International cyber norms: reflections on the path ahead

Ministerie van Defensie

International Cyber Norms: Reflections on the Path Ahead

Versie 1

Documentgegevens

Originele versie:
Citeertitel: International Cyber Norms: Reflections on the Path Ahead
Permalink: http://puc.overheid.nl/doc/PUC_248171_11

Soort document:
Type: Publicaties - Beschouwing
Bron: Ministerie van Defensie

Versie en datums:
Versie: 1
Laatste wijziging: 17-08-2018

Publicatiegegevens:
Uitgever: Ministerie van Defensie
Kanaal: MRT
Vorm: origineel PUC document
Referentienummer: PUC_248171_11
Toegankelijkheid: Intern
Publicatiedatum: 17-08-2018
Taal: en

Verrijking gepubliceerd bij document:
Thema's:
- Jaargang 2018
- Beschouwing

Inhoudsopgave

[geen titel]

Prof. Dr. Michael N. Schmitt[1]

Recent events have proven rather discouraging with respect to the recognition and further development of a normative architecture to govern operations in cyberspace. Of particular note is the failure of the 2016 – 2017 UN Group of Governmental Experts (GGE) to agree on text regarding cyber norms for inclusion in the report it had expected to issue.[2] Opposition from a number of states, most notably China and Russia, to any explicit mention of either the law of self-defense or international humanitarian law, as well as a degree of resistance to text that would implicate the right of states to take countermeasures (discussed below) pursuant to the law of state responsibility, prevented issuance of a consensus report by the group of 25 states.[3] This was particularly disheartening because the 2013 and 2015 UN GGE reports had made significant progress with respect to articulating both binding and hortatory norms applicable in cyberspace.[4]

Other efforts to identify cyber norms are underway, such as those of the Global Commission on the Stability of Cyberspace, which recently proposed adoption of a non-binding norm providing 'State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites'.[5] The private sector has also been active in the field. Perhaps most significant in this regard are Microsoft's proposed Digital Geneva Convention[6] and the Cybersecurity Tech Accord.[7] There are also growing rumors about the prospect of a future GGE to take up where the previous five iterations left off.

In my view, however, the greatest prospect for progress in the near term lies in states making clear their positions with respect to when and how specific international law principles and norms apply in cyberspace. Involvement of non-state actors, such as the private sector, nongovernmental organizations and academia, is appropriate in light of the multi-stakeholder approach to norms that of necessity must be taken due to the shared nature of cyberspace. Nevertheless, it remains the case that states, and only states, have the formal authority to craft new international legal regimes and authoritatively interpret international law's existing principles and rules. They do so through the adoption of treaties or by engaging in practices that when combined with expressions of *opinio juris* (expressions by states that the practice in which

---

1 Professor of International Law, University of Exeter; Charles H. Stockton Professor, United States Naval War College; Francis Lieber Distinguished Scholar, United States Military Academy at West Point; Director of Legal Affairs, Cyber Law International. The views expressed are those of the author in his personal capacity.

2 See discussion in Michael. N. Schmitt and Liis Vihul, *International Cyber Law Politicized,* Just Security (June 30, 2017), https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/.

3 Articles on State Responsibility, arts. 22, 49-53, International Law Commission, Report on the Work of its Fifty-Third Session, U.N. Doc. A/56/10, at 43 (2001), *reprinted in* [2001] 2 Yearbook of the International Law Commission 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2); Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Rules 20-25 (Michael Schmitt, gen. ed. Cambridge UP, 2017).

4 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174 (July 22, 2015) [hereinafter GGE 2015 Report]; Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/68/98 (June 24, 2013).

5 Global Commission on the Stability of Cyberspace *Call to Protect the Electoral Infrastructure,* May 2018, https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.

6 Microsoft, *A Digital Convention to Protect Cyberspace*, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.

7 Cybersecurity Tech Accord, https://cybertechaccord.org/accord/. *See also* David E. Sanger, *Tech Firms Sign 'Digital Geneva Accord' Not to Aid Governments in Cyberwar,* New York Times, April 17, 2018, https://www.nytimes.com/2018/04/17/us/politics/tech-companies-cybersecurity-accord.html.

they are engaged, or that they refrain from, is required by law) results in the crystallization of customary international law.[8]

I am relatively pessimistic about the likelihood of a multilateral cyber treaty that is general in scope, for, as demonstrated by the unsuccessful attempt to articulate norms during the 2016-2017 GGE, key cyberspace players appear to remain at some distance from each other vis-à-vis the role that international law should play in cyberspace. I am also doubtful about the possibility of new customary international law crystallizing in the near future. The almost mystical process of crystallization is both intricate and vague. Complicating matters in that regard are the secrecy that surrounds cyber activities and the practical difficulties of attribution to states of observed cyber activities. In other words, state practice is highly difficult to identify with the requisite clarity and objectivity.

This being so, the best hope for international law governance in cyberspace lies in state interpretation of extant norms. While the Convention on the Law of Treaties sets forth rules for treaty interpretation,[9] and mechanisms exist regarding the identification and understanding of customary international law,[10] the reality is that in this relatively new sphere of activity, what states actually say about how they understand treaty and customary international law is what will matter, especially given the paucity of visible state cyber practice. Over time, a critical mass of complementary state views on a particular cyber legal issue will accumulate and that interpretation may become binding law. There is no mathematical precision as to when this point is reached. Yet, states that fail to participate in the process must understand that they are surrendering the interpretive battlespace to those states willing to set forth their views or, indeed, even to non-state actors who deftly move in to fill a void ignored by states.[11]

Unfortunately, the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* is sometimes viewed as filling the interpretive void that has heretofore been unaddressed by states.[12] Speaking as director of the project, I can confirm that this was never the intention of the participants who made up the two International Groups of Experts (IGE) that prepared the Manual. On the contrary the IGEs assiduously sought to set forth all reasonable views with respect to the application and interpretation of international law to cyber operations so as to empower states to better understand the interpretive options available to them. In other words, the *Tallinn Manual 2.0* was always meant to be a tool for states in their own interpretive journey, rather than a document with any prescriptive effect, formal or informal.

The time is ripe for states to begin to set forth their positions with respect to the myriad issues of international law that arise in the cyber context. Presentations by the Netherlands' Ministers of Foreign Affairs and Defence made at the first anniversary celebration of *Tallinn Manual 2.0*'s publication, which are reprinted in this volume, are illustrative early steps in this process.[13] So too are, for example, important

8 Statute of the International Court of Justice, art. 38(1), June 26, 1945, 59 Stat. 1055, 33 U.N.T.S. 993.

9 Vienna Convention on the Law of Treaties, arts. 31-32, May 23, 1969, 1155 U.N.T.S. 331.

10 Stefan Talmon, *Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion,* 26 European Journal of International Law 417 (2015).

11 *See, e.g.,* Michael N. Schmitt and Sean Watts, *The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare,* 50 Texas International Law Journal 189 (2015).

12 Tallinn Manual 2.0, *supra* note 3.

13 Speech by [Netherlands] Minister Blok on First Anniversary of Tallinn Manual 2.0, June 20, 2018, https://www.government.nl/documents/speeches/2018/06/20/speech-by-minister-blok-on-first-anniversary-tallinn-manual-2.0; Keynote address by the Minister of Defence, Ms. Ank Bijleveld, marking the first anniversary of the Tallinn Manual 2.0, June 20, 2018, https://english.defensie.nl/downloads/speeches/2018/06/21/keynote-address-by-the-minister-of-defence-ms.-ank-bijleveld-marking-the-first-anniversary-of-the-tallinn-manual-2.0-on-the-20th-of-june-2018. See *also* Bert Koenders, Foreign Minister, Netherlands, Remarks at The Hague Regarding Tallinn Manual 2.0 (Feb. 13, 2017) (on file with author); Advisory

speeches by U.S. Department of State Legal Advisors,[14] submissions by states to international fora,[15] and the very recent address by the Attorney General of the United Kingdom at Chatham House.[16] Yet, in most cases such laudatory efforts, while substantively significant, fail to identify cyber norms with the granularity that is necessary to directly affect specific ongoing operations.

Accordingly, states need to redouble their efforts to shape the normative cyber architecture that will govern activities in cyberspace. Two tacks hold promise. First, they may do so by clearly articulating broad premises of law with which most states can agree, thereby allowing concentration on the narrower nuances of those positions. Second, there are certain areas of international cyber law where states need to immediately set forth their legal position in order to hold the line against assertions regarding international cyber law that are potentially destabilizing.

With respect to the former, states should confirm, and encourage other states to follow suit, the full applicability to cyber operations of the *jus ad bellum*, that is, the law governing the resort to force by states as an instrument of their national policy. Key to this legal regime are the customary law prohibition on the use of force codified in Article 2(4) of the UN Charter and the right of self-defense set forth in Article 51 of the Charter, which also reflects customary law.[17] There appears to be relatively broad agreement that any cyber operation that is physically destructive or injurious is a use of force. There also appears to be, despite politically motivated opposition in the GGE by certain states, broad consensus that when the destruction or injuries are significant, the victim state enjoys the right of self-defense by both cyber and kinetic means against the state that launched the cyber 'armed attack'.

Statements to this effect are useful in cementing these norms in place but could go further. In particular, states could publicly announce that cyber operations need be neither physically destructive nor injurious in order to trip over the 'use of force' or 'armed attack' thresholds respectively. Rather, they could announce their intention to assess harmful cyber operations against these thresholds based on the *severity* of the consequences that have manifested (or are expected to eventuate). An example is the Dutch Minister of Defence's statement in her Tallinn Manual 2.0 anniversary presentation that a cyber-attack targets the entire Dutch financial system ... or ... prevents the government from carrying out essential tasks such as policing or taxation ... would qualify as an armed attack." Although such statements may lack legal precision in terms of articulating clear-cut criteria, a broad severity of consequences-based approach would serve a deterrent purpose by placing other states (and in the case of self-defense, non-state actors) on notice that, if severe, such a cyber operation would risk not only condemnation as an internationally wrongful act, but also, in certain cases, a robust response pursuant to the law of self-defense. The approach also reflects reality. After all, few states facing, or observing, a nationally disruptive cyber operation having widespread deleterious effects would hesitate to label it a violation of the prohibition on the use of force or believe themselves constrained by international law from responding forcefully pursuant to the right of self-defense.

Council on International Affairs and the Advisory Commission on Issues of Public International Law, *Cyber Warfare*, No. 77 AIV/ No. 22, CAVV, (2011).

14 Harold Hongju Koh, Legal Adviser, U.S. State Department, Remarks at the U.S. Cyber Command Inter-Agency Legal Conference, Sept. 18, 2012, reprinted in 54 Harvard International Law Journal Online 1 (2012); Brian J. Egan, Legal Adviser, U.S. Department of State, Remarks at Berkeley Law School on International Law and Stability in Cyberspace, Nov. 10, 2016, https://perma.cc/B6TH-232L. On the Koh speech and the Tallinn Manual, see Michael N. Schmitt, *International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed*, 54 Harvard International Law Journal Online 13 (2012).

15 *Applicability of International Law to Conflicts in Cyberspace*, 2014 Digest of United States Practice in International Law, ch. 18, § A(3)(b), at 737.

16 Jeremy Wright, U.K. Attorney General, Cyber and International Law in the 21st Century, Speech at Chatham House, May 23, 2018, 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

17 UN Charter, arts. 2(4) and 51. On their customary nature, see Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S), Judgment, 1986 I.C.J. Rep. 14, paras. 176, 188-190 (June 27).

Articulation of such a position would beg many questions, the most important of which is *where* to draw the lines and *which* criteria to apply when doing so. However, the position has the benefit of focusing the attention and effort of states where it belongs – on drawing those lines and identifying the appropriate criteria for qualifying a cyber operation that is neither destructive nor injurious as a use of force and, in acute cases, an armed attack. Moving the discussion in this direction would have the further benefit of sidelining the unsupportable objection of a few states to overt references to the right of self-defense in cyberspace; as states begin to refine the thresholds, any assertion that no such line exists would soon be seen as puerile by the remainder of the international community.

States also should affirm the full applicability of the *jus in bello* (international humanitarian law) to cyber operations that take place during an armed conflict, whether international or non-international in character. Like the applicability of the *jus ad bellum*, no convincing argument supports the non-applicability of IHL to these operations. As noted, politically motivated opposition to reference to 'international humanitarian law' arose during the 2016 – 2017 GGE, but such opposition was without logical or normative foundation. Therefore, the advancement of international cyber norms would be fostered significantly by widespread public embrace of the position. Such declarations would contribute measurably to those already made by states such as the Netherlands, United States, and United Kingdom, as well as NATO and the European Union.[18] They would also help clarify the veiled reference to IHL implied by the reference to the principles of humanity, necessity, proportionality and distinction found in the 2015 UN GGE report.[19]

States could venture even further in adding granularity to this broad, and in my view self-evident, assertion. In particular, there is no reason that they should refrain from specifically acknowledging that the conduct of hostility rules appearing in the 1977 Additional Protocol I to the 1949 Geneva Conventions, most of which reflect customary IHL, apply to cyber operations during armed conflict. [20] Of particular note in this respect are the rules prohibiting attacks against civilian objects, which would include civilian cyber infrastructure, the rule of proportionality and the requirement to take precautions and attack. [21] The effect of such rules is very significant in the cyber context. For example, a commander considering an attack against a valid military objective must, pursuant to the requirement to take precautions in attack, consider whether directing cyber operations rather than kinetic attack against the target would avoid civilian collateral damage without sacrificing the military advantage that the operation is intended to achieve. [22]

There are unsettled issues with respect to IHL's application to cyber operations that merit further development. It is there that states should focus their attention. Three merit particular attention. The first is the meaning of the term 'attack' in the cyber context. Article 49 of Additional Protocol I defines an attack as 'an act of violence against the adversary, whether in offense or in defence'. This treaty provision, which is generally understood to reflect customary international law, confirms that a physically destructive or injurious cyber operation qualifies as an attack to which the prohibition on attacking civilian objects and other conduct of hostilities rules apply. It is important to note that despite the 'against the adversary text', it is well-accepted that violent cyber operations directed at civilians or civilian objects are attacks, as are

18 *See respectively, e.g.*, Bijleveld Address, *supra* note 13; Applicability of International Law, *supra* note 5; Wright Speech, *supra* note 6; NATO, Warsaw Summit Communique, para. 70, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm; European Commission, Cybersecurity Strategy of the European Union, Feb. 7, 2013, https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf.

19 UN GGE 2015 Report, supra note 4, para. 28(d).

20 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, Part IV, Section I, June 8, 1977, 1125 U.N.T.S. 3.

21 *Id*., arts. 48, 52 and 57.

22 *Id*., art. 57(2)(a)(ii).

cyber operations that, while not causing these effects with respect to the targeted system, nevertheless have indirect (collateral) consequences at that level.[23]

The unsettled issue is whether these rules apply to cyber operations *not* having physical effects or causing injury, such as those that interfere with the functionality of cyber infrastructure. It is my position that the rules governing attacks apply to many such operations,[24] although the precise threshold at which the resulting consequences qualify an operation as an attack is a matter that demands the attention of states. For instance, does a temporary loss of functionality do so? If the loss of functionality can be remedied through reloading either the operating system or data upon which functioning of the system relies, is the operation an attack? If this system continues to operate but does not do so in the intended manner, has the requisite loss of functionality occurred? These are important queries because a cyber operation that does reach the attack threshold arguably may be conducted against civilian cyber infrastructure, as is the case with many cyber psychological operations. States need to develop their positions on such matters lest their armed forces be left without guidance when crafting rules of engagement and other guidance.

A related issue deals with the rule of proportionality, which prohibits an attack that is expected to cause collateral damage to civilian objects or incidental injury to civilians that is excessive in relation to the military advantage anticipated to be achieved as a result of the attack. The rule, which is found in both Articles 51 and 57 of Additional Protocol I, specifically refers to 'damage'. The question is when does an effect on civilian cyber infrastructure that is *not* physically damaging nevertheless qualify as damage for the purpose of the rule? Again, I am of the view that a loss of functionality may amount to damage that must be factored into the proportionality calculation. In my estimation, states should be focusing their attention on determining *when* it does so.

Finally, a long-standing debate surrounds the treatment of data. The issue is whether data is an '*object*' such that the prohibition on targeting civilian objects[25] applies to cyber operations that delete or alter civilian data. Relatedly, it is unsettled whether deletion or alteration of civilian data qualifies as collateral damage to civilian objects for the purposes of the rule of proportionality. There is widespread consensus that if the consequence of the loss of, or change to, the data is physical in nature, as in the case of cyber infrastructure that suffers physical damage when its data is altered, the prohibition applies. An example would be manipulation of data upon which the cooling system for cyber infrastructure relies, thereby causing the system to overheat in a manner that damages the infrastructure.

The legal challenge surrounds cyber operations directed at data that do *not* have a physical effect, such as those targeting civilian financial systems. There are some experts who assert that data should be treated as an object.[26] In their view, broadly speaking, cyber operations against civilian data are unlawful attacks on civilian objects. Additionally, for them, any direct or indirect effect on civilian data that results collaterally during an operation directed against a lawful cyber target must be considered in the proportionality analysis and is subject to the requirement to seek to minimize civilian collateral damage (precautions in attack). This approach has the benefit of shielding the civilian population from the potential negative effects of cyber operations but is over inclusive in that it would include some cyber operations that states regularly engage in, like psychological operations.

---

23 Tallinn Manual 2.0, *supra* note 3, at 416, 418.

24 Michael N. Schmitt, *Rewired Warfare: Rethinking the Law of Cyber Attack,* 96 International Review of the Red Cross 189-206 (2014).

25 Additional Protocol I, *supra* note 20, art. 52(1).

26 Heather A. Harrison Dinniss, *The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives*, 48 Israel Law Review 39 (2015); Kubo Macak, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 Israel Law Review 55 (2015). *But see* Michael N. Schmitt, *The Notion of 'Objects' during Cyber Operations: A Riposte in Defence of Interpretive Precision*, 48 Israel Law Review 81 (2015).

Opponents of the approach note that data is intangible and therefore does not logically qualify as an object. This view seems to be consistent with the general approach in international law that terms should be interpreted in accordance with their ordinary meaning.[27] Yet, if data is not an object, the door is wide open for cyber operations directed against civilian data; indeed, it would be lawful to conduct cyber operations that are extraordinarily disruptive to civilian life.

There is no easy answer to either the question of where the threshold of attack lies or that of how data should be treated as a matter of law. In a forthcoming article in the *International Review of the Red Cross*, I suggest that states make two policy commitments to address the situation.[28] The first is that they accord special protection to certain 'essential civilian functions or services' by committing to refrain from conducting cyber operations against civilian infrastructure or data when doing so would interfere with those functions or services. The second proposal is states should commit to refraining from conducting cyber operations to which the IHL rules governing attacks do *not* apply (because, for instance, the operation is not at the attack level or data is not considered an object) when the expected concrete negative effects on individual civilians or the civilian population of the operation would be *excessive* relative to the concrete benefit related to the conflict that is anticipated to be gained through the operation. However, the adoption of policies does not resolve definitively the legal issues at hand. Therefore, states should begin to fashion their own stance on these issues and collaborate with other states in developing consensus positions, particularly within alliances like NATO.

As noted above, states also need to set forth their legal positions with respect to certain cyber issues that may prove destabilizing in the absence of rules governing them. Most significant among these is the question of sovereignty. Recently, assertions have been made that sovereignty is a *principle* of law that undergirds rules such as the prohibitions on intervention and the use of force, but not a *rule* that is separately binding of its own accord.[29] By this interpretation, which appears to have been embraced by the United Kingdom,[30] cyber operations are never rendered unlawful on the basis that they have violated the sovereignty of the target state.

This position makes operational sense if the objective is to avoid normative obstacles to offensive operations against other states. Yet, it must be cautioned that, pursuant to the principle of sovereign equality,[31] the approach would apply equally to all states. As a result, a state that adopts the position cannot subsequently claim that other states have violated its sovereignty when it is victimized by hostile cyber operations conducted by, or attributable to, another state. For instance, the United Kingdom has now deprived itself of that argument when other states, like Russia, remotely conduct cyber operations into British territory.

Additionally, a state adopting this view cannot resort to cyber or non-cyber 'countermeasures' pursuant to the law of state responsibility by making the assertion that its sovereignty has been violated. A countermeasure in the cyber context is an operation that would violate international law but for the fact that it is designed to put an end to an unlawful cyber operation directed against the state taking the

27 Vienna Convention on the Law of Treaties, *supra* note 9, art. 31(1).

28 Michael N. Schmitt, *Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations,* International Review of the Red Cross (forthcoming 2018).

29 Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 American Journal of International Law Unbound 207 (2017). *But see* Michael N. Schmitt and Liis Vihl, *Respect for Sovereignty in Cyberspace*, 95 Texas Law Review 1639 (2017); Michael N. Schmitt and Liis Vihl, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 American Journal of International Law Unbound 213-218 (2017).

30 Wright, supra note 6.

31 UN Charter art. 2(1).

countermeasure. Thus, disavowal of a rule of sovereignty eliminates a significant response tool when facing hostile cyber operations. Moreover, states taking this position undervalue the effect of naming and shaming states to which hostile cyber operations may be attributed. The fact that most states deny their involvement in hostile cyber operations, as is unambiguously illustrated in the case of Russian election meddling around the world, is evidence of the importance states place on not being named a lawbreaker.

The better approach is for states to acknowledge that sovereignty is a rule that can be violated.[32] and focus efforts on identifying *when* it is so violated. For instance, what types of effects must manifest before a remotely conducted cyber operation into a state's territory violates that state's sovereignty? When is an activity inherently governmental such that interference with, or usurpation of, the activity by another state is a sovereignty violation? Addressing the matter in this manner would allow retain the protective veil of sovereignty while tempering its restrictive effect through reasonable interpretation consistent with the state's national security imperatives.

A second issue regarding which states are at legal risk if they do not seize the opportunity to take a position is due diligence. Pursuant to the rule of due diligence, which was raised in the International Court of Justice's first case, *Corfu Channel*, a state is obligated to ensure that its territory is not used to the detriment of other states by either a state or a non-state actor.[33] In the cyber context, this means that a state would have to put an end to a hostile cyber operation being launched from its territory or that remotely employ cyber infrastructure on that territory to conduct the operation.

There appears to be a degree of state concern that such an obligation imposes an unbearable burden. Therefore, although a number of states have adopted the position that the rule of due diligence applies, others are hesitant to acknowledge the obligation in the context of cyber operations. Such concerns are overstated, for the rule is often misunderstood.[34] Most of the *Tallinn Manual 2.0* experts were of the view that the due diligence obligation only requires states to act to terminate ongoing hostile cyber operations; it imposes no obligation to take measures to prevent future operations or to otherwise ensure the hygiene of cyber infrastructure located on the state's territory. Moreover, the prevailing view is that it does not apply to all hostile cyber operations mounted from or through cyber infrastructure on the state's territory, but rather only operations that have serious adverse consequences for another state. This is a high bar to cross.

It is also generally understood that the rule does not apply to hostile cyber operations that only affect the *interests* of other states, as distinct from their *rights*. As an example, a hostile cyber operation against a bank's network that causes damage affects (in my view) the sovereignty rights of the state where that network is located. But if the operation affects the ability of individuals in third states to access their bank accounts remotely, an *interest* of those states would be implicated, not a right under international law. Most importantly, pursuant to the rule, states need only take those actions that are feasible in the circumstances. If a state lacks the ability to put an end to the hostile operations, it is not in breach of its due diligence obligation. In other words, the obligation is one of conduct, not a result. In light of these limitations, states need not be concerned that the due diligence rule imposes an overly onerous obligation on them. On the contrary, as a responsible member of the international community they should already be taking measures consistent with it.

32 Tallinn Manual 2.0, *supra* note 3, Rule 4

33 Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4 (Apr. 9), at 22. On due diligence, see Tallinn Manual 2.0, *supra* note 3, Rules 6-7.

34 See discussion in commentary accompanying Rules 6-7 of Tallinn Manual 2.0, *supra* note 3.

Additionally, what is sometimes missed is that the due diligence rule opens the door to conducting responses against cyber operations mounted by *non-state actors*.[35] Pursuant to the law of state responsibility, countermeasures are only available in response to internationally wrongful acts that are engaged in by states, or that are attributable to states under that body of law.[36] If a non-state actor's hostile cyber operations cannot be attributed to a state, the victim state ('injured' state in the law of state responsibility) has no right to take countermeasures to put an end to the hostile operations.

Yet, because the non-state actors are operating from another state, that state has a due diligence obligation to put an end to the hostile operations. Should it be unwilling to do so, the state would be in breach of its obligations under the rule of due diligence. This would allow the injured state to take countermeasures against the territorial state on the basis of that breach and those countermeasures could take the form of violating the territorial state's sovereignty by means of cyber operations against the non-state actor. The violation would be excused because the fact that the response qualifies as countermeasures is a ground for 'precluding the wrongfulness' of an action under the law of state responsibility.[37] Simply put, the rule of due diligence makes possible responses against hostile cyber operations by non-state actors in situations in which a robust response would not otherwise be available. If only for this reason, states should acknowledge the due diligence obligation.

Finally, states need to clearly articulate those response options that they believe are available under general international law. I have already addressed the issue of self-defense pursuant to Article 51 of the UN Charter and customary international law. However, most cyber operations do not rise to the level of an armed attack. Therefore, it is essential that two other response options be well understood and widely accepted.

The first, already mentioned, is the right to take countermeasures in the face of an unlawful cyber operation conducted by, or attributable to, another state. It should be cautioned that numerous restrictions apply to the taking of countermeasures, the most significant of which is a requirement that it be proportional in the sense of having some relation in terms of severity to the unlawful cyber operation to which it responds.[38] Nevertheless, considering the degree of push-back against countermeasures during the 2016 - 2017 GGE, states should quickly seize the opportunity to affirm that they reserve the right to take countermeasures in response to unlawful cyber operations directed against them. Absent such an affirmation, states will generally be limited to responses called retorsion, that is, unfriendly but lawful actions such as the expulsion of diplomats and the imposition of economic sanctions.

An additional response option that has received very little attention is based upon what is known as the plea of necessity.[39] Such responses, like countermeasures, may involve cyber operations that would otherwise be unlawful, but their wrongfulness has been 'precluded' because they are designed to put an end to hostile cyber operations directed against the state taking them. They are of particular importance because a response based on the plea of necessity is available against cyber operations mounted by non-state actors that are *not* attributable to a state or against those that cannot be reliably attributed to a state. In this sense, they differ from countermeasures. Thus, for example, a response based on the plea could be directed against non-state actors operating from a state that is in compliance with its due diligence obligation because it is willing to take measures to put an end to the non-state actor's hostile cyber operations but lacks the ability to do so.

---

35 Michael N. Schmitt, *In Defense of Due Diligence in Cyberspace,* 125 Yale Law Journal Forum 68 (2015).

36 Articles on State Responsibility, *supra* note 3, art. 49(1).

37 Id., art. 22

38 *Id.*, art. 51.

39 Id., art. 25; Tallinn Manual, supra note 3, Rule 26.

Although the plea of necessity remedies a number of the limitations that attach to countermeasures, it may only be resorted to when the 'essential interests' are facing 'grave and imminent peril'. The exact nature of these two phrases remains uncertain in international law. For example, states often designate certain infrastructure as 'critical', but that designation does not necessarily qualify the interest concerned as *essential* with respect to international law. Moreover, the point at which the harm being suffered can be characterized as grave is not only contextual, but also relatively vague. While these are complicated issues that states should be assessing with sensitivity to their own national interests, there is no obstacle to publicly taking the general position that the plea of necessity applies in the cyber contact.

Ultimately, the future of international cyber law lies in the hands of states, particularly as they interpret extant international law norms. They may choose to craft a relatively permissive environment in which international law plays little role in deterring hostile cyber operations or shaping the responses available thereto. This approach is exemplified in the British position that sovereignty is a principle of international law, but not a rule.

In my view, the better tactic is to employ the interpretive authority states enjoy vis-à-vis international law to safeguard the crucial activities of states and their societies in cyberspace, both during times of peace and armed conflict. With response options such as countermeasures, the plea of necessity and self-defence, states benefit from an array of lawful options for protecting these activities. And a well-developed IHL architecture applicable to cyber operations conducted during an armed conflict is consistent with the balancing of military necessity and humanitarian considerations that permeates all of international humanitarian law.[40]

Allow me to close by complementing the Kingdom of the Netherlands for its willingness to take the lead by beginning to announce its legal positions with respect to activities in cyberspace; other states must do the same. The Netherlands also has perceptively identified a lack of understanding of the complexity of international cyber law as an obstacle to international agreement on the applicable norms for behavior in cyberspace. I accordingly also complement the Netherlands for its Hague Process, which provides international cyber law training, in collaboration with other governments and international organizations, for government officials around the world. Such programs will empower states to intelligently, responsibly and constructively craft their own legal positions with respect to the shared domain that is cyberspace.

40 Michael N. Schmitt, Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance, 50 Virginia Journal of International Law 795 (2010).