"Network-enabled intellectual property theft and commercial espionage threaten to undermine our national competitive advantage. Ironically, an over-energetic regulatory or bureaucratic response could be equally damaging, by constraining future web-enabled economic gains. Rather, a middle ground is needed, where government stimulates the private sector to protect its most valuable assets."

—JOHN DOWDY

The Cybersecurity Threat to U.S. Growth and Prosperity

John Dowdy
Director
McKinsey & Company

> *"…we must remember that cyber crime, cyber terrorism, cyber espionage or cyber war are simply crime, terrorism, espionage or war by other means. Cyberspace adds a new dimension, but its use in warfare should be subject to the same strategic and tactical thought as existing means."*
>
> — UK Minister of State for the Armed Forces Nick Harvey
> in *The Guardian* ("Forget a cyber Maginot line," 30 May 2011)

Introduction

Cybersecurity has attracted a considerable amount of attention recently, due to a spate of attacks on high-profile government and business targets including the CIA, Sony, Lockheed Martin and Citigroup. Internationally, both governments and corporations are beginning to recognize the scale of this cybersecurity challenge. President Obama launched a legislative proposal to tackle the challenge following the release of a recently concluded policy review, which suggested that "threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies."[1]

This article explains why addressing the cybersecurity threat is critically important for U.S. economic prosperity and why the "same strategic and tactical thought"[2] will be ineffective. Government must realize that in addition to the shift it is making from traditional physical security era approaches and mindsets, it must also make a shift to recognize that it is responsible not only for the protection of its own assets, but for cybersecurity in the private sector, as well. The need for change is not limited to government: The private sector must also recognize the severity of the threat it faces and collaborate with government and cybersecurity vendors to address it.

The stakes are high. Cyberattacks seriously challenge U.S. competitiveness by threatening two of the core drivers of U.S. economic prosperity: intellectual property (owned by both government and the private sector) and the Internet. Both government and business leaders need to respond to the threat. Government is already investing in defending its own assets, but it cannot afford to stand aside with regard to assets held by the private sector for two reasons. First, some areas of the private sector are important in government's own supply chain; second, the private sector's intellectual property is vital for economic prosperity.

Unfortunately, our research suggests that while the private sector has significant economic value at risk from intellectual property theft, neither the high value of this intellectual property, nor its susceptibility to cyberattack is fully appreciated. Businesses tend not to prioritize cybersecurity, and the government is doing less to help businesses protect their intellectual property than it is doing to help protect critical national infrastructure or its own classified information. One reason for this may be that while the security agencies have a good understanding of the extent of the threat, this understanding has not been fully absorbed in other areas of government.

In order to address this threat without acting so drastically as to compromise the Internet's contribution to the U.S. economy, the government needs to promote the emerging "security-economic complex," a system with the potential to boost cyber defense capabilities much as the military-industrial complex boosted physical defense. Four key elements of this approach are: (1) Embracing government's responsibility to support the protection of both its own intellectual property and that of private enterprises; (2) Providing incentives to private enterprise and to cybersecurity vendors to encourage enterprises to adopt a more robust approach to the threats they face and incentivize vendors to increase their investment in research and development (R&D). In such an environment, private enterprise and cyber vendors can work together with government to bring about more effective technical and managerial security solutions; (3) Providing private enterprise with enough information and knowledge transfer on the extent and nature of the threat so that companies understand what they are up against; and (4) Establishing a framework within which companies can share details of the attacks that they have faced in order to help prevent future attacks.

The advantage currently lies with cyberattackers. As a result, if the government chooses not to act, the number of attacks will continue to increase—as growing online economic activity and data storage increase the incentive of the attackers—and U.S. competitiveness will suffer.

Cyber Threat is Poorly Understood

Public understanding of the extent of the threat from cyberattacks is poor because data on cyberattacks is scarce. It is very difficult to get a good picture of the real extent and cost of cyberattacks. What, for example, was the true cost of the 2007 attacks on Estonian websites, including those of the Estonian Parliament, banks, ministries, newspapers, and broadcasters? Or of the similar attacks on Georgia in 2008? What was the impact of the alleged loss of data relating to the F-35 Joint Strike Fighter, or the attacks on Sony's PlayStation Network and EMC Corp.'s RSA unit? What was the cost to the U.S. government of the release of its data by WikiLeaks?

Definitive public figures are very hard to come by for two reasons. First, although there are government agencies (such as the National Security Agency) that systematically monitor cyberattacks across the U.S. and hence have a good understanding of the extent of the threat, these organizations do not readily share their knowledge for the sake of protecting their sources and working methods. As a result, neither the public nor many areas of government outside defense and security share an understanding of the extent of the cyber threat.[3] Second, private enterprise and government bodies often do not publicly report the attacks they experience: They have little incentive to do so,[4] and the wide variation in reporting requirements by jurisdiction allows them not to report a breach. According to Dmitri Alperovitch, a cybersecurity expert at McAfee, less than 1 percent of cyberattacks discovered by the target are reported.[5] Moreover, it is difficult to quantify even the exact costs of attacks that are publicly acknowledged. Sony, for example, has announced that it expects its recent data loss will cost the company $173 million,[6] but others have estimated costs of up to $1.5 billion.[7] And the costs of security breaches are not contained to the company alone: Sony's share price fell by 7 percent and Lockheed Martin's fell by 4 percent in the days following their attacks,[8] with resultant losses to shareholders of $2.2 billion and $1.0 billion, respectively. In contrast, the share price of EMC rose in the days following the attack on its subsidiary, RSA. Thus market response would not appear to be a reliable indicator of the cost of cyberattack.[9]

Even fewer figures are available for the economic cost of attacks on government. At the extreme, the alleged attacks on the F-35 program could, by revealing technical specifications to other countries' armed forces, compromise the U.S. government's estimated $285 billion development cost.[10] It is hard even to guess the cost of disruptions in Estonia and Georgia.

The problem is compounded when cyberattacks are not immediately recognized. We have seen examples of companies that have not discovered attacks until after their systems have been breached for considerable periods of time. The "Kneber bot" attack, for example, began in 2008 and was only discovered in 2010, after breaching more than 75,000 computer systems.[11] Operation Shady RAT, revealed by McAfee, involved attacks on more than seventy organizations spanning five years.[12] And some organizations may not be aware of a breach at all. Alperovitch, who authored the McAfee report on Operation Shady RAT, observed that "There are only two types of companies—those that know they've been compromised, and those that don't know."[13] It seems reasonable to assume that there are numerous undetected, possibly significant attacks currently underway.

Overall, extrapolating these different kinds of events into economy-wide figures is problematic. How many attacks of each magnitude occur, and with what regularity? According to a 2011 survey, more than 80 percent of critical infrastructure providers reported being the victims of large-scale cyberattacks or infiltrations—but at what cost?[14] And what number should we assign to the many incidents that are detected but unreported?

This difficulty in estimating the true cost of cyberattacks has led a number of organisations to develop top-down estimates of the scale of the issue that rely on questionable assumptions, yielding implausible figures from which no government can reliably set policy.[15]

Assessing Cyber Threats

The key threats are to critical national infrastructure, the government's classified information, and the intellectual property of private enterprise. To date, neither the government nor private enterprise has acted sufficiently to protect intellectual property. As government (outside those areas dealing with defense and security) and business are unable to accurately determine the cost of attacks, they pay insufficient attention to the value they have at risk of cyberattack and their vulnerability to such attacks. Ignorant of the facts, they are unable to prioritize how they will respond to the most serious threats.

In order to help companies and government estimate how much of their value is at risk, our team at McKinsey examined—for the whole range of attackers and

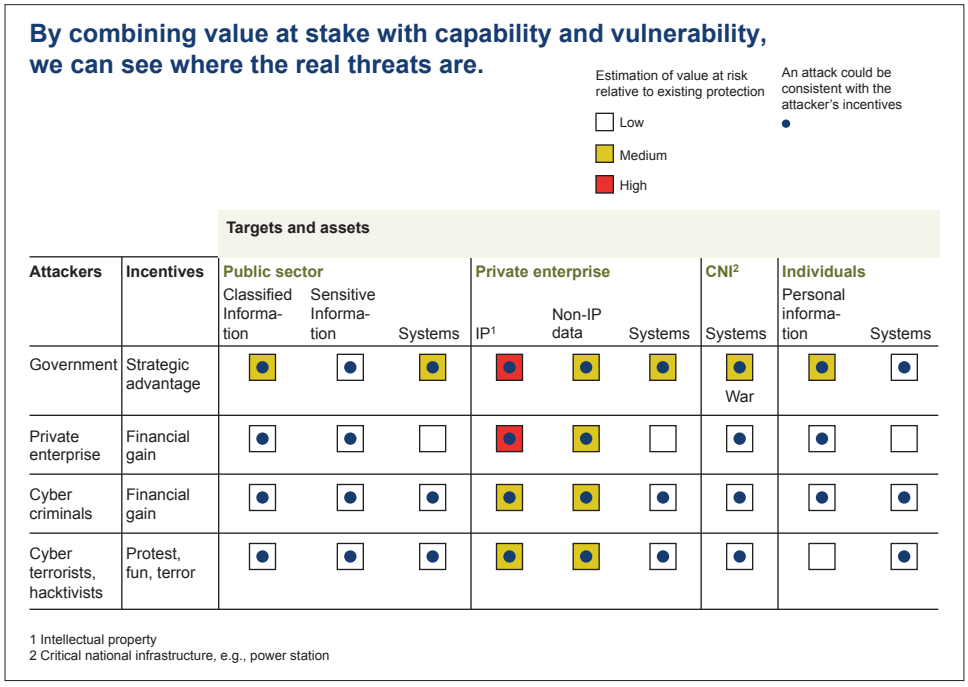
targets—the capabilities of attackers, the vulnerability of targets, and the value at stake in each case. As cyberattackers are not motivated exclusively by money, we also considered whether attackers had non-monetary incentives to attack each target.

This gave us a view of both the likelihood and impact of attacks for each combination of attacker and target. Our most striking finding was the level of threat against private enterprise. In particular, of all assets, the intellectual property of private enterprises has the highest value at risk of attack. This was recognized in a recent speech by Deputy Secretary of Defense William J. Lynn III, who noted that "In looking at the current landscape of malicious activity, the most prevalent cyber threat to date has been exploitation—the theft of information and intellectual property from government and commercial networks."[16] However, neither government nor private enterprise has fully acted on the extent of this threat.

Management in private enterprise almost always prioritizes customer experience over cybersecurity. But taking this approach can lead to irreparable damage. South Korea's largest consumer-finance firm, Hyundai Capital Services Inc., learned this lesson the hard way: Following a serious security breach, where hackers threatened to release stolen, confidential data unless a ransom was paid, the CEO now recognizes the extent of the threat and prioritizes cybersecurity; "We are now slowing down the whole organization. How things look and how they work is now secondary. Security is now first."[17]

Likewise, as a rule, government takes stronger action to help companies protect critical national infrastructure than to protect their intellectual property. The Departments of Defense and Homeland Security, for example, work together on the Defense Industrial Base (DIB) Cyber Pilot to help protect commercial suppliers to the DoD and other critical infrastructure providers from cyberattack and IP loss.[18] The Department of Energy (DoE) systematically tests the cybersecurity at power plants; a recent test in Idaho successfully breached a power plant's security and caused a generator in the plant to self-destruct.[19] The DoE also works with the nuclear industry to protect against IP theft, but we are not aware of any broader government action to protect economically important IP. The result is that more is being done to bolster cyber defenses for .mil, .gov, and critical national infrastructure than for .com.

EXHIBIT 1: Cyber Threat Matrix



The Threat to Economic Growth and Prosperity

Intellectual property and Internet-based commerce are two major drivers of U.S. economic growth and prosperity; cyberattacks threaten both. Innovative intellectual property generates significant current wealth and future growth: The World Intellectual Property Organization estimates that 45 to 75 percent of the wealth of individual companies comes from their intellectual property rights.[20] In total, intellectual property makes an estimated contribution of over $8 trillion to the U.S. economy.[21]

Similarly, the Internet is a remarkable engine for growth. A recent publication by the McKinsey Global Institute estimates that the Internet accounts for 3.4 percent of GDP in the thirteen countries examined and 21 percent of GDP growth in mature economies in the last five years. For the United States, this translates into additional total output of $440 to $580 billion, or $1,400 to $1,900 per capita—a contribution comparable to that made by the transportation, education, communication, agriculture, utilities, and mining sectors.[22]

But along with this boost to productivity and employment, the Internet brings with it new threats and vulnerabilities. Network-enabled intellectual property theft and commercial espionage threaten to undermine our national competitive advantage. Ironically, an over-energetic regulatory or bureaucratic response could be equally damaging, by constraining future web-enabled economic gains. Rather, a middle ground is needed, where government stimulates the private sector to protect its most valuable assets.

Government's Role in Protecting Private Sector Assets

Both government and business should be involved in protecting digital assets. Government needs to match its shift from a physical security mindset to a new cybersecurity mindset with a shift from "responsible for government assets only" to "responsible for key private sector assets." As Richard Clarke and Robert Knake note:

> At the beginning of the era of strategic nuclear war capability the United States deployed thousands of air defense fighter aircraft and ground based missiles to defend the population and the industrial base, not just to protect military facilities. At the beginning of the age of cyber world war the United States government is telling the population and industry to defend themselves.[23]

Government has a legitimate role in protecting intellectual property in the private sector for two reasons. Most obviously, private sector intellectual property is actually an important part of the government's own supply chain: Problems in relevant parts of the private sector are problems for the government. The best recent example of this is the alleged theft of F-35 Joint Strike Fighter data from Lockheed Martin, as the aircraft is destined for use by the U.S. armed forces and its allies. Secondly, intellectual property is an important driver of the success of the overall economy, and, as the Bipartisan Policy Centre makes clear, the success of the U.S. economy is one of the key drivers of America's global leadership: "in addition to its national security and military strength, America's global leadership derives from its economic vitality."[24] As a result, the government has a clear duty to protect. Unfortunately, the government, which has historically faced physical threats to its sovereignty and economy—threats it has countered through physical defense—is making a transition only in the areas of its sovereignty, and not in the area of its economy.

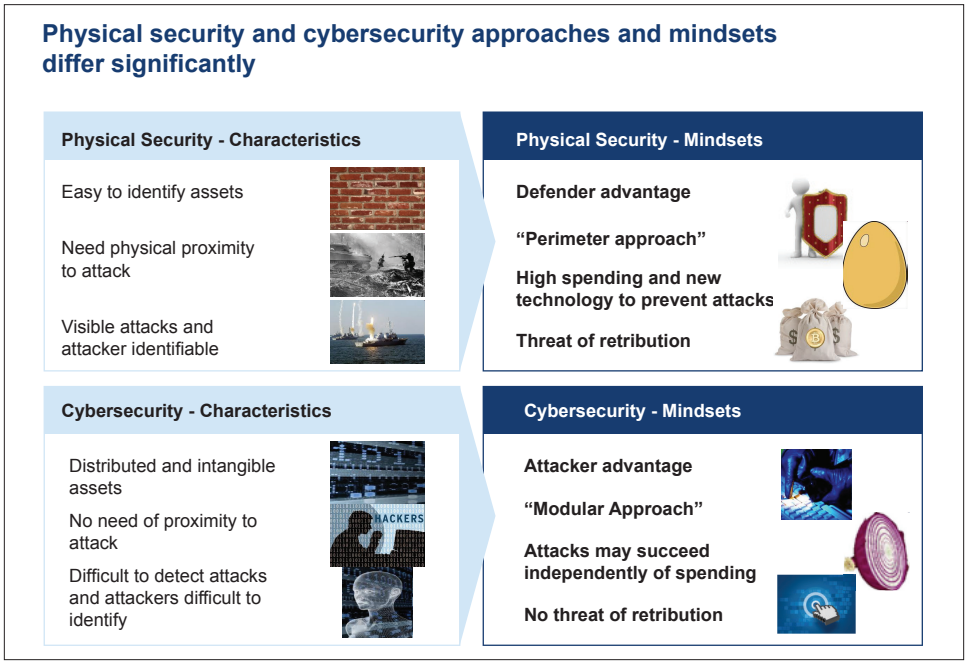
Several basic characteristics shape physical warfare. First, government can easily identify the assets it must protect (e.g., borders, bases) and the possible ways that these

could be attacked. Second, the attacker or its weapons usually need to be close to the target to execute an attack. Finally, attacks are usually visible and can almost always be attributed to a specific attacker. Therefore, in physical warfare, the defender has the advantage and can put in place effective physical counter-measures.

These realities have led government to adopt a successful "perimeter approach," in which it brings key assets together and protects them behind a secure perimeter. The majority of its defenses and related investments are concentrated on fortifying the perimeter, with highest spending and newest technologies resulting in the most successful defense.

The success of the perimeter approach has, in turn, led to the development of a "physical security mindset" among decision-makers and defense practitioners. In practice, this has meant that in countering any threat (including cyberattacks), decision-makers and defense practitioners automatically default to the tried and tested physical interventions of the perimeter approach: fortify the perimeter through developing better technology and threatening retribution as a disincentive to attack.

EXHIBIT 2: PHYSICAL VERSUS CYBERSECURITY



However, the structure of the cyber environment and the threat of cyberattacks fundamentally change the rules. Focusing on perimeter security against cyberattacks is akin to building a cyber Maginot Line. These attacks are not "easily addressed by just building the security walls higher and higher"[25] because many of the characteristics of physical warfare do not apply. The defender no longer has the advantage: there is no need for proximity as the attacker can be based at any Internet-enabled computer in the world; the attacks are difficult to detect and often hard to attribute to a specific attacker; key assets to defend can be hard to identify as they are often intangible and distributed; and methods of attack are very difficult to predict. The tried and tested approaches of physical warfare (the perimeter, technological superiority, and the threat of retribution) are not nearly as effective against cyberattacks. In simple terms, technical solutions like firewalls and security software can only provide a small portion of the protection required.

In the world of physical security, the advantage falls to the defender; in the world of cybersecurity, the advantage is to the attacker. As a result, a cybersecurity mindset is required. This is characterized by an assumption that attacks will eventually breach the perimeter. This makes it important to limit the ability of an individual attack to compromise multiple assets. Doing so requires a modular approach, in which defenders divide and separate key assets, so that compromising one will not compromise the whole. A cybersecurity mindset also recognizes that attacks can come from anywhere in the world and may not be prosecutable under current laws (the U.S., for example has very little power to seek legal redress against hackers based in other countries).

To its credit, there is evidence that certain areas of government, particularly the defense and security community, are moving away from a physical security mindset. Deputy Secretary of Defense William Lynn, for example, has observed that traditional deterrence models do not apply to cyberspace.[26] Additionally, the WikiLeaks exposure did not include the government's most highly classified documents, which were held on a different system. Clearly, however, modularization could have been carried much further in this case and further limited the damage. That is to say, the transition is not complete.

Such a positive state of affairs cannot, unfortunately, be reported in the area of intellectual property, where, by and large, the government appears not to have internalized its role in helping the private sector. Given the importance of intellectual property to the continued success of the economy, this needs to change: Government and business must work together to protect intellectual property.

The Need for a "Security-Economic" Complex

Underpinning the success of the perimeter approach and hence the development of the physical security mindset was a highly successful U.S. defense industry capable of building world-leading defense solutions—what became known as the military-industrial complex. Although the perimeter approach and the military-industrial complex that supports it cannot help defend against cyberattacks for the reasons specified above, they do suggest a parallel that can defend against such attacks. We see a security-economic complex emerging that could support better cybersecurity. This new complex is a system of relationships between government, private enterprises (as the owners of intellectual property and purchasers of security solutions), and cybersecurity vendors such as Cisco, IBM, HP, McAfee, and Symantec. The security-economic complex could operate in a similar fashion to the military-industrial complex in terms of creating a set of mutually reinforcing incentives from which all parties would benefit: Government would secure economic prosperity, private enterprise would effectively protect its assets, and cybersecurity vendors would earn returns to fund future development.

In the transition to the security-economic complex, the role of government evolves from direct purchaser of defense equipment to a key stakeholder in the national economy: It still has an incentive to protect, but no longer directly purchases the solutions to do so. A fully functioning complex would help protect the economy from the threat of cyberattacks. In this state, government recognizes it has a responsibility to protect the economy, and actively seeks to help private enterprise understand the economic value at risk of the intellectual property it owns. When private enterprise understands the true extent of the threat, it will raise its level of investment in cybersecurity (in terms of both improving technical defenses and investing more in management) to counter the threat. This would increase the revenues of cybersecurity vendors and allow them to invest in developing better ways to combat the evolving cyber threat. Cybersecurity vendors also close the loop by keeping the government fully informed of the extent of the threat and lobbying it to continue its role in helping private enterprise see the full cost of the threat. Government also receives information from the security agencies that reinforce the message it is receiving from the vendors.

The security-economic complex, however, is not yet fully operational. As noted above, private enterprise and areas of government outside the defense and security community don't fully understand the extent of the cyber threat that private enterprise faces. Moreover, the government as a whole has yet to appreciate that

supporting national prosperity extends to supporting the private sector in protecting its intellectual property. In practice, private enterprise underestimates how much of its value is at risk of cyberattack because neither the security agencies nor the broader government provide it with the information necessary to make this assessment.

Private enterprise is making this underestimation because it lacks two types of information, both of which could be provided by government. First, it lacks general information about the extent of the threat. Those areas of government, such as the National Security Agency, that do have good knowledge of the extent of the threat are not systematically sharing this with either private enterprise or with other areas of government. Second, private enterprise lacks specific information about vulnerabilities and specific attacks. At present, private enterprises do not know enough about the vulnerabilities in their own systems to invest sufficiently in cybersecurity. As the Sans Institute, a technology group that authors guidance for the Department of Homeland Security, put it, there is no "awareness high up in companies that there [are] such gaping holes in their software applications."[27] Private enterprises only receive this information through weak links—infrequent, ad hoc communication with the security agencies and marketing from security vendors. In addition, private enterprises perceive little, if any, incentive to share amongst themselves details of attacks they have experienced. (Although in some industries the consciousness of mutual benefit is beginning to develop, for example the Financial Services Information Sharing and Analysis Centre collects and shares cyberattack information in the financial sector; the board is formed of senior executives in the financial industry, while strategic sponsors come from the cybersecurity industry.) This second failure inhibits the development of protection approaches and technologies in a way that would not be possible with physical security, where it is visible and obvious when there has been a breach.

As a result, private enterprise underestimates its incentive to protect itself from cyberattack, which leads to misalignment of the incentives of government with those of private enterprise and vendors, and therefore insufficient protection against cyberattack. This represents a continued threat to U.S. competitiveness.

Policy Implications

Cyberattacks pose a significant threat to the continued prosperity of the U.S. economy. Government needs to play an active role in ensuring that this threat is mitigated. To do this, policymakers should drive private enterprise to protect

its intellectual property adequately, and support it in doing so. This could be achieved through supporting the security-economic complex to develop it into a fully functioning system in which the economic incentives of private enterprise and cybersecurity vendors align with government's incentive to protect long-term prosperity.

To make the security-economic complex fully functional, policy changes are required in two areas. First, private intellectual property protection should be on the government agenda. Government needs to understand, and act on, its responsibility to protect both its own and private enterprise's intellectual property, as this intellectual property is vital to continued economic prosperity. To do this, policymakers need to consider how to reinforce the message within government that important assets are not only physical assets under government control, but also—and increasingly—digital, and owned by the private sector. Policymakers should also consider how they can best ensure that details held by the security agencies on the extent of the cyber threat are shared with elected officials and hence ensure that knowledge on the extent of the threat to intellectual property is well understood across government.

The U.S. would not be the first government to take action. The Australian government has authorized agencies such as the Australian Security Intelligence Organization and the Attorney General's department to work directly with private enterprise to help address information failure and threat mitigation. The Australian Defence Signals Directorate supports them in this work.[28] Something similar, possibly including knowledge transfer from government to private enterprise, could be considered in the U.S.

Similarly, government must provide incentives for private enterprise and for cybersecurity vendors. For private enterprise, these should encourage a stronger management approach in dealing with the cyber threat. For vendors, these should encourage more R&D investment to help improve technical defenses. An example might include legislation on minimum cybersecurity standards for companies.

Second, more information should be shared on the extent of the cyber threat to incentivize private enterprise to invest in management and technology to protect intellectual property. Policymakers should consider the following questions:

1. How can government and security agencies best communicate the true extent of the threat? Government must provide private enterprise with enough information on the extent and nature of the threat so that companies can understand the risks they are facing. This may include being more active

in helping private enterprise detect attacks and more readily sharing the information government has on such attacks. One possibility would be to create a venue where the government can share information with businesses on the true nature of attacks.

2. How can government best help private enterprise detect attacks? Policymakers should consider how best to develop the links between security agencies and private enterprise so that they can pass on information on actual attacks without compromising sources and methods. One possibility would be to appoint business liaison officers in security agencies to work with companies on cyber issues.
3. How can government best ensure that private enterprises report the attacks they suffer? Policymakers need to encourage the development of a framework within which companies can share details of the attacks that they have faced while minimizing any detrimental impact of such reporting on the companies themselves. An independent body could be established to anonymously collect and share details of attacks.
4. Finally, how can government make sure private enterprise puts in place managerial and technical solutions to reduce the impact of a cyberattack? Policymakers should consider establishing requirements or providing incentives to ensure that enterprises have a minimum set of cyber solutions. Here, legislation and guidelines could be effective.

The Consequences of Inaction

Technological developments are leading to an increase in attacker capabilities faster than reduction in vulnerabilities, exacerbating the attacker advantage. This asymmetry suggests that the frequency and impact of attacks will continue to increase. At the same time, the incentives to attack are growing for many attackers, not least because of the increasing amount, and value, of data available. The McKinsey Global Institute estimates that enterprises stored more than seven exabytes of new data on disk drives last year (equivalent to 28,000 times the information stored in the Library of Congress), the effective use of which is the key to productivity and margin gains.[29]

The cyber threat will not diminish of its own accord. If no action is taken, attacks will continue to increase, the value at risk will continue to grow, and U.S. competitiveness and prosperity will suffer.

John Dowdy is a Senior Partner in the London office of McKinsey & Company, where he leads McKinsey's global defense and security practice, focusing on improving the efficiency and effectiveness of defense expenditure, improving supply chain and logistics processes, and conducting stability operations in fragile states. He also leads McKinsey's joint research project, in conjunction with the London School of Economics Center for Economic Performance and Stanford Business School, on global manufacturing productivity. Prior to that, he was responsible for all of McKinsey's government work in Europe, the Middle East and Africa. He also chaired McKinsey's global efforts in economic development and served as a member of Public Services Productivity Panel. His most recent publication is *McKinsey on Government's Special Issue on Defense & Security* (spring 2010), where he contributed multiple articles including *Improving US equipment acquisition, An expert view on defense procurement* and *Stabilizing Iraq: A conversation with Paul Brinkley*. Previously, he worked as a research associate at Harvard Business School, contributing to the book *Beyond Free Trade: Firms, Government and Global Competition*. Mr. Dowdy is a fellow of the Royal United Services Institute (RUSI), a fellow of the Royal Aeronautical Society (RAeS), a member of Chatham House and a member of the International Institute for Strategic Studies. Mr. Dowdy holds a B.S. in Electrical Engineering and Computer Science from the University of California at Berkeley and an M.B.A. with high distinction from Harvard Business School.

[1] U.S. National Security Council and Homeland Security Council, *Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, D.C., 2009).

[2] Ibid.

[3] Based on off-the-record discussions with government officials (2010-2011).

[4] As explained in Florencio Dinei and Cormac Herley, "Sex, Lies and Cybercrime Surveys," *Microsoft Research* (June 2011).

[5] Jonathan Masters, interview with Dmitri Alperovitch on the Council on Foreign Relations website, "Cybertheft and the U.S. Economy" (August 2011).

[6] Jonathan Soble, "Sony Battles Further Hacker Attacks," *Financial Times*, May 25, 2011.

[7] Sofia Mitra-Thakur, "Sony Faces Legal Costs of up to $1.5bn after Data Breach," *Engineering & Technology Magazine* (April 2011).

[8] Based on comparison of share prices on April 20 and April 25, 2011 (Sony) and May 19 and May 27 (Lockheed Martin).

[9] Based on comparison of share prices on Mar 17 and Mar 24, 2011.

[10] U.S. General Accounting Office, "Defense Acquisitions: Assessment of Selected Weapons Programmes" (Washington, D.C., 2011).

[11] InterComputer, "Massive Cyber Attack Shocks 2500 Companies," (February 2010).

[12] Dmitri Alperovitch, "Revealed: Operation Shady RAT," McAfee White Paper, (August 2011).

[13] Ibid.

[14] Stewart Baker, Natalia Filipiak, and Katrina Timlin, "In the Dark: Crucial Industries Confront Cyber attacks" a joint publication of McAfee and the Center for Strategic and International Studies (2011).

[15] Florencio Dinei and Cormac Herley, "Sex, Lies and Cybercrime Surveys," *Microsoft Research* (June 2011).

[16] Deputy Secretary of Defense William J. Lynn III, "Remarks on the Department of Defense Cyber Strategy" (Washington, D.C., July 14, 2011).

[17] Evan Ramstad, "Executive Learns From Hack: CEO Now Treats IT Department as Critical to Hyundai Capital's Operation," *Wall Street Journal*, June 21, 2011.

[18] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," (Washington, D.C., July 2011).

[19] SafteyIssues.com, "Power Plants Vulnerable to Cyber Attack" (undated).

[20] Ian Cockburn, "Assessing the Value of a Patent," *World Intellectual Property Organization* (undated).

[21] Robert Shapiro and Kevin Hassett, "What Ideas are Worth: The Value of Intellectual Capital and Intangible Assets in the American Economy," a report of the Sonecon Institute (2011).

[22] McKinsey Global Institute, "Internet Matters: The Net's Sweeping Impact on Growth, Jobs, and Prosperity" (May 2011).

[23] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: Harper Collins, 2010), p. 144.

[24] Bipartisan Policy Center, "Disciplining the Defense Budget: Lessons from a Joint BPC/Stimson Event", March 2011.

[25] UK Government Communications Headquarters Director Iain Lobban, remarks at the International Institute for Strategic Studies, London, UK, October 12, 2010.

[26] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (September/October 2010).

[27] John Gapper, "Companies Make it Easy for Hackers," *Financial Times*, June 29, 2011.

[28] Dylan Welch, "Call for More Money to Fight Growing Cyber Arms Race," *Sydney Morning Herald*, June 4, 2011.

[21] McKinsey Global Institute, "Big Data: The Next Frontier for Innovation, Competition and Productivity" (May 2011).