"Beyond the United Nations Group of Governmental Experts:
Norms of Responsible Nation State Behavior in Cyberspace"

by
Major General (Ret) John A. Davis
VP, CSO (Federal) Palo Alto Networks
and
Charlie Lewis
MAJ, US Army Reserves

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) had developed a useful set of norms for responsible behavior in cyberspace between nations over years. Although consensus – as it almost always is between nations - was difficult and uneven along the way, the Xi -Obama meeting started the process of a broader agreement on a set of norms that the G7 and then G20 later supported. The endorsed norms followed previous agreements and focused on information sharing, cooperation, protection, and avoiding malicious activities within a state's borders as well human rights violations. States were to avoid using their territory for attacks against technologies or critical infrastructure, not disrupt supply chain security, and should not harm other states through cyber means.[1] While considered a start of the discussion surrounding cyber norms, 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 or concerns around disadvantaging 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 nation's 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 existing examples, and discuss opportunities for implementation.

[1] Hinck, Garrett, "Private-Sector Initiatives for Cyber Norms: A Summary," *Lawfare*, June 25, 2018

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 with the militaries of responsible nations, this norm desires an increase in but not total transparency. Transparency for most actions can lead to greater trust, improving 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 that they protect against. Increased transparency, however, is not a requirement for, or even within, an intelligence agency's DNA, which is why they are excluded from this norm.

Previous examples of increased transparency include developing coalitions for conflict, as was done in response to Saddam Hussein's invasion of Kuwait. The international community witnessed an illegal act, providing transparency regarding objectives, and eventually launched a counter-invasion to free Kuwait. In cyberspace, the United States spoke openly about the creation and structure of its cyber force, including demonstrating when it was operational. The US military distributed white papers about the establishment of the Cyber Mission Forces under US Cyber Command and each of the Service Cyber Component Commands and briefed not only government and military partners of the US around the world, but countries such as Russia and China as well. These papers and briefings included information about the force composition, its purpose, missions and how it would be accountable and controlled by responsible oversight. Furthermore, the US military publicly declared that it was conducting cyber operations against ISIS in 2016. While not disclosing any classified information, these efforts demonstrate the US military's increased transparency with not only other partners, friends and allies around the world, but also with competitors and potential adversaries.[2]

Transparency, however, can be a hard goal to achieve. Typical norms, like law of the sea and space, were derived by consolidating years of mutual activities and laws. They were built after years of documented and understood conduct unlike the approach to cyber norms. Moreover, for transparency norms to succeed, large actors also need to participate, which is unlikely.[3] Despite these concerns, one dynamic making 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 DDoS of the US Financial Sector, and most recently the Russian 2016 election interference. There is good reason to increase clarity, accuracy and transparency by bringing these activities into the light of law enforcement,

[2] The Department of Defense, *The DoD Cyber Strategy,* April 2015

[3] Van De Velde, James, "Why Cyber Norms are Dumb and Serve Russian Interests", The Intercept, June 6, 2018

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 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. First, 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 reaction to the implementation of a cyber activity if it is discovered. Second, 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 turned against the nation using it. In additional, this is also a "technical assurance assessment", which provides low, medium, 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. Third, operational oversight with appropriate responsibilities, accountability, and command and control procedures that verify positive control within an authorized chain of command reinforce these risk management processes. Fourth, intelligence oversight, including an "intelligence gain versus loss" assessment, which provides the consequences of exposure and potential loss of intelligence sources, methods and resulting future insight if the cyber operation or capability is discovered or revealed. Finally, legal oversight including two types of legal review that provide an assessment for both the capability and for 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 – and trusted others to do the same - these oversight norms during the post-Cold War era. Nuclear treaties, the law of armed conflict, and an understanding about the effect of their use has resulted in minimal threat from responsible nations and may also explain why the international community signed a treaty to prevent Iran from developing their 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's cyberspace manual, Joint Publication 3-12, it is still looking to adjust the approval process for cyberspace operations.[4] Other nations as well may have different sets of controls on their cyberspace operations during peacetime, as evident by the Chinese use of civilian hackers.[5]

[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

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 with 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 therefore 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 aspect of intelligence cyber operations and activities is something to be addressed separately due to the likelihood that inclusion of them in an open discussion of this proposed norm will significantly complicate the ability to make progress.

Norm #3

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

Information sharing and alerting about various threats is standard amongst states for terror threats and large criminal operations. Within cyberspace, however, there is much less openness as it may give away operations.[6] 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 matching 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 (PII), protected health information (PHI), intellectual property (IP), content, or other types of information that create surveillance, privacy and liability policy and legal issues. Cyber threat information sharing should be done government to government in appropriate diplomatic, law enforcement, domestic security, intelligence and military channels. In addition, responsible nations should encourage sharing programs and platforms between government and industry, between industry and government, 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 cyber-criminal 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 UKUSA agreement between the United States, England, Canada, Australia, and New Zealand. Established to codify information sharing principles that occurred during World War II, the agreement leveraged that

[6] Excluding the five eyes consisting of the United States, Great Britain, Canada, Australia, and New Zealand

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.[7]

Opponents of information sharing rely on the same argument as transparent operations – providing information may give away trade secrets or cause malicious state actors to change their methods to avoid capture. In addition, the example cited was the result of success in World War II and occurred during a time of liberal institutional growth and trust. Today, however, a lack of that same trust is more evident, bring some to question effectiveness[8]. The US Cybersecurity Information Sharing Act of 2015 worked to reduce those concerns and demonstrated how 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 been government only, as in the case of the UNGGE. Industry's voice is important because the norms will be more practical and can be enforced by industry much more effectively than government by supporting government efforts or at least understanding the role government ought to play within the digital environment. Many contentious issues today, such as mandatory backdoors for law enforcement, counter terrorism and intelligence purposes, restriction of cross border data flows, private sector hack-back, and supply chain risk management all deserve industry's voice. 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.[9] 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 the financial markets and international monetary system by not manipulating or damaging financial institutes' data.[10] Many companies have taken positions about the technology industry's role in cyberspace norms and there's been recent outreach by many technology companies to join the cause for greater protections from cyber threats.[11]

---

[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

Global incentives and trust can be difficult to form. Sharing of ideas and secrets around security in a transparent manner may 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 international industry and government cooperation.

Norm #5

During peacetime responsible nations should NOT employ 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, lack the oversight and control as 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 that could result in an unacceptably high risk of escalation, especially during times of high tension. Preventing their use supports the success of the other norms. Unfortunately, the world is seeing an increasing use of loosely controlled third party entities by nation states. This an alarming trend because the risk of a mistake happening, or an unsanctioned action by someone with a personal motivation that results in significant consequence, is growing exponentially and there should be a common interest from all responsible nations to prevent that from happening.

The above norms of responsible nation state behavior in cyberspace, supported by a greater role from global industry, are designed to accomplish improvements to contribute to an improved international understanding, reinforcing positive and careful control and oversight of cyber activities, and bringing responsible partners to the effort in more effective ways. The key question, however, is are these norms realistic? The United States government, and an increasing number of US based cybersecurity private sector companies not only think norms will work but are increasingly and actively pursuing each of norms proposed in this paper. The US military has already led the way on the first two proposed norms. Additionally, the US Congress has focused its Cyber Information Sharing Act of 2015 on the third and fourth norms and both the US government law enforcement, domestic security, intelligence and even military organizations are implementing many various cyber threat intelligence and information sharing programs with an increasing number of international and industry partners. The United States can and is leading by example in these norms of responsible behavior. The US should be willing to engage with other great nations to broaden this effort, make it an international standard, and even improve upon it.