Microsoft

From Articulation to Implementation:

Enabling progress on cybersecurity norms

June 2016

Scott Charney

Erin English

Aaron Kleiner

Nemanja Malisevic

Angela McKay

Jan Neutze

Paul Nicholas

Building trust in technology through cybersecurity norms

The global dialogue on cybersecurity norms is evolving from a conceptual discussion about nation-states' rights and responsibilities toward an articulation of norms of state and industry behavior. Stakeholders from governments, the private sector, academia, and civil society are putting forward myriad norms proposals, addressing a range of challenges caused by exploitation of information and communications technology (ICT) systems. These proposals vary in their prescriptions. For example, most norms proposals from governments and international organizations recognize that nation-states should not permit malicious cyber activity to emanate from their territory and that critical infrastructures should not be targeted by cyber attacks in times of peace. However, only some proposals have acknowledged that nation-states should not compromise the ICT supply chain, and only a few recognize the need for public/private sector collaboration on norms.

Even though governments have acknowledged that international laws apply to the Internet, such laws are static and binding and do not necessarily address well new cyberspace scenarios. Greater experience with such scenarios is important and, therefore, stakeholders in cyberspace have advocated for the development and implementation of norms before creating new laws. There is great risk in moving hastily to apply new laws to cyberspace. Moreover, drafting them is inadvisable because the impact of such laws, in part due to the lack of scenario experience, may be problematic. Accordingly, stakeholders in cyberspace should endeavor to develop and implement norms before they are codified.

This paper addresses the development of cybersecurity norms. First, we put forward an organizing model for developing cybersecurity norms, built around three categories of proposed norms: offensive norms, defensive norms, and industry norms. We then outline the key elements necessary for further refinement of these proposals, using our four-part framework of actors, objectives, actions, and impacts.[1] This analysis is intended to guide further deliberations on proposed norms and to ultimately enable instantiation of norms in state practice, public policy, and law.

This paper then turns to the problem of implementation of cybersecurity norms, specifically two challenges in verifying compliance with agreed-upon norms. First, global connectivity, anonymity, and lack of traceability make the attribution of cyberattacks particularly difficult and allow actors to simply make blanket denials and assert lack of proof. Second, there are reasons not to act on information about an attacker, even if a government or private sector entity has evidence of attribution. Therefore, it is perhaps not surprising that norms agreements have been met with skepticism.

It is exceedingly difficult to isolate assets in cyberspace.

The global ICT industry's role in cybersecurity norms

Cybersecurity norms are particularly important to Microsoft, and the wider industry, because they will impact our customers, products, and services. In fact, it is commercial mass-market ICT, and the underlying infrastructure used to develop and operate it, that is often the battlefield for cyber conflicts and conduit for other attacks launched by governments and their proxies. Additionally, these ICT systems may be themselves targeted with serious implications for all ICT users.

Part of the problem is that it is exceedingly difficult to isolate assets in cyberspace. Collateral damage to the ICT ecosystem stemming from attacks against potential government and/or military targets can be difficult to foresee.[2] There are acute challenges in maintaining proportionality and precision in the deployment of offensive and defensive measures,[3] and errors can result in significant risks to ICT users, including considerable re-engineering costs across industry sectors, and other negative consequences. Paradoxically, governments and their proxies look to the global ICT industry to prevent, detect, respond to, and recover from nation-state attacks.

Microsoft is not alone in recognizing the need for an industry role in cybersecurity norms, nor would industry engagement in norms be unique. In its most recent report, the United Nations Group of Governmental Experts noted that the private sector and civil society should contribute to the development of cybersecurity norms.[4] This approach follows other scenarios where private sector engagement plays a critical role in ensuring the success of norms. For example, the Financial Action Task Force (FATF) routinely engages directly with financial institutions to understand the impacts of new and existing FATF guidelines, while the private sector uses certain FATF gatherings to raise issues of its own.[5] Similarly, the International Civil Aviation Organization, its member states, and industry stakeholders have collaborated for the better part of 70 years to create a successful regulatory framework.[6]

Input from the global ICT industry is also critical to ensuring that the language of cybersecurity norms accurately reflects the realities of defending technology users at global scale.

Input from the global ICT industry is also critical to ensuring that the language of cybersecurity norms accurately reflects the realities of defending technology users at global scale. With this practical guidance, norms implementation should become more feasible. By way of example, industry was not consulted adequately when governments negotiated changes to the Wassenaar Arrangement, and this resulted in the severe misunderstanding of the tools necessary for effective cybersecurity risk management and made the export restrictions on penetration testing software impractical and counterproductive.

Industry must also have an avenue to contribute to norms implementation, particularly with regard to technical elements of attribution. As described in depth later in this paper, industry often has technical information that can improve the threshold determination of whether an attack was launched by a nation-state. Moreover, industry is often best positioned to identify the key lessons from nation-state attacks, leveraging information about tactics, techniques, procedures, and indicators of compromise to strengthen defenses for technology users worldwide.

An organizing model for cybersecurity norms development

The cybersecurity norms dialogue is ready for an organizing model, particularly with regard to the challenge of disaggregating norms proposals into discrete areas for further refinement. As a starting point, categorization of proposed norms should begin with an analysis of the current state of the norms dialogue. The recent trend toward articulation of proposed norms is demonstrated in six governmental proposals that are currently driving the global dialogue on cybersecurity norms.[7] In chronological order, these governmental proposals are:

- Confidence building measures developed by the Organization for Security and Co-operation in Europe and published in December 2013 (OSCE CBMs)[8]
- The Code of Conduct submitted to the United Nations General Assembly by member states of the Shanghai Cooperation Organisation in January 2015 (SCO proposal), which is an updated version of similar submissions by this group[9]
- Norms outlined in remarks delivered US government officials in May 2015 (USG proposals)[10]
- Norms, confidence building measures, and related recommendations by the UN Group of Governmental Experts in June 2015 (UNGGE report), which is a follow-on to prior reports from this group[11]
- Agreement between the United States and China in September 2015 regarding cyber-enabled theft of intellectual property, law enforcement collaboration, and other cybersecurity measures (US-China agreement)[12]
- G20 Leaders Communique from the G20 regarding cyber-enabled theft of intellectual property, privacy, and international collaboration for cybersecurity (G20 Communiqué)[13]

In our 2014 white paper, *International Cybersecurity Norms: Reducing conflict in an Internet-dependent world*, Microsoft proposed six cybersecurity norms.[14] Our proposed norms, which are intended to protect global trust in technology and to protect ICT users, touch upon several important considerations for both cyber offense and defense: limiting nation-state activity against commercial, mass-market ICT; responsible handling of ICT vulnerabilities and cyber weapons; appropriate conduct of offensive operations in cyberspace; and support for private sector management of cyber events.[15]

Two categories of norms—offensive norms and defensive norms—have emerged from these norms proposals. These categories—self-restraint in the conduct of offensive operations and appropriate defensive norms—are complementary. For example, if countries agree that their Computer Emergency Response Teams (CERTs) should collaborate in the interests of network defense, a complementary offensive norm ensuring that CERTs are not attacked is equally important.

Stakeholders have suggested that there should also be norms for the global ICT industry. Microsoft is often asked about whether we would commit to certain norms, given that we have called upon governments to make such commitments. The answer is yes, and this paper outlines six industry norms that are reflective of both current practices and aspirational goals for the global ICT industry.

In the table that follows, we present these three norms categories against the four-part framework from our prior cybersecurity norms white paper, with the addition of a fifth element. We believe that this framework helps to identify key actors involved in developing and abiding by norms, those actors' objectives in the norms process, the necessary actions by those actors to accomplish these objectives, and the impacts of these actions, along with the forums for further refinement of norms proposals by those actors.

Following this table are discussions of each category with an emphasis on industry norms:

Categories	Actors	Objectives	Actions	Impacts	Forums
Offensive norms	Nation-states, particularly militaries and intelligence agencies	Reduce conflict between states, lower the risk that offensive operations escalate, and prevent unacceptable consequences	Exercise self-restraint in the conduct of offensive operations	Mitigate unacceptable impacts of ICTs by governments	Inter-governmental bodies
Defensive norms	Public and private sector cyber defense teams	Manage cybersecurity risk through enhanced defenses and incident response	Collaborate among defenders (such as sharing information and best practices, coordinating responses)	Protect government, enterprise, and consumer users of ICT	Cyber defense organizations
Industry norms	Global ICT companies	Deliver secure products and services	Support defense and refrain from offense	Protect ICT users and enhance their trust in technology	Global ICT market and emerging leadership venues

Offensive norms

There is growing convergence around offensive norms, or norms to guide offensive operations in cyberspace. In practice, offensive norms require that governments exercise some form of self-restraint in conducting offensive operations in cyberspace. International law often provides the basis for these limitations, consistent with nation-states' responsibilities under the UN Charter and other international legal instruments, as acknowledged throughout the UNGGE report and its predecessors.[16]

For example, there are several measures of self-restraint that appear in most of the norms proposals cited above: states should refrain from attacking critical infrastructures;[17] and states should refrain from impairing the work of CERTs (with both the USG and UNGGE further clarifying that CERTs should not be used in offensive operations).[18] Recently, in both the US-China Agreement and the G20 Communiqué, leading governments have acknowledged that cyber-enabled theft of intellectual property should be prohibited.[19] This development is particularly interesting because it applies to the conduct of intelligence agencies, which have typically operated outside of international governance.

In offensive norms, the key actors are nation-states, and primarily their militaries and intelligence agencies. They will be responsible for interpretation of—and adherence to—offense norms in the fulfillment of their missions. The objectives of offensive norms are to reduce conflict between states, lower the risk that offensive operations will escalate, and prevent unacceptable consequences. With respect to the actions necessary to accomplish this objective, offensive norms require self-restraint with respect to military and intelligence functions. Thus, offensive norms could be considered norms of inaction because success is achieved when nation-states choose not to undertake actions that violate emerging boundaries of responsible behavior. The impact of offensive norms is to reduce the risk of international conflict and to serve to protect ICT users, from governments to citizens, who are dependent on technology for most aspects of daily life.

Further development of these norms should be led by intergovernmental forums, including the following organizations and venues:

- G20, which has a vested interest in limiting cyber conflict because of the global financial system's reliance on secure and resilient ICT
- Global Conferences on Cyberspace process, through which governments and other stakeholders have driven a dialogue about cybersecurity norms, with helpful outcome statements that provide milestones in norms development
- OSCE, which has led the development of confidence building measures, which articulate a number of transparency measures and which enable voluntary exchanges of information and communication among states on several levels, from the practitioner to the policy-making and national security level
- SCO, an important contributor to the cybersecurity norms dialogue by delivering a shared perspective from two of the world's largest Internet user hubs, China and Russia, and several emerging economies with close ties to these global leaders
- UNGGE, which is the preeminent forum for development of cybersecurity norms and includes many of the leading governments as participants
- The United Nations Institute for Disarmament Research (UNIDIR), which has been analyzing cybersecurity and cyber norms for several years and continues to bring stakeholders from governments and the private sector together to advance cyber norms

Defensive norms

There is also convergence around defensive norms, or norms that enable cybersecurity risk management through enhanced defenses and incident response. These norms stem from nation-states' acknowledgment that cyber defense is a collaborative exercise, requiring cross-border partnerships and joint action against cybersecurity threats.

Some proposed defensive norms complement offensive norms. For example, as a complement to offensive norms against nation-states' targeting of critical infrastructure, most defensive norms proposals encourage governments to take measures to protect critical infrastructure from ICT threats. Most defensive proposals also encourage nation-states to support others victimized by cyber attacks.

There are more specific recommendations aimed at protecting sensitive assets, such as the ICT supply chain and cyber vulnerabilities. Both the UNGGE and Microsoft recommend responsible handling of cybersecurity vulnerabilities, which has been substantiated in US policy as demonstrated by the White House's public comments about the US government's approach to vulnerability management.[20]

Additionally, there is convergence on the importance of securing the ICT supply chain from attack, as called for in proposals from the UNGGE, SCO, and Microsoft.

With respect to the actors needed to further develop defensive norms, unfortunately, most norms proposals fail to acknowledge that defensive norms require engagement from cyber defenders across the public and private sectors. Indeed, participation from both government and industry is often required to achieve the objective of managing cybersecurity risk through enhanced defenses and incident response. The actions necessary for this objective show that both public and private sectors have roles to play. In some cases, actions may be strictly limited to players from a particular sector (including execution of a search warrant by police) but many activities in this space often depend upon the active participation of public and private sector players (such as disruption of a global botnet and sink-holing of its command-and-control server[s]). To put it simply, the ultimate impact of this work is improved protection of government, enterprise, and consumer users of ICT. However, unlike the self-restraint expressed in offensive norms, defensive norms require a high level of collaborative and purposeful work.

Further dialogue on these norms should be driven through collaborative processes that can involve public and/or private sector players. Forums that could serve for this include:

FIRST, an international organization composed of incident response teams from public, private, and academic sectors, with representation in nearly every country. Because of FIRST's focus on incident response, and because participation is not limited to one sector, it is an ideal forum for discussions about normative practices for cyber defense and incident response in particular.
Engagements with like-minded countries via mutual legal assistance treaties (MLATs), which are important to facilitating cyber defense because they enable law enforcement activity that may be targeted at cyber attackers and facilitate the transfer of information about the use of ICTs to accomplish criminal activity.
United Nations Office on Drugs and Crime (UNODC), which is responsible for assisting member states to find common strategies to combat their own efforts against illicit drugs and cyber crime.

Industry norms

Norms are not just for governments. Technology users in enterprises and at the consumer level have expectations of the ICT industry as well. In this regard, it is important to recognize that industry is not monolithic; not every provider of IT services can be bound by the same rules. Global ICT providers, who make global, mass-market products, in order to protect their customers and be successful in the global marketplace, must focus exclusively on protecting users. They cannot participate in offensive activities and help one customer attack another. By contrast, there are companies that work for a single government and may be involved in providing IT support for military operations, even helping to build cyber weapons. Clearly, those companies that take sides in geopolitical conflicts may be in a different position than global, mass-market suppliers, and may be beyond the purview of these norms.

Global ICT providers must agree to norms that enhance trust in ICT systems. Most notably, companies must be clear that they will neither permit backdoors in products nor withhold patches, either of which would leave technology users exposed. They will also address attacks—whatever their source—to protect customers. These norms, like government defensive norms, are meant to increase confidence in the global ICT supply chain, and to send a clear message to governments that global ICT providers will not help exploit ICT users, but will only help protect them.

The chart that follows provides a side-by-side view of Microsoft's proposed norms for nation-states, with our corresponding proposals for industry norms, followed by discussion of each proposed industry norm. While there is a strong complementary structure for nation-state norms and industry norms, they vary in two important instances: nation-states possess the ability to create mass effects through offensive cyber activities; and the global ICT industry has the ability to patch all customers, even during conflicts between and among governments.

Desired impacts of Microsoft's proposed norms	Cybersecurity norms proposed by Microsoft for nation-states	Cybersecurity norms proposed by Microsoft for the global ICT industry
Maintain trust	States should not target global ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.	Global ICT companies should not permit or enable nation-states to adversely impact the security of commercial, mass-market ICT products and services.
Coordinated approach to vulnerability handling	States should have a clear, principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.	Global ICT companies should adhere to coordinated disclosure practices for handling of ICT product and service vulnerabilities.
Stop proliferation of vulnerabilities	States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.	Global ICT companies should collaborate to proactively defend against nation-state attacks and to remediate the impact of such attacks.
Mitigate the impact of nation-state attacks	States should commit to nonproliferation activities related to cyber weapons.	Global ICT companies should not traffic in cyber vulnerabilities for offensive purposes, nor should ICT companies embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes.
Prevent mass events	States should limit their engagement in cyber offensive operations to avoid creating a mass event.	No corresponding norm for the global ICT industry.
Support response efforts	States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.	Global ICT companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace.
Patch customers globally	No corresponding norm for nation-states.	ICT companies should issue patches to protect ICT users, regardless of the attacker and their motives.

Global ICT companies should not permit or enable nation-states to adversely impact the security of commercial, mass-market ICT products and services.

Industry commitments against permitting nation-state interference with commercial, mass-market ICT products and services are as important as joint commitments from nation-states not to, for example, insert backdoors themselves. If governments refuse to engage in such conduct, and industry reinforces this through its own complementary norm, public concern about collusion between government and ICT vendors should decrease; violation of the norm now requires malfeasance by two separate actors, both with reasons to refrain from such conduct.

Global ICT companies should adhere to coordinated disclosure practices for handling of ICT product and service vulnerabilities.

Nation-state activity in cyberspace often depends upon exploitation of vulnerabilities in ICT products and services. One of the best mitigations against this risk is coordinated vulnerability disclosure. The global ICT industry benefits from vulnerability research and the reporting of ICT vulnerabilities, which are valuable tools for securing the ICT ecosystem. Indeed, coordinated vulnerability handling is continuing to mature as a defined set of practices.[21] For example, international standards driven by industry leaders set forth appropriate practices, including a five-step process that guides vendors through initial receipt and verification of the vulnerability, developing a resolution, releasing the final fix, and communication with ICT users after the fix is released. Because releasing exploit information before there is a patch puts users at risk, and because the exploitation of vulnerabilities in one product or service can often serve as the bridge to exploitation of vulnerabilities in other products and services, ICT users collectively benefit when vulnerabilities are reported and handled in a coordinated way.

Global ICT companies should collaborate to proactively defend against nation-state attacks and to remediate the impact of such attacks.

Global ICT companies may observe nation-state attacks because of the private sector's access to telemetry and visibility into network activity. Additionally, global ICT companies are often the first responders for cyber events, protecting their users and infrastructure against sophisticated threats. However, the impact of nation-state attacks may be felt across multiple companies, and efforts to protect against or respond to these events can be bolstered through collaboration across defense organizations from different companies. Accordingly, global ICT companies should seek opportunities to collaborate in the face of the shared threat posed by nation-state activity.

Global ICT companies should not traffic in cyber vulnerabilities for offensive purposes, nor should ICT companies embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes.

There have been numerous reports of nation-states buying zero day vulnerabilities on the black market.[22] Though governments will inevitably pursue vulnerabilities for offense and there will always be vendors willing to meet that demand, the global ICT industry should not support that market but rather leverage publicized bug bounty programs. When global ICT companies choose to participate in a black market, they are contributing to a vicious cycle that can ultimately lead to attacks against critical systems and against their own users.[23]

Global ICT companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace.

Just as we have called upon nation-states to support the private sector in defending against and recovering from events in cyberspace, industry should make a concomitant pledge to governments: industry's role in supporting governments must be limited to truly defensive scenarios.

Global ICT companies should issue patches to protect ICT users, regardless of the attacker and their motives.

Patching software and updating online services should be part of the software development lifecycle for every responsible ICT company. In the context of increased nation-state activity in cyberspace, it is critical that industry issues patches to all users. Industry should not withhold patches from any party and leave particular customers at risk.

The future challenge: verification of compliance with norms

The impact of cybersecurity norms depends on whether they are implemented faithfully and whether violators are held accountable. It is tempting to overstate the challenges here. Some have noted that the untraceable nature of Internet attacks (due to global connectivity, anonymity, and lack of authenticated connections) makes attribution unreliable, and certainly some governments, when accused of malfeasance, have simply issued blanket denials citing technical investigatory challenges. Additionally, some current norms depend not just on proving action but also on proving intent. For example, the United States and China agreed to a norm that prohibits the theft of intellectual property for commercial advantage but, since such technology may be dual use (for example, may also have military application), it may not be enough to prove that the information was stolen; the *purpose* of the theft must also be proven.[24] Finally, nation-states may use private actors as proxies, thus insulating itself from direct involvement in prohibited activities.

The impact of cybersecurity norms depends on whether they are implemented faithfully and whether violators are held accountable.

In reality, none of these challenges are new. When charged with crimes in the physical world, actors often assert that they did not commit the crime, either because they were not the actor (insufficient proof of identity) or they lacked the requisite mental state. Criminal ringleaders may also use proxies, insulating themselves from direct involvement in criminal acts. These issues are resolved by determining who has the burden of proof, the level of proof required for conviction, and whether the evidence presented meets the standard. In some cases, sufficient attribution and proof of intent may not be possible, but that is true in both the cyber and physical worlds. So while the Internet does pose challenges, it does not mean that norms verification is impossible.

Technical attribution

Both the public and private sectors have capabilities to attribute attacks, drawing upon expertise in network investigations within government, the private sector, and academia. Additionally, investigators may suspect nation-state attacks due to other factors, such as trade craft, artifacts, target selection, and the attacker's specialized knowledge:

Trade craft: Nation-states have very sophisticated techniques, tactics, and procedures (TTPs) that can be enhanced with trade craft. *Trade craft* is a term of art used in the intelligence community to describe the stealth manner in which operations are run. Hacking techniques can be further exploited by trained national security organizations to result in greater impact.

Artifacts: Nation-states, like individuals, can create signature patterns that may ultimately provide evidence of source. For example, if a certain cyber attack is attributed to a nation-state and the technical analysis gleaned from another attack is strikingly similar, these artifacts may indicate that the same nation-state is behind both attacks.

Target selection: Certain targets may be of natural and greater interest to nation-states; therefore, attacks against such targets may suggest a nation-state attacker.

Specialized knowledge: Nation-states that seek to target, acquire, disrupt, or destroy certain functions in or through cyberspace often possess unique knowledge. For example, the designers of the Stuxnet virus would have needed not only a thorough understanding of the network architecture of a sensitive nuclear facility, but also a sophisticated understanding of uranium enrichment. This is not just a matter of intelligence gathering, it is also a matter of employing professionals with deeply specialized subject-matter expertise.

Finally, there are a number of capabilities that nation-states in particular may use to identify the source of an attack. These unique capabilities may include signals intelligence (SIGINT), human intelligence (HUMINT), measurement and signatures intelligence (MASINT), and penetrating the systems of attackers to find evidence of culpability.

Making accusations

Even when technical attribution is possible and the burden of proof is met, it does not answer the question of what should be done next. In all cases, there are at least three options: (1) say nothing; (2) make a private accusation; and/or (3) make a public accusation. The "and/or" is important, as these options are not mutually exclusive. For example, one may decide to say nothing until the attacker's conduct goes too far (for example, too much information is stolen or damage is done), at which point the victim may make a private accusation or public accusation. Or, a victim may make a private accusation but go public if the response to the initial accusation seems inadequate.

The literature suggests that all of these options have been used. For example, governments have lodged complaints through diplomatic channels, made public accusations, threatened retaliatory actions (such as the imposition of sanctions) and indicted government actors. In the private sector, some companies have responded by adopting policies and practices that alert users of online services when it appears that they have been targeted by a nation-state.[25]

While norms verification would undoubtedly be helped by documenting and exposing violators, there are times when silence will nonetheless prevail. This is because there are consequences for exposing a norms violation. For example, a government that has identified a nation-state attack (or nation-state-induced taint of a product or service) may not want the adversary to know it has been detected.[26] The government "in the know" may want to engage in counter-intelligence activities, including seeing what the adversary is doing, or may have learned of the norms violation through sensitive techniques it does not want to expose, such as new detection capabilities, or may be concerned that the attacker will simply change tactics and be more difficult to detect in the future. Even if silence is not deemed necessary, the damage from the attack may be minor and raising a potentially contentious allegation may disrupt progress on other issues of importance.

> Even when technical attribution is possible and the burden of proof is met, it does not answer the question of what should be done next.

Industry too may have practical reasons to remain silent. Like a government victim, it may be concerned that notifying the attacker will provoke a change in tactics, thus making detection and remediation more difficult. Additionally, an attacking nation-state may be a customer and any accusation, whether public or private, may have serious business repercussions.

Whether a victim remains silent or makes an accusation, the decision may yield benefits and/or create risk. In the absence of a routine process for identifying inappropriate activity, the verification of adherence to cybersecurity norms is challenged and the norms themselves are potentially undermined.

While there is no simple answer to this problem, history provides a least one potentially workable model: the International Atomic Energy Agency (IAEA). The IAEA is renowned for its technical expertise, its board of governors and other organizational elements are made up representatives from around the world, and the Department of Safeguards conducts its verification work based upon established criteria and refers enforcement matters to the board as appropriate. Notably, the board's decision-making process is typically driven by consensus, which is also a desirable feature of a future cybersecurity norms governance regime.

There could be a similar mechanism by which governments and the private sector can provide evidence to support technical attribution and obtain some level of validation through rigorous peer review. At its core, this organization would consist of technical experts from across governments, the private sector, academia, and civil society with the capability to examine tactics, techniques, and procedures used by nation-state attackers, as well as indicators of compromise that suggest a given attack was by a nation-state. Its essential output would be a technical analysis of the attack and evidence of attribution. In some cases, based on agreed-upon criteria, it might publish its findings.

Some will of course oppose this approach. Governments in particular may be reluctant to empower an independent organization to make findings that may be both politically important and politically charged. To address these concerns, the organization must be structured in a way that promotes global acceptance. More specifically, it must have:

Strong technical expertise

The group would have to be staffed with true experts in cyber forensics and related disciplines. These experts would need advanced technical understanding to make qualified judgements about technical elements of nation-state attacks.

Cybersecurity risk management professionals face enormous challenges in addressing well-resourced and persistent nation-state adversaries.

Diverse geographic representation

At all levels of the group (executive, management, and staff), there would have to be representatives from a diverse set of nation-states and geographic regions. At a minimum, there would need to be representatives from countries that are permanent members of the United Nations Security Council given the group's potential geopolitical importance.

High threshold for attack severity

In order to work effectively, this group should only undertake analyses for significant cyberattacks based on a set of criteria. Initially, the scoping should be narrow and address a small set of norms, such as theft of trade secrets, attacks against critical infrastructure, and/or attacks against commercial mass-market products.

Peer review

Unlike nuclear weapons, which have long been the domain of nation-states, cyber activities often implicate private sector interests (thus, the need for a public/private partnership). Not surprisingly, therefore, nation-state attacks have been analyzed not only by governments, but also by the private sector.[27] To the extent that this domain is not solely for governments, any reports regarding attribution can be subject to peer review, improving the quality of the results.

In sum, having a public/private international body might be a highly constructive way to validate whether norms are being adhered to and may help create a more stable cyberspace in the future.

With or without such an agency, today's ad hoc attribution remains a worthwhile investment. Cybersecurity risk management professionals face enormous challenges in addressing well-resourced and persistent nation-state adversaries, and the study of nation-state attacks can lead to better user protections from the ICT industry. Therefore, industry will continue in its work on attribution so that ICT users are better protected and nation-states do not feel unbounded in their exploitation of cyberspace.

Conclusion

The development and implementation of cybersecurity norms is not a clean or linear process. The relevant stakeholders, implications of potential policies, and indeed, the very technologies themselves are still evolving. Unstoppable growth in international data flows, Internet dependency, and cyberspace empowerment should change the traditional calculus employed by diplomats and nation-states.

As governments commit increasing resources into offensive cyber capabilities, global ICT platform providers must strengthen their resolve and take active steps to prevent exploitation and adhere to a very clear set of cybersecurity norms that focus exclusively on protecting users. Industry cannot participate in offensive activities and help one customer attack another. This would undermine cyberspace itself and erode the very foundations of the global economy.

The development of cybersecurity norms will require new forms of cooperation and possibly even new mechanisms or organizations to effectively deal with the new challenges of today and tomorrow. Significantly improved public/private partnership—on a global scale—will be essential. Attributing attacks is one particular technology and policy area that can benefit from increased public and private cooperation. How such mechanisms or organizations should be developed, chartered, and supported will need much investigation and debate from a broad range of stakeholders.

The steps from articulation to implementation are many. We will have set backs and breakthroughs followed by failures and discoveries. Governments and ICT global platform providers must find a meaningful process to build technological innovations that ensure national sovereignty and legal frameworks that enable increased innovation in security and resilience. The challenge is immense and the significance immutable. Public/private partnerships will be the anvil on which we forge the cybersecurity norms to protect the foundations of the 21st century in cyberspace.

Endnotes

1 Charney, Scott, and Jeff Jones. *Governments and APTs: The Need for Norms*. Microsoft Corp. 2014. https://www.microsoft.com/en-us/download/confirmation.aspx?id=45011

2 "Written Testimony of Cristin Flynn Goodwin, Assistant General Counsel for Cybersecurity at Microsoft Corporation." Oversight and Government Reform Subcommittee on Information Technology Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies. Joint Subcommittee Hearing on Wassenaar: Cybersecurity & Export Control. January 12, 2016. https://homeland.house.gov/wp-content/uploads/2016/01/Testimony-Goodwin.pdf

3 Although proportionality is well-understood in the context of offensive actions (for example, harm to the civilian population must not outweigh the military objective), even defensive measures may disproportionately affect other interests. For example, the monitoring of networks may affect the privacy rights of IT users.

4 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." United Nations (UN) General Assembly A/70/174. July 22, 2015: "While States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society." www.un.org/ga/search/view_doc.asp?symbol=A/70/172

5 "Dialogue with the Private Sector." Financial Action Task Force (FATF) Private Sector Consultative Forum, Vienna. April 19–20, 2016. www.fatf-gafi.org/publications/fatfrecommendations/documents/private-sector-apr-2016.html

6 Benjamin, Raymond, International Civil Aviation Organization (ICAO) Secretary General, et al. *Global Aviation and Our Sustainable Future; International Civil Aviation Organization Briefing for RIO+20.* June 2012. www.icao.int/environmental-protection/Documents/Rio+20_booklet.pdf

7 Schmitt, Michael N., et al. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* 2009. https://issuu.com/nato_ccd_coe/docs/tallinnmanual

8 "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." Organization for Security and Co-operation in Europe 3 (OSCE) Permanent Council. December 2013. www.osce.org/pc/109168?download=true

9 "An Updated Draft of the Code of Conduct Distributed in the United Nations—What's New?" NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). February 10, 2015. https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html

10 Kerry, John. "An Open and Secure Internet: We Must Have Both." U.S. Department of State. May 18, 2015. www.state.gov/secretary/remarks/2015/05/242553.htm; and Painter, Christopher. "Testimony Before Policy Hearing Titled: 'Cybersecurity: Setting the Rules for Responsible Global Behavior.'" U.S. Department of State. May 14, 2015. www.state.gov/s/cyberissues/releasesandremarks/243801.htm

11 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." UN General Assembly A/70/174. July 22, 2015. www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=E

12 "Fact sheet: President Xi Jinping's State Visit to the United States." The White House Office of the Press Secretary. September 25, 2015. https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

13 "Communiqué Language on Commercial Espionage and Cyber Security." November 16, 2015. http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/

14 McKay, Angela, et al. International Cybersecurity Norms. http://aka.ms/cybernorms

15 Ibid.

16 "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." UN General Assembly A/70/174. July 22, 2015. Page 12. www.un.org/ga/search/view_doc.asp?symbol=A/70/174&referer=/english/&Lang=E

17 Ibid.

18 Ibid., and Kerry, John. "An Open and Secure Internet: We Must Have Both." www.state.gov/secretary/remarks/2015/05/242553.htm

19 "Communiqué Language on Commercial Espionage and Cyber Security." November 16, 2015. Paragraph 26. http://g20.org.tr/g20-leaders-commenced-the-antalya-summit/

20 Daniel, Michael. "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities." White House blog. April 28, 2014. https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

21 International Standards Organization (ISO) 29147 and ISO 30111 together provide vendors with a comprehensive set of best practices. ISO 29147 covers vulnerability disclosure, the process through which a vendor receives a vulnerability report and ultimately coordinates with a vulnerability reporter in communicating mitigation details externally. ISO 30111 covers vulnerability handling, the process through which a vendor internally triages and investigates a potential vulnerability and then develops a mitigation as necessary.

22 Perlroth, Nicole. "Governments Turn to Commercial Spyware to Intimidate Dissidents." *The New York Times*. May 29, 2016. www.nytimes.com/2016/05/30/technology/governments-turn-to-commercial-spyware-to-intimidate-dissidents.html?_r=0

23 Zetter, Kim. "Hacking Team Leak Shows How Secretive Zero-Day Exploit Sales Work." *Wired*. July 24, 2015. https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/

24 Similarly, although nation-states have agreed that critical infrastructures should not be attacked in times of peace, it may not be clear whether malware inserted in a critical infrastructure violates that norm or is merely preparing the battlefield in case there is war.

25 Charney, Scott. "Additional steps to help keep your personal information secure." Microsoft on the Issues. December 30, 2105. https://blogs.microsoft.com/on-the-issues/2015/12/30/additional-steps-to-help-keep-your-personal-information-secure/ ; additional references include: https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766; https://security.googleblog.com/2012/06/security-warnings-for-suspected-state.html; https://yahoo-security.tumblr.com/post/135674131435/notifying-our-users-of-attacks-by-suspected; http://thehill.com/policy/cybersecurity/263099-twitter-warns-users-of-state-sponsored-hack

26 This issue is not new. See Charney, Scott, and Eric T. Werner. *Cyber Supply Chain Risk Management: Toward a Global Vision of Transparency and Trust*. Microsoft Trustworthy Computing. July 26, 2011. p. 11. http://download.microsoft.com/download/3/8/4/384483BA-B7B3-4F2F-9366-E83E4C7562D6/Cyber%20Supply%20Chain%20Risk%20Management%20white%20paper.pdf

27 Attacks attributed to the United States, China, and North Korea have all been subject to private sector and public sector review. There were public and private analyses of attacks attributed to the United States, including the European Union Agency for Network and Information Security's (ENISA's): Stuxnet Analysis (https://www.enisa.europa.eu/news/enisa-news/stuxnet-analysis) and Langner's "To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve" (www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf), in addition to publicly reported attribution, such as "U.S. Cyberattacks Target ISIS in a New Line of Combat" (www.nytimes.com/2016/04/25/us/politics/us-directs-cyberweapons-at-isis-for-first-time.html?_r=0).

There were also public and private analyses of attacks attributed to China, including "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage" (https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor), "Mandiant Intelligence Center Report: APT1: Exposing One of China's Cyber Espionage Units" (http://intelreport.mandiant.com), and "Novetta: Operation SMN: Axiom Threat Actor Group Report" (http://novetta.com/wp-content/uploads/2014/11/Executive_Summary-Final_1.pdf), and to North Korea, including "U.S. Said to Find North Korea Ordered Cyberattack on Sony" (www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=1), and even private party accusations, including "Despite What the Cyber Skeptics Say, North Korea Is Behind the Sony Hack" (www.slate.com/blogs/future_tense/2014/12/23/north_korea_is_behind_the_sony_attack_don_t_listen_to_cyber_skeptics.html).

Microsoft