Microsoft

International Cybersecurity Norms

Reducing conflict in an Internet-dependent world

Authors

Angela McKay
Jan Neutze
Paul Nicholas
Kevin Sullivan

Contributors

Scott Charney
Kaja Ciglic
Erin English
Cristin Goodwin
Nemanja Malisevic
Theo Moore
Matt Thomlinson

Foreword

As societies expand their digital footprint, increasing connectivity among citizens, businesses, and governments, the world has also seen a concomitant increase in cyber incidents. At times, the attackers' motivations are financial, not unlike criminal behavior in the "physical world." The past several years have shown a new trend. Increasingly, states use the Internet to advance tried and true tenets of intelligence or even military operations: espionage, reconnaissance, and even sabotage. The targets of these operations, whether intentional or not, are often civilians. In an effort to encourage the international community to reverse this trend, *International Cybersecurity Norms, Reducing conflict in an Internet-dependent world*, analyzes the unique attributes that make cybersecurity conflict-prone and proposes a framework and norms for cybersecurity.

As the pace of activity in cyberspace increases, so does the likelihood of one state misinterpreting the actions of another. Moreover, the risk of a cyber-arms race cannot be discounted. It would be naïve to hope that states should fully pull back their military operations from the Internet. Nevertheless, just as there are universally accepted norms of behavior in other realms of conflict, it is no less important to establish norms for cybersecurity. These norms should not only strengthen cybersecurity but also preserve the freedoms of a globally connected society.

Some will contend that this search for norms is rather futile, as states might simply ignore or pay lip service to them. Smaller countries may be reluctant to disavow a powerful arrow in their quiver that could give them an asymmetric advantage. And would there even be consequences for violators at all? While valid, this kind of skepticism only underscores the need to move forward. Norms cannot guarantee that states will never violate agreed upon principles, but they will put violators on notice within the international community. And from norms that gradually become accepted a stronger framework can eventually emerge.

Yes, achieving global acceptance of new international norms in such a critical realm is difficult. In the deliberations leading to the Nuclear Non-Proliferation Treaty, Willy Brandt, then the German Foreign Minister, said, "We shall not be able to discuss security guarantees, disarmament, and the perspectives for the peaceful use of nuclear energy with any prospect of success unless a common will and joint proposals put right the rules of order the community of nations urgently needs." Nuclear power and cyberspace are different in many respects, but Brandt's argument very much applies here.

Ambassador Wolfgang Ischinger is Chairman of the Munich Security Conference. He was State Secretary of the German Federal Foreign Office and German Ambassador in Washington and London.

International Cybersecurity Norms contains many sound and thought-provoking ideas and recommendations to that effect and deserves the full attention of citizens, businesses, and governments alike.

Ambassador Wolfgang Ischinger

Introduction

Nation states are operating in cyberspace, and, in government buildings around the world, their activities are quickly moving from whiteboards to keyboards. Cyber conflict and cyber war are not just theoretical but are actual possibilities that need to be considered and addressed. Information and communications technology (ICT) creates benefits for states and their citizens alike, but technologies can—and are—being exploited by a variety of government actors with differing motivations and means. For nearly two decades, the cybersecurity community has consistently warned of the increasing number and sophistication of cyber attacks. But now, cyberspace is being operationalized by some nation states as a domain for conflict, dramatically escalating the threat. In this shared and tightly integrated domain, any escalation of hostilities could result in unintended—and even catastrophic—consequences.

This escalation of nation state activity comes just as technology is poised to penetrate even deeper into our lives. Over the next decade, the number of Internet users will grow to 4.75 billion, connecting more than 91 percent of people in developed countries and nearly 69 percent of those in emerging countries.[1]

They will connect through myriad mobile devices, leveraging cloud services, and creating volumes of data at unprecedented rates. The result of the deeper ICT penetration will be very positive: people will be more connected around the world, economies will continue to develop and grow, and new markets will emerge, all with increased efficiency. The downside is that Internet dependence will become an unavoidable fact of life. Internet dependence and growing interdependence within the online environment has and will continue to challenge our collective ability to manage the consequences of cyber attacks, at national and international levels. Offensive operations in cyberspace can result in serious unintended consequences. In light of the existing offensive cyber capabilities of some states and of the stated intent of other nations regarding future capabilities, and to define acceptable actions in cyberspace, Microsoft strongly supports the development of cybersecurity norms.

Cybersecurity norms should be designed not only to increase the security of cyberspace but also to preserve the utility of a globally connected society. As such, norms should define acceptable and unacceptable state behaviors, with the aim of reducing risks, fostering greater predictability, and limiting the potential for the most problematic impacts, including (and in particular) impacts which could result from government activity below the threshold of war. We conceptualize at least two types of norms:

- Norms for improving defenses, which can reduce risk by providing a foundation for national cybersecurity capacity and for domestic, regional, and international organizational structures and approaches that increase understanding between states
- Norms for limiting conflict or offensive operations, which will serve to reduce conflict, avoid escalations, and limit the potential for catastrophic impacts in, through, or even to cyberspace.

1 Burt, David, Aaron Kleiner, J. Paul Nicholas, and Kevin Sullivan. *Cyberspace 2025 Today's Decisions, Tomorrow's Terrain.* Microsoft. June 2014. http://www.cyberspace2025.com

Progress on either set of norms requires collaboration and dialogue among governments, supported by the private sector, civil society, and academia. This process is underway, and dialogue is ongoing, but progress has been limited. Microsoft seeks to invigorate the debate by publishing this paper, which presents a framework for evaluating actors' behavior in cyberspace, proposes six initial cybersecurity norms to limit conflict in cyberspace, and presents a multi-stakeholder approach for developing norms.

The concepts and norms proposed in this paper should be examined and challenged by policymakers and diplomats, in addition to thought leaders across academia and industry. The resulting discourse can and should be used to refine the proposal, foster political consensus, and promote positive action to improve defenses and to limit potential conflict. Microsoft encourages states with acknowledged cyber offensive capabilities to commit to developing meaningful cybersecurity norms and to making those norms politically binding. Adding cybersecurity into the current work in the United Nations (UN) on draft articles of state responsibilities would also be a positive step toward moving from politically binding to legally binding.

Moving from politically binding norms to legally binding norms will take time and commitment, and some policymakers might see our proposals as more aspirational than realistic. Although making meaningful progress will be a challenge, especially as demographic, political, and economic shifts test traditional models for collaboration, we are nevertheless optimistic that, through dialogue, development, and general practice, certain cybersecurity norms can evolve into customary international law over time. The consequences of inaction are unacceptable. Policymakers, diplomats, academics, and industry must commit to protecting the most vital cyberspace functions so that society can continue to realize the tremendous economic and societal benefits they enable.

The importance of norms to manage cyberspace risks

The relationship of governments with the Internet is complex, making their efforts to develop cybersecurity norms even more of a challenge. Governments are simultaneously:

- Users of ICT and data.
- Protectors of the Internet itself, as a critical part of national infrastructure, and protectors of individual cyberspace users' rights.
- Creators of laws and policies in support of cybersecurity and critical infrastructure protection,
- Exploiters of ICT and data for intelligence and military purposes.[2]

Consistent with these various roles, increasing numbers of nation states are currently developing not only defensive but also offensive cyberspace capabilities, predicated on policies or laws that reflect a nation's views on a wide range of security and economic issues.[3]

As governments are wrestling with the technical ability to both exploit and protect the Internet, they are also creating the justifications and rationales to support those activities. Different countries will have different tolerance for risks, and will choose to exploit certain aspects of the Internet or defend against certain types of attacks based on the nation's risk tolerance, as reflected in its laws and policies.

However, offensive cyber operations can result in unintended consequences. Given the interconnected nature of cyberspace and the speed and nature of cyber attacks, the effects of offensive operations might be very difficult to predict and/or limit, and they could cascade to affect operations beyond the intended targets, including critical functions in the energy, communications, banking, chemical, or transportation sectors, among others. In other instances, an offensive cyber operation gone wrong could disrupt the global Internet or corrupt data at a scale that impedes key functions of the global economy. Unintended consequences of this scale could very easily escalate hostilities from the keyboard to kinetics, in the absence of normative limits on such behaviors.

In addition to concerns about actual unintended consequences, the increasing development of defensive and offensive cyberspace capabilities will, in itself, promote cyber insecurity between nation states, especially without a normative framework around those capabilities. If a state, for example, shifts cybersecurity investments from civilian defense and law enforcement to offensive military capabilities, other states will react. The actions of individual nation states could exacerbate cyber insecurity regionally or globally, driving broader tensions in the international system. Furthermore, actions of nation states to reduce risk and to bolster military cyberspace capacity could result in policies that also constrain economic growth, limit innovation, or restrict trade and investment. As these policies diverge, it will become harder to rationalize cybersecurity norms at the international level. Even if a nation state decides an offensive action is justified in law and policy, the national security of these states might inadvertently be undermined in the long run, exacerbating the overall sense of insecurity—cyber or otherwise. If left unchecked, cyber insecurity at a global level could erode trust in the foundations of the Internet itself and in the global fabric of ICT-driven innovation.

2 Stoll, Clifford. *The Cuckoo's Egg.* New York: Doubleday, 1989.

3 *Cyber Index International Security Trends & Realities.* United Nations Institute for Disarmament Research. 2013. www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

A framework to evaluate actions and impacts in cyberspace

Despite a growing consensus in the international community that cybersecurity norms are needed, governments, industry, academia, and civil society are struggling to determine what those norms should actually be. Dialogue appropriately attempts to reference, draw analogies with, and derive insights from how norms and, eventually, international law, are developed in other interconnected, kinetic environments, including sea and space. Although useful, these analogies have also proven to be of limited value when seeking to address the complexity, speed, and range of intended and unintended consequences that could result from escalating nation-state activities in cyberspace.

As governments engage in activity in cyberspace, it is increasingly important to consider the potential impacts of their actions, including impacts to international security, national security, public safety, economies and the trust which society has in its governments and in the globally interconnected system. When confronted with seemingly conflicting priorities and a myriad of options, we need a framework that explores the components of the decisions which governments have to make. The framework should also enable them to make choices that appropriately balance their roles as users, protectors, and exploiters of the Internet and to take actions that have impacts which are acceptable to governments, industry, and society globally.

Evaluating behavior in cyberspace

The framework we propose evaluates various actors in cyberspace, the objectives those actors are seeking to advance, the corresponding actions that could be taken, and, finally, the potential impacts that can result. The framework is quite simple and can be portrayed as follows:

Figure 1. A framework of actors, objectives, actions, and impacts[4]

This paper focuses on leveraging the framework to develop cybersecurity norms for government actors. Governments are, of course, not the only actors in cyberspace. Criminals can cause significant damage, as well, but they are, by definition, engaging in illegal acts which violate domestic laws and social norms. However, in light of the sustained resources that governments (and government-sponsored entities) can apply to develop sophisticated cyber offense capabilities, they tend to be the most advanced actors in the cyber offensive domain.

Governments pursue many objectives in cyberspace. In defining cybersecurity norms, this simple rule should be applied: "If the objective is unacceptable, stop." No action is justifiable if the objective is wrong. As the most advanced actors in cyberspace, governments can also take a multitude of actions in cyberspace, both offensively and defensively, to support acceptable objectives. These actions and their resulting impacts, both intended and unintended, can precisely support defined objectives but can also advance one generally acceptable objective while simultaneously challenging another. In many cases, societal debate is not about objectives, such as degrading or delaying the spread of nuclear weapons or preventing terrorism, but whether the actions that can be taken—and the impact of those actions—are acceptable. With this framework in mind, when developing cybersecurity norms for governments, we can focus on discussing acceptable and unacceptable objectives, which actions may be taken by governments in pursuit of those objectives, what the possible impacts are, and whether they are acceptable for a civilized, connected society.

4 Charney, Scott. *Rethinking the Cyber Threat: An Overarching Framework. Microsoft*. November 2014. http://aka.ms/rethink2.

Understanding the impact of actions in cyberspace

Different types of information systems and data can be the vectors and targets of offensive cyber operations and cyber weapons. For the purposes of this paper, we define:

- *Offensive cyber operations* as state or state-sponsored actions, such as theft or manipulation of data, and tampering with the integrity of private sector products, services, and operations.
- *Cyber weapons* as a combination of information systems, programs, or data designed, equipped, or modified to destroy, disrupt, or corrupt critical physical or information cyber infrastructure.

- **Distinction:** How well can a particular asset be targeted
- **Discrimination:** Ability to manage the scope of potential consequences
- **Distribution:** Potential for malicious reuse of weapons or vulnerabilities

It is important to distinguish, in offensive operations, the objective from the action and its related impacts. Even assuming an appropriate objective, understanding distinction, discrimination, and distribution in the context of cyber conflict will help inform the formulation of practicable and achievable cybersecurity norms.

The inherently dual-use nature of most ICT often makes distinguishing government versus commercial uses as targets difficult, and it results in a high potential for reuse of weapons or vulnerabilities across domains. This complexity is the basis for concerns about unintended consequences. When state actors attempt to taint commercial ICT products or publicly available cloud services, the target cannot always be well distinguished, thus potentially exposing all who use those products and services. Employing this type of trade craft significantly increases the risk that the vulnerability will be found and exploited by others, and that widespread harm will more likely occur. In contrast, when states target and exploit custom software (such as government off-the-shelf [GOTS] software) only used by a single military or government agency, the risk of widespread use is greatly reduced.

In addition to reviewing the types of technologies used or targeted by cyber weapons, the consequences of violating the information security attributes of data contained within the system must also be considered. With greater numbers of people and businesses switching to cloud computing, this consideration will only increase in importance. First, availability and access to data becomes a critical concern when users are reliant on communications infrastructure to enable access to services. In addition, users want assurances that their data is (and will remain) confidential and that their privacy rights are respected. However, the real paradigm shift stems from increased concerns related to data integrity and non-repudiation when backups don't exist or if users don't know whether those backups can be trusted.

As shown in the following table, some offensive operations and the use of cyber weapons add another dimension to private sector management of data security risks. This aspect of data security needs to be elaborated upon and matured fully in the coming years. Users of cloud services, both public and private, must begin to assess their respective risk tolerance for each of the data security attributes outlined and to understand their options for recovery. Users can recover from a privacy breach. Outages can be fixed, and availability can be restored. Mass corruption of data, however, may create instances that are exceptionally hard to recover from and, in some instances, impossible. Loss of data integrity for certain essential functions enabling global finance, safe commercial transportation, and public health and safety may be considered by many states to be unacceptable impacts.

Data security attribute	Consequence of violation by cyber weapon	Example
Confidentiality	Potential for economic or reputational damage to organizations or individuals. If confidentiality is breached, it cannot be restored; however the data asset may still be useful.	A disclosure of financial records violates confidentiality but not necessarily the integrity of the data.
Integrity	Violation of integrity can fundamentally undermine trust in the data or in any systems that rely upon it.	Changing financial records would require restoring from backups that may be out of date or nonexistent.
Availability	Systems or data are unavailable for a period of time (perhaps indefinitely); however, the confidentiality and integrity of the data may be preserved.	A system is taken offline by a cyber attack but can be restored at the end of the conflict.
Non-repudiation	Commerce and financial systems depend on the undeniable proof that a transaction took place. Violation of this principle would render most electronic transactions meaningless and, as a result, make it very difficult to reestablish trust in IT systems.	A bank-clearing system unable to properly validate transactions would shut down and potentially need to recreate a large number of transactions.

Table 1: Consequences of cyber weapons on different data security attributes

Limiting and managing escalation of threats in cyberspace through norms

Cybersecurity norms that limit potential conflict in cyberspace are likely to bring predictability, stability, and security to the international environment—far more than any set of confidence-building measures (CBM). With a wide acceptance of these norms, governments investing in offensive cyber capabilities would have a responsibility to act and work within the international system to guide their use, and this would ultimately lead to a reduction in the likelihood of conflict.

Microsoft strongly supports a broader discussion and dialogue on the "other than war" scenarios, since limiting and managing state behavior will help mitigate against the possibility of conflict escalating to cyber warfare.

Conflict is often characterized as one of two discrete states: peacetime and war. In reality, whether talking about cyberspace or the physical world, there is an escalation path from more common (yet still complex) events that occur in peacetime, to increasing activity and incidents, disruptions, emerging conflict, conflict, and, eventually war, as shown in Figure 2. Different legal frameworks apply at these various stages.

International policy work to date has primarily focused on cybersecurity norms as a means to reduce risk from potentially complex cyber events at the national and regional levels and advance CBM efforts at the international level.

Authorities have paid particular attention to risks and events where there is broad societal agreement on the most significant of issues that face the world— such as armed conflict, nuclear non-proliferation, global resources, and trade. With this alignment on acceptable

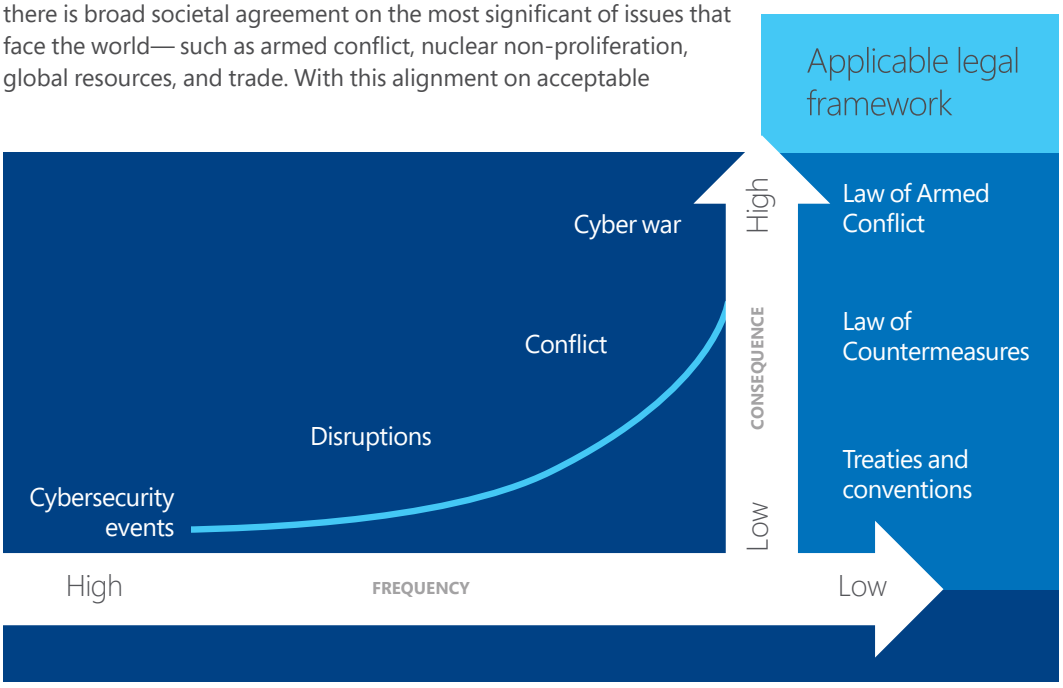

Figure 2. Escalation of cyber events and applicable legal frameworks

and unacceptable objectives, actions, and impacts, it seems increasingly appropriate to address cybersecurity risks and events through treaties and conventions. Work to address cyber crime through increased international collaboration is one such example. Another example is the work within the UN, which has looked at a relatively narrow, but vital, segment of cyber conflict for events of extremely high consequence but low likelihood and which would be addressed under the Law of Armed Conflict.

To date, cyber events have not risen to the level of armed conflict. However, while the boundaries between crime and conflict in cyberspace are often hard to discern, events within that space can have broad societal impact, and be challenging to defend against. When existing diplomatic efforts are laid over the spectrum of possible events and applicable legal frameworks, the opportunity for greater development of cybersecurity norms to both improve defense, but in particular limit conflict, is apparent. Figure 2 below illustrates the area where the greatest opportunity for cybersecurity norms exist.

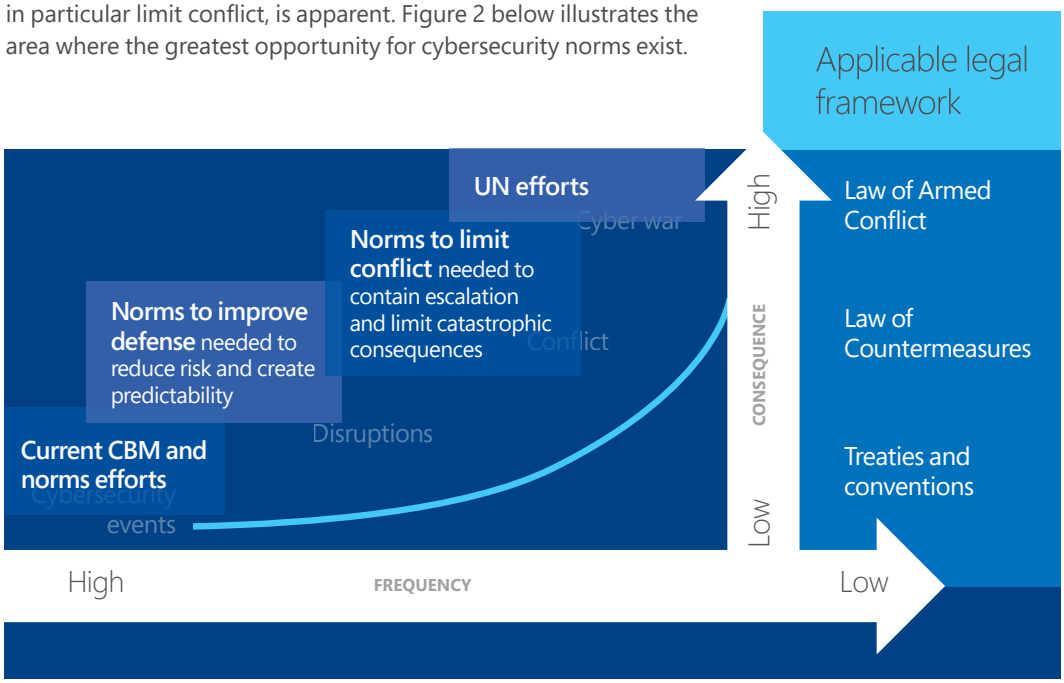

Figure 3. Opportunity space for cybersecurity norms

Six proposed cybersecurity norms to limit conflict

In light of the growing number of offensive capabilities, Microsoft believes that cybersecurity norms are needed to limit potential conflict in cyberspace and to better define what type of government behaviors in cyberspace should be "out of bounds" so that events don't escalate to warfare. These norms should not only be designed to strengthen cybersecurity but also to preserve the utility of a globally connected society.

We believe that if cybersecurity norms are to be effective, they have to meet four key criteria. First, they must be practicable. They also need to reduce risks of complex cyber events and disruptions that could lead to conflict. In addition, they need to drive behavioral change that is observable and that makes a demonstrable difference in the security of cyberspace for states, enterprises, civil society, and individual stakeholders and users. Finally, effective norms should leverage existing risk-management concepts to help mitigate against escalation, and, if escalation is unavoidable, they should provide useful insight into the potential actions of involved parties.

To help catalyze progress on the development of effective cybersecurity norms, Microsoft proposes six norms to limit conflict. The proposed norms are intended to reduce the possibility that ICT products and services could be used, abused, or exploited by nation states as part of offensive operations that result in unacceptable impacts, such undermining trust in ICT; set boundaries for how cyber weapons are developed, contained, and used; and create a meaningful global framework for managing vulnerabilities. We recognize that norms should not be an objective by themselves. Only if implemented, assessed for accountability, and, as appropriate, evolved, can they drive demonstrable changes in behavior.

NORM 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.

The global technology industry is founded on trust, in that consumers, enterprises, and governments depend on ICT for critical functions. Although the private sector can and does invest considerably in efforts to advance and demonstrate the assurance and integrity of products and services, states have the unique capability to direct disproportionately larger resources to exploit these products or services and to taint the broad ICT supply chains by which they are delivered. Exploiting of commercial off-the-shelf (COTS) products and services—which puts at risk every computer user dependent on that technology, even if that user is of no interest to a government—would be an action with the potential to create unacceptable impacts globally, since the degradation of trust in ICT would threaten innovation and economic security. Sophisticated state-resourced tradecraft targeting ICT companies to place backdoors or vulnerabilities in COTS products—or compromising signing keys to enable government to misrepresent the provenance of software—may exceed the commercially reasonable limits of the private sector operational security and integrity controls. Governments should also refrain from undermining international security standards efforts to benefit their own interests.

NORM 2: 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.

It is well-documented that governments around the world are active participants in the cyber vulnerability market and that they exploit gray and black markets.[5] The Heartbleed vulnerability, discovered in 2014, fueled additional speculation as to how governments stockpile vulnerabilities in ICT products rather than disclosing them to vendors to fix before they are exploited. In April 2014, in response to specific allegations against the US government, the White House published its framework approach to addressing if or when the federal government may withhold knowledge of a vulnerability from the public: "This administration takes seriously its commitment to an open and interoperable, secure and reliable Internet, and in the majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest. This has been and continues to be the case."[6] The White House further noted that building up a "huge stockpile of undisclosed vulnerabilities" while leaving the Internet vulnerable and people unprotected would not be in the national security interest of the United States.[7]

Although the White House reserved the right to use vulnerabilities as a method of intelligence collection, this approach does reflect a positive analysis that short-term gains to advance one objective could also create impacts that threaten other objectives, such as economic growth, technological innovation, and trust in government. We recommend that other governments similarly develop and publicly publish their policies on vulnerability handling and that they have a partiality for reporting vulnerabilities to vendors. When doing so, they should adhere to the principles of Coordinated Vulnerability Disclosure (CVD).

NORM 3: States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

Microsoft recognizes that governments will develop cyber weapons and protocols for their own use. When governments do build them, therefore, they should ensure that they are building cyber weapons that are controllable, precise, and not reusable by others, consistent with the concepts of distinction, discrimination, and distribution previously discussed, to limit the impacts associated with these actions.

5 "The digital arms trade." The Economist. March 30, 2013. http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade

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

7 ibid

NORM 4: States should commit to nonproliferation activities related to cyber weapons.

As states increase investments in offensive cyber capabilities, care must be taken to not proliferate weapons or techniques for weaponizing code. States should establish processes to identify the intelligence, law enforcement, and financial sanctions tools that can and should be used against governments and individuals who use or intend to use cyber weapons in violation of law or international norms. Furthermore, states should agree to control the proliferation of cyber weapons in cooperation with international partners and, to the extent practicable, private industry. Implementing this norm will not only help limit state actions that could have unacceptable impacts but also will help reduce the possibility that cyber weapons could be used by non-state actors.

NORM 5: States should limit their engagement in cyber offensive operations to avoid creating a mass event.

Governments should review and update their current policy positions with an appreciation for the unintended consequences or impacts in cyberspace that could escalate conflict, incite war or disproportionately harm civilian ICT. During an armed conflict, as regulated by the law of war, any attack must be justified by military necessity, intended to help in the military defeat of the enemy, with a military objective. Furthermore, the harm caused to civilians or civilian property must be proportional in relation to the concrete and direct military advantage anticipated. In other words, the action should be to advance defined and accepted military objectives and should not create disproportional impacts. These strictures can and should be applied to offensive cyber operations. States should recognize that attacks targeting the confidentiality, integrity, or availability of ICT systems, services, and data can have a mass effect beyond any reasonable sense of proportionality and required global action.

NORM 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Although governments play an increasingly important role in cyberspace, the first line of defense against cyber attacks remains the private sector, with its globally distributed telemetry, situational awareness, and well-established incident response functions. There has not been evidence of governmental interference with private sector recovery efforts following a severe cyber attack, but governments should commit to not interfere with the core capabilities or mechanisms required for response and recovery, including Computer Emergency Response Teams (CERTs), individual response personnel, and technical response systems. Intervening in private sector response and recovery would be akin to attacking medical personnel at military hospitals.

Additionally, governments should go one step further and, when asked by the private sector, commit to assist with recovery and response needs that have global and regional implications. For example, repairing cuts in underwater sea cables often requires permits and cross-border movement of technical equipment or experts, and governments can help ensure that those actions are expedited. Alternatively, a cyber event with large-scale impacts, such as the Shamoon attacks in 2012,[8] could require the rapid movement of hardware from one place to another, the need for international technical collaboration between and among governments and the private sector, and the waiving of legal barriers in times of national emergency to facilitate recovery.

8 Clark, Jack. "Shamoon malware infects computers, steals data, then wipes them." ZDNet. August 17, 2012. http://www.zdnet.com/shamoon-malware-infects-computers-steals-data-then-wipes-them-7000002807/

The need for a multi-stakeholder approach

The ecosystem of potential stakeholders in the development of cybersecurity norms is diverse. It involves a myriad of players with differing agendas, varying levels of expertise, and multiple cultures and values. Microsoft sees ICT industry, civil society, and academia as being necessarily involved alongside governments. Governments might avoid development of cybersecurity norms that limit conflict because they have concerns about the impact to their national security options. This view is short-sighted, since it not only ignores the other roles of government, as ICT user and protector, but also erodes the confidence of enterprises, citizens, and other governments. This lack of confidence would impede economic growth and technological innovation and would stifle engagement of civil society, thereby undermining the capability of the state to protect itself, its citizens, and its national interests in the long run.

As the Information Age matures, the roles and expectations of government, industry, and everyday users in relation to national security and public safety are rapidly changing. ICT innovations are driving exponential growth of data and are creating capabilities that may previously have been limited to governments with the resources to invest in R&D without an immediate return. In this context of complexity, all stakeholders—not just governments—must be prepared to adapt to changes, deal with differences, and constantly learn.[9]

In efforts to improve cybersecurity, the need for multiple stakeholders is an operational reality rather than an ideology. The development of cybersecurity norms cannot be a niche foreign policy issue reserved for diplomats. Cybersecurity norms are an imperative for all users, governments, the private sector, non-governmental organizations (NGOs), and individuals, in an Internet-dependent world—each contributes to the peace, security, and sustained innovation of a globally interconnected society. These stakeholders can and should contribute their expertise to the norm development process, acknowledging that all stakeholders may not be equal partners in every effort due to different levels of expertise. Developing soft norms that gradually morph into customary international law will allow for strong input by the private sector, academia, and civil society. Law-making or adoption of potential treaties, however, should remain the prerogative of governments and subject to national political processes.

9 Adapted from: "Complexity, a conversation with Brenda Zimmerman." Tamarack Learning Centre. 2005. http://www.outcomemapping.ca/download.php?file=/resource/files/simonhearn_en_Complexity__a_conversation_with_Brenda_Zimmerman__2005_155.doc

Exploring the role for the private sector

Although this document is largely focused on governments, the private sector has important work to do, as well. Microsoft works to provide all of our customers with secure, private, and reliable computing experiences. We do this by ensuring the security of our own products and services, by helping customers improve the security of their operations, and by working with others throughout cyberspace to manage risks. Providing our customers with secure computing also involves a wide range of efforts to protect, detect, and respond to threats. The following practices have proven effective, in our experience, and we encourage other ICT companies to adopt similar approaches, including:

- **Reduce attack surfaces and harden systems.** One of the most effective approaches to minimizing the possibility and potential impacts of cyber conflict is to leverage rigorous processes, tooling, and training to securely develop, operate, and maintain ICT products and services. The private sector should work toward this goal by following accepted best practices, such as those contained in ISO 27034. Other enterprises can follow cybersecurity risk management processes to reduce their own attack surface. Simply put, offensive operations and cyber weapons often leverage technical weaknesses in ICT products and systems, and reducing those is likely to mitigate the potential for and possible impacts of cyber conflict.
- **Coordinate vulnerability responses.** The private sector should continue to follow the principles of Coordinated Vulnerability Disclosure[10] and should encourage governments to do the same. If properly handled, all players will ultimately benefit from improved security and resilience stemming from vulnerability disclosure, and, just as importantly, from greater confidence in the system. Nevertheless, the ICT industry should also explore how actively tracking, recording, and sharing the number, types, and quality of vulnerabilities reported by governments would affect the ecosystem. Understanding this point is critical because, although sharing government-reported vulnerabilities might seem simple, it could easily create misperceptions or, worse, drive new irresponsible state behavior.
- **Exchange information to limit the number, diversity, duration, and impact of attacks.** The private sector should work to determine how it can best counter the proliferation of cyber weapons and limit their impact. This can be accomplished through exchange of information between affected entities. For example, to help protect their customers, software vendors can share information on new and suspected attacks. This collaboration should begin when an event is detected and continue until the associated risk has been appropriately managed. Similarly, software providers, security researchers, law enforcement, Internet service providers (ISPs), and CERTs can engage in coordinated efforts to eradicate specific strains of malware by combining legal and technical measures.

10 Coordinated Vulnerability Disclosure principles require that newly discovered vulnerabilities in hardware, software, and services be disclosed directly to the vendors of the affected product, to a CERT or other coordinator who will report to the vendor privately, or to a service that will likewise report to the vendor privately. http://technet.microsoft.com/en-us/security/dn467923.aspx

- **Respond to and recover from attacks.** The private sector should respond to vulnerabilities in its products and to attacks on its products, services, and customers and should bring to bear its telemetry, situational awareness, and incident response functions to deal with complex security attacks. ICT companies are experts at operational risk management and incident response and, on a daily basis, prevent countless attacks from becoming major incidents. However, responding to the consequences of state or state-sponsored attacks can be more challenging. For example, although Stuxnet targeted one location, it ultimately spread to over 100,000 systems in more than 100 countries.[11]

  Corporate response teams, such as the Microsoft Security Response Center (MSRC), and cross-industry organizations, such as Industry Consortium for Advancement of Security on the Internet (ICASI), provide real-time response to emerging threats. By working with governments, and by building confidence and mutual understanding over time, private sector response teams can enhance their effectiveness and help reduce the risks of misunderstanding or active non-cooperation during high-stress events.

Beyond directly defending cyberspace, we believe that the private sector has two additional roles to support and advance cybersecurity norms. First, the private sector is best placed to provide technical expertise for governments on a wide range of cybersecurity challenges, including on each of the norms proposed in this paper. The private sector is already an active contributor to the process. For example, public/private partnerships are central to helping countries reduce cybersecurity risks by protecting critical infrastructures, providing forensic support to law enforcement, implementing incident response, and working with policy experts to craft and revise effective national strategies and regulations. Second, the private sector delivers, in whole or in part, much of the critical information infrastructure on which society depends. Accordingly, discussions on protecting the most sensitive and vital functions from offensive cyber activities must necessarily involve the private sector to determine the infrastructure that supports those functions. For example, many core Internet services, such as the Domain Name Systems (DNS) or Public Key Infrastructure (PKI), underpin other vital services. Using the framework introduced earlier, actions against DNS and PKI would create unacceptable impacts and, therefore, should be out of bounds for offensive cyber activities.

11 Yeo, Vivian. "Stuxnet infections spread to 115 countries." ZDNet. August 9, 2010. http://www.zdnet.com/stuxnet-infections-spread-to-115-countries-3040089766/

Venues, structure, and fora to develop norms

Making progress in this context is not a trivial task. The development of cybersecurity norms challenges governments across user, protector, and exploiter roles. Furthermore, current discussions are taking place in numerous fora, each with varying actual and perceived ability or authority to control, influence, implement, or hold players accountable. As a result, if cybersecurity norms to limit conflict do emerge or evolve, it is likely that they will do so incrementally and from many different sources.

The post-war institutions that have, in modern times, provided a crucible for states' norm development processes are increasingly being challenged. The UN Human Development Report 2013 noted that developing countries (the Global South) with "…its growing diversity in voice and power, is challenging the principles that have guided policymakers and driven the major post–Second World War institutions. Stronger voices from the South are demanding more representative frameworks of international governance that embody the principles of democracy and equity."[12] If the development of cybersecurity norms is going to be a truly global endeavor, the perspectives of developed and emerging economies must be taken into account.

Despite this reality, there are currently no dedicated multi-stakeholder fora for developing cybersecurity norms. Indeed, as previously noted, many governments seem hesitant about including non-government actors in this process, even though multi-stakeholder environments are already defining national and international policy. Therefore, in forging a way ahead, key questions to answer must include:

- What (new or existing) bodies can bring together the breadth of expertise and equities to develop cybersecurity norms?
- Where are the institutional capabilities and energy to host the debate and dialogue needed to build a normative framework?
- Could there potentially be an incremental approach that resonates across the multi-stakeholder community?

We believe that there are (at least) five non-exclusive options for moving forward on cybersecurity norm development:

- **Bilateral consultations.** Many countries have set up bilateral consultations on cyberspace. This work is important, since it drives increased transparency around state behavior in cyberspace, as countries begin to identify relevant structures and to share contact lists and (military/national security) doctrine. However, as previously outlined, bilateral consultations alone are not sufficient to increase the stability and resilience of cyberspace. Moreover, it is often the case that private sector owners and operators of the impacted ICTs and civil society don't often get invited to such dialogue. Although many governments are confident in their ability to manage regulated telecommunications infrastructure in international negotiations, cyberspace is different—with software and services that are often not as clearly bound to geographic location.

12 *Human Development Report 2013: The Rise of the South: Human Progress in a Diverse World.* United Nations Development Programme. 2013. http://hdr.undp.org/sites/default/files/reports/14/hdr2013_en_complete.pdf

- **Regional approaches.** In developing new norms of behavior, another option is to leverage existing dialogues in this space. One example could be building on the debate on the Network and Information Security (NIS) Directive[13] in the European Union and extending the dialogue to international norms, first in Europe and then internationally. The similar focus of the NIS Directive and the Cybersecurity Framework[14] on cyber risk management and on protecting critical infrastructures in the United States provides opportunities for alignment. Building on those efforts to extend the normative behavior of the critical infrastructure to other regions around the world would be a meaningful step.
- **G20 + ICT20.** A third option could be leveraging existing frameworks, such as G20, and extending them to 20 leading ICT providers (ICT20). The G20 + ICT20 would have the advantage of being global in nature yet manageable in terms of size. An agreed-upon norms document between these stakeholders could represent a powerful contribution to a first cybersecurity norms baseline. It would also allow the 20 most developed economies to hold themselves and others accountable to the agreed-upon behaviors in cyberspace. The drawback of such a group is its lack of truly global representation and its limited input from civil society. However, creating a G20 + ICT20 and top 20 nongovernmental organizations (NGO20) could improve collaboration and improve outcomes on norms. It will not be easy to establish criteria for selecting the ICT20 and NGO20, but it is well worth the effort to address this challenge.
- **The London Process—conferences on cyberspace.** Another option is to create a standing committee for developing cybersecurity norms and to leverage existing cyberspace conferences (also known as the London Process) to drive debate, dialogue, and progress on norms. The London Process has many of the necessary players, but it is focused on a wide array of issues beyond advancing norms. While these issues are crucial in their own right, creating a standing committee to focus on norms would accelerate progress in this area.
- **NETmundial for cybersecurity.** An additional option is to leverage the NETmundial[15] model and see whether a similar process could be used for cybersecurity norms. NETmundial brought together an unprecedented set of stakeholders[16] and offered a model of participatory plurality. Although not perfect, it did prove that a broad-based multi-stakeholder environment could make progress on challenging issues like Internet governance.

Each of these fora has benefits and limitations for the development of cybersecurity norms, and, again, work in this space is likely to occur through all. Working to both synergize and to clearly differentiate among these efforts would likely optimize resources contributing to this multi-stakeholder approach.

13 "EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive." European Commission. July 2, 2013. http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

14 "Cybersecurity Framework." National Institute of Standards and Technology (NIST). November 12, 2013. http://www.nist.gov/cyberframework/index.cfm

15 "NETmundial: The beginning of a process." NETmundial. April 2014. http://netmundial.br/about/

16 The NETmundial High-Level Multistakeholder Committee is composed of ministerial representatives of 12 countries (Argentina, Brazil, France, Ghana, Germany, India, Indonesia, South Africa, South Korea, Tunisia, Turkey, and the United States of America), 12 members of the multi-stakeholder international community, representatives of the International Telecommunication Union (ITU), the Department of Economic and Social Affairs (DESA) of the United Nations, and representatives of the European Commission.

Conclusion

Cybersecurity norms are needed by states, the private sector, and citizens. Without them, there is a genuine risk that threats in cyberspace could escalate and undermine economic growth and technical innovation or, worse still, lead to substantial and lasting harm to physical or cyber critical infrastructure. However, even though discussions on the development of cybersecurity norms are ongoing, it seems that, short of a major cybersecurity event, governments are unlikely to develop and commit to effective norms that demonstrably reduce risk and the possibility of cyber conflict.

Governments have a leading role to play in developing cybersecurity norms; however their challenge is that they must do so while balancing diplomatic, intelligence, military, economic, and law enforcement agendas. On the other hand, ICT companies, academics, and NGOs have deep technical expertise, considered perspectives on the future, and practical understanding of the consequences of untrammeled state actions; their challenge is to build the necessary partnerships with governments to bring those insights to inform discussions.

Although nation states, intergovernmental organizations, and NGOs are traditional "norm entrepreneurs," private actors have taken leadership roles in the development of international norms in a variety of areas. In the 17th century, while counsel to the Dutch East India Company, Hugo Grotius wrote *Mare Liberum*, and, in the 20th century, government, labor, and business worked together to create the International Labor Organization and its associated standards. The Chemical Weapons Convention depended upon private sector experts to develop government positions and verification systems, without which similar treaties could not have been successfully formulated and ratified.[17]

Developing cybersecurity norms cannot be, and will not be, a linear process owned and controlled by any particular country or international institution. Progress toward a more secure cyberspace is only likely with a multi-stakeholder approach, one that starts with existing confidence-building measures and that ultimately arrives at comprehensive cybersecurity norms. These norms should take into account the sovereignty of nation states, must be rational and practicable, and should aim to make a noticeable difference. We believe that the results of such an approach will be in the interest of all stakeholders—from governments seeking to protect their sovereignty, economies, and citizens, to businesses seeking to protect their customers and to ensure that their products, services, and innovations aren't turned into weapons or conduits for cyber attacks.

It is time that the emerging discussion around cybersecurity norms takes on a more concrete form regarding substance, process, and possible outcomes. The development of cybersecurity norms is one of the critical tasks of our time, for governments, the private sector, and anyone relying on the confidentiality, integrity, and availability of the technologies that make up cyberspace. This paper does not provide all the answers needed, but it proposes six norms to move the debate forward and help reduce cyber conflict.

17 Clarke, Richard A. *Securing wwwCyberspace through International Norms: Recommendations for Policymakers and the Private Sector*. www.goodharbor.net/media/pdfs/SecuringCyberspace_web.pdf January 2013.

Six proposed cybersecurity norms

NORM 1: States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.

NORM 2: 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.

NORM 3: States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

NORM 4: States should commit to nonproliferation activities related to cyber weapons.

NORM 5: States should limit their engagement in cyber offensive operations to avoid creating a mass event.

NORM 6: States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.