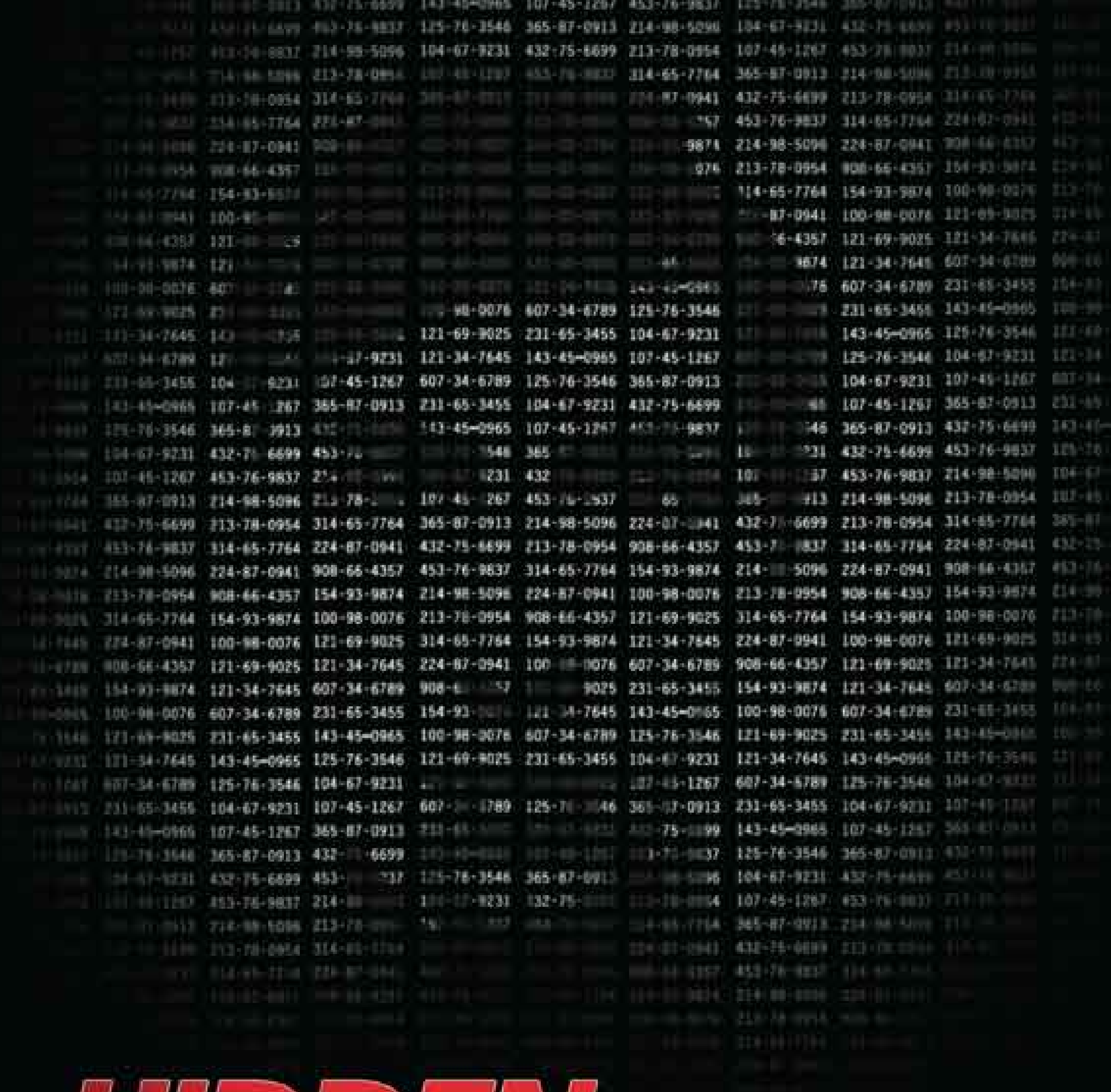


HIDDEN DANGER

THE THREAT TO AMERICA'S NETWORKS

Lexington Institute

FINDINGS IN BRIEF

- Digital networks are the nervous system of our civilization, essential to commerce and culture. The entire economy, from banking to utilities to manufacturing to healthcare, relies on internet-style communications. Even the military has reorganized for what it calls "network-centric warfare."
- But the internet empowers everybody, including criminals and foreign governments intent on weakening America. As digital networks have proliferated, so has malicious software designed to exploit the networks for destructive purposes. Internet predators are increasingly capable and sophisticated.
- Cyber threats are now so common that they pose a real danger to national security. Networks must be secured against intrusion, otherwise the nation risks severe economic damage and potential defeat at the hands of other countries. But the anonymity of the internet impedes efforts to deter and destroy threats.
- The federal government has taken a number of steps aimed at combating threats to digital networks, including a Comprehensive National Cybersecurity Initiative launched in 2008. However, the current federal framework for dealing with cyber threats is fragmented, and cannot keep up with emerging dangers.
- The new administration will have to determine whether current cyber-security efforts are sufficient, or additional resources are required. It will also have to decide whether the current federal framework for addressing cyber threats can do the job, and if not how to tap more agile sources of expertise in the marketplace.
- This report provides a concise overview of emerging threats to America's networks and the federal response, highlighting key issues for the new administration. It was written by Dr. Loren Thompson of the Lexington Institute staff.

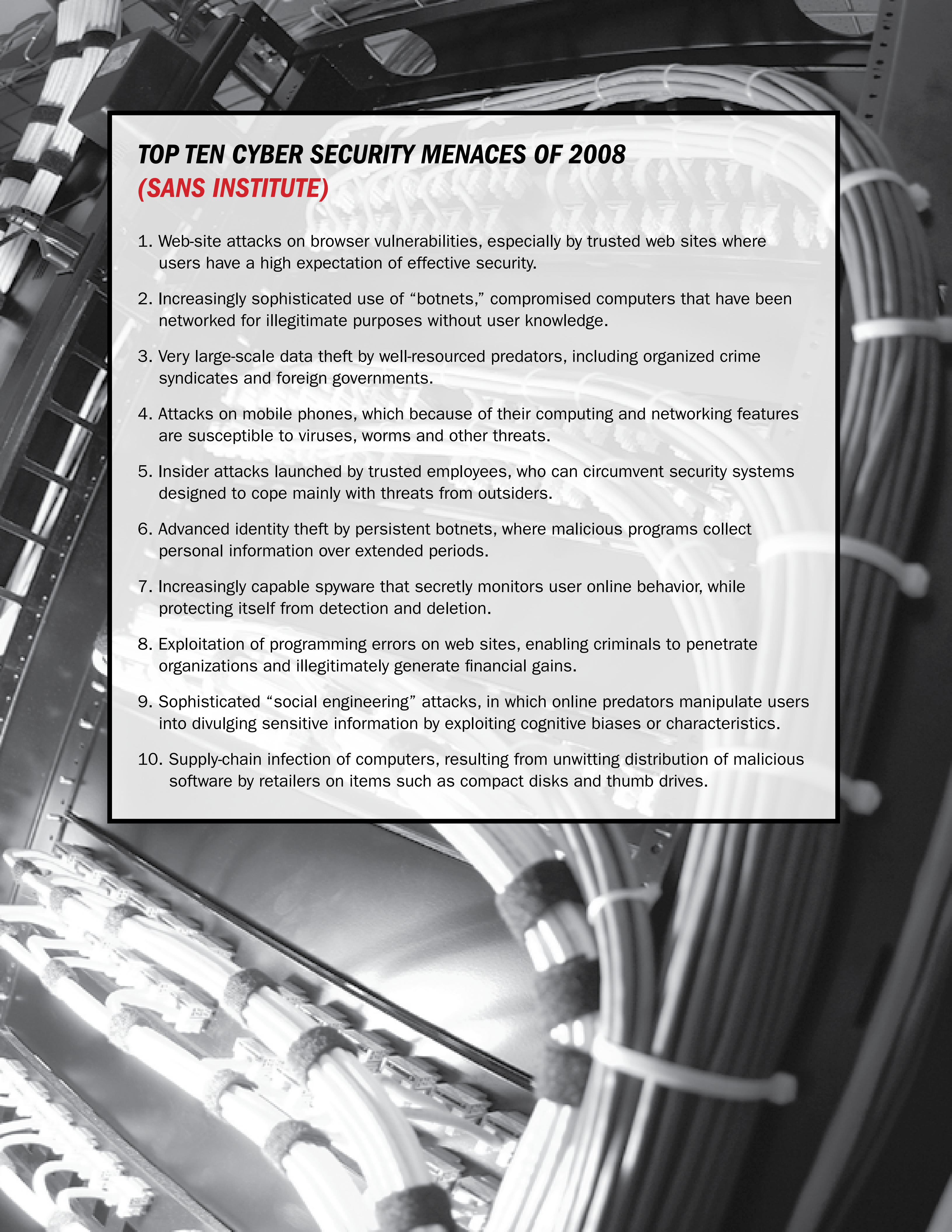
HIDDEN DANGER: THE THREAT TO AMERICA'S NETWORKS

In the 20 years since the cold war ended, the world has become connected in ways it never was before. A breakthrough called the internet has integrated previously isolated networks into a single global web that anyone with a computer can enter. The technology that made this possible, called internet-protocol communications, has torn down the barriers that once impeded interaction among diverse and scattered users. As a result, the world has become a more open and productive place. People who once had little say in how their society operated have been empowered, and opportunities for enrichment of every kind have multiplied.

But the paradox of the internet is that in delivering power to the edges, it has also delivered power to the fringes. Predators of every persuasion now have access and options they never would have enjoyed in the past. Some are agents of foreign governments seeking to subvert democracy, or steal its secrets. Others are criminals, cult members, transnational terrorists or nihilistic vandals. All have discovered that the internet provides a potential pathway to their goals. And increasingly, it is information networks themselves – the nervous system of our civilization – that such actors seek to target.

Most internet users have some awareness of this problem, since they encounter it in the form of spyware, viruses and other online nuisances. But the most disturbing "cyber" threats are largely invisible to the general public, because they involve attacks on specialized networks used by the armed forces, healthcare professionals, air traffic controllers, financial institutions, public utilities and heavy industry. Each of these vital components in modern society now relies on internet-protocol communications to run efficiently, and in most cases the new technology was assimilated without a careful assessment of its vulnerability to attack by outsiders.

This report provides an overview of the threat to America's information networks, especially the networks operated by the federal government. It begins by explaining the spectrum of cyber threats the nation currently faces, and then details the potential consequences for military, civil and commercial networks, the available remedies for dealing with the danger, and the steps the government has taken to date in implementing said remedies. It concludes with a series of recommendations, the most important of which is that government recognize its limitations and turn to the private sector for most of the expertise needed in defeating cyber threats.



TOP TEN CYBER SECURITY MENACES OF 2008 (SANS INSTITUTE)

1. Web-site attacks on browser vulnerabilities, especially by trusted web sites where users have a high expectation of effective security.

2. Increasingly sophisticated use of “botnets,” compromised computers that have been networked for illegitimate purposes without user knowledge.

3. Very large-scale data theft by well-resourced predators, including organized crime syndicates and foreign governments.

4. Attacks on mobile phones, which because of their computing and networking features are susceptible to viruses, worms and other threats.

5. Insider attacks launched by trusted employees, who can circumvent security systems designed to cope mainly with threats from outsiders.

6. Advanced identity theft by persistent botnets, where malicious programs collect personal information over extended periods.

7. Increasingly capable spyware that secretly monitors user online behavior, while protecting itself from detection and deletion.

8. Exploitation of programming errors on web sites, enabling criminals to penetrate organizations and illegitimately generate financial gains.

9. Sophisticated “social engineering” attacks, in which online predators manipulate users into divulging sensitive information by exploiting cognitive biases or characteristics.

10. Supply-chain infection of computers, resulting from unwitting distribution of malicious software by retailers on items such as compact disks and thumb drives.

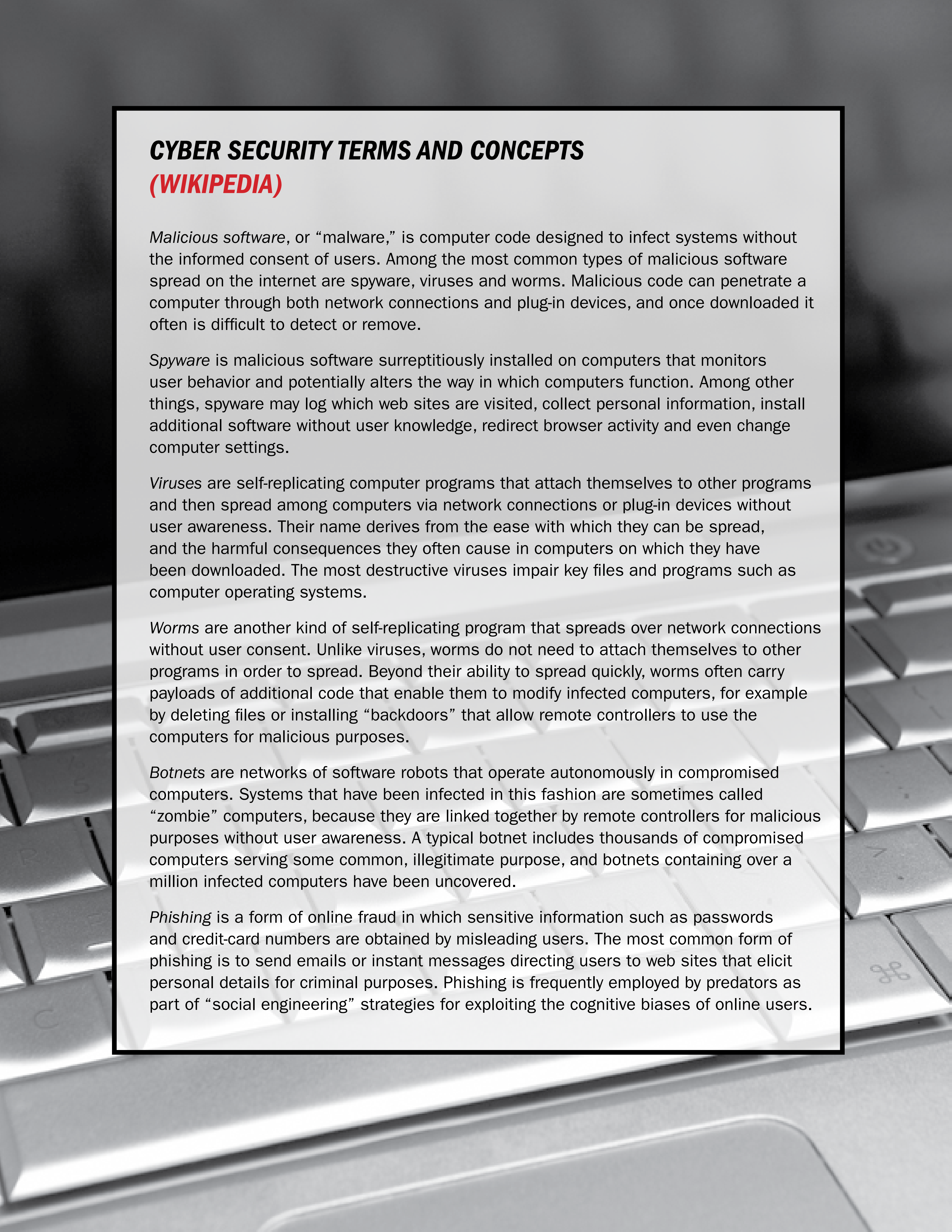
THE NATURE OF THE THREAT

Networks of one sort or another have existed since the dawn of civilization. Digital networks, though, are a relatively new thing. Whether wired or wireless, digital networks all operate using binary computer code – the language of ones and zeros that is the foundation for software. The basic architecture of the information age consists of computer nodes where digital information is stored and used, and links that convey that information between nodes. When a group of nodes and links are organized to accomplish some shared purpose, they become a network.

The internet codes digital information so that it can traverse many different networks as if they were a single unified web. Originally conceived to maintain connectivity in wartime, it grew into a worldwide phenomenon when tools became available that made it easy for people to use internet-protocol communications to send or access information anywhere a network connection existed. Unfortunately, predators quickly learned how to employ the new tools for their own purposes. Thus, from the earliest days of the information age, there has been concern about securing the internet against those who would misuse it.

Concern about cyber security grew as internet-style communications became the preferred means of conducting commerce, governance and other forms of social interaction. Today, digital networks are so ubiquitous that their sudden disappearance would lead to economic collapse, and yet many people are barely aware they are relying on networks when they turn on the lights, go to the grocery store or seek medical care. But the same features that make digital networks pervasive in everyday life also make them ready conduits for viruses, worms and other forms of malicious software that can destroy the wealth and welfare of unsuspecting users. More ominously, clever attackers potentially can manipulate the system so it ceases to function entirely, leading to widespread deprivation, disorder and even defeat at the hands of a foreign power.

Recent trends in the evolution of cyber threats have led many experts to believe the danger is growing worse. First, malicious software is proliferating at such an alarming rate that new applications may outnumber legitimate software releases. Second, as these malicious programs are shared on the internet, predators are becoming more subtle and sophisticated in their efforts. Third, attacks increasingly seem to be originating from well-resourced operators such as governments rather than disaffected freelancers. And fourth, the tools for combating threats – for detecting and blocking and tracing attacks – are not keeping up with the danger.



CYBER SECURITY TERMS AND CONCEPTS (WIKIPEDIA)

Malicious software, or “malware,” is computer code designed to infect systems without the informed consent of users. Among the most common types of malicious software spread on the internet are spyware, viruses and worms. Malicious code can penetrate a computer through both network connections and plug-in devices, and once downloaded it often is difficult to detect or remove.

Spyware is malicious software surreptitiously installed on computers that monitors user behavior and potentially alters the way in which computers function. Among other things, spyware may log which web sites are visited, collect personal information, install additional software without user knowledge, redirect browser activity and even change computer settings.

Viruses are self-replicating computer programs that attach themselves to other programs and then spread among computers via network connections or plug-in devices without user awareness. Their name derives from the ease with which they can be spread, and the harmful consequences they often cause in computers on which they have been downloaded. The most destructive viruses impair key files and programs such as computer operating systems.

Worms are another kind of self-replicating program that spreads over network connections without user consent. Unlike viruses, worms do not need to attach themselves to other programs in order to spread. Beyond their ability to spread quickly, worms often carry payloads of additional code that enable them to modify infected computers, for example by deleting files or installing “backdoors” that allow remote controllers to use the computers for malicious purposes.

Botnets are networks of software robots that operate autonomously in compromised computers. Systems that have been infected in this fashion are sometimes called “zombie” computers, because they are linked together by remote controllers for malicious purposes without user awareness. A typical botnet includes thousands of compromised computers serving some common, illegitimate purpose, and botnets containing over a million infected computers have been uncovered.

Phishing is a form of online fraud in which sensitive information such as passwords and credit-card numbers are obtained by misleading users. The most common form of phishing is to send emails or instant messages directing users to web sites that elicit personal details for criminal purposes. Phishing is frequently employed by predators as part of “social engineering” strategies for exploiting the cognitive biases of online users.

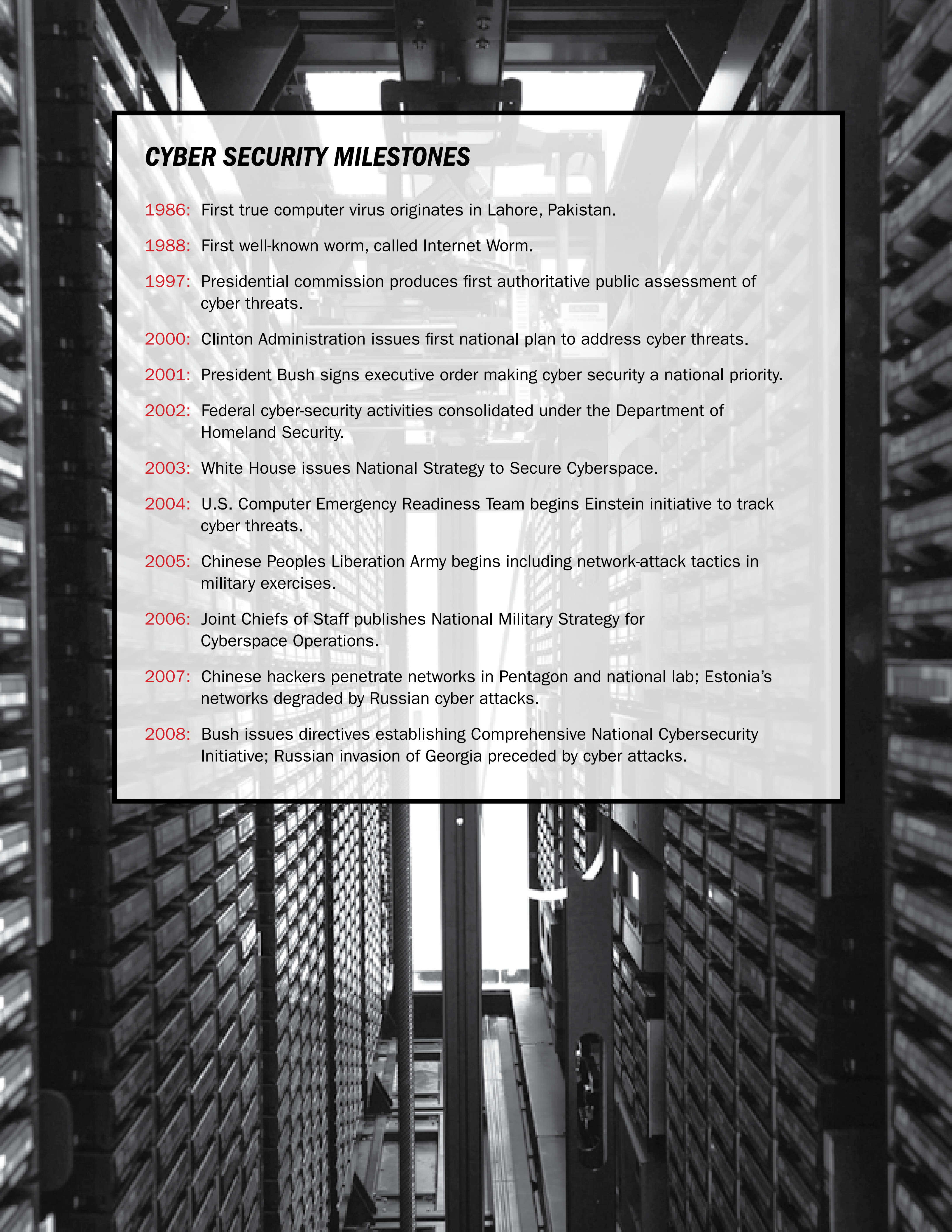
THE MILITARY DIMENSION OF DANGER

In recent years, America's armed forces and intelligence agencies have faced rapidly escalating attacks on their information networks from countries such as Russia and China, and from a vast array of less capable perpetrators. This facet of the cyber threat is largely invisible to the general public, because the government is not eager to advertise its vulnerabilities or how much it knows about who is mounting the attacks. One measure of the danger, though, is the Bush Administration's decision to launch a Comprehensive National Cybersecurity Initiative to protect government networks during its final year in office. The initiative was reported to be the biggest new item in the fiscal 2009 intelligence budget.

Military planners and intelligence analysts have long known that adversaries would seek to compromise U.S. networks in wartime. The idea of targeting key nodes in enemy networks has a long history that predates the information age, as reflected in the plan of the Army Air Forces to target electrical grids, refineries and communication nodes in World War Two. But the advent of digital networks has added a new twist to this strategy. In the past, the military was concerned mainly with "kinetic" attacks on its networks using high-explosive munitions, or gross "non-kinetic" effects such as the electromagnetic pulse generated by nuclear blasts. Today, it must also worry about more elusive dangers such as malicious software that undermines the reliability and security of vital systems.

Like civilian users, America's military has eagerly embraced the promise of internet-protocol communications, identifying myriad ways in which the new technology might enhance the survivability and effectiveness of warfighters. But as the joint force becomes increasingly net-centric, it also becomes more vulnerable to cyber threats. Cyber operatives have repeatedly penetrated Pentagon networks and other national-security sites such as the Energy Department's nuclear-weapons laboratories. Although military and intelligence networks are supposed to be isolated from the internet, it only takes one intrusion via a cell phone or laptop computer for whole organizations to be penetrated, and such attacks can be executed anonymously by predators on the other side of the world.

The greatest military danger raised by cyber threats is that America's armed forces and intelligence agencies will lose what they call "information dominance," the capacity to assure friendly information flows while impeding those of adversaries. That is a real possibility, because the battle for military supremacy now is conducted using tools available to many potential adversaries, and military organizations may lack the agility to keep up with such a diverse and fluid threat. It is hard to deter attacks when their point of origin cannot be identified, and harder still to know how compromised key networks may be until the moment when they are most needed. What can be said with certainty, though, is that virtually all of America's enemies grasp how important digital networks are to the effectiveness of the joint force.



CYBER SECURITY MILESTONES

1986: First true computer virus originates in Lahore, Pakistan.

1988: First well-known worm, called Internet Worm.

1997: Presidential commission produces first authoritative public assessment of cyber threats.

2000: Clinton Administration issues first national plan to address cyber threats.

2001: President Bush signs executive order making cyber security a national priority.

2002: Federal cyber-security activities consolidated under the Department of Homeland Security.

2003: White House issues National Strategy to Secure Cyberspace.

2004: U.S. Computer Emergency Readiness Team begins Einstein initiative to track cyber threats.

2005: Chinese Peoples Liberation Army begins including network-attack tactics in military exercises.

2006: Joint Chiefs of Staff publishes National Military Strategy for Cyberspace Operations.

2007: Chinese hackers penetrate networks in Pentagon and national lab; Estonia's networks degraded by Russian cyber attacks.

2008: Bush issues directives establishing Comprehensive National Cybersecurity Initiative; Russian invasion of Georgia preceded by cyber attacks.

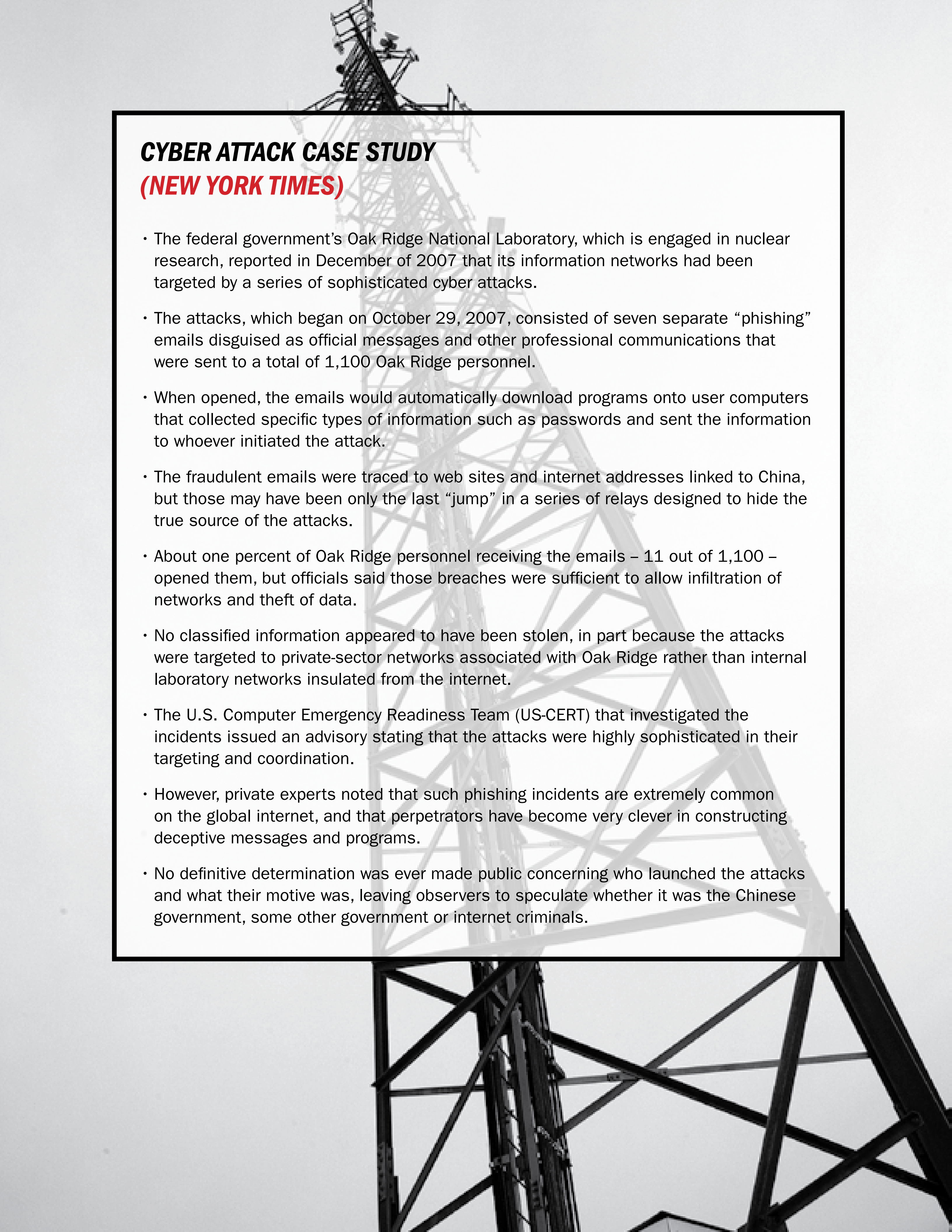
THE ECONOMIC DIMENSION OF DANGER

The information age has brought about a massive transformation of the American economy. Workers are more productive, borders are more open, relationships are more fluid and the pace of business activity is much faster. The foundation for most of these changes is a global infrastructure of information networks that has obliterated geographical, organizational and technological barriers to efficiency. Every major industry has assimilated internet-protocol communications into its operating procedures as a way of saving money and staying competitive. As a result, the entire economy is now so dependent on digital links that it could not function without them.

Because this transformation has unfolded over two decades in many different ways, most citizens do not grasp just how dependent they are on information systems. For example, if the information infrastructure were severely compromised, telecommunications and electricity grids would cease operating, food supplies would become depleted, financial transactions would be unexecutable, and air traffic control would be nearly impossible. One expert has compared the failure of the information infrastructure to the simultaneous arrival of fifty major hurricanes in terms of how disruptive it would be to the national economy.

Against this backdrop, the rapid proliferation of cyber threats and the apparent adoption by some countries of information warfare as a national strategy is very troubling. Most of the nation's economic infrastructure including the information grids is privately owned, and there are legal barriers to determining precisely how vulnerable parts of it may be. Experiments conducted by the Department of Homeland Security have demonstrated how internet predators might penetrate utilities and shut them down, but no one really knows the degree to which potential adversaries are already poised to do so. Even when it can be proven that electronic attacks on domestic networks were launched from places like China, there is no sure way of knowing where they actually originated.

The challenge of guarding networks supporting the national economy is exacerbated by the myriad ways in which digital operating systems and applications might be compromised. Malicious software is being generated and disseminated on such a vast scale that even when it is detected, there often is no immediate remedy for the problem. The internet is so ubiquitous and anonymous that there is no practical way of suppressing such software without severely impairing the functionality of the whole system, which itself could become a significant burden to the economy. Nonetheless, many experts fear that it is just a matter of time before cyber predators do serious damage to the national economy, and some contend that is already happening today.



CYBER ATTACK CASE STUDY
(NEW YORK TIMES)

- The federal government’s Oak Ridge National Laboratory, which is engaged in nuclear research, reported in December of 2007 that its information networks had been targeted by a series of sophisticated cyber attacks.
- The attacks, which began on October 29, 2007, consisted of seven separate “phishing” emails disguised as official messages and other professional communications that were sent to a total of 1,100 Oak Ridge personnel.
- When opened, the emails would automatically download programs onto user computers that collected specific types of information such as passwords and sent the information to whoever initiated the attack.
- The fraudulent emails were traced to web sites and internet addresses linked to China, but those may have been only the last “jump” in a series of relays designed to hide the true source of the attacks.
- About one percent of Oak Ridge personnel receiving the emails – 11 out of 1,100 – opened them, but officials said those breaches were sufficient to allow infiltration of networks and theft of data.
- No classified information appeared to have been stolen, in part because the attacks were targeted to private-sector networks associated with Oak Ridge rather than internal laboratory networks insulated from the internet.
- The U.S. Computer Emergency Readiness Team (US-CERT) that investigated the incidents issued an advisory stating that the attacks were highly sophisticated in their targeting and coordination.
- However, private experts noted that such phishing incidents are extremely common on the global internet, and that perpetrators have become very clever in constructing deceptive messages and programs.
- No definitive determination was ever made public concerning who launched the attacks and what their motive was, leaving observers to speculate whether it was the Chinese government, some other government or internet criminals.

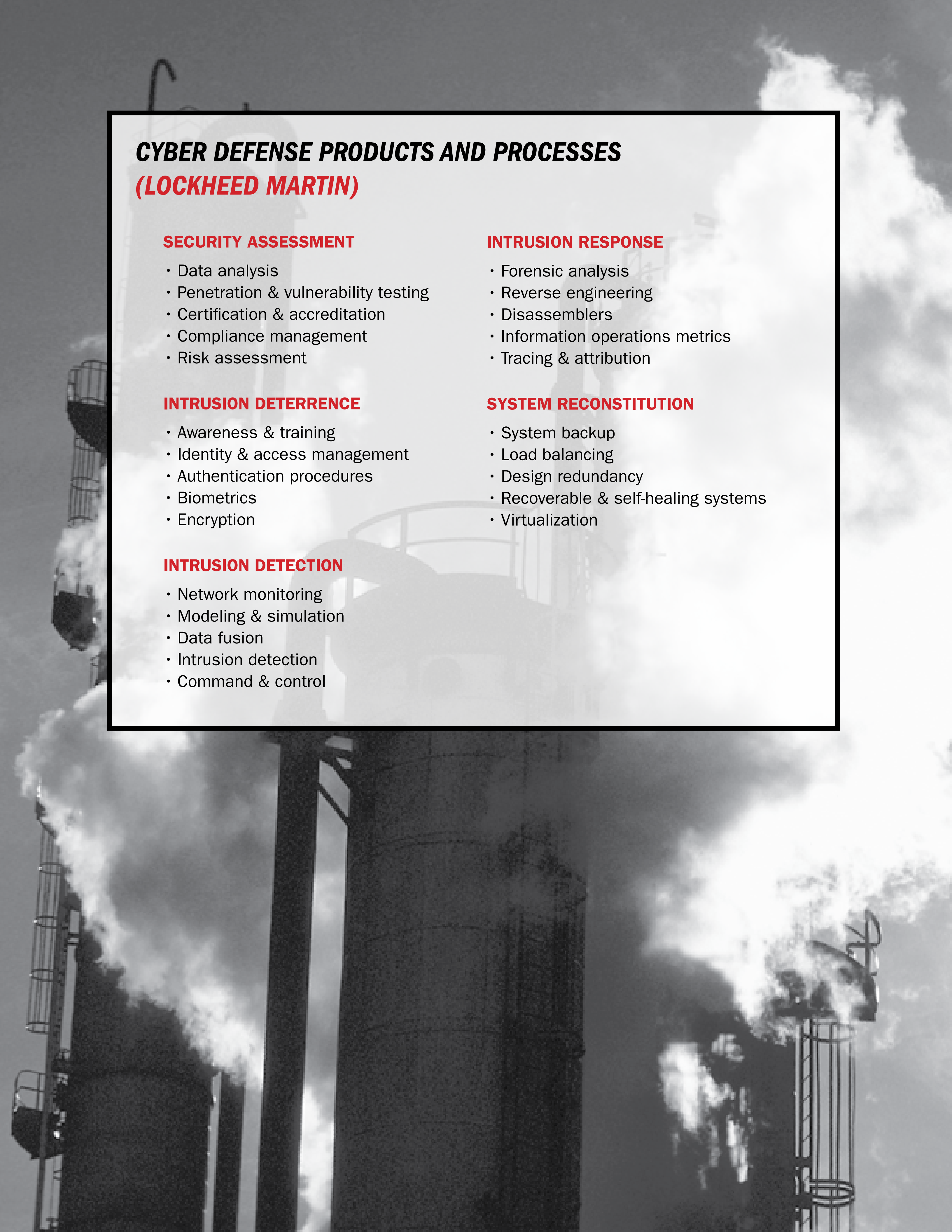
DEFENSES AGAINST CYBER ATTACK

Finding lasting solutions to the danger posed by cyber threats is an extremely complicated challenge. The threats take many forms, and are constantly evolving. The cyberspace domain in which they unfold is anarchic and anonymous, sprawling across political and geographical boundaries in a manner that defies regulation. Many of the remedies proposed to limit abuses also limit the freedom of users. However, if the federal government cannot find a workable approach to deterring and defeating cyber threats, then America may be unable to sustain its military and economic edge in the information age.

Most experts agree that a few basic principles are central to any effective defense. First, users must be aware of the danger and trained to avoid creating vulnerabilities that can be exploited by predators. Second, access to sensitive networks must be controlled by limiting points of entry, blocking or filtering traffic through those points, and instituting rigorous authentication procedures for legitimate users. Third, network software and procedures must be continuously updated to eliminate weaknesses, and tested to assure gaps have been successfully closed. Fourth, there must be a mechanism among network administrators for sharing information about threats that provides timely and useful warning of danger. Fifth, defensive measures must be sensitive to the missions of users, so that they do not impair network functionality in the process of providing protections.

The respected SANS Institute uses a six-step framework for explaining how cyber incidents should be addressed that begins with being prepared, and then proceeds through identification of danger, containment of the threat, eradication of the threat, system recovery and follow-up. Each of these steps may entail dozens of discrete actions aimed at detecting, characterizing, isolating and suppressing the danger, and then restoring the network to its beginning state. Experts typically stress the importance of being prepared before an attack occurs, and conducting post-mortems to derive useful lessons about how dangers can be minimized in the future. Military experts also emphasize the importance of developing offensive cyber capabilities as a way of deterring or countering attacks.

While the generic measures necessary to cope with cyber aggression are easy enough to identify, applying them to specific threats and mission areas can be devilishly difficult. Efforts to do so have revealed a number of chronic problems that policymakers must eventually address. First, vital national networks are so balkanized among military, civil and commercial operators that it is difficult to enforce any particular standard with regard to cyber defense. Second, the inability to trace attacks made over the internet to their point of origin severely hampers efforts to deter or punish predators. Third, network administrators seldom have the sort of enterprise-wide view of their information assets needed to fashion a durable and complete security regime. Finally, government by its nature is not well equipped to keep up with such a fluid and multifaceted challenge.



CYBER DEFENSE PRODUCTS AND PROCESSES (LOCKHEED MARTIN)

SECURITY ASSESSMENT

- Data analysis
- Penetration & vulnerability testing
- Certification & accreditation
- Compliance management
- Risk assessment

INTRUSION DETERRENCE

- Awareness & training
- Identity & access management
- Authentication procedures
- Biometrics
- Encryption

INTRUSION DETECTION

- Network monitoring
- Modeling & simulation
- Data fusion
- Intrusion detection
- Command & control

INTRUSION RESPONSE

- Forensic analysis
- Reverse engineering
- Disassemblers
- Information operations metrics
- Tracing & attribution

SYSTEM RECONSTITUTION

- System backup
- Load balancing
- Design redundancy
- Recoverable & self-healing systems
- Virtualization

FEDERAL ORGANIZATION FOR CYBER DEFENSE

The federal government acquired most of its information networks on a piecemeal basis, without much thought as to how the parts might one day fit together or how enemies might try to exploit them. The government's recent efforts to organize for cyber defense have been hampered by the fragmented character of federal information systems. This problem is compounded by the fact that many networks vital to the economy are in the private sector, and the legal authorities for implementing security measures there are incomplete at best.

Within the federal government, most of the funding allocated to information security and offensive cyber operations is spent by agencies of the Department of Defense. The biggest player is the National Security Agency (NSA) at Fort Meade, Maryland, which since the early days of the cold war has been engaged in collecting and analyzing signals intelligence. NSA appears to have lead responsibility for securing all intelligence networks, and it shares expertise with the Defense Information Systems Agency that oversees military networks. U.S. Strategic Command is the lead combatant command responsible for information operations and cyber security. In addition, each of the military departments – the Army, Navy and Air Force – has a dedicated command for managing information networks and assuring their security.

Although it receives much less money for network operations and security than the defense department, the Department of Homeland Security (DHS) is the lead federal agency for coordinating national cyber-defense initiatives. DHS maintains a National Cyberspace Response System that includes the U.S. Computer Emergency Readiness Team, or US-CERT, the best known domestic responder to cyber incidents. A National Cyber Security Center was recently established within DHS to oversee the Comprehensive National Cybersecurity Initiative begun by the Bush Administration in early 2008. That initiative, which extends over many years and entails dozens of different projects, is supposed to integrate the security efforts of both defense and civil agencies in addressing all of the government's cyber vulnerabilities.

However, as this brief description of federal organization for cyber defense demonstrates, the structure of the government does not lend itself to timely and consistent implementation of network-security measures. The threat is evolving too fast, and on too many fronts. Clearly, no single agency can address the entire cyber challenge, because it crosses all organizational and operational boundaries. Various departments or agencies may wish to lead the cyber-security effort, but they lack the authority to direct actions by organizations outside their budget or chain of command. Only the White House has the power to lead such a multifaceted undertaking, and the National Security Council is the logical mechanism within the White House. Without White House leadership, bipartisan support and public awareness, it is unlikely that America can defeat the danger to its vital information networks.

CYBER INSIGHTS

In the last century, geographic isolation helped protect the United States from a direct physical invasion. In cyberspace national boundaries have little meaning. Information flows continuously and seamlessly across political, ethnic, and religious divides. Even the infrastructure that makes up cyberspace – software and hardware – is global in its design and development. Because of the global nature of cyberspace, the vulnerabilities that exist are open to the world and available to anyone, anywhere, with sufficient capability to exploit them.

National Strategy to Secure Cyberspace, 2003

Our information infrastructure – including the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries – increasingly is being targeted for exploitation and potentially for disruption or destruction, by a growing array of state and non-state adversaries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year.

Director of National Intelligence Adm. Michael McConnell, 2008

We need to prevent terrorists or spies from hacking into our national security networks.
We need to build the capacity to identify, isolate and respond to any cyber attack.
And we need to develop new standards for the cyber security that protects our most important infrastructure – from electrical grids to sewage systems, from air traffic control to our markets.

President-Elect Barack Obama, 2008

ISSUES FOR THE NEW ADMINISTRATION

In 2008, the Bush Administration began a Comprehensive National Cybersecurity Initiative that will eventually spend over $10 billion strengthening defenses of government networks. During that year's presidential campaign, Senator McCain noted the growing military role of information operations, while Senator Obama stated that the government needed to build "the capacity to identify, isolate and respond to any cyber attack." It appears that national leaders grasp the importance of network security and information assurance. But seeing the problem isn't the same thing as solving it. Before that can occur, there are eight basic questions the new administration needs to answer.

1. Do current trends in cyber threats indicate the nation faces a real crisis of confidence in its networks, or are efforts like the comprehensive cyber-security initiative sufficient to deal with the challenge?

2. Given how important global connectivity is to information superiority, is it possible to secure essential networks while still maintaining links to the anarchic and anonymous internet?

3. Will the internet in its current form ever permit users to trace sophisticated attacks to their source, so that abuses can be effectively deterred and/or defeated?

4. What legal authorities are required so that the government can overcome barriers to dealing with attacks on critical private-sector networks, and establish consistent security standards?

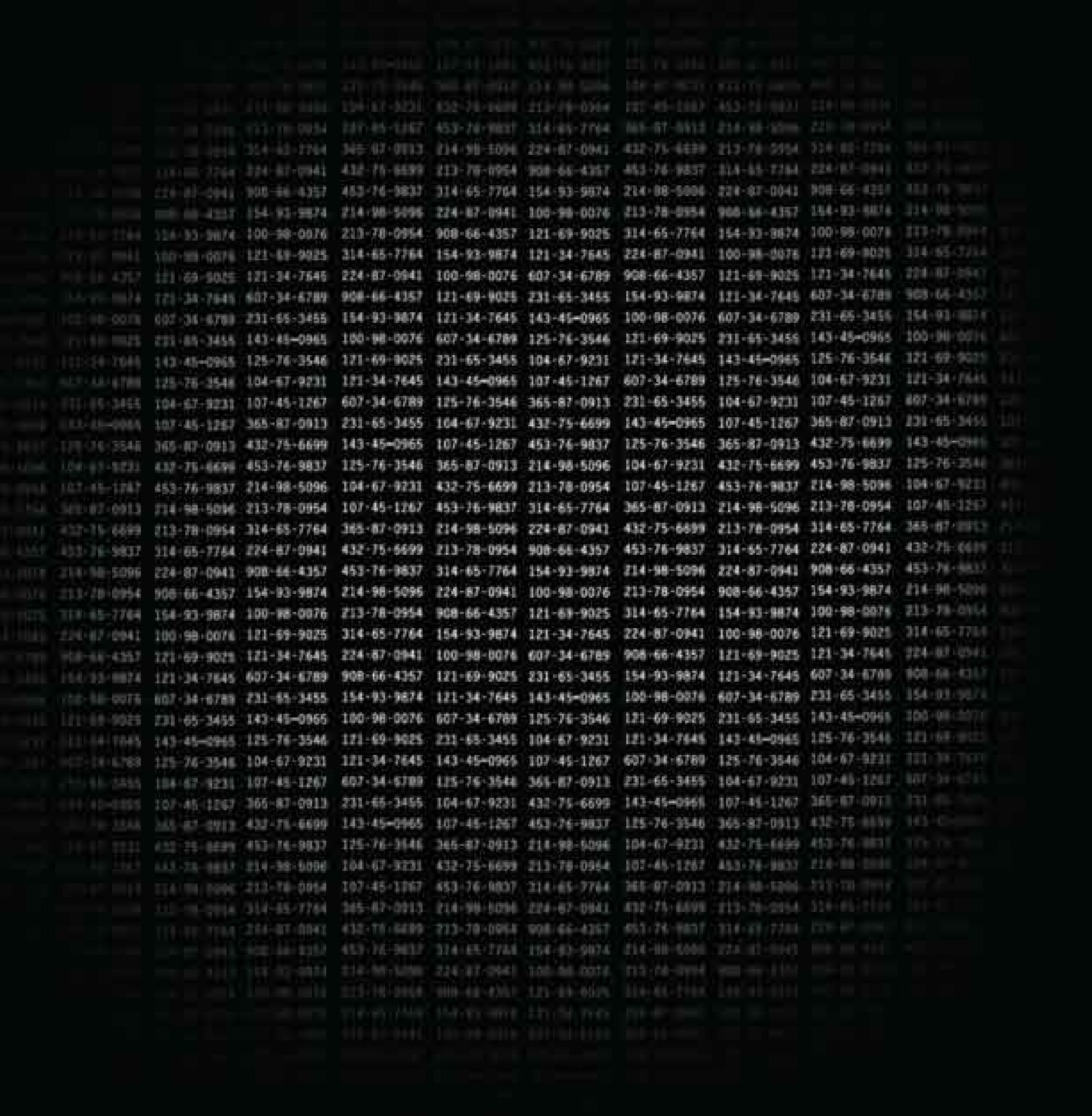
5. What is the proper relationship within the government between network defense and offensive information operations in formulating an integrated cyber-security posture?

6. How can the government encourage a holistic, enterprise-wide understanding of its network resources and challenges, so that solutions are developed in a truly comprehensive rather than piecemeal fashion?

7. Is the Department of Homeland Security an appropriate vehicle for managing government-wide cyber-security efforts, or is a more focused organization better suited to the task?

8. If the government is too slow or decentralized to keep up with the rapid proliferation of cyber threats, how can it tap more agile suppliers of network security in the marketplace?

These questions need to be answered before the nation suffers the digital equivalent of a 9-11 attack that so many experts have been predicting. Despite the growing array of problems associated with using and securing internet-style networks, virtually nobody in the government thinks it is desirable to return to a pre-internet way of doing business. So the real issue policymakers face in meeting the cyber-security challenge isn't whether they can live without digital networks, but how they prevent America's enemies from using those networks against us.



Lexington Institute

1600 Wilson Boulevard • Suite 900 • Arlington, Virginia 22209
tel 703.522.5828 • fax 703.522.5837
www.lexingtoninstitute.org • mail@lexingtoninstitute.org