INSTITUTE FOR DEFENSE ANALYSES

A Cyber Persistence Way to Norms

Michael P. Fischerkeller, Project Leader

June 2022

IDA Non-Standard D-33142

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project C5224, "Review and Editorial Prep for Non-sponsored Articles and Essays for External Publication," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Steve Peterson (CYBERCOM), Sean Kanuck (Research Director for Global Cyber Stability Commission)

For More Information

Michael P. Fischerkeller, Project Leader
mfischer@ida.org, 703-845-6784

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Copyright Notice

Rigorous Analysis | Trusted Expertise | Service to the Nation

A Cyber Persistence Way to Norms

Michael P. Fischerkeller

Cyberspace is a strategic competitive environment where continuous activity short of use of force has cumulatively threatened international peace and stability. States have sought to both manage and regulate this threatening behavior through the United Nations (U.N.) Group of Government Experts (GGE) and Open-Ended Working Group (OEWG) processes. These processes have resulted in deliberative products proposing peacetime cyber norms and an agreement that international law applies in the context of cyberspace.[1] However, the prohibitive norms advanced do not address ongoing threatening behavior. Although all states now accept that international law applies, it will likely take years for states to reach agreements on how it applies—a milestone that, if reached, would contribute to establishing new rules of customary international law in the context of cyberspace. Some argue that the slow steady pace over decades of state interaction and U.N. processes is consistent with how states have historically responded to major disruptive technological change (i.e., the "usual way").[2] But time is not a luxury we can afford in cyberspace as strategic ground is already shifting; conceding to the "usual way" threatens peace and stability.

Prohibitive cyber norms efforts need to immediately address ongoing state and non-state cyber behaviors that threaten peace and stability. Several prohibitive norms proposed by the Global Commission on the Stability of Cyberspace (GCSC) form a sound basis because they speak to empirical reality. In addition, a new approach to cultivating conformance is needed that acknowledges and leverages cyberspace's strategic imperatives and incentives for cyber persistence while also minimizing the potential for further instability. Over time, *opinio juris* being coaxed from states as part of U.N. processes can converge with this new approach to state practice and set the stage for new, binding rules of customary international law for the cyber context.[3]

GGE and OEWG Proposed Prohibitive Norms: Missing the Mark

[1] *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, May 28, 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf and *Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, March 10, 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

[2] Joseph S. Nye, Jr., "The End of Cyber-anarchy: How to Build a New Digital Order," January/February 2022, https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy.

[3] In international law, *opinio juris* is the subjective element used to judge whether, in the context of determining the existence of a customary international law rule, a state believes that it is legally obliged to do or refrain from doing a particular act. See *United Nations Report of the International Law Commission, Sixty-eighth Session (May 2 - June 10 and July 4 - August 12, 2016), A/71/10*, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/184/25/PDF/G1618425.pdf?OpenElement.

The UN GGE and OEWG processes have produced deliberative products proposing peacetime cyber norms, but these do not constitute norms in and of themselves. International norms are widely understood as state practice, not merely aspirations of state practice.[4] Of the 11 proposed norms identified in these products, many are best practices or positive duties, such as protecting one's own infrastructure and supply chains and responsibly reporting vulnerabilities and sharing remedies.[5] Two are prohibitive norms describing behaviors that states should eschew: for example, states should not conduct or knowingly support activity to harm the information systems of another state's emergency response teams and should not use their own teams for malicious international activity, and states should not conduct or knowingly support information communications technology (ICT) activity that intentionally damages critical infrastructure.

States are engaging in a range of cyber behaviors that undermine peace and stability but these proposed prohibitive norms do not address those behaviors. There is no reported instance of states engaging in cyber operations against another state's cyber emergency response teams or using their teams for malicious purposes. And, although states have targeted critical infrastructure in armed conflict and non-state actors have done so in peacetime, the proposed prohibitive norm is not framed in a manner addressing that context or those actors, respectively.

GCSC Proposed Prohibitive Norms: Credible and Salient

Unlike the UN GGE and OEWG products, the GCSC report proposes prohibitive norms addressing ongoing destabilizing behaviors: For example, state and non-state actors must not pursue, support, or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda, or plebiscites; state and non-state actors should not commandeer the general public's ICT resources for use as botnets or for similar purposes; and state and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace. These proposed prohibitive norms are more credible (i.e., supported by empirical evidence) and salient (i.e., comporting with state experience) than the U.N. prohibitive norms and thus are more likely to motivate action.[6]

---

[4] Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (July 2016): 425–479, https://doi.org/10.1017/S0002930000016894.

[5] North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/.

[6] Cristina Bicchieri, "Words and Deeds: A Focus Theory of Norms" in Julian Nida Rumelin and Wolfgang Spohn, eds., *Rationality, Rules and Structure* (Kluwer Academic Publishers, 2000): 153–184, https://www.researchgate.net/profile/Cristina-Bicchieri/publication/289670336_Words_and_Deeds_A_Focus_Theory_of_Norms/links/56992fe608ae6169e55171e2/Words-and-Deeds-A-Focus-Theory-of-Norms.pdf.

Threats to technical election infrastructure are highly credible and salient for the United States. The U.S. Senate Select Committee on Intelligence reports that, throughout 2016, Russia engaged in "an unprecedented level of activity against [the] state election infrastructure" of all 50 U.S. states.[7] The report identifies many failed efforts and a small number of successful exploitations.[8] Russian cyber actors were in a position to delete or change voter data in the Illinois voter database and in a position to modify county data in another state (other reporting suggests this is Arizona).[9] Threats persisted beyond 2016, as numerous actors continued to regularly target election infrastructure for different purposes, including disruption.[10]

Threats to technical election infrastructure are also credible and salient for several European governments. Many have been subject to influence campaigns attributed to Russian advanced persistent threat (APT) groups.[11] Fearing Russian attempts to disrupt vote counting technology, the Dutch government ordered all municipalities and electoral regions to tally all votes manually for the 2017 parliamentary election.[12] Concerns about an "extremely high risk" of cyber disruption led France's National Cybersecurity Agency to prohibit electronic voting—banned in France since 2012, with an exception for French overseas voters—entirely in the June 2017 legislative elections.[13] Germany's Interior Ministry shared similar concerns when it reported in September 2021 that a development server for the national census was "affected"

---

[7] Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume I: Russian Efforts against Election Infrastructure with Additional Views. The report can be access through Dana Farrington, "READ: Senate Intelligence Report on Russian Interference In the 2016 Election," NPR, July 25, 2019, https://www.npr.org/2019/07/25/745351734/read-senate-intelligence-report-on-russian-interference-in-the-2016-election.

[8] Ibid. 16–20 for reported failures and 22–28 for reported successes.

[9] See Wesley Bruer and Evan Perez, "Officials: Hackers Breach Elections Systems in Illinois, Arizona," CNNPolitics, August 30, 2016, https://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html and David E. Sanger and Catie Edmonson, "Russia Targeted Elections Systems in All 50 States Report Finds," *The New York Times*, July 25, 2019, https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html.

[10] Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures Campaigns and Interference in the 2016 U.S. Election , 21. The assessment offers case study from August 24, 2018, when there were multiple attempts to illegally access the State of Vermont's Online Voter Registration Application, which serves as the state's resident voter registration database. The malicious activity included a Cross Site Scripting attempt, seven Structured Query Language injection attempts, and one Denial of Service attack.

[11] Tim Maurer, *Five European Experiences with Russian Election Interference*, Carnegie Endowment for International Peace, May 23, 2018, https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435

[12] "Dutch to Hand-Count Ballots in March Vote Due to Hacking Fears," *Deutsche Welle*, February 1, 2017, http://www.dw.com/en/dutch-to-hand-count-ballots-in-march-vote-due-to-hacking-fears/a-37375137.

[13] "France Drops Electronic Voting for Citizens Abroad over Cybersecurity Fears," Reuters, March 6, 2017, https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233.

by a cyber operation. This server is part of the Federal Statistical Office's infrastructure, which also includes servers for elections and other inherently government functions.[14]

Botnet threats abound. The Mirai botnet Distributed Denial of Service operations against Dyn in October 2016 disrupted Internet traffic for most of the U.S. East Coast and served as an early indication of what is possible through commandeering public ICT resources.[15] At its peak, this botnet comprised 600,000 commercial Internet-of-Things devices.[16] On May 23, 2018, Cisco Talos published an alert regarding its discovery of "VPNFilter" malware on over 500,000 small and home offices routers and storage devices spread across at least 54 countries.[17] The malware was designed to conduct surveillance on its targets and gather intelligence, interfere with Internet communications, monitor industrial control systems, and conduct destructive operations.[18]

Finally, recent operations against SolarWinds and Kaseya make evident that supply-chain exploitations can cause significant disruption. Malware inserted into SolarWinds' network management system software—Orion—rapidly spread to customers' servers when they logged into the company's software development website.[19] In addition, a malicious actor launched a supply-chain ransomware operation by leveraging a vulnerability in Kaseya's VSA software against multiple managed service providers.[20]

The GCSC proposed prohibitive norms resonate more strongly than U.N. proposed norms, but absent an effective conformance mechanism, they also are merely aspirational.

Cultivating Conformance: The "Usual Ways" Are Failing

---

[14] Lorne Cook, "EU Warns Russia over Cyberattacks ahead of German Elections," AP, September 24, 2021, https://apnews.com/article/technology-russia-elections-media-foreign-policy-a9abb7e00e4430c402b07ae14cdd9c8c.

[15] Lily Hay Newman, "What We Know About Friday's Massive East Coast Internet Outage," *Wired*, October 21, 2016, https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/.

[16] Garrett M. Graff, "How a Dorm Room Minecraft Scam Brought Down the Internet," *Wired*, December 13, 2017, https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/.

[17] See William Largent, "New VPNFilter Malware Targets at Least 500K Networking Devices Worldwide," *Cisco Talos*, May 23, 2018, https://blog.talosintelligence.com/2018/05/VPNFilter.html and William Largent, " VPNFilter Update - VPNFilter Exploits Endpoints, Targets New Devices," *Cisco Talos*, June 6, 2018, https://blog.talosintelligence.com/2018/06/vpnfilter-update.html.

[18] "FBI Seizes Domain Responsible for Major Russian Botnet," *eyerys*, May 24, 2018, https://www.eyerys.com/articles/timeline/fbi-seizes-domain-responsible-major-russian-botnet?page=14#event-a-href-articles-timeline-sharewareshareware-a.

[19] Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," NPR, April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.

[20] Charlie Osborne, "Updated Kaseya Ransomware Attack FAQ: What We Know Now," *ZDNet*, July 23, 2021, https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/.

Norms on important contentious issues take significant effort; they do not magically appear.[21] Norm entrepreneurship plays a critical role.[22] This can entail calling attention to an issue and proposing aspirational norms. States calling for the GGE and OEWG processes and the organizers of the GCSC commission have played this role. Another role for entrepreneurs is cultivating conformance. The same actor(s) need not play both roles, although they may.

Martha Finnemore and Duncan Hollis outline three discrete mechanisms for cultivating conformance: persuasion, socialization, and incentives (positive and negative inducements).[23] *Persuasion* means causing someone to do or believe something in the absence of coercion by asking, arguing, or giving reasons. It describes a cognitive process of information exchange and argumentation to change minds, opinions, and attitudes. The U.N. processes leverage this mechanism to seek voluntary conformance. They also leverage *socialization*, a mechanism that rests on social relations and the identity ingredient of a norm. An actor wanting to establish or maintain a relationship with another actor or group of actors will conform to a proposed norm, not necessarily because of its content but because doing so is expected within a valued relationship. This mechanism underpins declarations of proposed norms by "like-minded" states, for example, the 2015 G20 Leader's Communique and 2017 G7 declarations on "responsible" behavior.[24] Norm entrepreneurs leveraging this mechanism may also adopt coercive tactics such as naming and shaming to pressure an actor concerned with reputational costs into conformance. While this form of coercion seeks behavioral changes through speech and social relations, the third mechanism for cultivating conformance—*incentives*, specifically negative inducements—cultivates conformance through material coercive actions ranging from economic sanctions to threats or uses of military force.[25]

All of these mechanisms have a poor track record, independently and in combination, for cultivating conformance by malicious state and non-state actors with proposed prohibitive peacetime cyber norms.[26]

Evidence that the persuasion mechanism has failed is overwhelming, although not systematically documented. It is clear even to the casual observer that numerous states persistently act in and through cyberspace in ways that do not conform to the GCSC-proposed prohibitive norms. Efforts premised on socialization to sustain a valued relationship have encouraged conformance among like-minded states, but that population does not include the

[21] Finnemore and Hollis, 449.
[22] Martha Finnemore and Kathryn Sikkink, "International Organization at Fifty: Exploration and Contestation in the Study of World Politics," *International Organization* 52, no. 4 (Autumn 1998): 887-917, https://www.jstor.org/stable/2601361.
[23] Finnemore and Hollis, 448–453.
[24] See http://www.g20.utoronto.ca/2015/151116-communique.pdf and https://www.mofa.go.jp/files/000246367.pdf, respectively.
[25] Incentives may also include positive inducements.
[26] See chapters 5 and 7 in Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace* (New York: Oxford University Press, 2022).

most egregious malicious cyber actors. Moreover, socialization premised on naming and shaming those actors has not succeeded either. When discussing the issue of Russian cyber operations seeking to influence the U.S. presidential election, U.S. President Obama stated, "[T]he idea that somehow public shaming is going to be effective, I think doesn't read the thought process in Russia very well."[27] Coercive inducements applied most frequently by the United States, such as indictments and economic sanctions, have also failed to stem the tide of malicious activity.[28]

These mechanisms fail not because they lack sufficient time to produce conformance—that is, the usual way—rather, they fail because they do not take into account the core characteristics and dominant behaviors of cyberspace. Some may also be counterproductive.

A New Approach

A new approach for cultivating conformance accepts that the dominant behavior requiring management, and ultimately regulation, is cyber persistence, which manifests as a threat through the malicious exploitation of cyber vulnerabilities. Cyber norm entrepreneurs seeking peace and stability must acknowledge and work through, rather than marginalize or disregard, cyber persistence. Thus, security-minded, status quo norm entrepreneurs must persistently and responsibly leverage exploitation-based activities that preclude, inhibit, or otherwise constrain behaviors inconsistent with proposed prohibitive norms. This approach to conformance holds promise because it acknowledges and aligns with cyberspace's structural imperative for achieving security—persisting in seizing and maintaining the initiative to set security conditions in one's favor by exploiting adversary vulnerabilities and reducing the potential for exploitation of one's own.[29]

This approach can reinforce explicit deliberations and also adapt more quickly to the rapid emergence of novel behaviors due to the dynamism of cyberspace and the ingenuity of malicious actors. Considering the UN processes as a valid indicator, it can take states years, if not decades, to first propose such behaviors as prohibitive norms and then deliberate about them through an explicit process. This is time during which unconstrained malicious behaviors threaten peace and stability. It is time better spent tacitly communicating to the malicious source by exposing, disrupting, and contesting threatening behaviors. Persistence supports tacit communication through an "unusually dense interaction" of cyber activities that creates a

[27] "Full Transcript: President Obama's Final End-of-Year Press Conference," *Politico*, December 16, 2016, https://www.politico.com/story/2016/12/obama-press-conference-transcript-232763.
[28] See Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory* and Michael P. Fischerkeller and Richard J. Harknett, "Initiative Persistence as the Central Approach for U.S. Cyber Strategy," *Kybernao* 1, no. 1 (July 2021), https://www.artsci.uc.edu/content/dam/refresh/artsandsciences-62/departments/political-science/ccsp/pdf_downloadableflyers/Kybernao_PaperSeries_Issue1_Final.pdf.
[29] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*.

"basic interpretive framework" for normative evaluation and conformance cultivation at the speed of relevance.[30]

A cyber-persistence-based approach also minimizes potential risks to instability relative to socialization (naming and shaming) and negative material inducements (economic sanctions). Covert operations scholarship suggests that secrecy dampens risks of instability by reducing potential pressures from domestic or other audiences and by allowing states to manage reputational concerns.[31] Leveraging the "open secrecy" of persistent, cyber campaigns is thus not just a more promising approach but also a more prudent one.[32] When considered in this light, overt naming and shaming, which seeks to exert such pressures to achieve conformance, may be counterproductive to stability. Similarly, material coercive inducements, given their coercive character, make the emergence of an escalation dynamic more likely than would responsible, persistent exploitative cyber campaigns.[33]

Operationalizing this New Approach

Cultivating conformance through a cyber persistence-based approach should aim to coordinate campaigns among government agencies with cyber capabilities and authorities and, where possible, private-sector actors having legal standing to engage in such behavior. Activities by the United States and its private sector serve as an example.

The U.S. Department of Defense (DoD) cyber strategy of defend forward as operationalized by U.S. Cyber Command's (CYBERCOM) doctrine of persistent engagement embodies the notion of achieving security through responsible, persistent exploitation-based operations, campaigns, and activities. By operating off the DoD Information Network, CYBERCOM seeks to preclude, inhibit, or otherwise constrain malicious cyber activity as close as practical to the threat source. This same doctrine can be leveraged to cultivate conformance with explicitly proposed prohibitive norms and to tacitly communicate a desired prohibition of emergent malicious

---

[30] Carson and Yarhi-Milo also refer to this process as establishing a communicative grammar that assigns meaning to observed covert behavior. Austin Carson and Keren Yarhi-Milo, "Covert Communication: The Intelligibility and Credibility of Signaling in Secret," *Security Studies* 26, no. 1 (November 2016): 126, 154.

[31] Carson and Yarhi-Milo, "Covert Communication: The Intelligibility and Credibility of Signaling in Secret": 124–156, 114 https://doi.org/10.1080/09636412.2017.1243921. Although Carson and Yarhi-Milo make this argument in the context of limited war, it applies equally well to cultivating conformance with proposed cyber norms.

[32] This "open secrecy" is possible because opponents expect that they have the capability to observe each other's covert activity. Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization* 70, no. 1 (Winter 2016): 103–131, 114, https://www.jstor.org/stable/24758287.

[33] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*. There is consensus among scholars studying state cyber behavior that coercion and escalation are not the dominant behavior and dynamic, respectively, in cyberspace. This is supported by the empirical record of the last 20 years showing that exploitation and competitive interaction are dominant.

behavior until a norm is explicitly proposed through a deliberative process. In fact, efforts to achieve security and cultivate norms in and through cyberspace must be deeply intertwined.

For example, to preclude technical disruption and interference in the U.S. 2020 election, USCYBERCOM reportedly engaged in an operation to temporarily disrupt what was then the world's largest botnet—Trickbot.[34] This provided an immediate security benefit. Were this operation extended and expanded to a persistent campaign, it could have served as a conformance mechanism for the GCSC proposed prohibitive norms that address technical infrastructure essential to elections and the commandeering of public's ICT resources for use as botnets.

Persistent campaigning is critical to cultivating conformance, as state and non-state actors can often quickly reconstitute cyber capability after being targeted with an exploitative operation. Two months after the CYBERCOM operation against Trickbot, its administrators had updated communication mechanisms and built a new command and control infrastructure based on a different router to better secure the infrastructure from exploitation.[35] Similarly, after a 2015 combined U.S. Federal Bureau of Investigation (FBI) and U.K. National Crime Agency (NCA) exploitation-based disruption operation against the Dridex botnet's command and control (C2) servers,[36] security vendors reported that Dridex was back in operation, albeit at a far lower capacity, less than 48 hours after the operation.[37]

CYBERCOM has reportedly targeted other malicious botnets, including a coordinated effort with the FBI and an unidentified third country to disrupt the REvil ransomware group in November 2021.[38] The FBI itself recently removed the CyclopsBlink C2 malware associated with a Russian APT-built botnet off of thousands of devices before it was activated toward malicious ends. It also closed the external management ports being exploited to access the C2 malware.[39] While these operations provided immediate security benefits, extending and expanding them into persistent campaigns could cultivate conformance to the proposed botnet prohibitive norm.

---

[34] Brian Krebs, "Attacks Aimed at Disrupting the Trickbot Botnet," *Krebs on Security*, October 2, 2020, https://krebsonsecurity.com/2020/10/attacks-aimed-at-disrupting-the-trickbot-botnet/.

[35] Liviu Arsene and Radu Tudorica, "Trickbot is Dead: Long Live Trickbot!" *BitDefender*, November 23, 2020, https://labs.bitdefender.com/2020/11/trickbot-is-dead-long-live-trickbot/.

[36] Matthew J. Schwartz, "Dridex Malware Campaign Disrupted," *BankInfoSecurity*, October 14, 2015, https://www.bankinfosecurity.com/dridex-malware-campaign-disrupted-a-8590.

[37] Eduard Kovacs, "Dridex Still Active after Takedown Attempt," SecurityWeek, October 19, 2015, https://www.securityweek.com/dridex-still-active-after-takedown-attempt.

[38] Ellen Nakashima and Dalton Bennett, "A Ransomware Gang Shut Down after Cybercom Hijacked Its Site and It Discovered It Had Been Hacked," *The Washington Post*, November 3, 2021, https://www.washingtonpost.com/national-security/cyber-command-revil-ransomware/2021/11/03/528e03e6-3517-11ec-9bc4-86107e7b0ab1_story.html.

[39] "Director Christopher Wray Announces Actions to Disrupt and Prosecute Russian Criminal Activity," FBI News, April 6, 2022, https://www.fbi.gov/news/press-releases/press-releases/director-christopher-wray-announces-actions-to-disrupt-and-prosecute-russian-criminal-activity-040622.

These responsible, exploitation-based operations also enable the United States to operationalize some of the positive duties outlined in the GGE and OEWG products, including protecting one's own infrastructure and supply chains and responsibly reporting vulnerabilities and sharing remedies. These duties are akin to anticipating persistent exploitation by malicious actors. CYBERCOM's hunt-forward operations enable anticipatory resilience by discovering adversary malware, techniques, tactics, and procedures as well as indicators of compromise and releasing this information through VirusTotal and Cybersecurity and Infrastructure Security Agency (CISA) alerts to inoculate U.S. companies from malicious cyber activity.

Many U.S. private sector companies have strong corporate incentives to support proposed prohibitive norms. Some also have the capability and legal standing to engage in exploitation-based activities. The U.S. government should encourage these companies to coordinate and bolster proposed prohibitive norms cultivation campaigns. As a case in point, consider Microsoft, a firm which has proposed prohibitive norms through its Digital Geneva Convention policy paper.[40] Its Digital Crimes Unit applies legal and technical solutions to identify, investigate, and disrupt malware-facilitated cybercrime and nation-state sponsored activity.[41] This helps cultivate conformance by state and non-state actors with the three GCSC-proposed prohibitive norms highlighted in this essay. Although no claims of coordination with CYBERCOM have been reported, less than two weeks after CYBERCOM disrupted Trickbot's operations, Microsoft engaged in operations toward that same end.[42] Microsoft has coordinated botnet disruptive operations with the FBI, including the 2013 operations against the Citadel and ZeroAccess botnets[43] and the recent disruption of the Zloader botnet.[44] However, there is no reported Microsoft coordination with CYBERCOM or the FBI specifically with the intent of cultivating conformance with proposed prohibitive norms.

Conclusion

The U.N. GGE and OEWG processes are not an immediate solution to ongoing cyber threats to peace and stability; but the processes support the continuing effort to create new, binding rules

[40] Microsoft, A Digital Geneva Convention to Protect Cyberspace, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH.
[41] Microsoft Digital Crimes Unit, https://news.microsoft.com/wp-content/uploads/prod/sites/358/2018/12/DCUOverview.pdf.
[42] See Tom Burt, "New Action to Combat Ransomware Ahead of U.S. Elections," Microsoft on the Issues, October 12, 2020, https://blogs.microsoft.com/on-the-issues/2020/10/12/trickbot-ransomware-cyberthreat-us-elections/ and David E. Sanger and Nicole Perlroth, "Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing the Same," The New York Times, October 12, 2020, https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html.
[43] Joseph Demarest, Assistant Director, Cyber Division, Federal Bureau of Investigation, Statement Before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, June 15, 2014, https://www.fbi.gov/news/testimony/taking-down-botnets.
[44] Amy Hogan-Burney, "Notorious Cybercrime Gang's Botnet Disrupted," Microsoft on the Issues, April 13, 2022, https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/.

of customary international law for the cyber context. The GCSC-proposed prohibitive norms are more credible and salient, but the conformance mechanisms being applied by states—persuasion, socialization (naming and shaming), and negative inducements (sanctions)—are failing. A new approach to conformance is needed, one that derives from the core characteristics of cyberspace—cyber persistence—and also, where possible, coordinates the actions of state agencies and private-sector actors based on common desired outcomes. This second track addresses the immediate security need and, in regard to state actions, further establishes state practice, which can converge with the *opinio juris* being coaxed from member states by the U.N. processes. In so doing, the stage will be set for new, binding rules of customary international law for the cyber context.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-06-22	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Cyber Persistence Way to Norms	HQ0034-19-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michael P. Fischerkeller	C5224
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305	NS D-33142

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 730 East Glebe Road, Alexandria, VA 22305	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michael P. Fischerkeller

14. ABSTRACT

The "usual way" for states to come to mutual understandings regarding norms of behavior threaten peace and stability in cyberspace. The United Nations Group of Government Experts and Open-Ended Working Group have resulted in deliberative products proposing peacetime cyber norms and an agreement that international law applies in the context of cyberspace. However, the prohibitive norms advanced do not address ongoing threatening behavior. And it will likely take years for states to reach agreements on how international law applies. Prohibitive cyber norms efforts need to immediately address ongoing state and non-state cyber behaviors that threaten peace and stability and a new approach to cultivating conformance is needed that acknowledges and leverages cyberspace's strategic imperatives and incentives for cyber persistence while also minimizing the potential for further instability.

15. SUBJECT TERMS

Cyberspace, cyber strategy, cyber norms

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	10	19b. TELEPHONE NUMBER (Include Area Code)