
McAfee
Virtual Criminology Report 2009
Virtually Here: The Age of Cyber Warfare

Virtual Criminology Report 2009

CONTENTS

Foreword

War is not a term to be tossed around lightly. That is why the growing debate over cyber war has caught our attention.

The annual McAfee Virtual Criminology Report has traditionally focused on the methods, targets and behavior of cyber criminals. And yet, as we put together the 2007 report, numerous experts pointed out that nation-states were not only spying on each other in cyberspace, but also developing increasingly sophisticated cyber attack techniques. Since that report was published, we have seen the concept of cyber war debated more often in the face of mounting attacks and network penetrations that appear to be motivated by political objectives instead of financial gain, making it a stretch to characterize them as cybercrime. We decided to revisit the possibility of war in cyberspace in this year's report.

Experts disagree about the use of the term "cyber war," and our goal at McAfee is not to create hype or stoke unwarranted fear. But our research has shown that while there may be debate over the definition of cyber war, there is little disagreement that there are increasing numbers of cyber attacks that more closely resemble political conflict than crime. We have also seen evidence that nations around the world are ramping up their capabilities in cyber space, in what some have referred to as a cyber arms race.

If cyberspace becomes the next battleground, what are the implications for the global economy and vital citizen services that rely upon the information infrastructure? What should those of us outside the military do to prepare for the next wave of cyber attacks?

Finding answers to these questions was not easy because much of this discussion is only happening behind closed doors. We believe this veil of secrecy around cyber warfare needs to be lifted.

There is little doubt that the impact of cyber war will extend beyond military networks. As our dependence on Internet technology grows, so does the need for thoughtful discussion on political conflict in cyber-space. This year's Virtual Criminology Report highlights the complexities and potential consequences that arise when political conflict goes online. Our hope is that the report will help encourage and frame a global dialogue on protecting our digital resources from the scourge of cyber war.

Dave DeWalt
President and CEO, McAfee, Inc.

Introduction

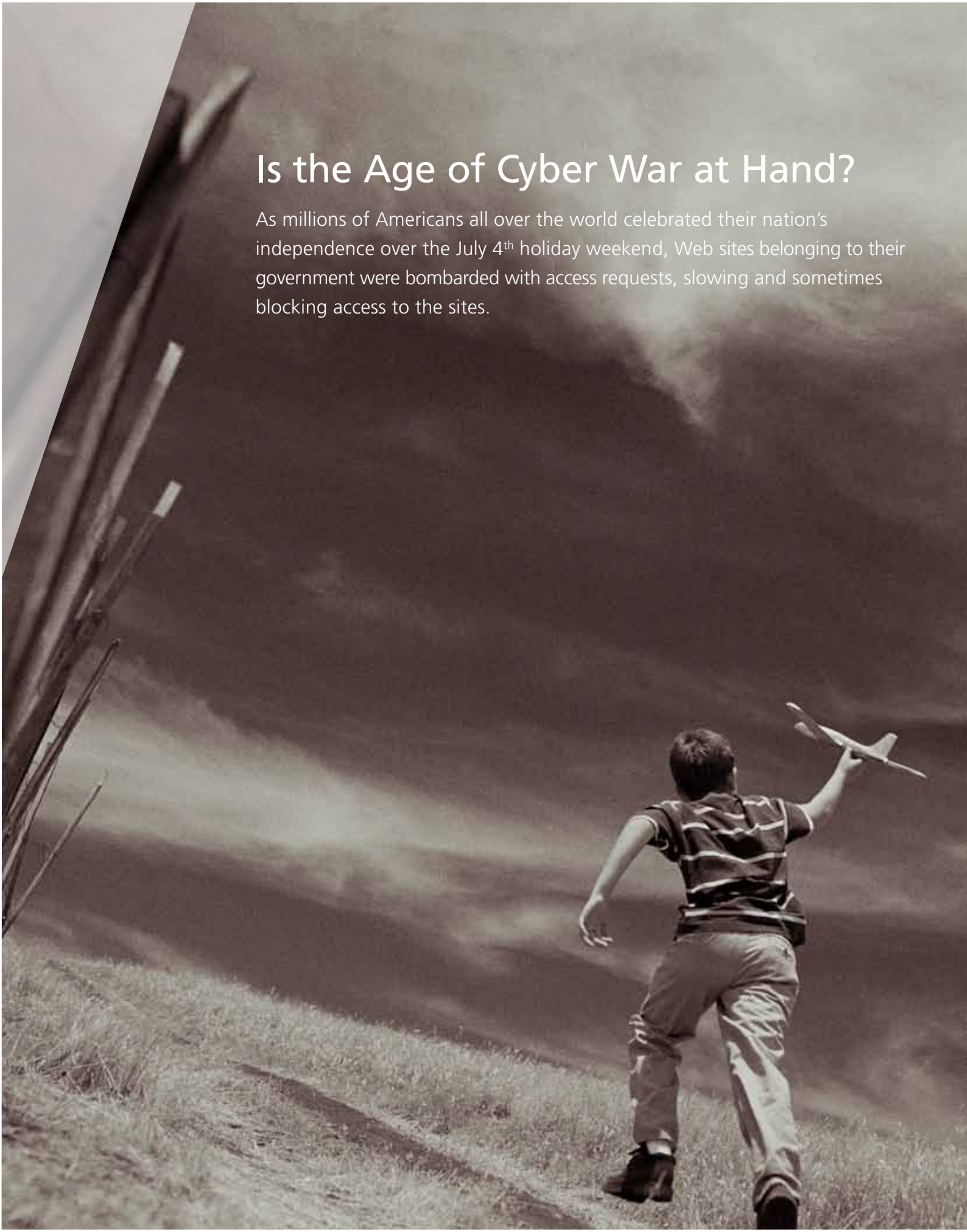
Is the "Age of Cyber War" at hand? This year, the fifth annual McAfee Virtual Criminology Report contemplates this question and others prompted by the fact that nation-states are arming themselves for the cyberspace battlefield. Since our 2007 report, when we last discussed the growing cyber threat to national security, there have been increasing reports of cyber attacks and network infiltrations that appear to be linked to nation-states and political goals. The most obvious of these attacks was the August 2008 cyber campaign against Georgia during the South Ossetia War. We decided it was time to further examine whether cyber warfare is now a part of human conflict that we should get used to seeing more often.

McAfee commissioned Good Harbor Consulting to research and write this report. The report was prepared by Paul B. Kurtz, a recognized cyber security expert who served in senior positions on the White House's National Security and Homeland Security Councils under U.S. Presidents Clinton and Bush, and David W. DeCarlo, with the support of Stacy Simpson. The team interviewed over 20 experts in international relations, national security and Internet security from around the world to assess their opinions on the definition of cyber war, its impact on the private sector and the priority of issues for public discussion.

There have been increased reports of cyber attacks and network infiltrations that appear to be linked to nation-states and political goals.

Three key findings emerged:

- **Although there is no commonly accepted definition for cyber war today, we have seen nation-states involved in varying levels of cyber conflict.** Further, while we have not yet seen a "hot" cyber war between major powers, the efforts of nation-states to build increasingly sophisticated cyber attack capabilities, and in some cases demonstrate a willingness to use them, suggests that a "Cyber Cold War" may have already begun.
- **If a major cyber conflict between nation-states were to erupt, it is very likely that the private sector would get caught in the crossfire.** Most experts agree that critical infrastructure systems—such as the electrical grid, banking and finance, and oil and gas sectors—are vulnerable to cyber attack in many countries. Some nation-states are actively doing reconnaissance to identify specific vulnerabilities in these networks. In the words of one expert, nation-states are "laying the electronic battlefield and preparing to use it."
- **Too much of the debate on policies related to cyber war is happening behind closed doors.** Important questions, such as where to draw the line between cyber espionage and cyber war, are being discussed in private, or perhaps not at all. Many governments have chosen to keep debate on cyber conflict classified. Since governments, corporations and private citizens all have a stake in the future of the Internet, it is time to open a global dialogue on how to manage this new form of conflict.



Is the Age of Cyber War at Hand?

As millions of Americans all over the world celebrated their nation's independence over the July 4th holiday weekend, Web sites belonging to their government were bombarded with access requests, slowing and sometimes blocking access to the sites.

These denial-of-service attacks targeted the White House, Department of Homeland Security, U.S. Secret Service, National Security Agency, Federal Trade Commission, Department of the Treasury, Department of Defense and the Department of State, as well as the New York Stock Exchange, Nasdaq, Amazon and Yahoo.

When these sites were attacked, however, the whole country was busy spending time with friends and family and grilling food on their patios. Hardly anyone seemed to notice that they could not access the latest news from the Federal Trade Commission or the Treasury Department.

The following Tuesday, 11 Web sites of the South Korean government were brought down by the same network of 50,000 computers used in the attacks on the United States. South Korean intelligence officials blamed North Korea as the source of the attacks, an allegation that was reported by the Associated Press. Suddenly a lot more people started paying attention.

Internet security experts quickly determined that an unsophisticated adversary launched the attacks on the U.S. and South Korea, and debated whether North Korea was behind the attacks. Many of the Web sites were able to return to their usual business within a few hours. Some security experts and policymakers concluded that the attacks were no more than a nuisance to the people of the United States and South Korea, regardless of whether North Korea was responsible.

What was the motive behind the July 4 attacks?

If the attacks did originate from North Korea, one motivation could have been to test the impact of flooding South Korean networks and the transcontinental communications between the U.S. government and South Korea on the ability of the U.S. military in South Korea to communicate with military leaders in Washington and the Pacific Command in Hawaii, suggests Dmitri Alperovitch, Vice President of Threat Research at McAfee. The ability of the North Koreans to severely diminish the information transmission capacity of those links would provide them with a significant advantage in case of a surprise attack on South Korea across the Demilitarized Zone.

The Georgian Cyber "Flood": A Model for Future Conflicts?

In August 2008 Russia attacked the nation of Georgia in a dispute over the Georgian province of South Ossetia. As the Russian military mounted its assault on the ground and in the air, a group of Russian nationalists joined the fray in cyberspace. Any civilian, Russian-born or otherwise, aspiring to be a cyber warrior was able to visit pro-Russia websites to download the software and instructions necessary to launch denial-of-service attacks on Georgia. On one Web site, called StopGeorgia, visitors could download a list of target Web sites and an automated software utility. The only effort required by the user was to enter the Web address of a target and click a button labeled "Start Flood."[2]

The coordinated assault inundated Georgia's government and media Web sites with access requests. While the effects were minor at first, with service going down on some Web sites sporadically, the denial-of-service attacks became more severe once the armed hostilities started. News and government Web sites were no longer reachable by anyone within or outside Georgia, severely hampering Georgia's public communications. Russia achieved a significant psychological victory by preventing Georgia from disseminating accurate information about the state of battle to the public. And, with Georgia's side of the story silenced, Russia practically won the battle over international public opinion by default.

Russia denied any involvement on the part of its military or government in the cyber attacks. But some people were suspicious that the Russian military had the serendipity to begin hostilities on the ground concurrently with an entirely independent civilian cyber assault. The U.S. Cyber Consequences Unit (US-CCU), an independent, non-profit research institute, began monitoring the situation almost immediately after the attacks, in part to determine how the campaign was organized. In a recently released report, the US-CCU concluded that all of the attackers and activities showed every sign of being civilian, yet someone in the Russian government must have given the organizers of the attacks advanced notice of the timing of Russia's military operations.[3]

Others had a different view of the attacks. By the end of the week, Representative Peter Hoekstra, a member of the U.S. Congress, was stating publicly that the U.S. should conduct a "show of force or strength" against North Korea for its alleged role in the attacks. "Whether it is a counterattack on cyber, whether it is, you know, more international sanctions…but it is time for America and South Korea, Japan and others to stand up to North Korea," he said, "or the next time…they will go in and shut down a banking system or they will manipulate financial data or they will manipulate the electrical grid…and they may miscalculate and people could be killed."[1]

The attacks were perhaps more than a simple crime in cyberspace, but did they warrant a U.S. political response or threat of military action? What was the motive of the attackers? Was there any truth to the assertion that North Korea was responsible for the attacks? If they were, what were the intended consequences?

The answers to all these questions were unclear. Yet these cyber attacks were not the first ones to raise such questions. In 2007 Estonia fell victim to a series of denial-of-service attacks on government and commercial Web sites. The attacks lasted for weeks, affecting the ability of Estonians to access their checking accounts online and conduct e-commerce. Technical analysis showed the attacks came from sources within Russia, but the Russian government denied any responsibility.

Although Estonia is a member of the North Atlantic Treaty Organization—an alliance established during the Cold War to deter attacks from the Soviet Union—the members of the NATO did not seriously consider an official military or diplomatic response to the attacks, according to Taimar Peterkop, Defense Counselor at the Embassy of Estonia in Washington. Some members of NATO did send technical advisors to help Estonia reduce the impact of the attacks, but the assistance was not provided as part of an official NATO mission.

1 "Hoekstra: 'Stand up to N. Korea,'" *Washington Times,* July 9, 2009.

Perhaps even more surprising than finding some level of coordination between Russian officials and the cyber attackers was that the Russians might have deliberately chosen to limit the damage caused by the attacks. No critical infrastructures were targeted, even though investigations by the US-CCU suggested that a number of these infrastructures were vulnerable and could have been attacked. "The fact that physically destructive cyber attacks were not carried out against Georgian critical infrastructure industries suggests that someone on the Russian side was exercising considerable restraint," the report says.

Scott Borg, Director of the US-CCU, believes the Georgia conflict may be a harbinger of how nation-states will orchestrate future cyber attacks. "People were provided with attack tools, targets and timing in the Georgia cyber campaign," Borg said. "So far this technique has been used in denial-of-service and other similar attacks. In the future it will be used to organize people to commit more devastating attacks."

2 "Marching off to cyberwar," *The Economist,* December 4, 2008.

3 "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," *US-CCU Special Report,* August 2009.

Once the attacks subsided, Estonia attempted to pursue the perpetrators through a law enforcement response to the attacks. The investigation was successful in identifying some of the attackers in Russia, but Estonian law enforcement officers reached a dead end when they sought help from their Russian counterparts. "Estonia has been unable to convince the Russian authorities to apprehend the offenders and bring them to justice," Peterkop said.

In the wake of these events and others, governments around the world are increasing their efforts to prepare for future cyber attacks. NATO has set up a "Center of Excellence" for cyber defense in Estonia to study cyber attacks and determine under what circumstances a cyber attack should trigger NATO's common defense principle that "an attack on one is an attack on all." In June 2009, U.S. Defense Secretary Gates announced the formation of the U.S. Cyber Command, a sub-unified organization under U.S. Strategic Command. Led by a four-star general, the new command is designed to defend vital U.S. military networks. The UK government recently announced plans to create a central Office of Cyber Security (OCS) to deal with the rising level of online attacks. The OCS will have a role in coordinating offensive capabilities and, in extreme cases, would have the ability to mount a cyber attack in response to intrusions on UK networks. Other nations are contemplating similar initiatives to protect their populations in cyberspace.

Cooperative Cyber Defence Centre of Excellence

The Cooperative Cyber Defence Centre of Excellence (CCDCOE) was established in May 2008 in Tallinn, Estonia to enhance NATO's cyber defense capabilities. The CCDCOE is an international organization with membership open to all NATO nations. Currently, Estonia, Latvia, Lithuania, Germany, Italy, the Slovak Republic, and Spain have signed the memorandum of understanding to provide personnel and funding as Sponsoring Nations. The mission of the CCDCOE is to improve the capabilities, cooperation and information sharing among NATO nations through education, research and development, consultation and evaluation of lessons learned from cyber conflicts.

Toward a Definition of Cyber War

War is typically defined as the use of force, or violence, by a nation-state to compel another to fulfill its will. Prussian strategist Carl von Clausewitz essentially defined it this way in his book *On War*—a classic for strategic military thinking from the early 19th century. Specifically, he described war as "the continuation of politics by other means."

In other words, military conflict is a way for nation-states to achieve their political objectives when other means, such as diplomacy, are not working or are less expedient than violence. Clausewitz's concepts continue to frame the way military strategists and international relations theorists think about war today.

The use of force, however, may no longer be as obvious as it was during Clausewitz's time. Clausewitz wrote about war soon after the Napoleonic Wars in which he served, when nation-states sent their armies of uniformed infantry to oppose each other on a battlefield a few hundred yards apart and fire musket rounds at one another. He likely could not have imagined a new battlefield made up of bits and bytes where the borders between countries blur, the weapons are difficult to detect and rarely seen, and the soldiers can easily be disguised as civilians.

The world's increasing reliance on information technology coupled with the growing sophistication of cyber attackers has prompted experts to examine the notion of "cyber war." Yet there is disagreement among cyber security, technology and international relations experts as to what kind of actions, if any, constitute warfare in cyberspace.

When determining whether a cyber attack is an act of cyber war, experts evaluate four key attack attributes:

Source: Was the attack carried out or supported by a nation-state?

Consequence: Did the attack cause harm?

Motivation: Was the attack politically motivated?

Sophistication: Did the attack require customized methods and/or complex planning?

Does This Mean War?

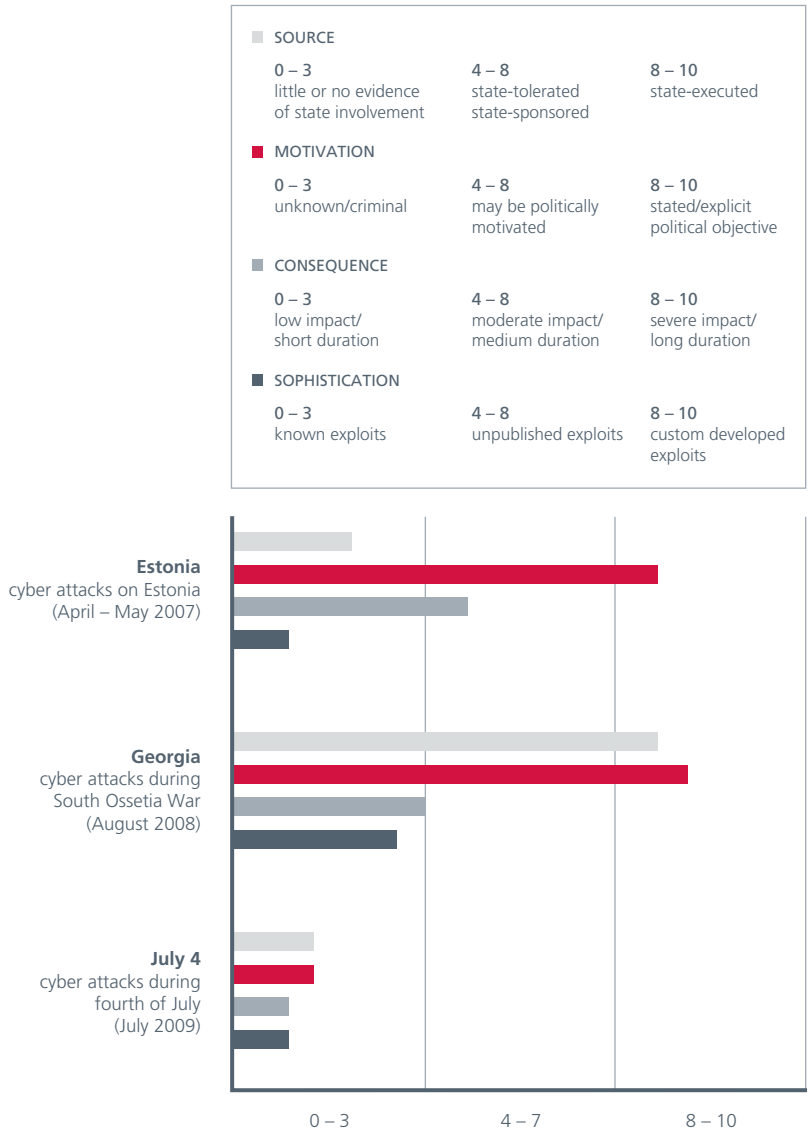


Figure 1. Evaluating Cyber Attack Attributes

Identifying the source, defining "harm," and understanding motivations in a cyber conflict can be more of an art than a science.

International relations experts today widely accept the basic definition that warfare is the use of force by one or more nation-states against another for political gain. In addition, an act of war is widely regarded as a serious event. Few nations would go to war over a nuisance such as rocks being tossed over their borders, but rockets would be another matter entirely.

It sounds simple in theory, but applying these concepts to the cyber world is difficult. Identifying the source, defining "harm," and understanding motivations in a cyber conflict can be more of an art than a science. For instance, what one nation may view as an inconvenience might be seen by another as an intolerable threat. And, if a nation encourages an attack, but does not actually carry it out with its own military, can it still be considered cyber war?

Cyber attack capabilities may not yet be the chief weapon in nation-states' arsenals, but events have shown that a growing number of nation-states do see them as part of the panoply of military power.

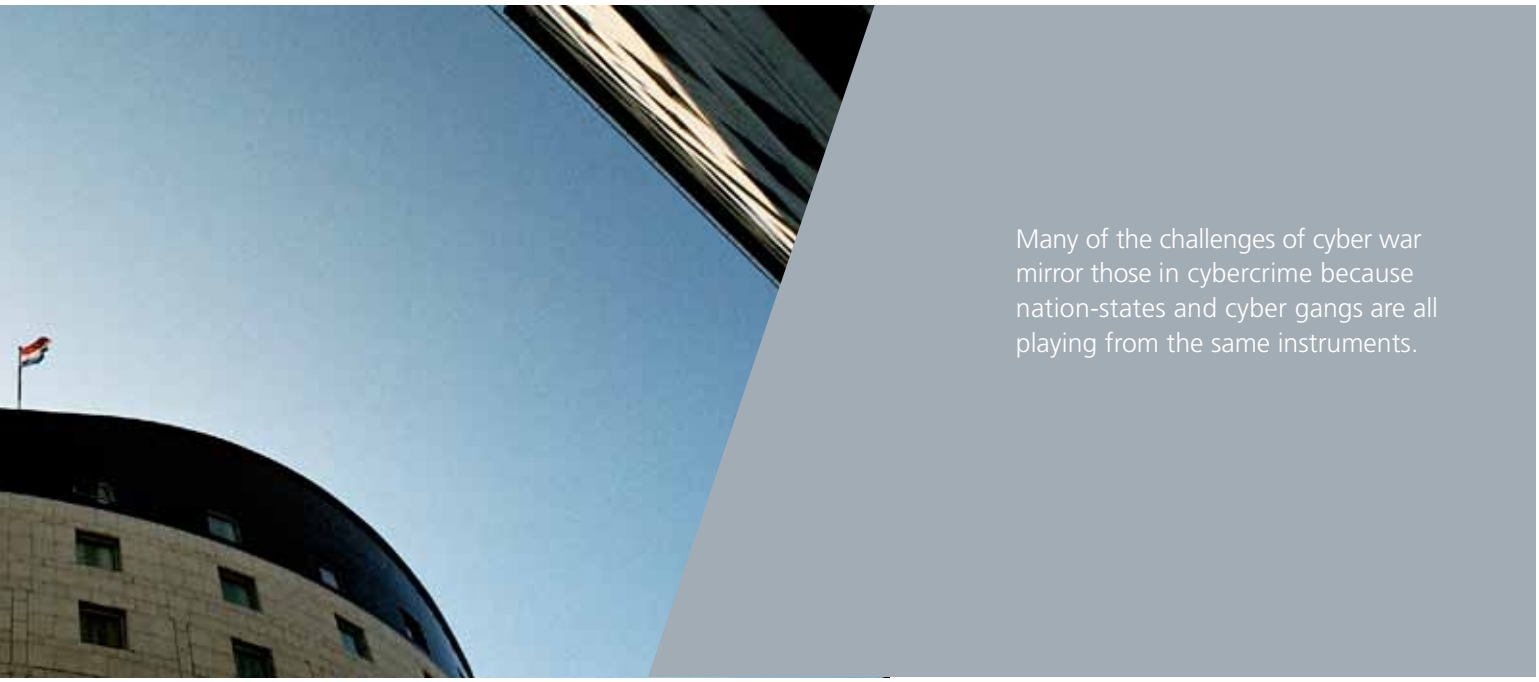
It is in answering these questions that experts start to differ on the definition of cyber war. While all experts agree that nations must have some role in carrying out the attack, their opinions tend to diverge on what is the threshold of damage or disruption where a cyber attack becomes cyber warfare. Indeed, some experts are skeptical that the cyber attack capabilities available today are capable of causing the severe physical consequences, such as casualties and permanent damage to property, that most nation-states would associate with warfare.

"The cyber weapons we have seen to-date, used alone, are not capable of achieving the level of damage necessary for an attack to rise to the level of warfare," according to Eugene Spafford, Director of the Center for Education and Research in Information Assurance and Security at Purdue University. "I don't think the idea of cyber warfare doesn't make sense, but it doesn't apply to any of the events we've seen so far."

Cyber attack capabilities may not yet be the chief weapon in nation-states' arsenals, but events have shown that a growing number of nation-states do see them as part of the panoply of military power. According to national security officials, several nation-states are developing advanced cyber offensive capabilities, the details of which are unknown to the public because they are strictly classified by governments.

The question remains whether the posturing of nation-states today means that cyber war, unaccompanied by physical conflict, will someday become a reality. "Over the next 20 to 30 years, cyber attacks will increasingly become a component of war," said William Crowell, a former Deputy Director of the U.S. National Security Agency, an intelligence organization. "What I can't foresee is whether networks will be so pervasive and unprotected that cyber war operations will stand alone."

It may be difficult to imagine an entirely virtual conflict where nation-states go to war without firing a single shot from a rifle, tank or airplane. Perhaps it will take a modern-day Clausewitz to lift the fog surrounding cyber war and help the rest of us peer into the future. In the meantime, there are more immediate concerns, such as the confusion that arises when nation-states enlist cyber criminals as allies to achieve their political objectives.



Many of the challenges of cyber war mirror those in cybercrime because nation-states and cyber gangs are all playing from the same instruments.

The Nexus Between Cyber Crime and Cyber War

The line between cyber crime and cyber war is blurred today in large part because some nation-states see criminal organizations as useful allies. Nation-states have already demonstrated that they are willing to tolerate, encourage or even direct criminal organizations and private citizens to attack enemy targets.

In the case of the cyber attacks on Georgia, for example, civilians carried out the cyber attacks on targets while the Russian military invaded Georgia by land and air. There is evidence that these civilians were aided and supported by Russian organized crime, according to a recent report by the U.S. Cyber Consequences Unit (US-CCU), an independent research institute. Russia denied that its government or military provided any help to the attackers or communicated with them. Yet the same US-CCU report found that "the cyber attacks were so close in time to the corresponding military operations that there had to be close cooperation between people in the Russian military and the civilian cyber attackers."[4]

Herein lies the challenge of unraveling whether an attack is a criminal act, an act of war, or something else entirely. The attacks on Georgia were motivated by Russia's political objectives, but, in large part, they were orchestrated by civilian attackers on civilian targets using methods that are not very different than those used by cyber criminals.

"Many of the challenges of cyber war mirror those in cybercrime because nation-states and cyber gangs are all playing from the same instruments," according to a German cybercrime investigator. "For instance, anyone can go to a criminal group and rent a botnet. We've reached a point where you only need money to cause disruption, not know-how and this is something that needs to be addressed."

4 "Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008," *US-CCU Special Report,* August 2009.

Cyber crime is often adjunct to or a cover for other kinds of malicious activities.

The hacking skills of criminal groups may make them natural allies for nation-states looking for a way to deny involvement in cyber attacks. In order to avoid or circumvent international legal norms on war altogether, nation-states may sponsor, encourage, or simply tolerate cyber attacks or espionage by private groups on their enemies. Crowell believes there is evidence of this ruse. "There is overlap between cyber war and cyber crime," Crowell said. "Cyber crime is often adjunct to or a cover for other kinds of malicious activities."

Furthermore, money is sometimes not the only motivation of criminal organizations. In a presentation on "Fighting Russian Cyber Crime Mobsters" given this year at the Black Hat briefings on cyber security, Dmitri Alperovitch, Vice President of Threat Research, McAfee, explained how some members of Russian cyber crime gangs are motivated by nationalism and a righteous attitude toward the West. These moral values are sometimes proclaimed in online forums. In one forum, a banner states the group's mission: "We will recreate historical fairness. We will bring the USA down to the level of 1928–33."

In theory, we already have concepts that apply separately to war and crime. In practice, it is sometimes difficult to apply these categories to specific attacks and their perpetrators. Countries around the world vary widely in their approach to combating terrorism; some treat terrorists as criminals, others treat them as prisoners-of-war, and the U.S. began treating captured terrorists as "enemy combatants" soon after the September 11, 2001 attacks, regarding them as unlawful combatants that did not qualify for prisoner-of-war status under the Geneva Conventions. There is no reason to presuppose that applying old concepts to a new kind of human aggression in cyberspace will be easy.

Cyber Cold War

Regardless of differences in the definition of cyber war, the increasing numbers of politically motivated cyber attacks that do not fall easily into the category of cyber crime are having an impact on international relations. While the world may not yet have seen a "hot" cyber war, many experts believe that nation-states are competing in a silent arms race to build cyber weapons. The situation is different, however, than the nuclear arms race between the Soviet Union and the U.S. after World War II. If that was a duel, then the cyber weapons race may be more of a free-for-all.

Countries Developing Advanced Offensive Cyber Capabilities

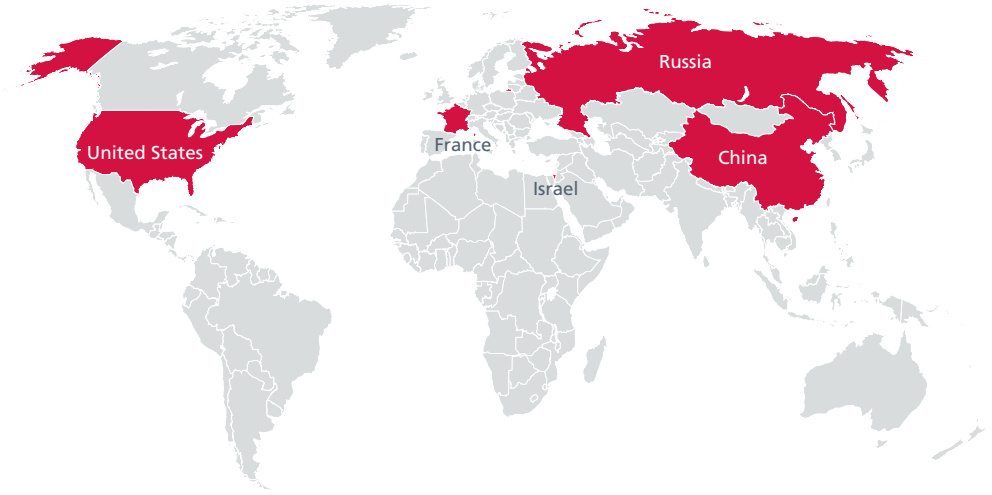


Figure 2

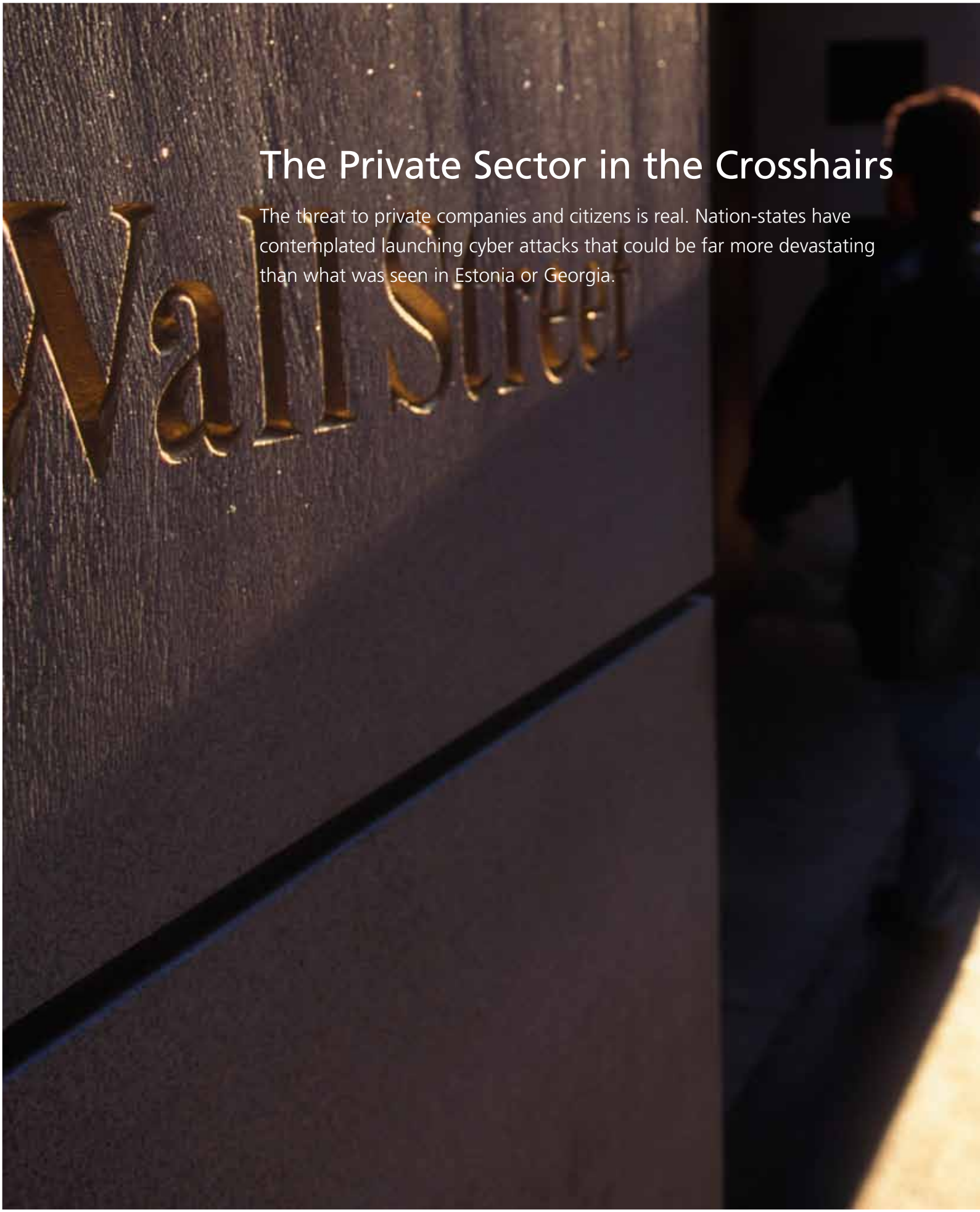
Cyber war is not occurring right now, but nation-states are definitely in competition.

Although Dr. James Lewis, Director of the technology program at the Center for Strategic and International Studies, does not believe we have seen an actual cyber war yet, he thinks the risk of cyber warfare is growing. "Cyber war is not occurring right now, but nation-states are definitely in competition," Lewis said. "Cyber weapons exist, and we should expect that adversaries might use them."

In another parallel to the Cold War, there has been a spate of recent media reports that nation-states are actively spying on each other's sensitive government networks and critical infrastructure systems, perhaps in preparation for future attacks on those systems. Mike Jacobs, former Information Assurance Director, U.S. National Security Agency, believes these reports are cause for concern. "Adversaries are learning as much as they can about power grids and other systems, and they are sometimes leaving behind bits of software that would allow them to launch a future attack," Jacobs said.

While some experts call these activities "cyber espionage," others see it as a form of low-level conflict, a constant cat-and-mouse game that may mark the beginnings of a Cyber Cold War. "If you are engaged in reconnaissance on an adversary's systems, you are laying the electronic battlefield and preparing to use it," Jacobs said. "In my opinion, these activities constitute acts of war, or at least a prelude to future acts of war."

While there is some difference in opinion on when a cyber attack crosses the line into cyber war, experts agree that nation-states and some non-state actors—such as criminal organizations, terrorists and activists—are developing sophisticated arsenals of cyber weapons and that some have demonstrated a willingness to use them for political objectives. If the virtual shooting starts, governments, corporations and private citizens may all get caught in the crossfire.



The Private Sector in the Crosshairs

The threat to private companies and citizens is real. Nation-states have contemplated launching cyber attacks that could be far more devastating than what was seen in Estonia or Georgia.

For instance, before the U.S. invasion of Iraq in 2003, the U.S. military and intelligence agencies planned a cyber attack on the Iraqi financial system. The attack would have frozen billion of dollars in Saddam Hussein's personal bank accounts and stopped payments to Iraqi soldiers and for war supplies. Everything was in place. Systems were ready, awaiting the go-code.

The Bush administration did not issue the attack order. Sources within the former administration said officials were concerned that the attack would ripple outward from the epicenter of the Iraqi financial system, potentially affecting banks in the Middle East, Europe, and the United States.[5] The risk of jolting the world into a financial crisis, U.S. officials may have reasoned, was not worth it. While in this case the U.S. decided to hold back due to the high risk of collateral damage, one can imagine what the consequences for the private sector might be if hostilities were to erupt between two major powers.

Consider the perspective of a chief executive officer at a large financial institution. He opens the paper one morning and starts reading a story about a small conflict that has flared up between rebel and government forces in a country thousands of miles away. An unnamed source says the CEO's government might be financing the rebels. Without finishing the story, he flips to the financial section, finishes his coffee, and then goes on with his day.

One can imagine what the consequences for the private sector might be if hostilities were to erupt between two major powers.

Meanwhile, the bank's information technology specialists are finding out that they suffered a major system breach during the middle of the night. The attack is more complicated than they are used to seeing and they are having trouble restoring their systems. The IT specialists inform management and the bank contacts law enforcement for help. The bank is told the problem is widespread, but no one is really sure what has happened or what to do next. By lunchtime the CEO receives a brief on the problem, and he thinks to himself that maybe, just maybe, the two events are related.

But it is too late. The attack has already compromised the data in the company's online banking system serving millions of customers. There is a back up of the data, but it will take days to restore it, and the customer service department is already flooded with calls from people concerned about their life savings. Confidence in the bank is at risk, potentially causing a classic run on the bank. While it may be theoretical, this scenario is not impossible.

5 "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times,* August 1, 2009.

A Target-Rich Environment

Many international security and cyber security experts say that the critical infrastructure of nation-states—banking and finance, electrical grids, oil and gas refineries and pipelines, water and sanitation utilities, telecommunications systems—are all likely targets in future wars. In many countries, especially in the West, private ownership of these utilities means that private companies will likely be caught in the crossfire.

The threat to critical infrastructures, however, is not unique to the Western world. Dr. Masaki Ishiguro works in the Information Security Group at the Mitsubishi Research Institute in Japan. "If adversaries intended to attack nations in cyber space, they would select targets which would cause the largest impacts and losses to their opponents with the least effort," Ishiguro said. "It is therefore a very reasonable assumption that adversaries would attack critical infrastructure systems via the Internet."

Although definitions of critical infrastructure may differ between countries, much of the information systems in the various critical infrastructure sectors, particularly in developed economies, are privately owned, according to Dr. Kim Kwang Choo, information security expert at the Australian Institute of Criminology. "Almost every business in developed economies makes use of the Internet and as businesses and governments continue to engage in electronic commerce they will become increasingly globalized and interconnected," Dr. Choo said. "The common use of information technologies and communications infrastructure creates various interdependencies between key sectors, with many of the same technology-related risks affecting one or more of these sectors. The consequences of a cyber attack could therefore continue to reverberate after the immediate damage is done."

The consequences of a cyber attack could therefore continue to reverberate after the immediate damage is done.

In some countries, for instance, the electrical grid, water supply and other critical utilities are essentially tied to the Internet. Remote control devices—known in some industries as Supervisory Control and Data Acquisition (SCADA) systems—help companies to cut the costs of running and maintaining the infrastructure that provides electricity and water and refines the fuel to run cars. When companies installed these systems, it does not seem they anticipated that adversaries might also want to control the systems remotely to disrupt or damage them. Greg Day, a Principal Security Analyst at McAfee, believes the situation today arose from human beings responding to basic economics. "I have yet to meet anyone who thinks SCADA systems should be connected to the Internet. But the reality is that SCADA systems need regular updates from a central control, and it is cheaper to do this through an existing Internet connection than to manually move data or build a separate network," he said.

Experts say that it is not trivial to hack SCADA systems and other digital control systems. The hurdle is not so much the availability of hackers with the right technical skills as the amount of planning that is required for an attack. Despite the challenge of mapping out vulnerabilities in systems, there is evidence that it can be done and that attacks on utilities can be carried out successfully. One senior analyst for the U.S. Central Intelligence Agency said last year that hackers were able to attack the computer systems of utility companies outside the U.S, and in one case caused a power outage in multiple cities.[6]

Despite the challenge of mapping out vulnerabilities in systems, there is evidence that it can be done and that attacks on utilities can be carried out successfully.

6 "CIA: Hackers shut down power to entire cities," *Telegraph.co.uk*, January 25, 2008.

Critical infrastructures may not be the only targets of an attack. Nation-states are also likely to use cyber attack as a new means for conducting propaganda campaigns. Dmitri Alperovitch, Vice President of Threat Research, McAfee, believes that Russia used such tactics in its campaign against Georgia. "It's interesting to note that Russia had complete military superiority. They didn't need a cyber attack to win the war," Alperovitch said. "But it was critical for Russia to win the war of international opinion. Russia executed a very intense effort to destroy Georgia media operations through both physical and cyber means."

The targets of a propaganda war may range from traditional news Web sites to social media sites, such as Twitter and Facebook. Any site that influences public perceptions of current events might be the target of an attack during a conflict, and perhaps even during times of peace. Recently, in August 2009, Twitter, Facebook and other Web sites came under a coordinated denial-of-service attack that appeared to be directed at one man. He was a 34-year old professor at a university in Georgia who had been blogging about the Georgian conflict. Because the attacks were timed closely with the one-year anniversary of the Georgia war, some people suspect that someone inside Russia wanted to silence the professor's opinions.[7]

The attacks also affected hundreds of millions of other users. Although they were "collateral damage," few users seemed to care. In fact, once Twitter came back online, a group of users started a tongue-in-cheek discussion about what happened to their lives "when twitter was down." The consensus was that the outage had not changed their lives at all.

But, as seen during the South Ossetia War, attacks on the media may not always be so innocuous when the stakes are higher.

7 "Twitter Snag Tied to Attack on Georgian Blog," *Washington Post,* August 8, 2009.

The rapid evolution in offensive capabilities means that private sector defenses will need to be hugely adaptable.

Challenges for the Private Sector

Given the increasing sophistication of the threat from nation-states, private companies need to think about how they can improve their cyber defenses, according to Dr. Greg Rattray, author of *Strategic Warfare in Cyberspace.*

"The private sector is generally responsible for protecting themselves, but cyber war could change the types of attacks companies see. The rapid evolution in offensive capabilities means that private sector defenses will need to be hugely adaptable. This puts the private sector in a tough spot." Instead of confronting this challenge, business executives may be tempted to rely on help from the government in the event of an attack. One of the chief roles of governments around the world, after all, is to provide for the common defense.

Some experts caution business executives that relying on the government may provide only a false sense of security. "There's a danger that businesses think they will get bailed out when a catastrophic attack happens," said Scott Borg, Director of the U.S. Cyber Consequences Unit (US-CCU), an independent research institute. "This is not a good assumption for businesses to make. In the event of an attack, they may not be able to count on the government because the government is tied up with other problems. Or, the government may react in a way that businesses don't like."

Borg's organization investigates the consequences of possible cyber attacks and the cost-effectiveness of possible counter-measures. According to Borg, the US-CCU's studies generally show that a business that can continue functioning during an attack will gain an economic benefit. "In many industries, businesses that can weather cyber attacks better than their competitors stand to gain considerable market share during a wave of cyber attacks," Borg said. "And their reputations will emerge from the crisis in better shape than businesses that were less prepared."

The US-CCU's findings might make a strong case for private companies to be preparing for cyber attacks on their own, without the help of government. But business executives may wonder, if I can't count on the government to respond rapidly to a serious attack, should my company consider striking back at attackers? IT security experts call this "active defense." In contrast to the passive defensive measures of, say, installing a firewall or encrypting sensitive transactions, an example of

Information sharing can be critical to recognizing that a serious network infiltration is happening or has occurred.

active defense would be to target the source of a cyber attack with a denial-of-service attack on the offending Web server.

These active defense measures might be effective, but they are also probably illegal, said John Woods, a Washington lawyer specializing in privacy and information management. Woods offered the example of a credit card company that is hacked and wants to know if there are any tools that could be used to track where the company's data is going. "While there are such tools available," he said, "they would have to be embedded in the company's data, and would then need to download themselves onto the hacker's computer system." Woods said that a number of countries have laws on the books that may treat this activity as criminal.

Since private companies may not be able to "hack-back" against an attack that has compromised their passive defenses, whom should they call for help? Law enforcement, the military, intelligence agencies? Experts believe that private companies and governments generally need to improve their information sharing mechanisms so that both will be working together and sharing resources in the event of a serious cyber crisis.

Information sharing can be critical to recognizing that a serious network infiltration is happening or has occurred. There have been several examples where a private company did not know they had been penetrated until they were told by a government agency or law enforcement. For example, according to a report earlier this year, electrical utility companies in the U.S. did not find out that other nation-states were probing their networks for vulnerabilities until U.S. intelligence officials told them.[8]

"The problem is that government organizations are not always forthcoming about detailed threat information on attacks and without the detail it is not always possible to respond to the threat," according to William Crowell, former Deputy Director of the U.S. National Security Agency. He said there have been cases where the U.S. government told companies that they might be under attack yet did not provide any detail on the specifics of the attacks. "Clearly, we need to find a way to share information about the detailed nature of cyber attacks," Crowell said. "We should reduce the bars to the government sharing information with private entities on cyber threats and vice versa."

8 "Electricity Grid in the U.S. Penetrated by Spies," *Wall Street Journal,* April 8, 2009.

Stuck in the Middle

Creating further challenges, much of the communications, software and network infrastructure is owned and operated by the private sector. Because of the central role of technology companies, most experts agree that they will need to play some role in responding to attacks.

The fact is that many already do work closely with governments and law enforcement on attack mitigation. But the limits of private sector responsibility and the exact nature of their role in detection and response remain unclear. "Understanding the role of the private sector and where they have responsibility is one of the key questions that no one really has a good answer to right now," said Dr. James Lewis, Director of the technology program at the Center for Strategic and International Studies.

Experts have focused on the private sector's responsibility to improve the security of software and systems and further educate consumer users on protecting themselves from botnets and other forms of malicious code. "While it would be unfair to blame computers and their users that are stepping stones to a botnet, software vendors have a responsibility to make users aware of security issues," said Dr. Neil Rowe, Professor of Computer Science, Naval Postgraduate School.

Some nation-states may be willing to go a step further, requesting or requiring help from telecommunications companies and software vendors in the name of national security or foreign policy interests. During Iran's presidential election in June, for example, Twitter was planning an update to its Web site that would have cut daytime service to Iranians who were protesting the election. The protesters were relying on Twitter, a social networking service, to spread messages about rallies and communicate with the outside world. The U.S. State Department recognized the consequences for protesters and contacted Twitter to ask the company to delay the planned update.[9]

9 "U.S. State Department speaks to Twitter over Iran," *Reuters,* June 16, 2009.

These events suggest that nation-states may seek to enlist the support of private companies, perhaps even forcing them to choose sides in a time of crisis. Dr. Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School, notes that "Internet service providers and security firms have already helped detect and shut down some attacks." Nation-states could ask telecommunications companies to do even more, perhaps requiring them to routinely screen Internet traffic for the signatures of malicious software before an attack even occurs.

Proposals to introduce such screening mechanisms are a touchy subject due to concerns about protecting privacy rights. In several countries, debates are striking up on how to balance the desire to improve security with preserving the open and anonymous Internet that we know today. Brazil's legislature is now considering a bill that would require Internet service providers to keep logs of all Internet traffic for a period of three years. Vanda Scartezini, a partner at POLO Consultores Associados, an IT consultancy in Brazil, believes that this approach strikes the right balance. "While telecommunications companies should be able to help government officials figure out the source of attacks, they should not be made responsible for the content of the Internet," she said. Other countries have already adopted similar measures that require action by telecommunications companies to ensure that certain data will be available in case of future criminal investigations.

Jonathan Shea, CEO of the Hong Kong Internet Registration Corporation, agrees that Internet service providers and domain name registries have a specific role to play in helping to prevent attacks and collaborating with the government in response to attacks. "When it comes to collective interests like national security, governments in many countries tend to trade in their people's privacy for greater security," Shea said. "I see this as an increasing trend in cyber security, and I hope that we can come up with new ways to detect and prevent security breaches without impacting too much on personal privacy."

Both the public and private sectors have a shared risk and shared responsibilities when it comes to cyber security.

Exploring the Options

There is little doubt that cyber warfare will have a significant impact on the private sector. Yet the roles and responsibilities of the private sector in a time of conflict remain unclear.

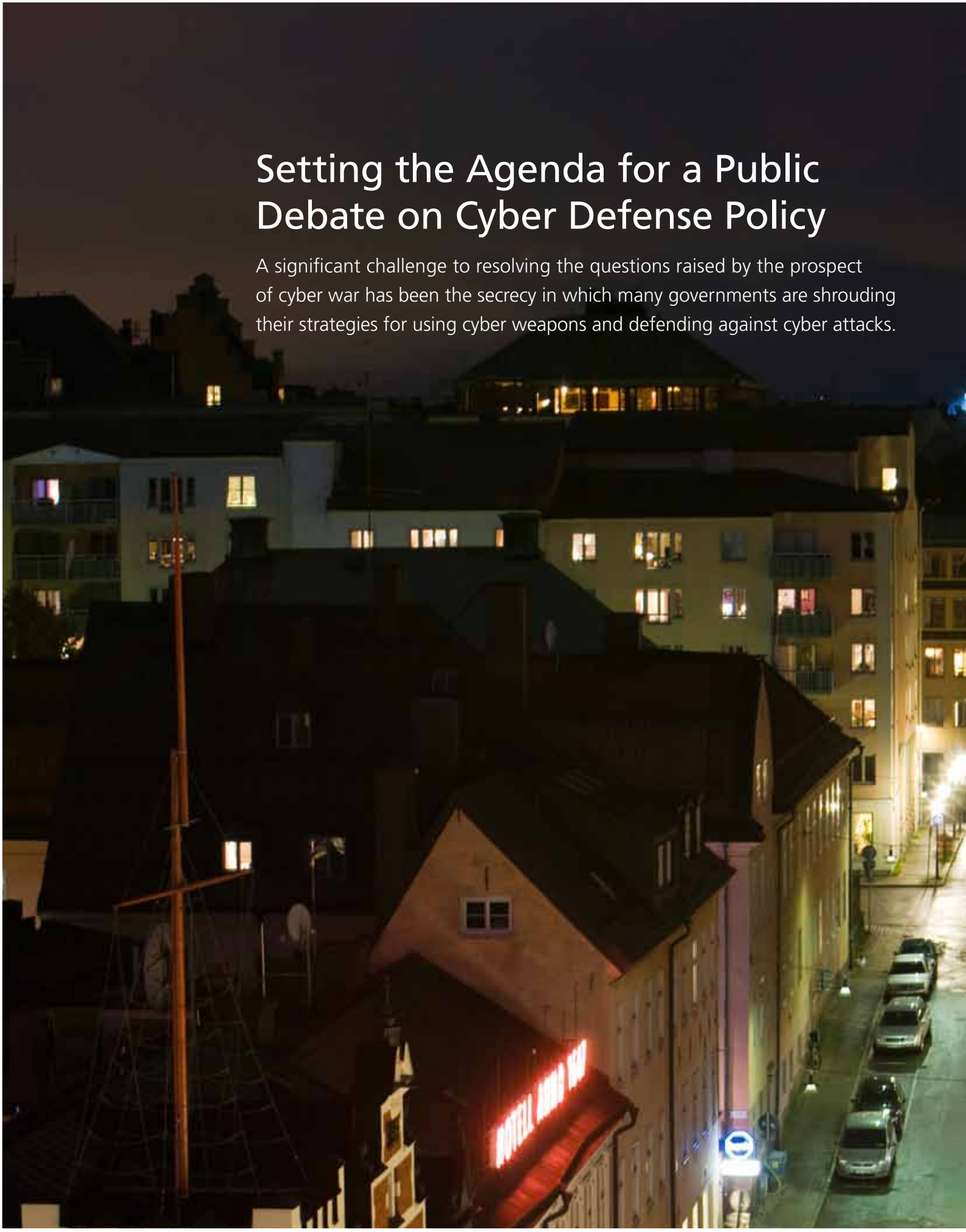
The public and private sectors need to share information, particularly threat intelligence, more effectively together.

Experts believe the private sector should work with government to explore new defensive measures such as prioritizing computer network assets, developing mitigation and response plans, creating separate networks for highly critical systems, and developing a synoptic view of network activity to improve situational awareness across sectors. "Both the public and private sectors have a shared risk and shared responsibilities when it comes to cyber security. It is in the interest of both the public and private sectors to engage each other to take preventive action against situations and conditions that facilitate cyber exploitation opportunities," said Dr. Choo. "Both the public and private sectors should continually work together to identify and prioritize current and emerging risk areas, develop and validate effective measures and mitigation controls, and ensure that these strategies are implemented and updated."

In general, the public and private sectors need to share information, particularly threat intelligence, more effectively together. If such measures are adopted proactively, before a major cyber attack happens, they might even obviate the need for governments to ever contemplate a Big Brother approach to cyber security.

Setting the Agenda for a Public Debate on Cyber Defense Policy

A significant challenge to resolving the questions raised by the prospect of cyber war has been the secrecy in which many governments are shrouding their strategies for using cyber weapons and defending against cyber attacks.



The lack of a clear doctrine for cyber defense reminds Richard Clarke, former Special Advisor to the President for Cyber Security at the White House, of the development of U.S. nuclear strategy after World War II. "In the 1950s to 1960s, civilians—many of them outside of the government—came up with a complex strategy for the use of nuclear weapons. This strategy was then debated publicly and later incorporated into national policy," Clarke said. "Today, planning for cyber war is at a similar stage. For example, the U.S. has a cyber command, but there hasn't been a public discussion about when and how cyber weapons should be used. There hasn't been an academic discussion either. Computer scientists and international relations experts are not talking to each other right now."

In the 1950s U.S. nuclear policy was to launch its entire nuclear arsenal at the Soviet Union and its allies if the Soviet Union invaded Western Europe and managed to overwhelm U.S. conventional forces—even if the Soviet Union did not use a single nuclear weapon in its attack. The purpose of this policy, known as "massive retaliation," was to deter the Soviet Union from launching such an attack. In the 1960s a group of nuclear strategists, many of them from academia, pointed out that the U.S. could not be certain that its first strike would destroy all of the Soviet Union's nuclear arsenal. This uncertainty put the lives of Americans and Europeans at risk.

Computer scientists and international relations experts are not talking to each other right now.

The group of strategists developed the concept of "counterforce" as an alternative policy: the U.S. would first target only Soviet military targets in response to Soviet aggression, but would also warn the Soviet Union of impending attacks on its cities if it did not recall its forces. The U.S. eventually adopted counterforce in place of the strategy of massive retaliation. It is not known for certain whether the plan would have helped to forestall Armageddon—luckily, it has never been tested. Nonetheless, experts from outside the military and public debate certainly helped to shape U.S. nuclear strategy.

Today, many experts say that there has not been enough discussion about the use of and appropriate responses to cyber attacks. Debate has been lacking on a number of different levels: between nation-states, within governments, between the military, civilian and intelligence agencies, and between the public and private sectors. According to Dr. Greg Rattray, author of *Strategic Warfare in Cyberspace,* cyber warfare entangles so many different actors in so many different ways that public debate is required to sort out all the issues. "We need to have a national debate on how far governments should go in protecting the security of their citizens," Rattray said. "Cyber warfare is a major form of conflict that the public should weigh in on and have the chance to decide how they want their governments to defend them."

Experts have identified several issues that should be put on the agenda for public discussion, such as: Will a cyber deterrence strategy work? Should there be an international treaty on the use of cyber weapons? What is the line between espionage and warfare in cyberspace? Public debate among policymakers, diplomats, academics and private sector experts on these issues will influence national cyber strategies and may even lead to international agreements that address cyber war.

Will a Cyber Deterrence Strategy Work?

Nuclear deterrence was a mainstay of relations between the U.S and Soviet Union during the Cold War. The nuclear stockpiles of both nations reached such levels that each side was capable of annihilating the other, and then some. Summed up neatly in the phrase "mutually assured destruction," some experts credit this defensive posture with deterring the U.S. and Soviet Union from getting into a "hot war" directly with one another. Will the proliferation of cyber attack capabilities deter conflict in a similar way today?

Not every country is similarly vulnerable to a catastrophic cyber attack.

Experts advise against going too far with the analogy to nuclear deterrence because cyber weapons are quite different from nuclear weapons. First, not every country is similarly vulnerable to a catastrophic cyber attack. Whereas the U.S. and Soviet Union were more or less equally vulnerable to the obliteration that would have followed a nuclear strike, cyber warfare can be asymmetric. For instance, developed nations tend to have more connections to the Internet than developing ones. Furthermore, some nations have connected critical infrastructure systems and networks to the Internet; others have not, or have done so to a lesser degree. If a less-connected nation were to launch a cyber attack on a more-connected one, the more-connected nation might have few, if any, targets upon which to launch a cyber counterattack. A country need not commit itself to only in-kind reprisals—that is, taking an eye for an eye, or an e-commerce server for an e-commerce server— in order to deter attacks. But when a cyber counterattack is not feasible, nation-states must decide what kinds of military, diplomatic and economic actions are proportional responses to particular cyber attacks.

Some experts point to the difficulty of attributing the source of cyber attacks as another reason why a strategy of deterrence may not work. Attackers can essentially mask their identity or forge someone else's through techniques that exploit the trusting nature of the mechanisms behind the Internet. University researchers developed the Internet protocols in the 1970s for communications and data exchange with other researchers; they did not have any reason to suspect that a person on the other side of an information transaction would be an imposter. Attackers have been able to take advantage of these basic flaws, making it difficult to ascertain who is responsible for an attack. If adversaries believe they can carry out an attack with impunity, they are not likely to be deterred by a threat of reprisal, whether by cyber, physical, diplomatic or economic means. Furthermore, attribution becomes even more complex when confronting sophisticated supply chain attacks where an adversary surreptitiously embeds "backdoors" in hardware or software during development, production, or distribution of products.

Researchers are working on improving the ability to identify attackers—or what many in the field call the "attribution problem"—by developing techniques to geo-locate attackers and by creating mechanisms, such as authentication processes, that would make the Internet less anonymous overall. "The attribution problem can be resolved," said Jamie Saunders, Counselor at the British Embassy in Washington. "Maybe 100 percent accuracy is not possible, but you can create doubt in the adversary's mind that they can get away with an attack and not be found out."

Notwithstanding efforts to find a silver bullet for attribution, adversaries may still have little reason to doubt they can get away with a cyber attack, especially if governments do not make clear their policies for retaliation. Military strategists may argue that it is advantageous to keep response plans secret or indefinite to keep the enemy guessing. Confusion leads to fear and fear is a powerful deterrent. But there is always the chance that an adversary miscalculates, a chance perhaps made more likely when rival powers keep information on new weapons and their intent to use them a secret. In the 1964 movie Dr. Strangelove, a satire set during the Cold War, the Soviets build a "doomsday device" that is programmed to destroy the world if it detects a nuclear strike on the Soviet Union. Unfortunately, the Soviets forget to tell the Americans about it until after a rogue U.S. general has ordered a nuclear attack. The dire news prompts the title character, a mad scientist, to say, "Of course the whole point of a Doomsday Machine is lost if you keep it a secret! Why didn't you tell the world?"

Should There Be an International Treaty on the Use of Cyber Weapons?

Previous advances in weaponry—the longbow, the machine gun, the tank, the atomic bomb—have sometimes influenced the way nation-states prepare for war, when they go to war and how they conduct warfare.

Cyber weapons are the newest addition to the offensive capabilities of nation-states and perhaps some non-state actors. As such, people have begun to wonder whether current international legal and ethical regimes on war and conflict need updating.

Although cyber attacks are a relatively new form of human conflict, most experts believe that they are subject to international laws of armed conflict and the Charter of the United Nations. That is, nation-states should still follow principles guiding when it is justified to use force against another nation—a body of law known as *jus ad bellum*—and what actions combatants may take when in armed conflict—a separate body of law known as *jus in bello*.

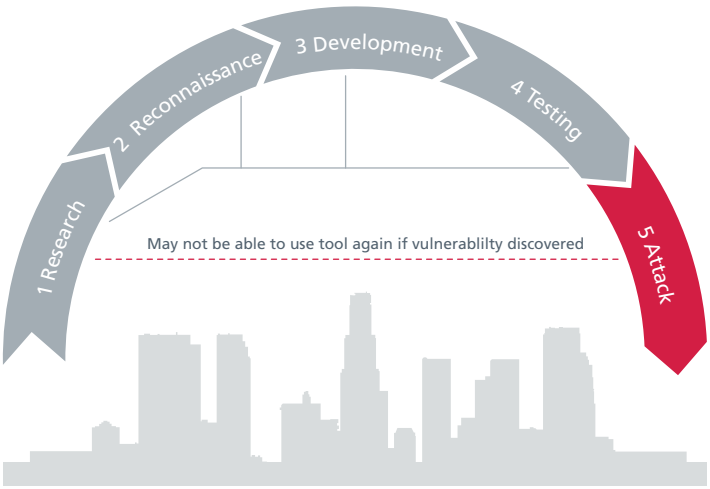
Applying these general principles to specific events, however, is likely to require a great deal of analysis. The National Research Council, a U.S. institute for independent investigations and analysis, issued a report in April 2009 on the technological, legal, ethical and policy implications for the potential acquisition and use of cyber attack capabilities. The report argues that cyber weapons are not altogether so different from kinetic attacks that international laws do not apply. Nevertheless, the report also states that because cyber weapons are so novel, "there will be uncertainties in how [laws of armed conflict] and UN Charter law might apply in a given instance." The report continues: "An effects-based analysis suggests that the ambiguities are fewest when cyberattacks cause physical damage to property and loss of life…The ambiguities multiply in number and complexity when the effects do not entail physical damage or loss of life but do have other negative effects on another nation."[10]

Some legal experts have suggested that substantial updating to the laws of armed conflict may be necessary. "Current international law is not adequate for addressing cyber war," said Eneken Tikk, legal adviser for the Cooperative Cyber Defence Centre of Excellence in Estonia. "Analogies to environmental law, law of the sea and kinetic war all break down at some point. Answering the question of when to use force in response to a cyber attack needs its own framework."

Other experts have noted the need to establish common norms and behaviors for actions in cyberspace. For example, rather than seeking to bar the development of cyber weapons, nation-states could establish protocols for what is acceptable and unacceptable behavior in cyberspace. For example, establishing an understanding that it is unacceptable for a nation state to attack civilian infrastructure via cyberspace, and that such action would justify retribution, could deter a nation state from organizing or launching such attacks.

Even if nation-states generally agree that an entirely new legal regime is not needed, their proposals so far have conflicted on how best to address the ambiguities in the current framework. Some nation-states are arguing for a ban on the offensive use

Life Cycle of a Cyber Attack



Note that once a cyber attack tool is used, the enemy may discover the vulnerability and patch it, rendering the tool useless in the future.

Figure 3. There are five general stages to developing and deploying a cyber "weapon"

10 William A. Owens, et al., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* Committee on Offensive Information Warfare, National Research Council (2009).

"If you were a half-clever adversary, you probably wouldn't perpetrate an attack that everyone agrees is cyber warfare; you would play in the shades of gray."

– Michael Rothery, First Assistant Secretary, National Security Resilience Policy Division, Attorney—General's Dept. (Australia)

of cyber weapons, similar to international bans on biological and chemical weapons. Other nations say that because it would be difficult, or impossible, to verify compliance with such a treaty, the international community should instead be working on cooperative measures to decrease cyber crime. One example is the Council of Europe Convention on Cybercrime. Over 40 nations have signed the treaty, which pledges each nation to assist others in identifying and bringing to justice the perpetrators of criminal activity in cyberspace.

A number of experts point to the benefits of increased international cooperation on cyber crime. According to Dr. Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School, "strong security plus effective law enforcement may be the best deterrent for criminal cyber attacks. We need to remain focused on fighting cyber crime and this is the area where international cooperation can make a positive impact."

Rattray suggests that reducing cyber crime may help to make the Internet more secure as a whole. "The security of cyberspace needs to be considered like an ecosystem. Cyber crime is making the Internet a messy place today. If we were to clean up crime in cyberspace, it would be easier for governments to attribute attacks to their actual sources," he said. Having less to worry about from cyber criminals, governments may be able to keep a better eye on each other.

There is still an argument to be made for formal and informal international frameworks that would more directly address cyber conflict, according to one expert. "Identifying threats and their sources is no easy task; it is compounded when we remember the impossibility of drawing a clear definition of territorial borders to determine, for example, legal issues, such as the jurisdiction of a cyber crime lawsuit," said Raphael Mandarino, Jr., Director of the Department of Information Security and Communications, Institutional Security Cabinet of the Presidency of Brazil. "Because cyberspace threats are global in nature and their technology is ever-evolving, the struggle to keep up with this evolution demands an enhanced legal structure and increased international cooperation." Manadarino recommended that each country's cyber security strategy should foster close cooperation with international organizations and other countries. Furthermore, he suggested the debate agenda for the international community should include issues such as the definition of 'cyber borders.'

Where is the Line Between Espionage and Warfare in Cyberspace?

Espionage is always a shadowy game. Played beneath the façade of peace, nations vie to steal state secrets from each other, the specter of conflict distant, but recognizable. In some ways, cyber espionage is no different.

"The last decade is replete with stories of infiltrations by sources that were unidentifiable, but clearly malicious in intent. These events together represent a reconnaissance method that is part of an attack philosophy," said Mike Jacobs, former Information Assurance Director, U.S. National Security Agency. "But what has always worried me is the stuff you can't see happening."

From what has been reported in the media, it appears that nation-states are engaging in cyber espionage on a massive scale. From around 2002 to 2005, for instance, an unknown source managed to download 10 to 20 terabytes of information from a sensitive, but unclassified, U.S. Department of Defense network in an episode code-named "Titan Rain." To put this amount of information in perspective, consider that digital copies of all the books (more than 18 million) in the U.S. Library of Congress would represent 20 terabytes of data. Most experts agree that downloading sensitive information—even vast amounts of information—in this fashion is no more than espionage. "Espionage is espionage," said Dmitri Alperovitch, Vice President of Threat Research, McAfee. "It's dangerous to call every spy action an act of war."

Once a hacker gains access to a system, it may be a relatively simple transition from downloading data to sabotaging it.

Yet some current and former national security experts warn that cyber espionage is not necessarily your typical game of espionage. In the days of the Cold War, espionage might have involved tapping into an adversary's telephone system or radio transmissions or sending a spy to break into a secure facility to snap some photos of secret files. In either case, the goal was usually to collect information rather than to manipulate or destroy it—these forms of sabotage would have risked alerting the enemy. Today, once a hacker gains access to a system, it may be a relatively simple transition from downloading data to sabotaging it. According to Richard Clarke, "The distinction between intelligence collection and damage to systems is a few keystrokes."

National security experts and intelligence officials confirm that nation-states are leaving back doors on each other's systems while spying in order to guarantee future access to those systems. In some cases, hackers may even plant malicious pieces of software that could be activated in a future conflict to gain an advantage over the enemy.

These kinds of activities seem more like forward deployment for a future attack than the collection of intelligence. The challenge is in deciding where to draw the line since it may be more difficult to discern an adversary's motives in cyberspace than in the physical world. "We can see physical war about to happen through satellite images of tanks building up at borders or major shifts in military personnel," said John Woods, a Washington lawyer specializing in privacy and information management. "But we may not have this same visibility in cyberspace. When you discover a network intrusion by a foreign nation, are you looking at intelligence gathering, intelligence gathering gone too far or forward advancement for an impending act of war?"

A nation's response to cyber espionage also poses questions. Nation states are turning to "Active Network Defense," which involves more than seeking to identify the origin of the attack but also redirecting such attacks without the adversary's knowledge. Active Network Defence could involve feeding the adversary disinformation, but it could also involve disrupting and disabling systems through more specialized covert attacks. Such activities could escalate, leading to a wider conflict involving both government and private sector infrastructure.

Most governments do not seem to have made up their minds about whether these potentially damaging activities constitute acts of war, according to Saunders. "The relatively easy transition from espionage to disruption may be the only unique characteristic of cyberspace, maybe the one reason why we can't simply apply the laws of armed conflict to the virtual world," he said. "While governments are aware that there is a level of cyber espionage under way, they probably need to think more on the subject and clarify what will not be tolerated."

Moving Forward

While experts may disagree on the definition of cyber war, there is significant evidence that nations around the world are developing, testing and in some cases using or encouraging cyber means as a method of obtaining political gain. Much of this activity is shrouded in secrecy, but one national security expert remarked that there is already a constant, low level of conflict occurring in cyberspace. Whether these attacks are labeled as cyber espionage, cyber activism, cyber conflict or cyber war, they represent emerging threats in cyberspace that exist outside the realm of cyber crime.

International cyber conflict has reached the tipping point where it is no longer just a theory, but a significant threat that nations are already wrestling with behind closed doors. The impact of a cyber war is almost certain to extend far beyond military networks and touch the globally connected information and communications technology infrastructure upon which so many facets of modern society rely. With so much at stake, it is time to open the debate on the many issues surrounding cyber warfare to the global community.

International cyber conflict has reached the tipping point where it is no longer just a theory, but a significant threat that nations are already wrestling with behind closed doors.

Contributors

EUROPE, MIDDLE EAST, AFRICA

Greg Day—Principal Security Analyst for McAfee

Greg Day is the Principal Security Analyst for McAfee in EMEA (Europe, Middle East, Africa), the primary analyst of security trends and McAfee strategy in the region. As an active spokesperson for the company, he is a frequent contributor to journals, has had numerous papers published and is a keynote speaker on all aspects of information security at conferences and events. Mr. Day is the EMEA lead for the McAfee initiative to fight cyber crime globally and has spoken at the Council of Europe (CoE) and the Organization for Security and Cooperation in Europe (OSCE) events on cyber crime, warfare and terrorism. Mr. Day is also a member of a range of security industry forums, including the Cyber Security Industry Alliance (CSIA), the Cyber Security Knowledge Transfer Network and the Internet Security Forum (ISF).

Taimar Peterkop—Defense Counselor, Embassy of Estonia, Washington, D.C.

Taimar Peterkop is the Defense Counselor at the Embassy of Estonia to the U.S. in Washington, D.C. Prior to his current position, Mr. Peterkop worked as Director of Operations and Crises Management department at the Estonian Ministry of Defence, with the main task of oversight of the Estonian Defence Forces operations in and outside of Estonia. He had this position during the April cyber attacks against Estonia in 2007. Before that, Mr. Peterkop was Director of International Law Section where he was responsible for legal aspects regarding Deployment of Estonian Defence Forces to Iraq, Afghanistan and other conflicts. He also dealt with Status of Forces issues and legal aspects of Estonia's accession to NATO. Mr. Peterkop has also worked as a lecturer on international law and published articles on the role of the military in peacetime and status of forces agreements of the visiting forces.

Dr. Jamie Saunders—Counselor at the British Embassy

Dr. Jamie Saunders is a counselor at the British Embassy in Washington, where he leads on cyber security policy. He has over 20 years experience in the government of the United Kingdom, working on the application of technology to a range of national security problems including Counter Terrorism, Counter Proliferation and Counter Narcotics. Before joining the Embassy in 2008, he worked for 5 years as a member of the Senior Civil Service supporting CONTEST (the UK Government's Counter Terrrorism strategy).

Eneken Tikk—Advisor in Public Law, Cooperative Cyber Defence Center of Excellence

Eneken Tikk is Legal Advisor to the NATO Cooperative Cyber Defence Centre of Excellence. She is also the head of the Cyber Defence Legal Expert Team at the Estonian Ministry of Defense and an adviser on information law and legal policy to the Estonian Ministry of Justice. Ms. Tikk is a legal expert on personal data, databases and public information law. She is a lecturer on information law and legislative drafting at Tartu University, and is currently working in various research programs, including the "Harmonization of Information Law and Legal Theoretical Approach to Regulation of Information." Ms. Tikk has previously been a lecturer in the field of international law and law of armed conflicts for the Estonian Military College.

UNITED STATES

Dmitri Alperovitch—Vice President of Threat Research at McAfee

Dmitri Alperovitch is the Vice President of Threat Research at McAfee. He leads the company's research in Internet threat intelligence analysis and correlation, as well as development of in-the-cloud reputation services. With more than a decade of experience in the field of information security, he has significant experience working as a subject-matter expert with all levels of U.S. and International law enforcement on analysis, investigations and profiling of transnational organized criminal activities and cyber threats from terrorist and nation-state adversaries. In addition, Mr. Alperovitch is a recognized authority on online organized criminal activity and cyber security, and has been quoted in numerous articles, including those by Associated Press, Business Week, New York Times, Los Angeles Times, USA Today, and Washington Post. He has been a featured speaker and panelist at numerous law-enforcement, industry and academic security conferences.

Dr. Scott Borg—Director and Chief Economist of the U.S. Cyber Consequences Unit (US-CCU)

Dr. Scott Borg is the Director and Chief Economist of the U.S. Cyber Consequences Unit (US-CCU), an independent, non-profit research institute that carries out extensive field investigations into the likely consequences of possible cyber attacks. He is responsible for many of the concepts that are currently being used to understand the implications of cyber attacks in business contexts. He has been a guest lecturer at Harvard, Yale, Columbia, and other leading universities, and is currently a Senior Research Fellow in International Security Studies at the Fletcher School of Law and Diplomacy of Tufts University. Dr. Borg's comprehensive book *Cyber Attacks: A Handbook for Understanding the Economic and Strategic Risks* should be available later this year.

Richard Clarke—Chairman of Good Harbor Consulting and Former Special Advisor to the President for Cyber Security

Richard A. Clarke is an internationally-recognized expert on security, including homeland security, national security, cyber security, and counterterrorism. He is currently the Chairman of Good Harbor Consulting, a global security consulting firm, and an on-air consultant for ABC News. Mr. Clarke served the last three Presidents as a senior White House Advisor. Over the course of an unprecedented 11 consecutive years of White House service, he held the titles of Special Assistant to the President for Global Affairs, National Coordinator for Security and Counterterrorism and Special Advisor to the President for Cyber Security.

William P. Crowell—Independent Security Consultant and Former Deputy Director, U.S. National Security Agency (NSA)

William P. Crowell is an Independent Consultant specializing in Information Technology, Security and Intelligence Systems. Crowell previously served as President and Chief Executive Officer of Cylink Corporation, a leading provider of e-business security solutions. Prior to Cylink, he held a series of senior positions in operations, strategic planning, research and development, and finance at the U.S. National Security Agency. He served as Deputy Director of Operations from 1991 to 1994 running its core signals intelligence mission. In February 1994 he was appointed as the Deputy Director of NSA and served in that post until his retirement in September 1997. Crowell is an expert on network and information security issues. In December 2008 Security Magazine selected him as one of the 25 most influential people in the security industry. In May 2007 he co-authored the book, *Physical and Logical Security Convergence.*

Dr. Dorothy E. Denning—Distinguished Professor of Defense Analysis at the Naval Postgraduate School

Dr. Dorothy E. Denning is a Distinguished Professor of Defense Analysis at the Naval Postgraduate School, where her current research and teaching encompasses the areas of conflict and cyberspace; trust, influence and networks; terrorism and crime; and information operations and security. She is author of *Information Warfare and Security* and has previously worked at Georgetown University, Digital Equipment Corporation, SRI International, and Purdue University.

Michael J. (Mike) Jacobs—Former Information Assurance Director, U.S. National Security Agency (NSA)

Michael J. Jacobs is an independent consultant on Information Assurance matters. Previously, he served for five years as a Vice President and Director of the Cyber and National Security Program for SRA International, Inc. Prior to SRA, Mr. Jacobs was the Information Assurance (IA) Director at the U.S. National Security Agency (NSA). Under his leadership, NSA began implementing an Information Assurance strategy to protect the Defense Information Infrastructure and as appropriate, the National Information Infrastructure. He is an industry veteran with 45 years of experience (38 in the U.S. Federal government) in information security and information assurance.

Paul B. Kurtz—Partner, Good Harbor Consulting

Paul B. Kurtz leads Good Harbor's cyber and IT security practice group to provide strategic and tactical planning advice to a wide variety of international and domestic clients. He is also the executive director of SAFECode, the Software Assurance Forum for Excellence in Code, a global non-profit organization dedicated to promoting effective software assurance methods. Mr. Kurtz is an internationally recognized cyber security and homeland security expert who has worked at the highest levels of government, serving under Presidents Clinton and George W. Bush. Most recently, he served on President Obama's transition team, evaluating cyber security policy and strategy for government agencies including the Department of Defense, the Department of Homeland Security, the National Security Administration and the CIA.

Dr. James Andrew Lewis—Senior Fellow and Program Director at CSIS

Dr. James Andrew Lewis is a Senior Fellow and Program Director at CSIS where he writes on technology, national security and the international economy. Before joining CSIS, he worked in the Federal government as a Foreign Service Officer and as a member of the Senior Executive Service. His assignments involved Asian regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, sanctions, Internet policy, and military space programs.

Dr. Greg Rattray—Principal at Delta Risk Consulting

Dr. Greg Rattray is a Principal at Delta Risk Consulting, which establishes risk management strategies and cyber security capacity building approaches for government and private sector clients. Previously, Dr. Rattray served 23 years as a U.S. Air Force officer. His assignments included Director for Cyber Security on the White House National Security Council staff, leading national policy development and NSC oversight for cyber security programs and oversight of Iraqi telecommunications reconstruction. He also served as an Assistant Professor of Political Science and Deputy Director of the USAF Institute of National Security Studies at the Air Force Academy. He is the author of numerous books and articles including *Strategic Warfare in Cyberspace,* a seminal work in the cyber conflict field.

Dr. Neil Rowe—Professor of Computer Science, Naval Postgraduate School

Neil Rowe, Ph.D., E.E. is a Professor of Computer Science, Center for Information Security Research (CISR), U.S. Naval Postgraduate School. His interests include a broad range of topics in applied artificial intelligence. Dr. Rowe's recent work has focused on modeling and implementation of deception in cyberspace as well as automated surveillance for suspicious behavior. He has authored numerous publications on a range of cyber security issues.

Dr. Phyllis Schneck—Vice President and Director of Threat Intelligence for the Americas for McAfee, Inc.

Dr. Phyllis Schneck is Vice President and Director of Threat Intelligence for the Americas for McAfee, Inc. In this role, she is responsible for design and applications of McAfee's threat intelligence, strategic thought leadership and evangelism around technology and policy in cyber security, and leading McAfee initiatives in critical infrastructure protection and cross-sector cyber security. Schneck has had a distinguished presence in the security and infrastructure protection community, most recently as a Commissioner and a working group Co-Chair on public-private partnership for the CSIS Commission to Advise the 44th President on Cyber Security. She holds three patents in high-performance and adaptive information security, and has six research publications in the areas of information security, real-time systems, telecom and software engineering.

Dr. Gene Spafford—Professor of Computer Science and Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS)

Dr. Gene Spafford has been on the faculty at Purdue University since 1987. He is currently a Professor of computer science and Executive Director of the Center for Education and Research in Information Assurance and Security (CERIAS). Dr. Spafford is widely known for work in information security and privacy, software engineering, and computing policy. Some people consider him a polymathic futurist, and others simply think he's an iconoclastic crank. He is a Fellow of the ACM, IEEE, AAAS and the (ISC)^2. He has been repeatedly honored for his contributions in research, education, and service, including an ACM President's Award, the CRA Distinguished Service Award, the IEEE Booth Award, and the NIST/NSA National Computer Systems Security Award.

John Woods—Partner at Hunton & Williams

Mr. Woods is a Partner at Hunton & Williams, LLP in Washington, DC and his practice focuses on conducting internal investigations, advising on information security legal issues and representing corporations in government investigations and business crimes. He has a particular focus in advising corporations in the legal response to network security intrusions and data breaches. He advised RBS Worldpay in its investigation of a network intrusion incident, a Fortune 500 retailer in the largest reported hack of credit card data in history, and is advising several companies in the US defense industrial base regarding legal issues associated with the advanced persistent threat hacking problem.

Amit Yoran—Chairman and CEO of NetWitness Corporation

Amit Yoran serves as the Chairman and CEO of NetWitness Corporation, a leading provider of network security analytic products. He is a Commissioner of the CSIS Commission on Cyber Security advising the 44th Presidency and serves on several industry and national advisory bodies. Prior to NetWitness, Mr. Yoran served as a Director of the National Cyber Security Division at the Department of Homeland Security, and as CEO and advisor to In-Q-Tel, the venture capital arm of the CIA. Formerly, he served as the Vice President of Worldwide Managed Security Services at the Symantec Corporation. He formerly served as an officer in the United States Air Force in the Department of Defense's Computer Emergency Response Team.

LATIN AMERICAS

Renato Blum—CEO of Opice Blum Advogados Associados

Renato Blum is the CEO of Opice Blum Advogados Associados. He is a lawyer and an economist by training. Currently, he teaches an MBA course in Information Technology Law at the Escola Paulista de Direito. He is also the President of the Supreme Council of Information Technology at the Federation of Trade/SP. Mr. Blum was the coordinator and co-author of the book, *Manual de Direito Eletrônico e Internet (Electronic Law and Internet Manual).*

Raphael Mandarino, Jr.—Director of the Department of Information Security and Communications, Institutional Security Cabinet, Presidency of the Federative Republic of Brazil

Mr. Raphael Mandarino Junior is currently the Director of the Department of Information Security and Communications (DSIC—Departamento de Segurança da Informação e Comunicações) of the Institutional Security Cabinet of the Presidency of the Federative Republic of Brazil, since May 2006. He is also responsible for the Coordination of the Management Committee of Information Security (CGSI—Comitê Gestor da Segurança da Informação), group of the Council of National Defense (Conselho de Defesa Nacional), since September 2006. He is a member of Management Committee of Infrastructure Public Key of Brazil (CG ICP-BRASIL—Comitê Gestor da Infra-Estrutura de Chaves Públicas do Brasil), since April 2007.

Vanda Scartezini—Partner, POLO Consultores Associados

Vanda Scartezini has held many management positions with private technology companies and public institutions. She is the co-founder of and has been an active partner in Polo Consultores, a Brazilian IT consulting company, since 1985. She also acts as President of Altis, a Software & Service outsourcing company and as chair of the board of FITEC, an ICT R&D foundation. She is also an associate partner of Getulio Vargas Foundation Projects and member of the board of ABES, the Brazilian Software Industry Association. She has acted as a Brazilian Government representative in many international missions around the world as well as an expert and consultant for international institutions.

ASIA-PACIFIC

Dr. Kim Kwang (Raymond) Choo—Australian Institute of Criminology

Dr. Kim Kwang (Raymond) Choo works for the Australian Institute of Criminology and is currently in the U.S. to undertake a project funded by a 2009 Fulbright Scholarship to research the future of the cybercrime threat environment. He is also a Visiting Fellow at The Australian National University's ARC Centre of Excellence in Policing and Security, and a member of the International Consultant Group (Research) in the United Nations Office on Drugs and Crime-Korean Institute of Criminology "Virtual Forum against Cybercrime" Program. In June 2009, he was named one of 100 Emerging Leaders (Innovation category) in The Weekend Australian Magazine/Microsoft's Next 100 series. In September 2009, he received the 'Highly Commended' award at the 2009 ACT Pearcey Award for Young Achievers. Other awards include the '2008 Australia Day Achievement Medallion' and the 'Wilkes Award' for the best paper published in the 2007 volume of Oxford University Press's Computer Journal.

Dr. Masaki Ishiguro—Senior Researchers at the Information Security Research Group, Mitsubishi Research Institute, Inc.

Dr. Masaki Ishiguro is a Senior Researcher at the Information Security Research Group, Mitsubishi Research Institute, Inc. His work includes research and development on Internet threat detection systems, risk evaluations for information security, formal verification of security protocols, and the trend of information security policy. Dr. Ishiguro received his master's degree at the graduate school of Information Science at the University of Tokyo and he received his doctorate in Information Science at Japan's Advanced Institute of Science and Technology.

Michael Rothery, First Assistant Secretary, National Security Resiliency Policy Division, Australian Attorney-General's Department

Michael (Mike) Rothery heads the National Security Resilience Policy Division created in March 2009, which is responsible for policy and legal policy advice related to developing national resilience to the full range of natural and human made hazards, including the areas of critical infrastructure protection, chemical, electronic and identity security, and protective security policy. The Division runs the Trusted Information Sharing Network for Critical Infrastructure Protection (TISN), the Document Verification Service and the Australian Government Computer Emergency Readiness Team (GovCERT.au). In this position Mr. Rothery chairs the Protective Security Policy Committee and the E-Security Policy and Coordination Committee. From December 2004 to March 2009, he led the Emergency Management Policy and Liaison Branch of Emergency Management Australia, the E-Security Policy and Coordination Branch and the Critical Infrastructure Protection Branch. Earlier at the Attorney-General's Department, Mr. Rothery worked on counter terrorism policy & training, e-security and secure communications.

Jonathan Shea—CEO, Hong Kong Internet Registration Corporation

Jonathan Shea is the Chief Executive Officer of the Hong Kong Internet Registration Corporation, a non-profit-making and non-statutory corporation responsible for the administration of Internet domain names under '.hk' country-code top level domain. Since Mr. Shea joined HKIRC in 2002, the number of .hk domain names has increased from around 60,000 to more than 100,000 at present. Mr. Shea has over 20 years of experience in IT, telecom and Internet industries. Starting as an electronics and telecommunications engineer, Mr. Shea has in-depth knowledge in the technological development of data networking and the Internet. Before taking up the CEO role in HKIRC, Mr. Shea was the Chief Technology Officer and Chief Information Officer at a number of telecom and Internet service operators.

Dr. Paul Twomey—Former President and CEO of ICANN

Dr. Paul Twomey served as President and CEO of ICANN (Internet Corporation for Assigned Names and Numbers) from March 2003 to June 2009. As Senior President, he now acts as advisor and assistant to new President and CEO Rod Beckstrom. Dr. Twomey's background brought a balance of public and private experience to ICANN during his tenure, including numerous leadership positions in commercial enterprises, government, and in chairing ICANN's Government Advisory Committee. Widely published in academic and popular journals, Dr. Twomey has contributed to books on industry policy, foreign and defence policy, and development issues.

About Good Harbor Consulting

Good Harbor Consulting is a global provider of strategic security, safety and risk management consulting services to public and private sector clients. Led and staffed by personnel with decades of knowledge and experience in the government and private sector, Good Harbor provides strategic counsel to help clients understand their operating environment and manage their safety and security risks. Good Harbor is headquartered in Arlington, Virginia and has branch offices near Boston, Massachusetts and in Abu Dhabi, United Arab Emirates.

About McAfee

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

For more information, visit:
http://www.mcafee.com

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

6735rpt_virtual_criminology_1009