2018 10th International Conference on Cyber Conflict
CyCon X: Maximising Effects
T. Minárik, R. Jakschis, L. Lindström (Eds.)
2018 © NATO CCD COE Publications, Tallinn

Pressing Pause: A New Approach for International Cybersecurity Norm Development

Cedric Sabbah
Office of the Deputy Attorney General (International Law)
Ministry of Justice
Israel[1]

Abstract: Over the last few years, the international community has devoted much attention to the topic of "international cyber norms". However, there appears to be a fundamental tension between these norm-development efforts and their real-world application as effective tools to reduce cyber risk and deter or prevent malicious state and non-state actors. Furthermore, in the current geopolitical climate, a broad agreement on global cyber norms seems improbable, as suggested by the lack of consensus in the course of the UN GGE 2017 process.

In the meantime, government officials tasked with developing and deploying cybersecurity policy and law face day-to-day challenges and are operating on a different track. Questions continuously arise with respect to the role of the state in formulating cybersecurity standards, information sharing, active defense and privacy protection. These questions are dealt with mostly in the "civilian" cybersecurity sphere and are occurring largely under the radar of the global "international cyber norms" community.

Against this backdrop, the paper suggests a shift in the approach to cyber norms. Its central thesis is that, at this juncture, rather than attempting to create a set of pre-defined aspirational norms aimed at achieving global stability, the international community should pay greater attention to discussions that are already occurring between cybersecurity regulators/authorities and should proactively support such discussions. Incremental and "bottom-up" processes, covering technical, policy and legal challenges at the domestic level, create fertile grounds for discussions that

1 The views and opinions stated herein belong to the author only, and are not reflective of Israel's Ministry of Justice or the Israeli government.

can be scaled up. This civilian, bottom-up approach is admittedly more mundane than the "aspirational cyber norms" track. Both tracks can and should continue to coexist in parallel, though the "civilian" track is more likely to result in a common taxonomy, legal/policy interoperability or common understandings that states can readily endorse, all of which could potentially ultimately lead to norms that enhance cybersecurity more pragmatically.

Keywords: *cyber norms, international law, cybersecurity law*

1. INTRODUCTION

The subject of "cyber norms" has been discussed at length in recent years, especially following the report on the subject issued in 2015 by a United Nations Governmental Group of Experts (GGE), regarding the use of information and communications technologies (ICT) by states.[2] Building upon the 2013 GGE Report,[3] the 2015 GGE Report acknowledged the application of basic concepts of international law, such as self-defense and state responsibility for internationally wrongful acts, to the cyber domain. It also recommended a series of "voluntary, non-binding norms" applicable in peacetime, which according to the Report were intended to reflect the international community's expectations as to "responsible behavior by states" in order to "increase stability and security in the global ICT environment."[4] The suggested norms covered a range of topics, from information sharing between states, to providing assistance to other states in dealing with cyber incidents, to protection of critical infrastructure.[5] The report was considered a significant development because representatives of 20 countries holding widely divergent views had produced a consensus text on certain topics that had previously been considered highly contentious. Another GGE was convened in 2016, with a mandate to expand on the 2015 GGE Report.[6] However, amid reports of profound rifts among the participating countries,[7] this GGE ended its work in 2017 without a consensus text being issued. Despite this setback, the subject

2 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (22 July 2015) ("2015 GGE Report").

3 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (24 June 2013).

4 2015 GGE Report, para. 9 and 10.

5 Id., par. (c), (f) and (h).

6 UNGA Resolution A/RES/70/237 (23 December 2015).

7 Michele Markoff, US Expert to the GGE, Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, June 23, 2017, <https://usun.state.gov/remarks/7880>. See also Arun M. Sukumar, Lawfare Blog, Tuesday, July 4, 2017 <https://lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well>.

of "cyber norms" continues to draw attention, with some arguing that states should expand this exercise.[8]

The working assumption in this discussion, it seems, is that norms are inherently a good thing: broadly defined as "shared expectations about appropriate (or inappropriate) behavior within a given community",[9] they can lay down the "rules of the road" between states, and thus contribute to international stability.[10] This has generated a wide range of proposals and ideas in an effort to identify the "right" forum in which a discussion can be held[11] or the "right" norm that states can settle on,[12] and to devise ways in which to implement the 2015 GGE norms.[13]

To be sure, the general notion that norms might eventually play a positive role in stabilizing cyberspace remains relevant, and the work of the GGE processes has arguably advanced the global conversation.[14] However, these approaches have not yielded concrete results beyond the 2015 GGE Report. Finnemore and Hollis refer to "fatigue" from the multiplicity of projects in this field.[15]

Against this backdrop, this paper argues that a moderate shift in approach is called for, beginning with a reassessment of current norm-development efforts and their underlying premises. The first part presents a critique of cyber norms and the global community's expectations of them. It argues that given the present political context and divergences between the main players, the focus on "global stability" – arguably, the underlying theme of the 2015 GGE Report – is, at this point in time, overly ambitious, and that norm-development efforts should be untethered from this goal. The second part proposes to shift the emphasis, from "global stability" to domestic cybersecurity. Its central thesis is that, rather than the current top-down approach that

8 See for example Kubo Mačák. (2017). From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. Leiden Journal of International Law, 30(4), 877-899. doi:10.1017/S0922156517000358.

9 This paper adopts on the definition used by Duncan B. Hollis in his article, "China and the US Strategic Construction of Cybernorms: The Process Is the Product". Hoover Institute, Aegis Paper Series No. 1704, July 6, 2017, <https://www.hoover.org/research/china-and-us-strategic-construction-cybernorms-process-product>, at p. 1.

10 See for example UK National Cyber Security Strategy 2016-2021, para.6.3.3; Australia Cyber Security Strategy, p. 42, which emphasize this point.

11 See James A. Lewis, "Revitalizing Progress in International Negotiations on Cyber Security", in Centre for International Governance Innovation (CIGI), *Getting beyond Norms: New Approaches to International Cyber Security Challenges*, edited by Fen Osler Hampsen and Michael Sulmeyer, Sept. 5, 2017, pp. 13-18; Joseph S. Nye Jr., "Normative Constraints on Cyber Weapons", in Getting Beyond Norms, ibid., pp. 19-22.

12 For example, Tim Maurer, Ariel (Eli) Levite, George Perkovich, "Toward a Global Norm Against Manipulating the Integrity of Financial Data", White Paper, Carnegie Endowment for International Peace, March 27, 2017.

13 E.g. East-West Institute, "Promoting International Cyber Norms: A New Advocacy Forum", Dec. 2015; ICT4Peace open consultations on the United Nations Cybersecurity Norms Proposals, <https://ict4peace.org/call-for-global-open-consultations-on-the-united-nations-cybersecurity-norms-proposal/> (accessed on March 11, 2018); Mariarosaria Taddeo, "Deterrence by Norms to Stop Interstate Cyber Attacks", Minds & Machines (2017) 27:387–392, 390.

14 Eneken Tikk and Mika Kerttunen, "The Alleged Demise of the UN GGE: An Autopsy and Eulogy", Cyber Policy Institute, 2017.

15 Martha Finnemore and Duncan B. Hollis, Constructing Norms for Global, Cybersecurity, 110 AM. J. INT'L L. 425, 469 (2016).

has characterized norm-development efforts to date, the cybersecurity community would be better served by focusing more on bottom-up processes emanating from cybersecurity policies as they are developed and deployed domestically. It contains a non-exhaustive overview of topics and issues that pose concrete challenges in this sphere. It argues that, while some of these topics are already the subject of bilateral and multilateral conversations to a certain extent, they could benefit from more expanded regional and multilateral conversations. A broad roadmap for taking the discussion forward is then submitted.

Most critically, the approach suggested herein is not focused on a specific set of norms around which to center a global process, but on issues-based discussions between government officials tasked with developing and implementing cybersecurity policy and law at the domestic level. There is no predictable outcome for such an exercise – it may or may not produce guidelines, common understandings or norms, and the outcomes might be global or between like-minded countries only. Neither does this approach negate the importance of maintaining existing multilateral cyber norm diplomatic efforts. However, the paper argues that, short of achieving "global stability", as current norms processes set out to do, such a bottom-up, needs-driven approach can help enhance cybersecurity for the parties involved in a concrete way.

2. A CRITIQUE OF CYBER NORMS

A. Advantage of Cyber Norms

Cyber norms have undeniable political and policy advantages for states. As defined in the 2015 GGE Report, norms differ from international law rules in that they are not binding on states. As such, they provide a certain flexibility, allowing states to coalesce around a particular principle or value without compromising their official legal positions. In the case of the 2015 GGE, this may have enabled the United States, the United Kingdom, Germany, China and Russia – countries with profoundly different approaches to the application of international law to cyberspace and what "information security" means – to agree on a set of broad principles.[16]

Another argument in favor of cyber norms, for states, is signaling or deterrence. By expressing support for or adherence to a certain norm, states are putatively indicating to each other that they would treat the violation of such a norm as non-trivial. The 2015 GGE Report makes this goal explicit: "norms reflect the international community's expectations, set standards for responsible State behaviour, and allow the international community to assess the activities and intentions of States".[17] Cyber norms can

16 Finnemore & Hollis, n. 15, p. 470.
17 GGE Report 2015, para. 10.

indicate red lines, providing states with a justification to respond, for example through diplomacy or trade sanctions, when the line is crossed.[18]

The process by which norms are developed can also be seen a positive element. The very fact that governments are speaking with one another, voicing their disagreements and attempting to hash out a consensus, allows the discussion to move forward. The process provides an outlet for states that hold opposing positions to interact with each other and seek common ground. Even if the process does not necessarily generate concrete results, it does foster dialogue between countries, which ultimately is a stepping stone towards global stability. To paraphrase Finnemore and Hollis, the process is the product.[19]

These arguments are valid and sound. However, they should be weighed against the challenges, disadvantages and costs of current cyber norm development efforts.

B. Critical Perspective on Current Cyber Norm Development Efforts

1) Political Challenges

The question of how to achieve global stability in the use of ICTs is an intrinsically political one. The lack of consensus at the 2017 GGE regarding the applicability of international law to the use of ICTs, including specifically the availability of self-defense - despite statements to that effect in previous GGE reports[20] – underscores the ideological and political gaps that remain between the positions of the US and European states on the one hand, and Russia and China on the other.[21] These gaps have been further highlighted in recent months, as China and Russia have each enacted laws tightening controls on Internet access.[22] In parallel, Russia has been actively promoting a new "cybercrime" treaty[23] which adopts an approach to ICTs that is fundamentally different from that found in the Council of Europe's Cybercrime Convention.[24] It is unlikely that these gaps will be resolved in the short term via another iteration of the GGE process or some variant thereof.

18 See for example EU Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), June 7, 2017.

19 Finnemore and Hollis, n. 15, p. 453.

20 2015 GGE Report, par. 28(d) and (e); Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013), para. 19.

21 United Nations, General Assembly, Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, A/69/723 (13 January 2015).

22 Samm Sacks, "China's Cybersecurity Law Takes Effect: What to Expect", Lawfare Blog, June 1, 2017, <https://www.lawfareblog.com/chinas-cybersecurity-law-takes-effect-what-expect>; Janet Burns, "Russian Laws Will Ban VPNs And Force Chat Users To Register, Giving Censors An Edge", Forbes, July 30.2017, <https://www.forbes.com/sites/janetwburns/2017/07/30/new-russian-laws-ban-vpns-and-force-chat-users-to-register-giving-censors-an-edge/#637dd7d02d7e>.

23 David Ignatius, "Russia is pushing to control cyberspace. We should all be worried", Washington Post, Oct. 24, 2017 <https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014bcc6-b8f1-11e7-be94-fabb0f1e9ffb_story.html?utm_term=.30f8621ccc5c>.

24 Council of Europe, Convention on Cybercrime, ETS 185 (2001).

Furthermore, one cannot dissociate the cyber norms debate from the broader geopolitics at play. For example, the United States' qualification of the Sony attacks and of Russia's alleged interference in the 2017 US elections was couched in terms of core principles and values such as free speech and civil liberties.[25] US interests in those cases extended beyond questions of how ICTs are used, and touched on broader questions of interference in another state's internal affairs. Similarly, in a briefing regarding the United States' attribution of WannaCry to North Korea, Tom Bossert, then-current Assistant to the President for Homeland Security and Counterterrorism, made a connection between North Korea's behavior in its use of the ransomware and its nuclear missile program.[26] The difficult topics that successive GGEs wrestled with cannot be analyzed solely from a perspective of information and communication technologies – they are intrinsically tied to a complex web of national interests and alliances, national and international security, international trade and diplomacy.

Finally, the norms discussion is occurring against the backdrop of a broader debate on the future of Internet governance. As is often recalled, the International Telecommunications Union (ITU) has been an unfortunate battleground for this debate, and it remains so to date.[27] The question of whether the Internet can or should be "regulated" in any way at the ITU – a dicey question in itself – has become intertwined with questions of sovereignty "over" the Internet,[28] further complicating the norms debate.

There are good arguments to be made that, notwithstanding the above, agreement on core "global stability" issues is desirable and could conceivably be achieved. Some of the proposals advanced recently include protecting the integrity of financial data,[29] dealing with "states' responsibility arising from the actions of their citizens," a commitment to ensure that actions in cyberspace do not contravene their international commitments, treatment of election processes as protected infrastructure and norms for cybercrime.[30] While it may be possible to achieve a consensus around these types of issues in the medium or long term, the doubts raised in this paper relate to whether

25 White House Office of the Press Secretary, Statement by the Press Secretary on the Executive Order Entitled "Imposing Additional Sanctions with Respect to North Korea", January 2, 2015, <https://obamawhitehouse.archives.gov/the-press-office/2015/01/02/statement-press-secretary-executive-order-entitled-imposing-additional-s>; White House Office of the Press Secretary, Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment, December 29, 2016 <https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity>.

26 White House Press Briefing transcript, Dec. 19, 2017 <https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/>.

27 Samantha Dickinson, "How 'Cyber' Sidelined 'Development' at the ITU's World Telecommunication Development Conference", CFR Blog, Nov. 17, 2017 <https://www.cfr.org/blog/new-cyber-brief-countering-russian-information-operations-age-social-media>.

28 Paul Rosenzweig, "The Continuing Struggle for Control of Cyberspace--and the Deterioration of Western Influence", Lawfare, Jan. 13, 2014 <https://www.lawfareblog.com/continuing-struggle-control-cyberspace-and-deterioration-western-influence>.

29 Maurer, Levite, and Perkovich, n. 12.

30 *Getting beyond Norms*, n. 9, pp. 16 and 21.

such agreements could emerge as a result of a self-styled norms process, and whether this approach is appropriate for the near future.[31]

2) Practical Limitations

Several factors limit the practical utility of norms. For one, the purported effect of a particular cyber norm cannot be gaged with certainty, since cyber operations are not usually made public. Second, since the GGE norms of 2015 and subsequent reiterations of those norms by the G7 in 2016 and 2017,[32] the world has seen several cyber incidents attributed to nation-states. Public testimony given by the US Director of National Intelligence to a Senate committee in May 2017 attests to the magnitude of cyber threats by states.[33] Indeed, major incidents at least partially attributed to states, like WannaCry, NotPetya, the DNC hack, and election hacks in France,[34] occurred after the adoption of the 2015 GGE norms. Of course, since this list only represents attacks that have been reported, definitive conclusions cannot be drawn from these and similar data. And certainly, the occurrence of these incidents should not be attributed to a "failure" of the norms process. What is evident, however, is that these kinds of incidents illustrate the challenge of applying broad aspirational cyber norms to actual scenarios.

States are also developing their doctrines and strategies at their own cautious pace, based on actual operational needs and existing legal frameworks. The merits of making their conclusions more transparent can be debated, but the national defense and security community is currently on a somewhat slower and more prudent track than the one reflected in current efforts to promote cyber norms.[35] To the extent that a given norm might impact national defense/security interests, the more conservative approach of governmental departments and agencies entrusted with these interests must be acknowledged.

The broader issue here is not whether a particular cyber norm is in fact being implemented. It is that declaring the existence of a norm at a UN forum or similar forum does not guarantee its effectiveness. Norms may provide guidance and declare red lines, but when a country's core interests are at stake, norms arguably play a lesser role. As Tikk and Kerttunen noted,

31 White House, Fact Sheet: President Xi Jinping's State Visit to the United States, 25 September 2015,<obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

32 G7 Principles on Actions in Cyber, May 27, 2016, <http://www.mofa.go.jp/files/000160279.pdf>; G7 Declaration on Responsible States Behavior on Cyberspace Lucca, 11 April, 2017, available at <www.mofa.go.jp/files/000246367.pdf>.

33 Daniel R. Coats, Director of National Intelligence, Statement for the Record, "Worldwide Threat Assessment of the U.S. Intelligence Community," Senate Armed Services Committee, 23 May 2017.

34 See full list at CSIS website, <https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity>.

35 Max Smeets, "Europe Slowly Starts to Talk Openly About Offensive Cyber Operations", CFR Blog, Nov. 6, 2017 <https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations>; Robert Hackett, "Gasp! China admits to having cyber warriors", Forbes, Mar.26, 2015 <http://fortune.com/2015/03/26/china-admits-cyber-warriors/>.

> "[given] the premature understanding what cyber security is about and how it can or may affect international peace and security, it is hard to see how the necessary level of peer pressure can manifest between 193 actors with (justifiably) sovereign interests and authority."[36]

One notable case study in the norm-development process is the norm prohibiting cyber industrial theft, which was excluded from the 2015 GGE Report. It was embodied in a bilateral commitment between China and the United States in 2015,[37] after which it was replicated in other international texts.[38] There have been conflicting reports as to the extent to which China has actually adhered to that commitment.[39] If reports of a partial reduction in cyber industrial theft are accurate, they reinforce the point made above, that at present bilateral commitments based on reciprocal interests are more likely to be effective than multilateral ones. The replication of this particular norm, specifically in bilateral commitments between China and other countries, also suggests that it emerged from a concrete need of states to address a specific concern (theft of intellectual property by companies), as opposed to a broad attempt to promote international stability. Other bilateral agreements based on a pragmatic need to resolve specific issues might also work in similar fashion.[40]

3) Taxonomy and the Ambiguous Value of Constructive Ambiguity

Joseph Nye has shown that the international cyber domain is a "regime complex", composed of a multiplicity of sub-regimes (incident response, law enforcement, international standards, international law, etc.), each with its own set of frameworks and actors.[41] The discussion on cyber norms can be confusing because different states frame the issue differently. Among Western states, cybersecurity, cybercrime, and the applicability of the laws of armed conflict to the cyber domain are distinct (though related) concepts, each governed by its own legal or political regime. By contrast, the concept of "information security" as understood by Russia and China is significantly different.[42]

36 Tikk and Kerttunen, n. 12, p. 26.

37 White House, Fact Sheet: President Xi Jinping's State Visit to the United States, 25 September 2015,<obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

38 G7 Declaration on Responsible States Behavior on Cyberspace Lucca, n.32 para.12.; G20 Leaders Communiqué, Antalya Summit, 15-16 November 2015, para. 26 <https://www.g20.org/profiles/g20/modules/custom/g20_beverly/img/timeline/Turquia/2015-g20-final-declaration-eng.pdf>; Reuters, "China, Canada vow not to conduct cyber attacks on private sector", June 26, 2017, <https://www.reuters.com/article/us-canada-china-cyber/china-canada-vow-not-to-conduct-cyber-attacks-on-private-sector-idUSKBN19H06A>.

39 Andy Greenberg, "China Tests the Limits of its Us Hacking Truce", in Washington Post, Oct. 31, 2017, <https://www.wired.com/story/china-tests-limits-of-us-hacking-truce/>; David Sanger, "Chinese Curb Cyberattacks on U.S. Interests, Report Finds", New York Times, June 20, 2016, <https://www.nytimes.com/2016/06/21/us/politics/china-us-cyber-spying.html>.

40 See, for example, Jack Goldsmith, "Contrarian Thoughts on Russia and the Presidential Election", Lawfare Blog, Jan. 10, 2017, <https://www.lawfareblog.com/contrarian-thoughts-russia-and-presidential-election>.

41 Nye, Joseph S. 2014. The Regime Complex for Managing Global, Cyber Activities. Global Commission on Internet Governance, Paper Series, 1.

42 UNGA, n. 21.

The 2015 GGE Report attempted to bridge this divergence of views through vaguely-drafted norms. For example, the 2015 Report includes a norm against attacking a country's "critical infrastructure" contrary to international law but provides no workable definitions or guidelines.[43] This is also the case with the norms regarding "due diligence", supply chain oversight and reporting of vulnerabilities.[44] One may argue that this type of constructive ambiguity is helpful in that it conveys an intelligible concept that states are free to define going forward.[45] One may also point to the current norm-development forums as positive efforts to infuse content to these norms. These arguments are certainly persuasive. However, the fundamental difficulty with this type of top-down push for achieving consensus is that it places the carriage before the horse: it glosses over the constructs around which the norms are built, declares a particular norm into existence, and only then seeks a way to operationalize it. This approach is not conducive to widespread implementation by states.

Indeed, events are unfolding at a rapid pace, challenging a short or mid-term conception of what a "stable ICT environment" might look like. The domestic policy landscape is continuously evolving: for example, it has recently been reported that Germany is actively exploring the possibility of enacting legal authority for state "hackbacks",[46] while China has adopted a sweeping cybersecurity law.[47] Moreover, the use of cyber tools by diverse actors – state, non-state, hacktivist groups and individuals – continues to rise, presenting new practical and legal challenges to states.[48] In short, it is difficult to deal with long-term stability through cyber norms, when the short and medium-term reality are filled with moving targets.

In summary, it is not argued that there is no room for a discussion on cyber norms involving core "global stability" issues. However, there is another, potentially more fertile ground for discourse in the field of domestic, "civilian" cybersecurity (defined below). Given the above factors, a more promising approach to cyber norms would be to promote and expand existing discussions in the domestic civilian sphere and allow norms within that sphere to emerge and evolve in a more organic fashion. The next part proposes a multi-stage analysis for how such a process might take place.

43 2015 GGE Report, para.13(f).
44 Ibid., para. 13(b), (h), (i), (j).
45 See discussion on "incompletely theorized" norms in Finnemore & Hollis, n. 15, p. 21.
46 Andrea Shalal, "German spy agencies want right to destroy stolen data and 'hack back' ", Reuters, Oct.5 2017, <https://www.reuters.com/article/us-germany-cyber/german-spy-agencies-want-right-to-destroy-stolen-data-and-hack-back-idUSKBN1CA1IN>.
47 Sachs, n. 22.
48 Paul Rosenzweig, "The Reality of Cyber Conflict: Warfare in the Modern Age", Heritage Foundation, 2017, <http://index.heritage.org/military/2017/essays/reality-cyber-conflict/>.

3. REFRAMING THE GLOBAL DISCUSSION ON CYBER NORMS: A POSSIBLE PATH FORWARD

The stated purpose of the cyber norms in the 2015 GGE Report was to "help to prevent conflict in the ICT environment and contribute to its peaceful use." Those objectives were ambitious, to say the least, and the current state of play suggests that the goal of global stability may be too much to pin on cyber norms.

Rather than attempting to tackle large, controversial issues that are fraught with political baggage, it may be more useful to enhance and broaden existing discussions around more mundane – yet no less important – issues of cybersecurity policy and regulation in the domestic, civilian sphere. Put otherwise, rather than asking "which cyber norms can enhance global stability in the cyber domain?", it is worth asking "what issues do cybersecurity officials have in the domestic arena, that could benefit from a broader conversation with their counterparts around the world?" As one commentator noted:

> "Given these near-dead ends, real issues might best be taken up bilaterally or multilaterally between countries and entities that have mutually agreed priorities and issues. Given political sensitivities, technical-level cooperation – be it between computer emergency response teams, law enforcement entities or judicial authorities – is likely more efficient than politicized formats."[49]

This admittedly unassuming starting point will not in and of itself produce world peace. However, if cybersecurity professionals engage in greater discussions of the type described below, this could help the international community or coalitions of like-minded countries to achieve a few discrete objectives in the field of domestic policy and law. This might contribute to greater security in the cyber domain, which could in turn enhance global stability over time. The approach proposed below is not intended to replace or subsume current large-scale "global stability" norm development efforts. Rather, it is a parallel track, which at this juncture should be afforded greater attention.

A. Framing the Discussion: Cybersecurity in the Civilian Sphere

Since the 1980s and 1990s, the body of policies and laws for protecting critical networks has matured into a full-fledged discipline. States are beginning to develop and update comprehensive cybersecurity strategies,[50] and are being increasingly active in the legislative sphere, as exemplified by the US Cybersecurity Information Sharing Act of 2015 and the EU NIS Directive. Furthermore, cybersecurity has percolated into the

49 Eneken Tikk, "Norms à la Carte", in Getting Beyond Norms, n. 9, p. 25.
50 See n. 10.

spectrum of regulatory issues, with regulators in the financial sector,[51] energy,[52] and transportation,[53] for example, developing sector-specific cybersecurity policies and rules. In the private sector as well, insurance companies, accounting firms, law firms and consulting firms have begun offering services in cybersecurity to their clients.[54]

For the most part, the topics covered by these areas do not involve complex questions of international law or international relations. They are mainly focused on building up robustness (sharing information about threat indicators, regulatory incentives for the private sector to improve defense, cyber awareness campaigns, supply chain oversight, etc.), and resilience (breach incident notification requirements, intervention of the national CERT, etc.), at the domestic level.[55] By way of illustration, on the domestic "civilian" end are topics such as how to protect personally identifiable information as part of an organization's information sharing with the government, application of the NIST framework to private entities, regulation of cybersecurity professionals, breach incident disclosure requirements in consumer protection law and securities law, cybersecurity regulation on the cloud, active defense in the private sector, and labeling requirements for software. The processes for policy development in these areas are usually unclassified and involve open consultations with the private sector. Similarly, these measures operate mainly in the civilian sphere, and they aim to promote domestic cybersecurity in the narrow sense of the term – reducing the risk of cyber incidents and the damages caused when such incidents occur.

At the other end of the spectrum are measures regarding the interface with the attacker or associated actors in the international sphere, for example deterrence tools, permitted actions above or below the "use of force" threshold under Article 2(4) of the UN Charter, the proposed norm about refraining from manipulating financial data, and broad questions of sovereignty and jurisdiction. Such topics are inherently more

51 Financial Services Board, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, Oct. 13, 2017, <http://www.fsb.org/wp-content/uploads/P131017-2.pdf>, Tom Gilheany, "The State of Cybersecurity Laws in the Financial Services Industry", in Talking Tech With Cisco Blog, May 18, 2017 <https://learningnetwork.cisco.com/blogs/talking-tech-with-cisco/2017/05/18/the-state-of-cybersecurity-laws-in-the-financial-services-industry>.

52 Energy Expert Cyber Security Platform, "Cyber Security in the Energy Sector Recommendations for the European Commission on a European Strategic Framework and Potential Future - Legislative Acts for the Energy Sector", February 2017, available at <https://ec.europa.eu/energy/en/news/new-report-cyber-security-energy-sector-published>.

53 For example: UK Government, Department of Transport, "Principles of cyber security for connected and automated vehicles", Aug. 6, 2017 <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles/the-key-principles-of-vehicle-cyber-security-for-connected-and-automated-vehicles>.

54 OECD (2017), Enhancing the Role of Insurance in Cyber Risk Management, OECD Publishing, Paris. http://dx.doi.org/10.1787/9789264282148-en; Lexis Nexis Business of Law Blog, "Beautiful Minds: 41 Legal Industry Predictions for 2016", Dec.16, 2015 <http://businessoflawblog.com/2015/12/legal-industry-predictions-2016/>.

55 Regarding the distinction between "robustness" and "resilience", see Matania, E. & Yoffe, L. & Mashkautsan, M. "A Three-Layer Framework for a Comprehensive National Cyber-security Strategy." Georgetown Journal of International Affairs, vol. 17 no. 3, 2016, pp. 77-84. Project MUSE, doi:10.1353/gia.2016.0038.

sensitive, approaching the core of a country's national security interests and raising complex international relations and international law questions.

This distinction between "domestic civilian" and "international" realms does not profess to create entrenched categories of cybersecurity policy and law, nor to suggest that any particular area in the cybersecurity discussion belongs exclusively to either realm. It merely highlights that certain areas of policy and law will tend to be easier for states to discuss in an open and transparent manner than others.

It should be stressed that the proposal to focus on the domestic civilian sphere is not meant to exclude the evolution of other norms in the field of defense and security, such as how to apply the law of state responsibility to attacks attributable to non-state actors, what "sovereignty" means,[56] and what "responsible state behavior" could look like in practice. Processes in both these areas can coexist and complement one another. The thrust of the argument here is that the domestic civilian cybersecurity sphere should garner more attention from the international community than it has to date, and may reveal itself to be a promising path forward.

B. Bottom-up Process Led by Domestic Cybersecurity Professionals

Having broadly defined the types of issues that could be discussed, it is equally important to describe the contours of possible discussions around these issues. Civilian cybersecurity discussions are driven by those government officials tasked with creating and deploying domestic policy and law. This includes officials involved with cyber education and awareness, defense of critical and non-critical infrastructure networks, handling of cyber events in real time within a CERT, policy development, engagement with the private sector, regulation and oversight.

Through this dialogue, cybersecurity professionals with diverse backgrounds develop a common language, share issues and questions of concern, learn from best practices, and achieve informal capacity building. The dialogue is technical, legal or policy-oriented or multidisciplinary. This is fundamentally a bottom-up process, which draws from the experience and expertise of cybersecurity professionals.

To be sure, there are already formal and informal discussions under way between different actors around these topics (within FIRST, the network of CERTs including national CERTs, as well as between sector-specific industry regulators). Our suggestion here is to expand upon, and refocus the international community's efforts around, these types of discussions.

56 Gary Corn, Tallinn Manual 2.0, Advancing the Conversation, Just Security (Feb. 15, 2017) <https://www.justsecurity.org/37812/tallinn-manual-2-0-advancing-conversation/>.

The process suggested above can be distinguished from the OSCE's confidence-building measures of 2013 and 2016.[57] Finnemore and Hollis have shown how, among other factors, the choice of a particular type of forum to promote a particular norm can be just as important as the content of the norm.[58] For example, when a proposed norm is developed within an existing organization (in this case, the OSCE), this has an impact on the way the norm is understood and its reach to a particular target audience. The OSCE's confidence-building measures were developed primarily in a top-down fashion, mostly through diplomatic action, and thus far, it does not appear that they have been "adopted" by the national CERT community. By contrast, a bottom-up process focused on "civilian cybersecurity" on the topic of confidence building, would likely result in a more technical set of standards based on the perceived needs of national CERT officials, which could then percolate upwards with the assistance of cyber diplomats.

The COE Cybercrime Convention can be taken as illustrative of the ways in which top-down and bottom-up efforts can converge. On the one hand, the Convention constitutes a relatively successful exercise in international law development in a different though related field. Adopted in 2001, it has been ratified by 56 countries and remains the benchmark text in the field of cybercrime. Thus, one might view the Convention as an example of the success of the "top-down" approach. At the same time, the Convention is an example of how the law developed bottom-up from a concrete specific need, namely, law enforcement cooperation to deal with cross-border cybercrime. The conference of state parties of the Convention constitutes a useful forum which is currently tackling several important issues, such as access to data on the cloud, and is attended by a mix of diplomats and practitioners.

An additional clarification is in order. The suggested focus on "domestic cybersecurity" should not be seen as a negating the need for discussions on "global stability". Similarly, diplomatic efforts should not compete with, or come at the expense of, bottom-up civilian-based technical efforts, or vice versa. On the contrary, these two processes can and should complement each other. However, the point made here is that up until now, bottom-up processes have been largely ignored in the cyber norms discussion.[59] A few concrete examples of how such processes can be amplified and harnessed will be suggested below.

57 Organization for Security and Co-operation in Europe, Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1106, OSCE Permanent Council, 975th Plenary Meeting, 3 December 2013), <http://www.osce.org/pc/109168?download=true>; Decision No. 1202: OSCE Confidence-Building Measures To Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1202, OSCE Permanent Council, 1092nd Plenary Meeting, 10 March 2016, <https://www.osce.org/pc/227281?download=true>.

58 Finnemore and Hollis, n. 15, p. 468.

59 A notable exception is the "CERT diplomacy" initiative raised at the 2017 Internet Governance Forum, which is addressed below.

C. Potential Areas of Discussion

As noted previously, there is no definitive list of cybersecurity topics that can neatly fit into a "civilian" category. Similarly, not every issue is necessarily conducive to broad multilateral discussions. Still, there are areas where common ground, or at least shared understandings, are more realistic. We provide below a few examples of such areas.

1) The Role of the State

The hybrid private-public nature of Internet infrastructure, coupled with the pervasiveness of connected devices, presents new challenges for domestic cybersecurity regulators. One of these is identifying the instances in which a national cybersecurity agency can and should intervene in the market in order to prescribe minimum standards. The need for government cybersecurity officials to manage risk, prioritize and classify types of organizations and networks, balance between rules-based and principles-based regulation making and optimize the use of deterrents and incentives, while maintaining the core authority to intervene when national security or public order or safety are at stake, requires difficult choices, constant engagement with the private sector, and an adaptive modus operandi. While domestic cybersecurity agencies might be developing this approach on their own, there could be much benefit to an expanded discussion on regulatory choices, pitfalls and best practices. The NIST Framework,[60] the OECD Recommendations on Digital Risk Management[61] and the OECD workshop on protecting critical infrastructure[62] provide useful starting points for such discussions.

2) Information Sharing Between the Public and Private Sectors

An underlying issue of concern for cybersecurity regulators is how to generate trust between the public and private sectors within a particular jurisdiction.[63] Relevant questions to be asked include: are current domestic policies and practices in this field optimal? Do they lead to actionable results? How can data collection practices be streamlined? Can and should a common information sharing standard be adopted? What type of approach vis-à-vis the private sector is desirable? In what cases are incentives more appropriate? How can individuals' personal information be protected in the course of information sharing? An expanded dialogue on how to improve

60 NIST, "Cybersecurity Framework," <www.nist.gov/cyberframework>.

61 OECD (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en.

62 See workshop website at <http://www.oecd.org/going-digital/digital-security-in-critical-infrastructure/>, accessed on March 11, 2013.

63 See, for example, the discussions held at the 2017 Internet Governance Forum regarding this topic: International cooperation between CERTS: technical diplomacy for cybersecurity (https://igf2017.sched.com/event/CTrn/international-cooperation-between-certs-technical-diplomacy-for-cybersecurity-ws38?iframe=no&w=100%&sidebar=yes&bg=no>); Cybersecurity 2.0 - Leveraging the Multistakeholder Model to Develop and Deploy Cybersecurity Policy (<https://igf2017.sched.com/event/CTri/cybersecurity-20-leveraging-the-multistakeholder-model-to-develop-and-deploy-cybersecurity-policy-of70?iframe=no&w=100%&sidebar=yes&bg=no>).

information sharing between the private and public sectors could lead to real solutions to such dilemmas.

3) Active Defense in the Private Sector

For the purposes of this paper, we define "active defense" as actions and measures taken to:

> "detect, analyse, identify and mitigate threats to and from communications systems and networks in real-time, combined with the capability and resources to take proactive or offensive action against threats and threat entities including action in those entities' home networks".[64]

The issue has been analyzed at length, leading to growing calls for a more sophisticated discussion on active defense in the private sector.[65] Possible policy discussions to be held include whether some of the risks attendant to active defense could be mitigated by adding elements of *ex ante* and *ex post* government oversight and entrusting the task to reputable cybersecurity companies under an accreditation system. Another policy issue is whether the perceived need to allow active defense could be diminished if "internet infrastructure" entities such as ISPs were better incentivized to take a more active role in detecting and mitigating attacks transiting through their networks.

4) Cybersecurity on the Cloud

The UN Commission on International Trade Law (UNCITRAL) has begun grappling with the contractual aspects of cloud services in the private sector,[66] and this topic seems ripe for further study from a cybersecurity perspective, particularly with respect to government procurement of cloud services from third party vendors.[67]

64 Robert Dewar, "The 'Triptych of Cyber Security': A Classification of Active Cyber Defence" (6th Annual Conference on Cyber Conflict, 2014), NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/cycon/2014/proceedings/d1r1s9_dewar.pdf.

65 Joe Uchill, "New bill would allow hacking victims to 'hack back' ", *The Hill*, Oct.13, 2017 <http://thehill.com/policy/cybersecurity/355305-hack-back-bill-hits-house>. See also Paul Rosensweig, Steven P. Bucci and David Inserra, "Next Steps for U.S. Cybersecurity in the Trump Administration: Active Cyber Defense", Heritage Foundation Backgrounder 3188, May 5, 2017 <www.heritage.org/sites/default/files/2017-05/BG3188.pdf >.

66 UNCITRAL Working Group IV on e-commerce.

67 American Technology Council, "Report to the President on Federal It Modernization", Dec. 13, 2017 <https://itmodernization.cio.gov/>UK Government Digital Service, "Government Cloud First Policy", Feb. 3, 2017 <https://www.gov.uk/guidance/government-cloud-first-policy>.

Other relevant topics include:

- cyber insurance (whether and how the market should be regulated, guidance on how to quantify cybersecurity risks);
- cybersecurity for the Internet of Things;[68]
- labeling and rating of software;[69]
- developing a common ontology and technical standards for cybersecurity.[70]

At the same time, it should be borne in mind that not all civilian efforts are worth pursuing at a global scale.[71] The challenge is to identify topics that could both benefit from and lend themselves to an international conversation.

D. The Formats of Potential Discussions

The format of an international discussion about a particular area can be as important as the topic itself, as it sets the stage for the types of discussions that are held and the expectations of participants.[72] Accordingly, we offer the following basic principles regarding the format for potential discussions around topics such as the ones discussed above.

1. A non-prescriptive process is more likely to enable participants to engage in an exploratory dialogue in which they consider a range of options. A discussion on norms should be allowed to emerge naturally as a result of the discussions, rather than established as a goal from the outset.
2. As mentioned earlier, the agenda should be set by cybersecurity officials involved with policy development and deployment. They are arguably best placed to define and discuss the challenges they face on a day-to-day basis.
3. The level of engagement (multilateral, regional or like-minded) plays an important role in expectations and outcomes. To state the obvious, the more global the forum, the more challenging it is to achieve consensus.
4. One cannot ignore the place of bilateralism. Several countries have opened lines of dialogue and entered into bilateral agreements and memorandums of understanding in the field of cybersecurity[73] and this trend will likely

68 Laura DeNardis & Mark Raymond, "The Internet of Things as a Global Policy Frontier", UC Davis Law Review, Issue 51:2 (December 2017), 475.

69 E.g. DHS designation of Kaspersky products as presenting security risks - DHS Statement on the Issuance of Binding Operational Directive 17-01, Sept. 13, 2017 <https://www.dhs.gov/news/2017/09/13/dhs-statement-issuance-binding-operational-directive-17-01>; see also Cyber Independent Testing Lab, founded by Sara and Peter Zatko (a.k.a Mudge).

70 Claire Vishik, Mihoko Matsubara, Audrey Plonk, "Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms", in International Cyber Norms Legal, Policy & Industry Perspectives, Anna-Maria Osula and Henry Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016.

71 Columbia School of International Public Affairs New York Cyber Task Force, "Building a Defensible Cyberspace", Sept. 2017, <https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF>, p. 14.

72 Finnemore and Hollis, n. 15, p. 468.

73 See, for example, Mapping of India's Cyber Security-Related Bilateral Agreements, <https://cis-india.org/internet-governance/blog/india-cyber-security-bilateral-agreements-map-dec-2016> (accessed on March 11, 2018), Australia Cyber Security Strategy, n. 10, p. 43.

continue in the near future. While the resulting texts may be phrased in broad language that encourages general cooperation rather than requiring compliance with concrete obligations, they create the framework for engagement between states within which future cybersecurity discussions can be held.

5. The creation of yet another global forum dealing with cybersecurity should be avoided. The focus should not be on adding to the high-level discussions that already exist, but on expanding the bottom-up, professional discussions that are currently under-exploited.

One practical way forward was recently explored at the Internet Governance Forum of 2017 in Geneva. There, national and private CERTs were identified as technical and largely apolitical actors at the frontline of incident response. These attributes position CERTs advantageously, as potentially significant actors on the global sphere. To tap into this potential, governments could further empower CERTs to engage with one another, broaden the scope of their discussions and cooperation, and take the lead in "cyber diplomatic efforts".[74] That being said, any expanded role for CERTs should be carefully crafted to avoid unduly politicizing their activities and tainting their technical mission. Another interesting outcome of the 2017 IGF was the proposal, in one of the panels, to leverage the multi-stakeholder model to enhance cybersecurity policy development and deployment.[75] While this panel was primarily focused on domestic cybersecurity, examples were given of how bottom-up domestic policy development processes can have international ripple effects. The NIST Framework was frequently cited as a useful standard for countries and entities outside the United States.

Another example could be to expand the work of technical, policy and legal working groups in bodies such as UNCITRAL and the OECD. These bodies enjoy broad membership with established structures and work methods, and their work is typically produced by subject-matter experts. As noted above, they have each undertaken work that touches on cybersecurity issues in the past, and they could be tasked with more such issues going forward. This requires a "bottom-up" push from cybersecurity officials to suggest clear mandates for working groups within these organizations, followed by a "top-down" push from capitals to promote these mandates when the relevant organization decides on its future work program.

Finally, a more adventurous endeavor could consist of creating one or more *ad hoc* topical and specialized forums, not necessarily tied to existing organizations. For example, one might imagine a forum similar to the Financial Action Task Force

74 A transcript of the session can be accessed at: <https://www.intgovforum.org/multilingual/content/igf-2017-day-3-room-xi-ws38-international-cooperation-between-certs-ws38-technical-diplomacy>. See summary here: <https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/5902/858>.

75 A transcript of the session can be accessed at <https://www.intgovforum.org/multilingual/content/igf-2017-day-3-room-ix-of70-cybersecurity-20-leveraging-the-multistakeholder-model-to>. See summary here: <https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/5921/1042>.

(FATF), which could work on developing global cybersecurity standards in specific areas (information sharing, professional qualifications, etc.). The FATF is a product of high-level ministerial cooperation and it has been highly influential in setting standards to combat money-laundering and the financing of terrorism. Arguably, a similar model could be adopted by cybersecurity agencies wishing to promote concrete steps towards enhancing global cybersecurity through domestic measures.

It goes without saying that the diplomatic community has a role to play in each of the examples provided above. Diplomatic efforts are needed to initiate, support and sustain the contacts between technical and policy professionals between different states, especially if some of the states will not be "like-minded". Such efforts will also be needed to lend visibility to the discussions taking place, so as to increase their reach and effectiveness.

4. CONCLUSION

The analysis above conveys a few recurring themes. The first is a shift in expectations: while acknowledging that some discussion of cyber norms might contribute to global stability, it would be unrealistic to expect that such stability can be achieved by declaring the existence of a norm or by attempting to operationalize a particular norm. The second theme is the need for a bottom-up approach, driven by actual needs of, and challenges faced by, government cybersecurity organizations. The third and most fundamental theme is the shift in emphasis, from the current discussions focused on global "stability", towards the more mundane goal of domestic cybersecurity.

In their comprehensive paper on cyber norms, Tikk and Kertunen have stated:

> "[...] cyber incident and risk assessments indicate more than state-on-state hostilities. Data breaches, website defacements, increasing cybercrime and botnet topologies, more than they speak of the potential of cyber warfare, testify of a cyber crisis surface where the risk of unwanted or unforeseen developments cannot be effectively prevented due to the still low awareness or obvious capacity gaps. Therefore, the GGE has, without necessarily meaning to, developed at least two separate agendas of international cybersecurity: one that can be understood and explained by way of traditional geopolitics and where the likelihood of conflict or no conflict does not depend significantly on ICT as such. Absent ICTs, the relationships between the US, China, Russia, Iran and North Korea remain largely the same. What geopolitics cannot

> exhaustively explain, is the surface of potential cyber crisis that has emerged by way of extensive adoption of ICTs across the world, without due acknowledgment of the accompanying risks and ways of their mitigation. Jumping on the international information highway has been too fast, too soon, for countries that are not able to run sustainable information systems and services: States that have to run on Windows XP, cannot be helped by any of the UN GGE recommendations."[76]

In very broad terms, the two agendas described above summarize the distinction made in this paper between "global stability", which current cyber norm efforts have been promoting, and domestic cybersecurity, which deserves greater attention from the international community. The effect of the suggested bottom-up, domestic cybersecurity approach is a series of open-ended processes, the milestones of which will likely be more incremental. Its successes will hopefully be enduring and substantive, though they will not grab national headlines. Under this approach, the role of civil society is crucial. Think-tanks, multinational corporations and academics can generate valuable ideas outside conventional thinking, conduct large-scale empirical research and provide a diversity of perspectives that can all feed in to these bottom-up processes. Diplomacy, too, plays a critical role in taking the domestic civilian cybersecurity discussion to the global arena. The challenge for the multi-stakeholder cybersecurity community, then, is to reassess current cyber norm development efforts, adjust expectations, refocus and leap forward with a new sense of purpose.

5. ACKNOWLEDGMENTS

The author thanks Paul Rosenzweig and Duncan Hollis for their insight and comments.

76 Tikk and Kerttuen, n. 14, p. 31.