Controversy can occur, however, as the targeted state or third parties may not share the responding state's view that its self-help measures are themselves lawful. For example, the United States has claimed to "exercise unilateral restraint[—which can be understood as a form of retorsion—]in the export of arms in cases where such restraint will be effective or is necessitated by overriding national interests. Such restraint will be considered on a case-by-case basis" under certain conditions, and on the assumption that there is no legal obligation to sell arms in the first place.[44] The United States has also stressed that "any actions by a state that are not otherwise prohibited under international law . . . would not, by definition, constitute counter measures."[45]

It is understandable that the whole concept of counter-measures has not received affirmative support from technologically less developed countries, nor from Russia and China, who strongly oppose unilateral action, and find themselves in an underdog position in the current technological race.

Accordingly, the discourse and exercise of retorsion will often involve a discussion of the decision-making processes, limits, and substance of existing international law. For an example translated into the cyber-context, states wishing to use self-help that reduces access to ICT infrastructure might assume that there is no international legal obligation to afford other states (including the targeted state) such access, a position that the targeted state (among others) might dispute.[46] Over time, however, state practice will accumulate. Coordinated and consistent exercises of retorsion (and reactions thereto) are susceptible to the creation of state practice of legal relevance that can help us understand and accept how international law is to be understood and exercised.

C. Will Consequences Lead to More Agreement and Understanding?

It is likely that the U.S. and European views on the triggers, as well as the appropriate remedies, will differ. The United States has a strong interest in limiting infiltrations, exploitation, and manipulation of their digital systems. While some states in Europe share those concerns, many E.U. countries have not experienced

43. *Id.* at 677–78.

44. Such conditions include: "transfers involving states whose behavior is a cause for serious concern, where the United States has a substantial lead in weapon technology, where the United States restricts exports to preserve its military edge or regional stability, where the United States has no fielded countermeasures, or where the transfer of weapons raises concerns about undermining international peace and security, serious violations of human rights law, including serious acts of gender-based violence and serious acts of violence against women and children, serious violations of international humanitarian law, terrorism, transnational organized crime, or indiscriminate use." U.S. Dep't. of State, Digest of United States Practice in International Law, 2014, at 748–49, https://www.state.gov/documents/organization/244504.pdf.

45. U.S. Dep't. of State, Digest of United States Practice in International Law, 2001, at 365, https://www.state.gov/documents/organization/139600.pdf.

46. *See* Michael Schmitt, *US Transparency Regarding International Law in Cyberspace*, JUST SECURITY (Nov. 15, 2016), https://www.justsecurity.org/34465/transparency-international-law-cyberspace/, for an example in which a denial of access to infrastructure based on a state's territory is considered unfriendly, but lawful, conduct.

large-scale or serious cyber-attacks or hostile attempts. Without coordination, individual states might contour further differences, among the otherwise like-minded states, about international law and its implementation.

A crucial question is whether differences on international law between the like-minded states are a matter of mere reading and understanding, or of principle. In the first case, differences in implementation might follow an initial or occasional interest, pertaining to a temporary state of affairs that had compelled the state to interpret the norms and the underlying situation in a certain way. Such action by states could be corrected as further practice emerges and as views are coordinated on the matter. Such corrections would be closely tied to the perception and occurrence of violations, as these would trigger relevant reactions and merit an exchange of views among states.

In the second case of differing principles, we are dealing with a recurring, and more fundamental, rejection of a view, accepted or allowed by others. As discussed above, states have rejected among others the binding nature of Draft Articles and the concept of due diligence. By doing so, they systematically dismiss the binding nature of a norm that other states acknowledge as legally binding. In such an occasion, a violation is not a necessary attribute of differences—it becomes about persistent objection to particular interpretation and implementation of a norm.

Where these two attributes—both highly disruptive to the uniform understanding and implementation of international law—coincide, the issue might become a chief concern. Frequent and notable violations of a norm that other states consider established, might lead to calls for renewed, or de novo, international law. Ultimately, they might merge into the currently rejected proposition, introduced (and tabled) by Russia and China: that there is need for a special legal regime to determine the boundaries of the permissible in cyberspace.

IV. CONCLUSION

When thinking of remediation of the many issues that the development and use of ICTs have brought about, it is essential to remember that there is not one "policy of consequences." Each state and organization will have their own views on what constitutes a threat to national security, a breach of international law, or a threat to international peace, security, and stability—and what should be done. This tendency, by default, will produce different readings of international law. Also, the parallel lexicons will likely not match in their usage and definitions of 'sanctions,' 'countermeasures,' 'restrictive measures,' and 'diplomatic response.' To an extent, these notions will be overlapping. At the same time, and much more importantly, they will be nuanced in ways that testify to the potential developments in international law as it is hoped to apply to both state and non-state actor uses of ICTs. At best, the emerging state practice can promote practical cooperation and help to find normative consensus; at worst, the emerging practices will drive a wedge between the states and widen the gap between the interpretations of international law.