Microsoft

Five Principles for Shaping Cybersecurity Norms

Contents

Introduction

Today, societies are increasingly dependent upon a global network of information and communications technology (ICT) to control the critical infrastructures and communications systems essential to modern life. This dependency will only increase as developing nations build modern ICT infrastructures. The World Economic Forum estimates that 70 percent of the world's population lives in countries that are still in the process of "digitizing" or coming online.[1]

ICT offers great benefits for states and their citizens alike—increased efficiency and transparency in government, improvements in civil society, and economic growth.

Yet along with these benefits have come new threats, including cybercrime such as identity theft and fraud, politically motivated attackers who threaten critical infrastructure, and sophisticated economic and military espionage. ICT can also be exploited to cause significant harm at a national level, including damage to critical infrastructures (energy, communications, banking, transportation, etc.), theft of intellectual property, exploitation of government systems, or criminal attacks against citizens.

For example, a series of recent cyberattacks has disrupted the critical operations of major energy and financial companies. A 2012 attack against a national oil and natural gas company took down 30,000 computers;[2] and in 2013, an attack froze many of the computers of a major bank, affecting ATMs and mobile payments.[3]

To respond, states are under significant pressure to develop and maintain capabilities for defending the nation in cyberspace; maintaining appropriate intelligence capabilities; enforcing criminal law; and reducing risk in its critical infrastructures and its broader economy.

Governments are acting to bolster the range of their national security capabilities in cyberspace. A study by the United Nations Institute for Disarmament Research (UNIDIR) in 2011 identified 33 nation states that address cyberwarfare in their military planning and organization, including "the use of cyber capabilities for reconnaissance, information operations, the disruption of critical networks and services, for cyberattacks, and as a complement to electronic warfare and information operations."[4]

33

NATION STATES INCLUDE CYBERWARFARE IN THEIR MILITARY PLANNING AND ORGANIZATION

---

[1] *The Global Information Technology Report 2012*, World Economic Forum, June, 2012.
http://www3.weforum.org/docs/Global_IT_Report_2012.pdf

[2] *The Cyber Attack on Saudi Aramco*, Survival: Global Politics and Strategy April–May 2013.
aka.ms/Survival-Saudi-Cyber

[3] *South Korea Bank Attack Is a Warning to Bankers*, American Banker, March 20, 2013.
aka.ms/American-Banker-Korea

[4] *Cyber security and Cyber warfare - Preliminary Assessment of National Doctrine and Organization*, Center for Strategic and International Studies for UNIDIR, 2011.
aka.ms/CSIS-CyberConflict

However, conflict in cyberspace, unlike physical warfare, does not have a widely agreed-upon set of conventions, or more significantly, norms, for regulating conflict. A 2012 academic study, the *Tallinn Manual on the International Law Applicable to Cyber Warfare*,[5] summarizes the problem:

> *One of the challenges States face in the cyber environment is that the scope and manner of international law's applicability to cyber operations, whether in offence or defence, has remained unsettled since their advent. After all, at the time the current international legal norms (whether customary or treaty-based) emerged, cyber technology was not on the horizon. Consequently, there is a risk that cyber practice may quickly outdistance agreed understandings as to its governing legal structure. The threshold questions are whether the existing law applies to cyber issues at all, and, if so, how.*

This potential for legal uncertainty, coupled with the technical difficulties of attributing cyberattacks to specific actors—whether state-sponsored or not—creates an opportunity for nation states to engage in a range of problematic behaviors, including espionage, surveillance, and attacks. State insecurity can also erode ICT innovation either by continued exploitation of ICT products in the name of national security, or through unnecessary regulation in an effort to reduce risk.

As a result, the need for diplomatic dialogue among nations has reached a critical juncture. Developing a global understanding of cybersecurity priorities is essential to the long-term stability and security of cyberspace, and requires collaboration among governments.

[5] *Tallinn Manual on the International Law Applicable to Cyber Warfare,* The International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, March, 2013.
aka.ms/Tallinn-Manual

Cybersecurity Norms

Governments are initiating dialogue regarding norms of behavior in cyberspace, highlighting the importance of the subject, which likely will be a diplomatic priority for years to come. The current process is reminiscent of how the law of the sea emerged in the 17th century as states became seafaring, and again more recently as states developed air and space capabilities. Nation states recognize their dependency on the Internet and on interconnected systems, and the lack of clarity on foundational issues such as the applicability of borders to a borderless technology makes issues of conflict in cyberspace even more challenging.

While it is impossible to determine how this discussion will evolve, the use of the term "norms" highlights the importance of cybersecurity and that significant legal and political work remains before consensus emerges among governments on how to develop norms that apply to cyberspace.

The discussion around "cybersecurity norms" currently centers on a wide range of themes. Some of these themes may not reach the status of international norms in traditional diplomatic terms, but they may well evolve into norms that benefit the development of positive behaviors among governments and ICT providers.

Defining Norms

International law codifies a number of behaviors at the nation state level that reflect a normative approach that binds all nations.[1] The clearest statements of government agreements are treaties or conventions, which reflect express statements of nations and create an obligation to act in good faith.[2] However, if a norm of state conduct is established, no treaty can contradict it. Specifically, "a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character."[3] This principle, known in international law as "jus cogens" or "peremptory norms," includes state sovereignty, prohibitions of slavery, genocide, piracy, and other crimes against humanity.

[1] *Statute of the International Court of Justice*, Art. 38. http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0

[2] *Vienna Convention on the Law of Treaties.*

[3] *Vienna Convention on the Law of Treaties,* Art. 53.

The current themes in the norms discussion are:

- **Avoiding conflict.** Some nations are advocating the need to create internationally accepted, agreed-upon norms that establish clear boundaries to help prevent and manage conflict in cyberspace. Others are calling for treaties or conventions to address this issue, while still others seek to maintain the status quo. At the same time, a recent UN study has found that the development of military capabilities in cyberspace is increasing,[6] highlighting the need for further international discussion.
- **Managing threats and vulnerabilities.** Currently, governments are reported to be buying data about vulnerabilities in private sector technology products,[7] for the purpose of exploiting the vulnerabilities to target an entity and advance a national objective. Currently there are no international prohibitions against the trade of cybersecurity vulnerabilities. Norms or other international legal measures may be needed to address this practice.

[6] *Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* page 10, June, 2013 http://aka.ms/GGE-Report

[7] *The Digital Arms Trade, The Economist,* March 30, 2013. aka.ms/Economist-Digtial-Arms

- **Building trust and transparency.** Some discussions about "norms" include ways to develop and implement confidence-building measures (CBMs) between nation states. CBMs are activities between states designed to reduce the likelihood of misunderstanding the scope, intent, or consequences of activities such as the deployment of forces about to be or being conducted. CBMs, which may not involve two state parties, may involve exchanges of information, steps to increase transparency including the use of observers, enhanced communications such as advanced disclosure of activities or dedicated channels of communication between states, and agreements to limit the scope or nature of certain activities.
- **Sharing threat and vulnerability information and coordinating among nations.** Improving incident response and mutual assistance mechanisms among nation states and key communities such as law enforcement are critical requirements. Sharing threat-based information such as vulnerabilities, hacking trend data, new threat identification, or even unexplained anomalies impacting a product or service can enable the ICT sector and government to better protect critical systems and respond to emerging issues, while simultaneously being respectful of privacy and civil liberties.
- **Cybersecurity capacity-building.** Improving global baselines for cybersecurity capabilities in developing countries including software development, operations, response, policy, and risk management is vital. One key international expert fora examining the issue of norms is the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN-GGE), which in its 2013 report stated:

  > *Capacity-building is of vital importance to an effective cooperative global effort on securing ICTs and their use. Some States may require assistance in their efforts to: improve the security of critical ICT infrastructure; develop technical skill and appropriate legislation, strategies and regulatory frameworks to fulfill their responsibilities; and bridge the divide in the security of ICTs and their use.*[8]

The Role of the Private Sector

Unlike the historical evolution of international norms, the development of "cybersecurity norms" should engage the private sector, which creates and operates most of the infrastructure that underpins the Internet. While it is true that only nation states can create actual legal norms, a challenging aspect of the cybersecurity discussion is that a significant portion of the infrastructure of the Internet resides in the private sector. This affects cybersecurity discussions because some security actions are outside the control of national governments. In many instances, previous efforts to build cybersecurity norms benefited from private sector technical assistance.

---

[8] *Report of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* page 10, June, 2013
http://aka.ms/GGE-Report

The private sector influenced such agreements as the Missile Technology Control Regime, Financial Action Task Force on Money Laundering efforts, and the norms promoted by the International Civil Aviation Organization for civil air travel. The private sector was also vital in garnering critical congressional or parliamentary support for the ratification of these agreements.[9]

Governments would also benefit from the experience and perspective of the private sector, which has had to think through the technical challenges and priorities of securing billions of customers around the world. The previously mentioned UN-GGE report recommends, "While States must lead in addressing these challenges, effective cooperation would benefit from the appropriate participation of the private sector and civil society."[10]

[9] *Securing Cyberspace Through International Norms Recommendations for Policymakers and the Private Sector.* Richard A. Clarke Good Harbor Consulting, pages 7–10, 2013.
http://www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf

[10] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* page 7, June, 2013.
http://aka.ms/GGE-Report

Cybersecurity Principles That Influence Norms

Microsoft works closely with governments, enterprises, and customers around the world to assess, manage, and respond to risks in cyberspace. In addition, Microsoft has a unique view of threats in cyberspace, as each month the company receives threat information from more than 600 million computers, mobile devices, and servers globally who have opted into anonymously sharing telemetry back to Microsoft. Microsoft regularly publishes its findings in the semi-annual Security Intelligence Report (SIR).

Based on this broad and long-standing cybersecurity experience, Microsoft has observed five important principles that should underlie international discussions of "cybersecurity norms": harmonization, risk reduction, transparency, proportionality, and collaboration. These principles are important to keep in mind when governments are discussing which issues of cybersecurity rise to the level of normative behavior, which require conventions among a large number of states, or smaller, bilateral or multilateral agreements, or which are simply adopted into domestic laws or public policies.

Harmonization of Laws and Standards

Given the global and ubiquitous nature of the Internet, developing global cybersecurity laws and standards rather than unique domestic approaches is an important principle. The use of common cybersecurity approaches promotes understanding, predictability, and enables collaboration on problem solving among countries.

Harmonization of cybersecurity law and international standards helps establish a more secure Internet. Governments are well suited to contribute technical expertise and political support for creating approaches to international cybersecurity. Given the global nature of ICT development, creating products and services to meet hundreds of differing national requirements is unworkable. Default requirements that are contradictory or don't work internationally will slow the development of ICT and hinder innovation, domestically and internationally.

One example of harmonization in international law has been the many domestic laws developed at the national level as a result of the *Budapest Convention on Cybercrime*.[11] The Cybercrime Convention has greatly advanced harmonization in cybercrime enforcement. The current efforts to create a Network and Information Security Directive for European Union Member States, if successfully implemented, could help drive harmonized approaches to cybersecurity laws across 28 countries, and underscore the importance of harmonization in order to ensure the successful implementation of the Directive, if it becomes required in Europe.

In addition, international standards play a key role in harmonization. Relevant standards can bolster readiness in government agencies, as well as in private enterprises. For example, when governments choose to base their software assurance and supply chain policies on international standards and globally recognized best practices, they create flexibility for vendors and suppliers and increase the range of available solutions. International standards such as ISO 27034 for secure software development and emerging international standards for supply chain risk management are useful references for developing such policies. In some instances, cybersecurity risks evolve too fast to be addressed by international standards alone, and may require best practices—even at the international level.[12]

---

[11] Convention on Cybercrime, Budapest, 23.XI.2001 .
aka.ms/budapest-cybercrime

[12] *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation.* Cristin Goodwin and Paul Nicholas, Microsoft Corporation 2013

Risk Reduction

As an essential part of diplomacy, governments put much effort into reducing geopolitical risk. Yet, reducing risk is not a well-developed concept under international law or public policy, because risks are not usually managed on a global level. The Internet alters that paradigm, and brings about the need to discuss risk reduction whenever government address cybersecurity. All stakeholders in cybersecurity should work to improve the security of the Internet through collective responses to threats by sharing information about threats and vulnerabilities, and by engaging in the active prevention of cybercrime. Governments and the ICT industry should:

- Engage in systematic activities to identify and respond to threats that impact cyberspace.
- Share information about vulnerabilities, hacking trends, and new threats or unexplained anomalies that negatively impact technology products and services. This will enable the private sector and government to better protect critical systems and respond more efficiently to emerging issues, and can lead to the development of new protections or mitigations, sometimes in advance of any negative impact. If done widely and efficiently, sharing threats can constrain the head start afforded to an early discoverer of security vulnerabilities and prevent their exploitation.
- In light of the international nature and rapid development of new threats in cyberspace, stakeholders should shift from a reactive to a more proactive approach to fighting cybercrime. Instead of relying primarily on criminal prosecutions and cleanup efforts following a sophisticated attack, they should focus on prevention, which is itself a national reduction of cybersecurity risk.

These actions could manifest themselves in different ways in discussions of cybersecurity norms, and may never rise to the level of an actual norm of international law, but the principle of risk reduction should be recognized and adopted whenever cybersecurity is discussed by nation states.

Transparency

Governments can help to build trust and increase predictability and stability in cyberspace by practicing greater transparency in their cybersecurity practices. The principle of transparency in cybersecurity depends on a number of factors. A recent report by the ICT4Peace Foundation cited key examples, including:

- *A publicly available cybersecurity strategy, complete with aims, intentions, internal structures, and budgetary allocations.*
- *A declared military doctrine, including command/control structures, on the use of cyber tools in times of conflict.*
- *Publicizing a CERT's [Computer Emergency Readiness Team] organizational structure and contact info.*
- *Updated points of contact for routine and urgent contacts at operational levels.*[13]

Microsoft supports greater government transparency, and recently released a paper promoting the development of a national cybersecurity strategy to articulate priorities, principles, and approaches for managing national level risks in cyberspace.[14] At its foundation, a national strategy must reflect the cultural values and beliefs of the nation. It must have a clear set of principles that help frame decisions about how to identify, manage, or mitigate

---

[13] *Confidence Building Measures and International Cybersecurity, ICT4Peace Foundation, 2013.* aka.ms/ICT4Peace-CBM

[14] *Developing a National Strategy for Cybersecurity: Foundations for Security, Growth, and Innovation.* Cristin Goodwin and Paul Nicholas, Microsoft Corporation 2013.

cybersecurity risks in a way that balances civil rights and liberties, costs, and a range of other possible priorities. Additionally, a national strategy should set out principles for cybersecurity, appoint a clear leader to coordinate and develop those principles and best practices, and establish a process for communicating positions in existing international forums. The development of cybersecurity policies and best practices is a long-term commitment for the security and stability of cyberspace, and every country should have a voice in this critical dialogue.

Collaboration

As governments construct cybersecurity practices to address security concerns at the international level, they should seek input from a variety of stakeholders, including the private sector, civil society, and academia. While the principle of collaboration with the private sector has some precedents in international law, given the shared ownership, management, and control of the Internet, collaboration will be key to successfully developing any norm, enacting any law, executing any treaty, or creating any public policy. There are many possible collaborative efforts that will help foster a more secure cyberspace, including exchanges of information regarding threats, capacity building, and verification exercises.

Collaborating among states can be difficult, especially on a highly sensitive matter like cybersecurity. Currently, the European Union is developing a framework through the Network and Information Security Directive that will, if enacted, require collaboration on significant cybersecurity incidents and greater harmonization of member state laws and capabilities. It will take several years to evolve and operationalize these capabilities, and the EU has actively engaged the private the sector in the development of this approach.

Collaboration among private sector technology participants is not always easy. However, they are already working together to help create a more secure ecosystem. One prominent example is the The Industry Consortium for Advancement of Security on the Internet (ICASI).[15] Its mission is to "enhance the global security landscape by driving excellence and innovation in security response practices, and by enabling its members to proactively collaborate to analyze, mitigate, and resolve multi-vendor, global security challenges." ICASI has developed a mechanism that enables vendors to share sensitive information in a secure forum, thereby removing a critical obstacle to effective collaboration in the face of emerging security threats.

Proportionality

Proportionality refers to the well-established principle in international law that policies and responses must be proportional in relation to the need for self-defense. The issue of proportionality is challenging, because it not yet clear how proportionality in cyberspace will be interpreted, and it will likely be analyzed by international tribunals and scholars in conjunction with the principle of "necessity." However, nations should begin to develop interpretations of proportionality in cyberspace under customary international law, as it is likely that this principle will be tested when, for example, a nation state responds as a result of an attack using cyberspace and causes damage to another state.

[15] www.icasi.org

Moving Forward

The discussion of "cybersecurity norms" has gained global momentum. The UN-GGE concluded in its 2013 report:

> *The report recognizes that the application of norms derived from existing international law relevant to the use of ICTs by States is essential to reduce risks to international peace, security and stability. The report recommends further study to promote common understandings on how such norms apply to State behaviour and the use of ICTs by States. Given the unique attributes of ICTs, the report notes that additional norms could be developed over time…The Group recommends the holding of regular institutional dialogue on these issues under the auspices of the United Nations as well as regular dialogue in other forums, to advance these measures.*[16]

Microsoft supports a four-step process for driving the development and understanding of global cybersecurity norms and practices forward:

1. Prioritize issues in cybersecurity that require diplomatic engagement from an international legal perspective; identify ways to build consensus to modify current international laws to incorporate changes caused by technology and innovation.
2. Analyze existing cybersecurity best practices and policies at the national, regional, and international level and determine where global principles or practices need to be developed. Key areas to explore should include confidence-building measures, responses to security incidents, assessment and mitigation of risk to critical ICT infrastructure, risk management, supply chain security, and protecting core encryption and trust mechanisms of the Internet.
3. Develop a set of cooperative measures for trust, stability, and reliability in cyberspace, with appropriate responsibilities for the public and private sectors, including at the international level.
4. Drive for consensus on the most important issues in cybersecurity, as legal processes take many years to develop and become established both domestically and internationally.

The international implications of cybersecurity are immense. How countries behave in cyberspace from a security perspective is no longer the private matter of an individual state; it is an international issue. Countries need to articulate a clear policy on how they approach security in cyberspace, and how they will organize to ensure their respective economic security, defense, and public safety as it relates to cybersecurity. While development of some of these positions should be led by government, many policies and the confidence-building measures that can enable effective cybersecurity practices are highly dependent upon the cooperation of the private sector. We support an inclusive global dialogue on the continued development of principles that advance cybersecurity.

[16] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* June, 2013.
aka.ms/GGE-Report


Microsoft