Beyond the United Nations Group of Governmental Experts

Norms of Responsible Nation-State Behavior in Cyberspace

Major General (Ret.) John A. Davis
VP, CSO (Federal) Palo Alto Networks

Charlie Lewis
MAJ, U.S. Army Reserve

While the September 2015 meeting between President Xi of China and President Obama of the United States seemed like a tipping point for norms in cyberspace, the United Nations Group of Governmental Experts (UNGGE) has been developing a useful set of norms for responsible conduct among nations in cyberspace for years. Although consensus was difficult to establish along the way, as it almost always is between nations, the Xi–Obama meeting started the process of establishing a broader agreement on a set of norms that was later endorsed by the Group of Seven and Group of 20. The endorsed norms followed previous agreements and focused on information sharing, cooperation, protection, and avoiding malicious activities within a state's borders, as well as human rights violations. States were to avoid using their territory for attacks against technologies or critical infrastructure, abstain from disrupting supply chain security, and refrain from using cyber means to harm other states. However, the UNGGE norms effort wavered during 2017 when several key countries backed away from the original agreement for a variety of reasons ranging from inability to enforce it to concerns around its effect on future operations.

Despite the struggles of previous norms efforts, opportunities exist to reframe norms around peacetime activities. This paper proposes five peacetime norms of behavior that responsible nation-states should strive to achieve. Responsible nation-states are those that act rationally, participate in other international norms and organizations, and have not demonstrated violations of other nations' sovereignty. The five proposed norms are designed to accomplish the following objectives:

1) Contribute to an improved, common, international understanding at the technical, operational, and policy levels of cyberspace activities
2) Reinforce positive and careful control and oversight of cyber activities
3) Bring additional responsible partners to the effort in more effective ways
4) Reduce risks and chances of misinterpretations that lead to mistakes and escalation

The following sections define each norm, provide examples, and discuss opportunities for implementation.

NORM #1

Responsible nations should be more transparent about what they are doing in cyberspace and why they are doing these things.

Applicable to law enforcement; homeland security; and, especially, the militaries of responsible nations, the goal of this norm is to increase transparency, not establish total transparency. If the majority of nations' actions were transparent, this would lead to greater trust and improve cooperation and teamwork on issues of common interest. To increase transparency, a responsible state can take actions that range from announcing the development of cyber forces to publishing a cyber strategy and overall goals. Law enforcement and homeland security can also discuss prohibited activities against which they protect. Increased transparency, however, is not a requirement for, or even within, an intelligence agency's DNA, which is why these organizations are excluded from this norm.

A previous example of increased transparency is the development of coalitions to address conflict, as was done in response to Saddam Hussein's invasion of Kuwait. The international community witnessed an illegal act, established transparency regarding objectives, and eventually launched a counter-invasion to free Kuwait. The United States spoke openly about the creation and structure of its cyber force and demonstrated when it was operational. The U.S. military distributed white papers about the establishment of the Cyber Mission Forces under U.S. Cyber Command and each of the Service Cyber Component Commands and briefed not only government and military partners of the U.S. around the world, but also countries such as Russia and China. These papers and briefings included information about the force composition, its purpose, its missions, and how it would be accountable and controlled by responsible oversight. Furthermore, the U.S. military publicly declared that it was conducting cyber operations against the Islamic State of Iraq and Syria in 2016. While not disclosing any classified information, these efforts demonstrated the U.S. military's increased transparency with not only other partners, friends, and allies around the world, but also competitors and potential adversaries.

Transparency, however, can be a hard goal to achieve. Typical norms, like maritime and space law, were derived by consolidating years of mutual activities and laws. They were built after years of documented and understood conduct; this was not the case with cyber norms. Moreover, for transparency norms to succeed, major actors need to participate, which is unlikely. Despite these concerns, one dynamic that makes increased transparency possible is the increasingly lower bar for classification of all things related to cyber. There are open, even public discussions today that simply could not have occurred only a few years ago. Additionally, recent public examples of greater transparency in threat attribution include the North Korean attack against Sony Pictures Entertainment; the Iranian distributed denial-of-service attack on the U.S. financial sector; and, most recently, Russian interference in the 2016 presidential election. There is a good reason to increase clarity, accuracy, and transparency by bringing these activities into the light of law enforcement; domestic security; and, especially, uniformed military operations to contribute to a reduction in uncertainty and an increase in stability.

NORM #2

Responsible nations should establish and enforce standardized procedures for effective oversight of military, law enforcement, and homeland security cyber operations.

Standards for bureaucratic oversight provide the layers of decision-making to ensure that norms and other requirements are met in cyberspace. Furthermore, procedural oversight includes risk management assessment and control procedures that contribute to the following five effective outcomes.

1) **First** is domestic and foreign policy oversight from a competent authority as established by the nation so that adequate consideration is given to the potential impact on both domestic and foreign reactions to the implementation of a cyber activity if it is discovered.

2) **Second** is technical oversight, which includes a “technical gain versus loss” assessment to address the unintended consequences resulting from the discovery of the technical capability and its use against other targets or the nation that used it in the first place. In addition, this is also a “technical assurance assessment”, which provides low, medium, and high assurance levels that the capability will produce technical outcomes or effects as intended and not produce unintended consequences, such as escalation or cascading effects.

3) **Third**, operational oversight with appropriate responsibilities, accountability, and command and control procedures that verify positive control within an authorized chain of command reinforces these risk management processes.

4) **Fourth** is intelligence oversight, including an “intelligence gain versus loss” assessment, which provides the consequences of exposure to and potential loss of intelligence sources and methods and the resulting insight if the cyber operation or capability is discovered or revealed.

5) **Fifth** is legal oversight, including two types of legal review that provide an assessment for both the capability and the operation as it applies to either the International Law of Armed Conflict or other applicable domestic and international laws and agreements.

Responsible nations applied these oversight norms during the post–Cold War era and trusted others to do the same. Nuclear treaties, the law of armed conflict, and an understanding about the effect of their use has resulted in a minimal threat from responsible nations, and may also explain why the international community signed a treaty to prevent Iran from developing its own nuclear weapons. Oversight for cyber operations is much more difficult to ascertain. While the United States lays out its various legal codes in its military cyberspace manual, Joint Publication 3-12, it is still looking to adjust the approval process for cyberspace operations. Other nations as well may have different sets of controls over their cyberspace operations during peacetime, as made evident by the Chinese use of civilian hackers.

Many believe this norm should apply to intelligence operations as well. Notably, most nations' significant cyber capabilities began within their own national and military intelligence organizations for the purpose of espionage. In many cases, the reckless use of intelligence cyber activities can significantly complicate the cyber environment, making it increasingly difficult to determine intentions, and can lead to misperceptions, miscalculations, and mistakes in cyberspace that might "spill over" into the physical world in an unwarranted escalation. There is definitely a case to be made for addressing espionage activities in cyberspace within the norms discussion. However, perhaps the topic of intelligence cyber operations and activities is something to be addressed separately due to the likelihood that its inclusion in an open discussion would significantly complicate nations' ability to make progress.

NORM #3

Responsible nations should share cyber threat intelligence on criminal and terrorist threats of common interest.

Information sharing and alerting about terror threats and large criminal operations is standard amongst states. Within cyberspace, however, there is much less openness, as it could potentially give away operations. Instead of withholding information, responsible nations should establish and enforce effective information sharing programs and platforms that are automated and format-standardized to account for the speed and scale of today's modern criminal and terrorist cyber threats. These cyber threat intelligence and information sharing programs should be focused on cyber threat indicators of compromise along the cyber threat life-cycle steps as well as contextual information. However, a certain level of sanitization is required. These reports should not include personally identifiable information; protected health information; intellectual property content; or other types of information that create surveillance, privacy, and liability issues. Cyber threat information sharing should be done government-to-government through appropriate diplomatic, law enforcement, domestic security, intelligence, and military channels. In addition, responsible nations should encourage sharing programs and platforms between government and industry and among industry entities as appropriate to national and international laws and agreements. The result of increased and effective information sharing as described is to help reduce the "noise-to-signal" ratio so that responsible nations are able to better focus on what is important and not be confused or distracted by the ever-increasing amount of cybercriminal and terrorist activity that might cloud an already confusing cyber landscape and contribute to misinterpretation, miscalculation, mistakes, and inadvertent escalation.

This norm currently exists in the signals intelligence world under the United Kingdom–

United States of America agreement among the United States, the United Kingdom, Canada, Australia, and New Zealand. Established to codify information sharing principles that occurred during World War II, the agreement leveraged that success to create an information sharing practice between the British Empire and the United States. The agreement not only shows how effective information sharing occurs, but also demonstrates how to adapt it for new technologies, as the partnership still exists today.

Opponents of information sharing rely on the same argument that proponents of transparency do—providing information may give away trade secrets or cause malicious state actors to change their methods to avoid capture. In addition, the example cited is the result of success in World War II and occurred during a time of liberal institutional growth and trust. Today, however, a lack of the same trust is more evident, causing some to question the agreement's effectiveness. The U.S. Cybersecurity Information Sharing Act of 2015, which attempted to reduce these concerns, demonstrated an increase in the collective ability to chase down common enemies and reduce noise in cyberspace.

NORM #4

Responsible nations should encourage and incentivize increased industry participation in the development and enforcement of these and additional norms of responsible behavior in cyberspace.

Industry owns, operates, and maintains the vast majority of the underlying infrastructure and technology of cyberspace, yet the norms discussion has traditionally involved government only, as in the case of UNGGE. Industry's involvement would make the norms more practical and effective, partly because industry better understands the role that government should play in the digital environment. Many contentious issues today, such as mandatory backdoors for law enforcement, counterterrorism, and intelligence purposes; restriction of cross-border data flows; private-sector hack back; and supply chain risk management warrant industry's involvement. The Australian Strategic Policy Institute has done some excellent research on a greater role for industry in the development of cyberspace norms, highlighting the success of the United States' consortium while developing a structure for trusted information flow within Australia. Additionally, the Carnegie Endowment for International Peace has taken a detailed look at how to more effectively apply norms that could impact global stability in financial markets and the international monetary system by not manipulating or damaging financial institutes' data. Many companies have taken positions on the technology industry's role in cyberspace norms, and some have attempted to join the cause to establish greater protection from cyber threats.

Global incentives and trust can be difficult to form. Sharing ideas and secrets in a transparent manner can create opportunities for malicious actors to conduct reconnaissance. A violation of this trust or even the perception of a lack of trust may end any cooperation between international industry and government.

NORM #5

During peacetime, responsible nations should NOT deploy loosely controlled third-party actors and organizations to engage in cyber activities.

The use of surrogates, front companies, “technical research” organizations, criminal entities, moonlighters, and even patriotic hackers limits government control over actions and can violate the transparency and trust created by the previous four norms. These types of actors and organizations increase uncertainty, reduce stability, and lack the oversight and control discussed in norm #2. They are driven by an assortment of high-risk motivations and increase the chance of a miscalculation in attribution, as described in norm #3, which could result in an unacceptably high risk of escalation, especially during times of high tension. The prevention of the use of these actors increases the likelihood of the other norms succeeding. Unfortunately, the world has seen the increased use of loosely controlled third-party entities by nation-states. This is an alarming trend because the risk of a mistake happening or an unsanctioned action being perpetrated by someone with a personal grievance is growing exponentially, and all responsible nations should share a common interest in preventing these events from occurring.

The above norms of responsible nation-state behavior in cyberspace, supported by the increased involvement of global industry, are designed to accomplish improvements to contribute to an improved international understanding, reinforce positive and careful control and oversight of cyber activities, and more effectively encourage the participation of responsible partners. However, questions remain about the degree to which these norms are feasible. The U.S. Government and an increasing number of U.S.-based, private-sector cybersecurity companies not only think that the norms will work, but are increasingly and actively pursuing each of norms proposed in this paper. The U.S. military has already led the way on the first two proposed norms. Additionally, the U.S. Congress focused its Cyber Information Sharing Act of 2015 on the third and fourth norms, and U.S. law enforcement, domestic security, intelligence, and even military organizations are implementing many cyber threat intelligence and information sharing programs with an increasing number of international and industry partners. The United States is leading by example in the effort to establish norms of responsible behavior. The United States should be willing to engage with other great nations to broaden this effort, make these norms an international standard, and improve upon them in a progressive manner.

NOTES

1. Garrett Hinck, “Private-Sector Initiatives for Cyber Norms: A Summary,” *Lawfare*, June 25, 2018.
2. The Department of Defense, *The DoD Cyber Strategy*, April 2015.
3. James Van De Velde, “Why Cyber Norms are Dumb and Serve Russian Interests”, The Intercept, June 6, 2018.
4. Department of Defense, *Joint Publication* 3-12, Department of Defense, June 2018.
5. Guest Blogger for Net Politics, “When China’s White-Hat Hackers Go Patriotic,” *Council on Foreign Relations*, retrieved from https://www.cfr.org/blog/when-chinas-white-hat-hackers-go-patriotic.
6. Excluding the five eyes consisting of the United States, Great Britain, Canada, Australia, and New Zealand.
7. UKUSA Agreement Release 1940-1956, retrieved from https://www.nsa.gov/news-features/declassified-documents/ukusa/ on 10/9/2018.
8. Van De Velde.
9. Liam Nevill, “Cyber Information Sharing: Lessons for Australia”, *Australian Strategic Policy Institute,* May 2017.
10. Tim Maurer, Ariel Levite, George Perkovich, “Toward a Global Norm Against Manipulation the Integrity of Financial Data,” *Carnegie Endowment for International Peace*, March 27, 2017.
11. Hinck.