Governments and APTs: The Need for Norms

SCOTT CHARNEY
Corporate Vice President
Trustworthy Computing Group
Microsoft Corporation

Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA

[1] Version 1.0 of this paper was originally titled, “Rethinking the Cyber Threat: An Overarching Framework.” The paper was renamed to provide distinction from the predecessor paper and reflect the key discussion point.

TABLE OF CONTENTS

Introduction

In 2009, I published a paper entitled "Rethinking the Cyber Threat."[2] The premise of that paper was that then-current efforts to craft meaningful cybersecurity strategies were challenged by the range of threats we faced. Instead of trying to "boil the ocean," it was important to decompose cyber threats into discrete categories because different threats required different strategic and operational responses. I broke these threats into four buckets -- -- cybercrime, military espionage, economic espionage and cyber warfare – and then wrote about the strategic challenges in each area.

In the years since that paper was published, new threats to computer security have emerged, existing threats have been amplified, and proposed operational tactics have led to serious debates on the trade-offs between security and civil liberties. In the first category (new threats), there have been disclosures regarding surveillance programs targeting world leaders and terrorists (most of this reporting focused on the United States' National Security Agency even though such activity is clearly not limited to the American spy agency). These programs may have a valid purpose (stop terrorist attacks) but nonetheless represent a threat to computer security, long defined as the protection of the confidentiality, integrity and availability of data and systems. In the second category (amplified threats), there have been widespread reports of countries engaging in economic and military espionage, as well as reports that several countries are increasing their offensive cyber capabilities. Additionally, we have now seen widely destructive attacks, such as the attack on Saudi Aramco.[3] This is important because one response to these amplified threats is to promote new operational tactics, tactics that are often controversial. For example, a directive supporting the retention of telecommunications data in the European Union was adopted and then struck down by the European Court of Justice,[4] and information sharing legislation was proposed in the United States (e.g., the Cyber Intelligence Sharing and Protection Act, or CISPA) but challenged on civil liberties grounds.[5]

In light of these changes to our environment, it is clearly time to revisit my earlier work and provide a new way to think about cyber threats and operational responses more generally. In this paper, I propose a new framework for thinking through these issues and then test that framework against recent events and the concerns that prompted my earlier paper.[6] In the end, I believe this framework will permit us to work through a host of challenges, creating clarity by either facilitating consensus on strategies and tactics or, in some cases, bringing into sharper relief those areas where people may "agree to disagree."

[2] http://www.microsoft.com/en-us/download/details.aspx?id=747.
[3] http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0
[4] http://epic.org/privacy/intl/C0293-2012-EN.pdf
[5] http://www.pcworld.com/article/2035682/house-approves-cispa-over-privacy-objections.html
[6] The author thanks Jeff Jones of Microsoft for his significant contributions to this framework.

In the end, the framework leads to five conclusions. First, in many cases, the societal debate is not about "objectives," but whether the actions taken – and the impact of those actions – are acceptable. Second, the time has come for countries with espionage programs to acknowledge that they target other governments or engage in military espionage without, of course, sharing particulars. Third, after doing so, governments need to have separate discussions about espionage programs that target private sector intellectual property (i.e., economic espionage). Fourth, governments must agree that the doctrine of proportionality, long applicable in times of war, must be expanded to address attacks on civilian products, services, and infrastructures in times of peace. Fifth, it is important for governments to appreciate that while private sector companies can help improve the overall cybersecurity ecosystem through technology and operational advances, they have limited abilities to curb nation-state hacking related activities.

The Need for a New Framework

My original paper addressed four specific types of threats: cybercrime, military espionage, economic espionage, and cyber warfare. While these threats remain quite real, they have been supplemented by recent allegations regarding the surveillance of government officials and the existence of bulk collection programs designed to combat terrorism by "finding needles in haystacks" (that is isolate terrorist activities from a much broader swath of communications activities). These allegations involve access to and surveillance of computer networks in ways that I did not address in my original paper and that do not neatly fit into the four categories described earlier. For example,

- Governments may conduct surveillance to uncover another country's future diplomatic position, such as whether it will support sanctions against a third state, but this does not constitute military espionage or cyber warfare;

- Governments may surveil communications to discover another country's economic position prior to a trade negotiation. This activity – which could be described as "economic espionage" because it is, after all, spying on economic matters – was not the focal point of my prior paper where economic espionage was used to refer to the stealing of private intellectual property and transferring it to the victim's competitors to create an unfair competitive advantage in the marketplace; and

- Government may collect telephone transactional records and surveil communications to identify terrorists and/or disrupt terrorist plots, but such activity does not neatly fit into the category of cybercrime because the actions may be legally authorized and, even if legal violations are found, the next steps will be guided not by the implementation of cybercrime strategies but a public policy process that determines whether such programs should be terminated, re-authorized, or re-authorized with modifications.

Other threats, such as those related to economic and military espionage, have escalated over time, leading to increased tension between nation-states and stronger calls for operational responses. This has included a range of options, from increased information sharing, to active defenses, to even calls for private companies to "hack back" and disable their attackers. With so many threats, actors and options, we need a framework that allows us to act in a principled and consistent way as we seek to address the threats to information networks, as well as traditional threats.

The New Framework

The new framework is quite simple and can be portrayed as follows:

Each of these elements has unique relevance. The "actor" may be government or civilian, an important point because governments can engage in activities that the private sector cannot. For example, governments can use military force, leverage compulsory processes, and arrest individuals. The "objectives" are important since they must both be lawful and socially acceptable. The "actions" taken must support the objectives in responsible ways; arguments that "the ends justify the means" (i.e., if the objective is acceptable, any action in support of that objectives is acceptable) rightfully fails. Finally, the impact relates to the impact of an "action" relative to the "objective," as well as any collateral impact caused by the action. This "impact" analysis will often be challenging in part because, as we will see, measuring impact is often difficult. Notwithstanding that fact, the beauty of this framework is that it allows us to focus our debates on the areas that matter most, and clearly identifies those issues of greatest strategic and/or tactical concern. By focusing our discussions in this way, the framework helps parties achieve consensus or identify points of disagreement.

The value of this framework can be seen if we apply it to a real-life experiences regarding airport security. Airport security is a governmental function (even if private companies provide some of the services at government direction) and the objective is airplane and passenger safety. As this is universally agreed to be an appropriate objective, one then looks to the actions taken to protect planes. First, airports used metal detectors. The impact of this "action" was that weapons could be found but

that people had to be screened, causing some delay and impacting privacy. Most people concluded that the beneficial impact outweighed the negative impacts and metal detectors were widely accepted.

After a plot was revealed in which liquids might be used to destroy airliners, the U.S. Government moved to full body scanners based upon x-rays. Once again, there was government action with an accepted objective, but now the impacts included exposure to radiation and graphic images of bodies. Notwithstanding government assertions that these issues were minor, the public reaction suggested otherwise; that is, even if the "objective" was still proper, the "impacts" from these "actions" were deemed unacceptable. In response, the government moved to backscatter technology (radio waves) and more opaque images. The "impacts" now reduced, the "actions" reasonably supported the "objectives" and public opposition abated.

The framework works equally well for the allegations of NSA surveillance programs designed to prevent terrorist attacks. Once again, there is government action and an acceptable objective. Thus, we can turn our attention to the actions taken: domestic and international programs designed to collect and analyze information to find "needles in haystacks." Turning to the "impact" of these programs, there were many. First, the U.S. Government's NSA director stated that these surveillance programs prevented 54 terrorist attacks around the world, including 13 in the United States.[7] Some questioned, however, whether these surveillance programs played a significant role in preventing these attacks.[8] Second, many expressed concerns that these programs constituted a massive invasion of privacy, in part because such mass collection means that data related to innocent people is also collected. Third, the impact of this collection has strained international relations, particularly with some key U.S. allies. Fourth, these collection programs – as well as the United States Government's ability to compel those doing business in the U.S. to provide data in secret – has injured U.S. competitiveness globally.[9] Thus, the framework highlights that the important debate is not on the program's objectives, but whether the actions in support of that objective were appropriate as measured by an impact analysis.[10]

Applying the New Framework to Cybercrime and Espionage

To be viable, the framework described must also apply to and yield insights on some of the challenges addressed in my original paper. Turning to cybercrime, it is easy to conclude that combatting cybercrime is an objective valued by citizens, businesses, and governments. Indeed, Microsoft itself has

[7] http://www.cnn.com/2013/07/31/tech/web/nsa-alexander-black-hat/index.html.
[8] See President's Review Group on Intelligence and Communications Technologies, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[9] See "NSA Snooping's Negative Impact On Business Would Have The Founding Fathers 'Aghast'," http://www.forbes.com/sites/realspin/2013/12/20/nsa-snoopings-negative-impact-on-business-would-have-the-founding-fathers-aghast/; "NSA spying hurts business of large U.S. hardware makers," http://www.usatoday.com/story/tech/columnist/shinal/2013/12/08/nsa-spying-has-damaged-overseas-business-of-strongest-us-tech-companies/3891765/; and The Foreign Policy Essay: Cheng Li and Ryan McElveen on "NSA Revelations Have Irreparably Hurt U.S. Corporations in China," http://www.lawfareblog.com/2013/12/the-foreign-policy-essay-cheng-li-and-ryan-mcelveen-on-nsa-revelations-have-irreparably-hurt-u-s-corporations-in-china/.
[10] Reasonable minds may often differ on these difficult issues. For example, Microsoft has stated clearly that it opposes the bulk collection of data while government officials have continued to defend it. The key point in this paper, however, is that the framework gives us a structured way to identify the core issues that warrant discussion and resolution.

dedicated resources to combat cybercrime, through botnet takedowns in the civil court system, and through leveraging technology. Still, the new framework yields two important insights. First, while some have proposed that private companies "hack back" against adversaries, this ignores the importance of defining the "actor." Simply put, private sector actors do not have the authority to engage in such conduct, nor can it leverage the domestic and international legal regimes designed to authorize government investigations. Moreover, while the parties may agree on that combatting cybercrime is a proper objective, this does not mean there is complete agreement on the "actions" that should be taken in support of that objective. For example, as noted above, programs supporting data retention and information sharing have been controversial. In short, the framework highlights the core question: "what actions are appropriate in the fight against cybercrime?" It is a question that can only be answered by an impact analysis that weighs the efficacy of a given approach against any negative consequences, in particular where privacy is concerned. Moreover, such an analysis suggests that a comparative process must be used; in evaluating actions and impacts we must ask whether other actions will yield a better result (more positive impact; less negative impact).

The framework also helps sort through complicated espionage issues. In my initial paper, I focused on two types of espionage: military espionage and economic espionage. Recent events make it clear that a more nuanced taxonomy is required. Some governments do, of course, commit espionage for such purposes, but they also commit espionage for other reasons related to affairs of state. This is because a government may want to understand another country's position on a wide range of issues, including political and trade issues. Such information collection has been going on since time immemorial and continues today; as such, it is time to admit the existence of such state-to-state programs.

At first blush, it may seem like heresy for governments to admit they spy on each other, but there are many reasons why such an admission would shock no one yet still be productive. First, of course, countries frequently admit their prowess in espionage, at least after enough time has passed so that it no longer reveals specific and important capabilities.[11] Second, current research and reporting makes clear that certain governments engage in such activities routinely.[12] Third, one could argue that many citizens fully expect their intelligence services to be engaging in some forms of espionage, particularly military espionage, to protect national security. Finally, the United States has made such an

[11] See, e.g., F.W. Winterbotham, "The Ultra Secret," 1975.

[12] For an example of such allegations, see the following stories: "US retaliation risks a trade war with China," http://www.todayonline.com/commentary/us-retaliation-risks-trade-war-china (All governments conduct espionage on both friends and rivals, focusing on their political plans and military capabilities.); "Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies"; May 27, 2013, (http://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html); "Five myths about Chinese Hackers", http://articles.washingtonpost.com/2013-03-22/opinions/37923854_1_chinese-hackers-cyberattacks-cold-war ("The Internet, poorly secured and poorly governed, has been a tremendous boon for spying. Every major power has taken advantage of this…."); and "China cyber victim claims a red herring: analysts", http://www.globalpost.com/dispatch/news/afp/130221/china-cybervictim-claims-red-herring-analysts' "'Major nations could be expected to carry out military and spy work in cyberspace as part of traditional war-planning and information-gathering,' said [James] Lewis, director of CSIS's technology and public policy programme."

admission without causing shock among either allies or adversaries,[13] at least until the breadth of those programs were revealed. In short, particularly for those countries that are technologically advanced, governments would merely be admitting the obvious.

If it is generally recognized that such activity occurs, why is it important to explicitly confirm this fact; why not let it remain an open secret? There are two reasons. First, as use of our framework makes clear, a proper objective may be pursued with actions that some believe cause inappropriate impacts. Thus, by admitting the existence of such programs, governments can have a more focused conversation about what actions and impacts are permitted in pursuit of legitimate nation-state objectives. Indeed, recent calls for norms of behavior are based, in part, on the concern that states pursuing legitimate objectives have used or may use inappropriate tactics.

A second and related point is that because the term "espionage" has multiple meanings, there has been a lack of clarity in these normative discussions; countries accusing each other of "espionage" may be referencing state-related espionage (including military espionage) or economic espionage. By admitting the former, countries can focus more clearly on the latter and we can eliminate the blanket denials that have long impeded the nuanced discussions that ultimately must occur.[14] They must ultimately occur because even if one leaves aside that a country's embrace of economic espionage depends on many factors (including moral convictions, political convictions, economic theory, and practical assessments of advantages and risks), such philosophical conflicts between nations may seriously impact future relations and threaten global commerce.[15]

To be clear, the term state-related and economic espionage must be appropriately scoped. "State-related espionage" cannot solely be about governments attacking government systems because the private sector may be actively and directly involved in critical governmental functions. By way of example, private sector companies may be involved in the production of military aircraft, tanks, and other weapons. To the extent countries have an interest in understanding the military capabilities of potential adversaries, they will undoubtedly target private sector companies making weapons of war. Similarly, "economic espionage" cannot broadly refer to any economic information, since countries may engage in espionage on trade related matters. The real issue is whether a government is engaging in

---

[13] See "Obama: Difference Between Spying And Hacking", Associated Press, Tue, 06/18/2013. Calling such spying "standard fare" between nations, President Obama said that every country engages in intelligence gathering, which he called an occasional source of tension. But the President also said there is a big difference between China trying to find out what he is saying in meetings with the Japanese and a hacker connected with the Chinese government breaking into U.S. companies. http://news.yahoo.com/obama-difference-between-spying-hacking-125922007.html. Similarly, while the U.S. Government has categorically denied attacking its ally the French (http://www.theverge.com/2012/11/21/3674804/us-france-sarkozy-cyberattack-hack-spyware-virus), the Director of the National Security Agency has said, "we have an interest in those who collect on us as an intelligence agency." http://abcnews.go.com/Politics/week-transcript-nsa-director-gen-keith-alexander/story?id=19457454&singlePage=true#.UcjKnk_n-Un. (The ABC News Website noted that the transcript was rushed and may be updated.)

14 See, for example, "China's military denies hacking allegations," http://money.cnn.com/2013/02/20/technology/china-cyber-hacking-denial/index.html; Ministry Denies Hacking Charge, http://www.kommersant.com/p-13701/r_500/information_security/ (Russian Foreign Ministry calls charges that Russia is behind cyber-attacks on the U.S. Pentagon unproven and irresponsible).

[15] For competing views of the impact of this issue on international relations, see "Cyber-espionage: Is industrial cyber-espionage the biggest threat to relations between America and China?" at http://www.economist.com/debate/days/view/961.

(or permitting) attacks against commercial entities for the purpose of assisting domestic companies and ensuring they have a competitive advantage in a global and supposedly fair marketplace. In the terms of our framework, the critical question is whether the "objective" is appropriate. If one concludes that it is not, then any actions taken in support of that objective – and the resulting impacts – are unacceptable as well.

In deciding whether the objective is appropriate, it is important to recognize that economic espionage creates a unique set of problems, especially when governments engage in such activities. If a government is the actor, it can utilize a range of tactics and capabilities that private sector actors would not, and victim companies cannot reasonably expect to withstand such tactics even if they maintain best-practices in terms of IT technology and operations. For example, government are more likely to engage in supply chain attacks, intercept communications, engage in surreptitious physical searches, and/or affirmatively embedding spies into private sector organizations of interest. Additionally, if a government supports such activities either directly or tacitly, then there is no likelihood of meaningful criminal prosecution against those actors who engage in intellectual property theft, eliminating an important deterrent.[16]

It is safe to say that governments do not have a unified view on whether economic espionage is an appropriate objective. Some may rely upon the simple argument that if economic security is critical to national security, then using state powers to enhance a country's economic competitiveness is appropriate. Others argue against such programs, believing such conduct is both immoral (theft is theft, even if the property is intangible) and, in many cases, illegal. But more importantly, in a macro-economic sense, such espionage has a distorting effect on the global economy if those who bear the expense of research and development are unable to realize the profits that come from a lack of competition in the early phases of a market for a novel product or capability.[17] By accelerating the transfer of economic value from the original owner to the recipient of the stolen property, such activities undermine a major incentive for innovation: the monetary reward that accrues to the innovator.

The Framework and the Creation of Cyber Norms for Government Actors

To the extent the framework brings into sharper relief the issues to be resolved, it is also the starting point for more meaningful discussions of government cyber norms. Put another way, any cyber norms discussion has to begin with the question, "what objectives, actions and impacts are or are not acceptable in the pursuit of national interests"?

---

[16] With great fanfare, the United States Government indicted five members of the Chinese Government for economic espionage. There is little likelihood that the prosecution of these individuals will move forward and the indictment has served to be a noisy demarche as opposed to a major deterrent.

[17] "The moral justification of espionage (let alone covert action) is highly dubious in the service of preserving or enhancing the global competitiveness…." David Perry, ""Repugnant Philosophy": Ethics, Espionage, and Covert Action, http://www.scu.edu/ethics/publications/submitted/Perry/repugnant.html.

This issue is taking on increasing importance as societal dependencies on Information and Communications Technologies (ICT) grows and attacks become more destructive. Even if one accepts that governments will conduct certain forms of cyber activities, there remains the question of whether government activities that impact civilian infrastructure and commercial products must be bounded in some agreed upon and potentially formal way (e.g. a treaty). It is of course true that critical infrastructures and commercial products are used by governments and their militaries: power is needed at military bases, financial institutions may be used to pay soldiers and purchase weapons, phone networks may allow military personnel to communicate with commanders, and commercial-of-the-shelf (COTS) hardware and software may be used to run government and military networks. But unlike military weapons which are meant to be used solely by militaries, citizens all over the world rely upon these critical infrastructures and COTS products for every aspect of digital life and digital work. Power, telecommunications and IT systems may be necessary in times of war, but they are also necessary in times of peace; for example, civilians use these systems to address everything from the mundane (e.g., online shopping) to the critical (e.g., responding to life threatening medical emergencies).

That ICT is "dual use" (used by both governments and civilians; used for both military and civilian purposes) has important global implications. This is all the more true now that computer attacks, long-focused on computer exploitation (the theft of data), have become destructive. These new types of peacetime attacks, such as Stuxnet and the attacks on the oil and gas industry[18] may have impacts on the civilian population that are immediate, severe, and widespread. Additionally, the impacts may unfold in unintended and unpredictable ways.

In exploitation cases involving information theft, the impact can well be serious, but often the impact is not immediate. This explains, in part, why it is hard to mobilize organizations to address trade secret theft. When physical property is stolen, the impact is virtually instantaneous. When a car is stolen, there are police and insurance reports to file, a new mode of transportation must be acquired, and there are other related inconveniences and expenses. By contrast, if a company has its customer and price lists "stolen" (i.e., copied), the victim still has its information and can continue operations without immediate disruption. Yes, the loss of this material may result in the loss of customers and even the complete failure of the business, but that will occur over time and causation (that the theft led to the failure) may be hard to prove. Moreover, while people tend to have visceral reactions to threats against their person and property, the theft of "bits" does not cause a fight or flight response. This helps to explain why people may tense up when confronted by a stranger on the street, but often share personal information with unknown individuals over the Internet.

Second, the impact of destructive attacks on the Internet may be severe and widespread, with a disproportional impact on the civilian population. This is in large part because of the interconnectivity between – and the dependency among – different systems. A kinetic attack on a power station may

[18] These attacks involved Saudi Aramco, a state-owned enterprise (http://www.saudiaramco.com/en/home/about/who-we-are.html), and RasGas, which is jointly owned by Qatar and ExxonMobil (http://www.rasgas.com/AboutUs/AboutUs_TheCompany.html).

have dramatic implications for a local area, but malware attacks that spread across a nation or the globe with rapidity pose a fundamentally different hazard, as evidenced by the Morris worm (which crippled the Internet) and Slammer (which affected a multitude of systems in different sectors such as finance and transportation). With increased dependency on IT networks, attacks against critical infrastructures pose significant risk; for example, an attack on a telecommunications system may result in a heart attack victim being unable to reach emergency medical services.

Finally, even when governments attack government targets, the results may be unpredictable. For example, the Stuxnet worm, which leveraged four zero day vulnerabilities and which was allegedly launched by governments to target another government's nuclear facility,[19] leaked into the public domain. This led to malware variants, attacks on innocent parties, and the releasing of updates that needed to be deployed by IT users worldwide. In short, cyber weapons used by governments may be uncovered by a global community of cyber-actors which includes both government and civilian cyber-security professionals. This community then deconstructs the weapon on an accelerated basis and the learnings become useful not just to these communities for defense, but to other actors for less noble purposes. At that point, not just the targeted victim is impacted; rather, there is an increased risk that a non-state actor who cannot be deterred by other means will have a new capability, one initially thought to be in the province of only the most-sophisticated nation-state actors.

To the extent governments cause these effects, they are responsible for evaluating appropriately whether their actions outweigh societal costs. In the wartime context, governments do think about proportionality. Proportionality requires a balancing test between the concrete and direct military advantage anticipated by attacking a legitimate military target and the consequences of the attack, often expected incidental civilian injury or damage. Under this balancing test, excessive incidental losses are prohibited.[20] Thus, even though attacks against civilian infrastructures are not uncommon in times of war, they are not unfettered. If an attack that impacts civilians must be constrained in times of war, it would be odd indeed to provide less protection in times of peace. Indeed, such a balancing test is already used in some cases.[21] Thus, even though countries may debate whether or not the Laws of Armed Conflict apply to the Internet[22] -- and they may even debate when a cyber-event constitutes an act of war -- the time has certainly come for countries to agree that proportionality applies to destructive attacks even in the absence of armed conflict. This means, too, that countries must ensure

[19] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=1&_r=0 (describing the worm as developed by the United States and Israel, and citing interviews with unnamed current and former American, European and Israel officials involved in a cyber-program designed to undermine the Iranian nuclear program).

[20] See, e.g., http://usmilitary.about.com/cs/wars/a/loac_2.htm.

[21] See the White House Blog on conducting an equities analysis when deciding whether to share a 0 day vulnerability with a vendor for repair. http://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

[22] Increasingly, countries seem to agree that the Laws of Armed Conflict apply to Cyberspace. See "New Pact Reduces Risk of US-Russia Conflict in Cyberspace," http://www.voanews.com/content/new-pact-reduces-risk-of-usrussia-conflict-in-cyberspace/1684245.html; June 18, 2013 ("The United States and Russia already recognize that the law of armed conflict applies in cyberspace, and China recently indicated it agrees with that principle." But see, "China, International Law, and Cyberspace," http://thediplomat.com/china-power/china-international-law-and-cyberspace/ (noting that Chinese analysts see extreme difficulties to applying the Laws of Armed Conflict to the new domain). Also, see "China and International Law in Cyberspace," http://origin.www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf; May 6, 2014.)

that they consider fully the consequences of their actions, including the potential impact on the rest of the cyber ecosystem.

The Role of the Private Sector

Much has been written about the need for public-private partnerships and I will not repeat the arguments in full here. Simply put, since the private sector designs, deploys and maintains the vast majority of critical infrastructure, any government strategy to protect effectively the security, privacy, and reliability of the Internet requires a strong partnership between the public and private sector.

As both exploitation of and destructive attacks against public and private organizations have increased, many are trying to identify more meaningful responses. As an obvious first step, private parties can better protect their systems and their trade secrets, in large part by shoring up their computer security. Second, companies can sometimes pursue civil actions, although there may be issues related to jurisdiction and the ability to enforce remedies, even if ordered by a court. Third, companies can collect and present to their national governments evidence of cyber-attacks and economic espionage, thus permitting countries to use their traditional law enforcement and diplomatic powers to respond.

These responses, however, have been viewed as too weak to deter offensive activity and, therefore, the question has arisen whether private parties should be doing more to help protect themselves and the Internet more broadly. It is important to recognize that even as governments and industry struggle with exploitation and destructive attacks, the ability of private parties to meaningful drive behavioral change by governments is limited, and the public private partnership has inherent limitations.

One suggestion has been that victimized companies should refuse to engage in economic activity with the offending country, thus "retaliating" for any improper conduct. The problem with this approach is pure economics. For example, there are two major commercial airplane manufacturers: Boeing and Airbus. Which one should, to make a point, cede a major market to the other? This is not to say that commercial interests should always trump political and moral questions; to the contrary, there are clearly times when the opposite is true.[23] But the "red line" so frequently talked about in political matters is not to be drawn lightly in a complex world, and particularly when there are both philosophical and economic reasons to remain engaged even when a country's activities are problematic. For example, it is arguable whether ICT companies better promote freedoms by withdrawing from challenging markets or by spreading communications technologies. And for publicly traded companies working in a very competitive environment, abandoning economic opportunities too quickly may be a breach of fiduciary duty.

[23] Much has been written about the relationship between IBM and Nazi Germany, including Thomas Watson's return of a German medal. See generally, "IBM and the Holocaust," http://en.wikipedia.org/wiki/Thomas_J._Watson; and "IBM Statement on Nazi-era Book and Lawsuit," http://www-03.ibm.com/press/us/en/pressrelease/1388.wss.

A second suggestion is that private parties should be given the right to take offensive action against attackers, or at least that approach should be more thoughtfully considered.[24] Leaving aside problems of targeting (i.e., the inability to accurately identify the source of an attack may result in innocent parties being impacted by a counterattack), this approach is simply not viable unless every country implicated in a particular event agrees to this approach. The reason for this is that countries throughout the world have been enacting computer crime laws that prohibit hacking and, as a result, private parties would be exposing themselves -- and their employees -- to criminal charges if they took matters into their own hands.

Third, some have begun to question how the public private partnership should work as governments build new offensive capabilities to deter attacks and prepare for potential cyber warfare. As offensive capabilities have grown, there has been much written about whether particular companies may help their national authorities on *offensive* operations, as opposed to *defensive* operations.

In fact, global companies who build mass market products must, as a matter of both principle and economic survival, focus on information assurance, not offense. One cannot "take sides" and empower one customer to attack another customer, nor can one take sides and expect to be successful in a global marketplace. That being true, however, does not completely answer the question, for even a commitment to information sharing may involve sharing information – such as vulnerability information -- that may be used for either defensive or offensive purposes. Since governments have complex missions that involve both protecting and exploiting the Internet,[25] those parties sharing information with governments must appreciate that they can use the information to improve the security of the ecosystem or exploit an adversary.[26] Put another way, vulnerability information – like ICT products and services themselves – are dual use.

While it is naïve to think governments will not engage in this balancing act, the concept of dual use is not unique to the IT industry. A person can buy a car to drive to work or run over a neighbor. A

---

[24] See "Should US companies be allowed to hack China in revenge? New report says yes" http://www.theverge.com/2013/5/22/4356196/report-tells-congress-companies-should-hack-back. Notwithstanding the headline, the actual report did not promote such hacking; rather, the authors noted that while there are techniques that could cause severe damage to the capability of those conducting IP theft, they were not ready to endorse this recommendation because of the larger questions of collateral damage caused by computer attacks, the dangers of misuse of legal hacking authorities, and the potential for nondestructive countermeasures such as beaconing, tagging, and self-destructing data that are currently in development to stymie hackers without the potential for destructive collateral damage. http://ipcommission.org/report/IP_Commission_Report_052213.pdf.

[25] See Charney, Scott "Trustworthy Computing Next (February 2012), available at http://www.microsoft.com/about/twc/en/us/twcnext/default.aspx. ("While it would certainly be easier if governments were solely concerned with protecting the Internet, they have reasons to exploit it too. Economic and military intelligence may give a country a competitive advantage against friend and foe alike, and offensive military capabilities are seen as important in terms of both cyber conflict and as a force multiplier during kinetic warfare.")

[26] As Reuters has reported, the U.S. Government may develop malicious software itself or discover it through its own network monitoring. In some cases, it discloses indicators of these cyber weapons to ISPs. "CenturyLink, AT&T Approved to Immunize Key Private Networks Against Classified Threats, Nextgov," May 21, 2013. http://www.nextgov.com/cybersecurity/2013/05/centurylink-t-approved-immunize-key-private-networks-against-classified-threats/63332/.

person can buy a screwdriver to tighten a screw or break into a home. "The fruits of human inventiveness – whether punch-card machines, miracle drugs, atom bombs, or plowshare -- contain no morality whatever in themselves, but how they are used is absolutely always a moral matter."[27] Thus, the private sector must be guided by principle, and the principle must be whether the information shared is substantially related to information assurance and is being shared with others in an even-handed way. This means that whether information is shared with a particular party must depend on whether the recipient can both protect and improve assurance with the information provided.

Conclusion

In a world where every individual is increasingly dependent on information technology, it is important that governments reach agreements on cybersecurity norms of behavior and that the activities of governments and businesses be scoped appropriately. In the end, therefore, four things must happen. First, the time has come for countries with espionage programs to admit they target other governments without, of course, sharing particulars. Second, after doing so, governments need to discuss the espionage programs that target the private sector. Third, governments must agree that the doctrine of proportionality applies to attacks on civilian products, services, and infrastructures. Finally, it is important for governments to appreciate that while private sector companies can help improve the overall cybersecurity ecosystem through technology and operational advances, global companies cannot take sides in governmental disputes; rather, they must focus on information assurance and act to protect all of their customers with equal fidelity.

[27] "Hitler and IBM, Did a Company and a Machine Spawn Evil?" http://www.americanheritage.com/content/hitler-and-ibm