

THE 9/10/11 PROJECT



CYBER
SECURITY

Are We Ready for the Day Before Tomorrow?

Imagine it is September 10, 2011 – 9/10/11 – a full decade since the devastating terrorist attacks of September 11, 2001. Is our nation equipped for whatever catastrophe may happen tomorrow? How have our prevention, preparedness, response and resiliency structures changed, matured and become operational?

The Homeland Security & Defense Business Council's 9/10/11 Project looks at how far the country has come since the day before 9/11/2001. Through fresh interviews with industry leaders the Council is seeking to vividly illustrate the strides our government at all levels, working with the private sector, has made to secure the country and to stay at least one step ahead of events and disasters that could destroy our way of life.

On the 10th of each month between now and through September 2011, the Council will provide a historical context for how far we have come and where we are now, as well as an assessment of the future of the most pressing homeland security issues. Each monograph will include a running timeline (interactive on our website) illustrating the events, incidents, and critical government responses pertinent to that month's topic. This month's monograph focuses on Cyber Security.

It was an absolutely gorgeous Saturday afternoon and the Jones family was at play. During the past 10 years, the family has joined the inter-connected Internet world, embracing all of the technological advances – and vulnerabilities – it has to offer. And so have the hackers.

The Jones' all have smartphones. Suzy, now 13, lives on hers, and has more than 800 Facebook friends she can talk to via her phone's Internet connection. Jim, now 17 and looking to go to college next year, also hangs out online a lot, either chatting with his friends or playing interactive video games with online buddies he finds through his PlayStation 3. Dad and Mom, too, are attached at the hip to their phones, which double as offices when they aren't at work. Sometimes, mom jokes that she doesn't really even need to go online via her "old" computer anymore – her phone brings her the Internet, a GPS locator, a notepad for grocery lists, a navigation map, an iPod, and her office email; dad's phone does the same and more for him, he has an app that can program TV shows, look at a "webcam" to check his home and property; and get real time game scores. The family is completely connected. Yes, they'd heard countless stories about identity theft, and credit card theft – their bank even calls them now if there was an unusual withdrawal and they have learned to contact their credit card company to alert them in advance of a trip out of town – but so far, they've escaped. Even so, if they looked closer and thought a bit more, they'd see that the Internet had taken over their world, because not only were the Jones' completely connected, so were factories, utilities, nuclear facilities, and financial institutions – virtually all our country's critical infrastructure.

On this particular September day, when Jim visited Twitter, a tiny piece of software was downloaded into his computer. He never knew anything had happened; he received no alerts from his antivirus or firewall software. Sure, a few days later his computer seemed sluggish, but that was all.



1979

Engineers at Xerox Palo Alto created the first computer worm

1984

OCTOBER 1984

The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 enacted



1986

OCTOBER 1986

The IETF held its 4th meeting. It was the first meeting that non-government stakeholders attended

1979

The Internet Engineering Task Force (IETF), the principal organization involved in the development of new Internet standard specifications, held its first meeting

JANUARY 1986

Programmers in Pakistan released "The Brain," one of the first PC viruses ever created

SPONSORED BY

GENERAL DYNAMICS
Information Technology



Delivering Trusted Cyber Solutions

General Dynamics delivers proven cyber solutions that increase situational awareness, reduce vulnerabilities and prevent network attacks.

- **Defend:** Delivering proven and comprehensive cyber defense in-depth products and services to actively defend enterprise networks, weapon systems and platforms.
- **Exploit:** Fusing deep domain knowledge and mission understanding to provide the most cost-effective and timely exploitation and analysis solutions across the life cycle.
- **Integrate:** Integrating cyber information assurance into enterprise and network systems to delivery modernized, cross-domain, secure mission-critical cyber systems.
- **NetWar:** Providing proven, timely and secure end-to-end mission systems and solutions to dominate against adversaries in network warfare.



What is happening to Jim's computer happens to millions of innocent computers every day. It is the opening volley in what could amount to an attack on Jim and his personal information, or worse, it could be the first shot in a targeted cyber war. Since the advent of PCs and the subsequent invention of the Internet, networks and interconnectedness have resulted in great advances and great vulnerability. These threats range from someone emptying your bank account to hijacking your PC and inflicting harm unbeknownst to you. Though work has been done, we are still not ready for tomorrow – because the cyber battle has already begun....and we are playing catch up.

Initial Steps – Government & Industry's Response

The first signs of the vulnerabilities posed by an increasingly networked world were recognized by President Clinton, who realized that information and communications, along with banking and finance, our water supply, transportation, emergency law enforcement, emergency fire service, emergency medicine, electric power, oil, and the gas supply and its distribution, law enforcement and internal security, intelligence, foreign affairs, and national defense were *all* increasingly being tied together via computers and computer networks. While this inter-connectedness brought huge innovation, instantaneous communications, and much greater efficiencies, it was also making the increased number of users, as well as our entire nation extraordinarily vulnerable to cyber-attacks. The publicity and widespread concern surrounding the Y2K bug further highlighted the extensive damage that disruption of computer networks could inflict, but also set the stage for greater awareness evolving into increased preparedness. Recognizing the country's increasing dependence on digital communications, President Clinton issued Presidential Decision Directive No. 63 (PDD 63), designed to develop and implement plans to protect the networks and data of our critical infrastructure and create mechanisms to share intrusion data and attack trends in the private sector through Information Sharing and Analysis Centers (ISACs).

The federal government also recognized that this interconnectedness made its systems vulnerable. In 2002 the Federal Information Security Management Act (FISMA) was implemented and required agencies to create cyber security plans, perform risk analysis of IT systems, and submit their plans for accreditation. Industries were circling around Information

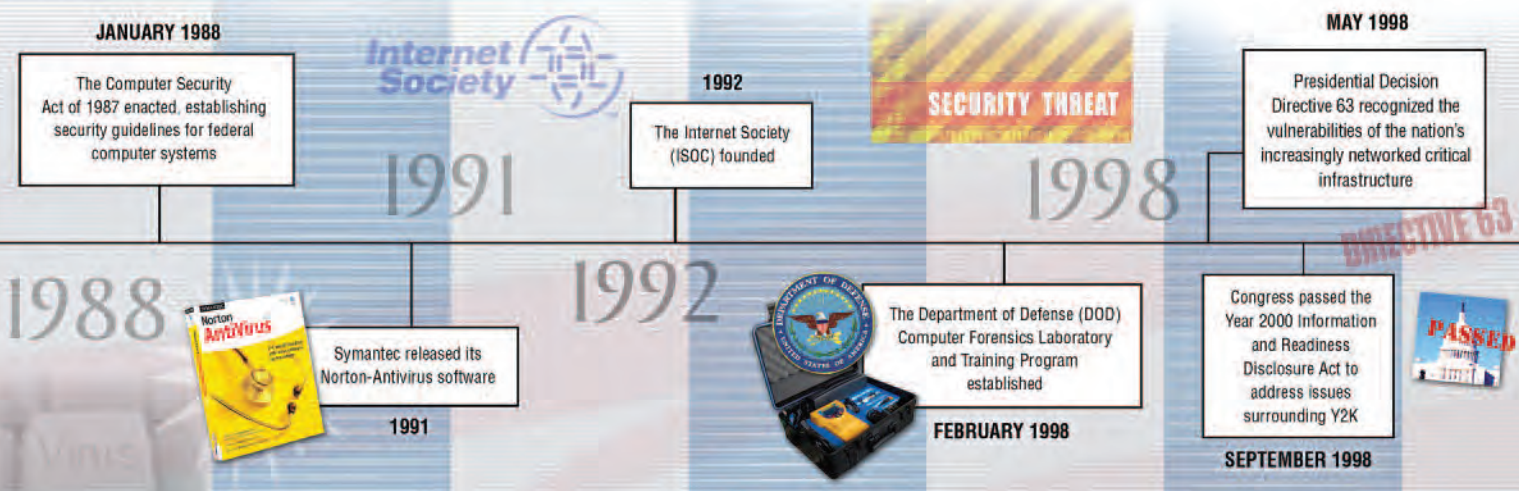
Sharing and Analysis Centers, created by PDD 63 and renewed after 9/11 by Homeland Security Presidential Directive 7 to share attack and intrusion data in each of our critical infrastructure. Internet security companies like Norton and McAfee were developing solutions for personal PCs.

Yet there remained a nagging question – Who was going to be in charge of securing the Internet and how could it be done effectively?

The Department of Defense responded to the growing threat by creating two commands responsible for defensive and offensive operations, respectively: Joint Task Force – Computer Network Defense in 1998 and Joint Functional Component Command – Network Warfare in 2005. The Defense Information Security Agency (DISA) assumed responsibility for protecting the military's telecommunications and information systems. The Air Force announced plans to create a Cyber Command in 2006 to handle cyber warfare and network defense; the provisional command became operational in late 2008. Recognizing the need for a coordinated Department of Defense response to cyber threats, in June 2009, Secretary of Defense Robert Gates laid the groundwork for the creation of an overall Cyber Command. U.S. Cyber Command, operating under U.S. Strategic Command and integrating existing cyber units, began operation in May 2010.

At the federal level, the Department of Homeland Security (DHS) consolidated several offices associated with cyber defense in 2003 by creating the National Cyber Security Division (NCSD) tasked with protecting the government's computer systems from Internet-based attacks. In 2009, President Obama announced the creation of a Cyber-security Coordinator under the National Security Council and the National Economic Council responsible for implementing cyber-security policies and facilitating inter-agency development of strategy and policy. In 2010, the White House gave DHS primary responsibility in overseeing FISMA compliance throughout the government to address one of the major criticisms of the DHS' cyber response – a lack of clear authority within the government.

Our defenses in this battle, however, do not lend themselves to easy analysis, to information sharing, or even to finding a defensive solution, because once a virus is found, it is extremely hard to trace its origins, usually disappears immediately, and the damage is already done. Because entities—both private and governmental—have experienced increasingly numerous and serious cyber disruptions, and because we all utilize the same fiber-optic cables, system routers and servers, many are finally starting to



feel intense urgency as they better comprehend the significance of cyber events that literally happen every day. But everything moves slowly against lightning-fast attacks.

Fighting Cyber War

Estonia learned this firsthand when a political dispute over a giant bronze statue of Tallinn caused riots and the first cyber-attack that shut down a nation state. Servers that Estonians relied upon to do online banking, read newspapers or utilize their government's online services were pinged so much that they crashed and shut down. The botnets sent for the onslaught attacked servers running parts of the telephone network, the credit-card verification system and the Internet directory; more than a million computers were involved in that one attack alone.

When a computer user unwittingly downloads malignant code, it could be the beginning of a distributed denial of service attack ("DDOS"). Put simply, a DDOS is a preprogrammed flood of Internet traffic that is designed to crash or jam networks rendering them useless. The attacking computer is called a "botnet," which becomes part of a robotic army of "zombies," that are under remote control. Once that tiny, manipulative piece of software is in a computer, it can lie dormant for a long time as it waits for its orders. If it was only meant to spread infection, and other computers get it, a "worm," is formed.

Estonia isn't the only country that's been hit, nor was that event isolated to Russian hackers using other countries' routers and servers. Our government's computers, as well as defense contractors and many other companies, have been hacked *hundreds of millions* of times. In 2008, for example, the Pentagon acknowledged at a closed House Intelligence Committee meeting that its vast computer network was being scanned or attacked by outsiders more than 300 million times each day.

Thus, the more "connected" we are, the more that inter-connectivity spreads vulnerability. It doesn't matter if you are the Jones family, the head of Interpol or the Department of Defense.

Even given our heightened sense of vigilance, preparedness and awareness, sophisticated bad guys are still producing increasingly complex new cyber worms every day. In the summer of 2010 it was discovered that a

worm, called Stuxnet, was created specifically to target Siemens' PLC (programmable logic controller) programs that are used to manage large-scale industrial systems on factory floors, in military installations and chemical and power plants. Researchers at Symantec were able to crack its cryptographic system, and said it was the first worm built not only to spy on industrial systems, but also to *reprogram* them. According to an article in the September 10, 2010 issue of *TechWorld*, the software operated in two stages following infection. First it uploaded configuration information about the hijacked system to a command-and-control server. Then the attackers, perhaps sitting at a bar in Paris, were able to pick a target and actually reprogram the way it works.

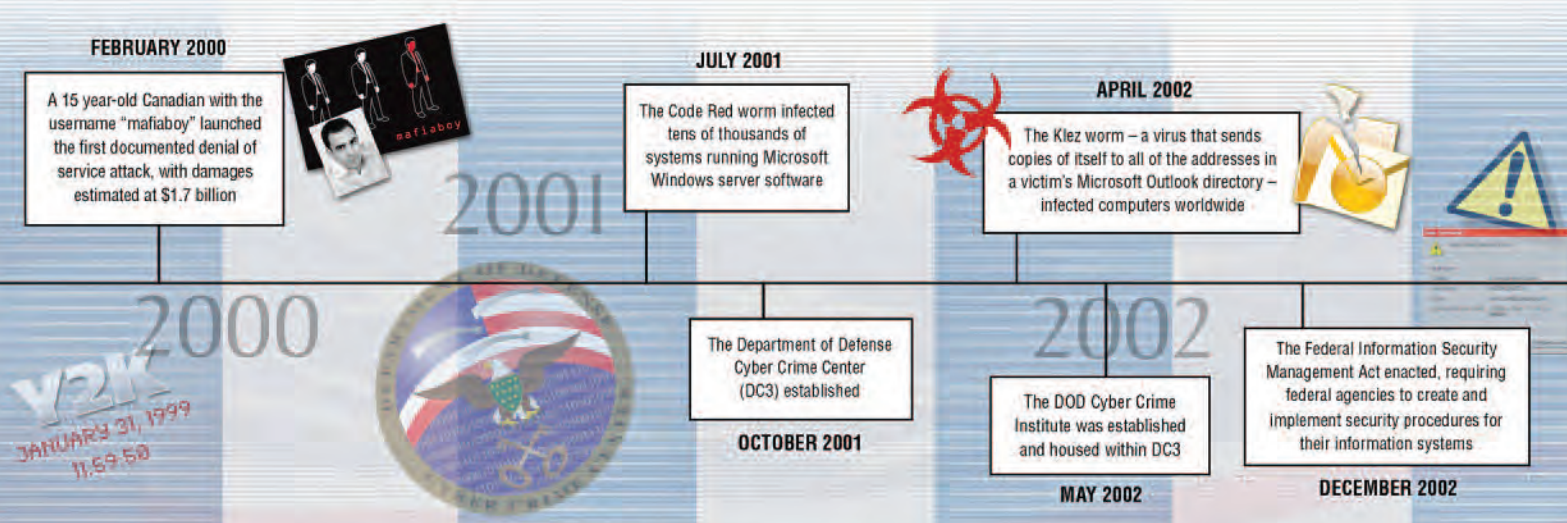
Hackers decide how they want the programs to work for them, and then they send code to the infected machines that will change how they work. By mid-September, the worm had attacked nuclear equipment primarily in Iran, but who knows what the day after tomorrow will bring?

U.S. defense contractors and companies with valuable intellectual property have been hit with targeted attacks for many years. They have recruited their own dedicated group of *cyber warriors* who are tasked to fight back. The Stuxnet worm, however, marked the first time the factory floor itself was targeted and because it can control the way physical machines work, the fear is that it (or a progeny) could be used to target our most essential technologies: electricity, nuclear power, oil and gas, etc.

Even scarier is the fact that, according to numerous experts, 'logic bombs' (inserted code that is triggered remotely or timed to go off) have already been placed in our electric grid. At a recent meeting held by the SANS Institute and *GovExec Magazine*, the security of the DoD's cyber system was questioned, because it runs on the same open Internet and over the same (perhaps counterfeit) routers that everyone else uses, including our enemies. While it is not easy to infect a fiber optic cable, it is not impossible.

Networked at War

The same mechanisms used to attack PCs and domestic infrastructure, plagues our warfighters as well. A hardened laptop and a computer transponder bring virtual command-and-control abilities right to the field of battle. This may be a devastating Achilles heel if technology cannot provide secure networking.





A number of companies, including Telos, General Dynamics, Northrop Grumman, Raytheon, and Lockheed Martin among others, are trying to ensure that our warfighters have secure networks. Telos, for example, has delivered more than 30,000 Combat Service Support Automated Information System Interface (CAISI) modules to the Army that create a mesh network using government secure wireless standards. The companies continually develop new technologies for the military that search for viruses and provide basic firewall protections.

The military can't afford to do anything less. There have been a number of reported breaches of military systems including those used by the Central Command in overseeing combat zones in Iraq and Afghanistan. These incidents have "...served as an important wake-up call...[marking] a turning point in U.S. cyber-defense strategy," said Deputy Secretary of Defense William J. Lynn III in the September/October 2010 issue of *Foreign Affairs*.

Yet, "The best-laid plans for defending military networks will matter little if civilian infrastructure—which could be directly targeted in a military conflict or held hostage and used as a bargaining chip against the U.S. government—is not secure," Lynn said. "The Defense Department depends on the overall information technology infrastructure of the United States...The Pentagon is therefore working with the Department of Homeland Security and the private sector to look for innovative ways to use the military's cyber-defense capabilities to protect the defense industry."

Policy and Privacy

Although government policy makers have made numerous attempts to "fix cyber," many issues still plague efforts to secure our systems. One revolves around privacy concerns and ultimately to institutional trust, which goes straight to a point David Abel, vice president of IBM Global Business Services, makes: "How does the government only use pieces [of data] tied to a potential threat, when and if it should start looking at the innards of our personal computers?"

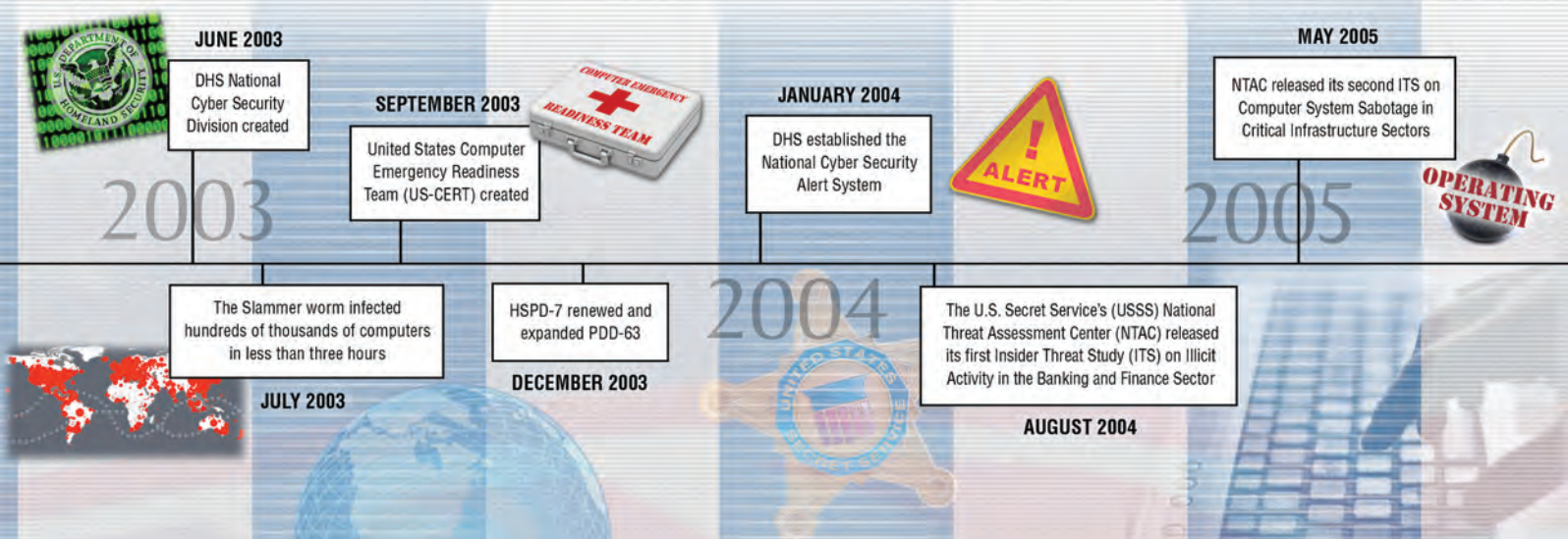
Abel says that "If you're an analyst, you can never ask enough questions to find out what is in the data. You need the data to show you the patterns and anomalies that are occurring every day." But, he asks, "How can that be done in a manner that is sensitive to civil liberties and personal privacy?" This is a vital question.

If you use a computer and the Internet in any way, you are already sharing a lot of information, so to think that anyone has privacy is ridiculous. You could, like our 17-year-old friend Jim, already be part of a botnet; your computers lying dormant waiting for a signal to spring into action. Even the head of Interpol, Secretary General Ronald K. Noble, recently had his identity stolen on Facebook when impersonators created two fake accounts in his name and used them to find details on dangerous criminals.

Anne Petera, director of homeland security programs for Lockheed Martin Corporation says "I don't think people even realize how much they give up, just by using, say, a customer key tag, using a public wi-fi network or just giving a store your zip code. Those stores know where you live, what you buy and how often. Every little piece of information we give makes us a little more vulnerable."

She suggests that people think about why the population is resisting the idea of *true* cyber security, because, as she says, "we don't protect our own privacy nearly as well as we demand the government do before they protect cyber space. If there is some huge denial of service attack tomorrow, and suddenly all the electronic funds transfer systems are rendered useless so you can't clear checks overnight, or swipe your debit cards, buy groceries or even pick up your dry cleaning, the country would come to a standstill and the panic would be enormous." Too true. Electric generators, by the way, are sometimes as big as a house and are usually one-offs, which prevents utilities from being able to fix the grid quickly. Imagine six months without power, and then think about privacy issues, especially if you belong to any sort of Internet social network.

Petera and many other experts interviewed for this monograph agree that an acceptable level of government monitoring, with the expressed purpose of protecting cyber space to keep our commerce flowing, is crucial. "At some level we have to trust that government will monitor only with an eye towards protecting cyber space and electronic commerce, and not misuse the information," she says, while acknowledging that simply because there are humans involved, there is still risk. Regardless, the question comes down to this: What we are willing to give up so we can continue to do our business transactions in the manner to which we have become accustomed?



The ultimate solution has to be developed jointly between the government and the private sector. As Petera says, "Everyone who will benefit from a less risky cyber space environment needs to have some skin in the game – every step toward a more networked, advanced world comes with significant vulnerabilities and we are all responsible to mitigate them."

Are we any closer to understanding who's responsible for our cyber security?

As it stands right now, the Department of Homeland Security is responsible for protecting dot-gov (.gov) and dot-com (.com) addresses; U.S. Cyber Command is responsible for dot-mil (.mil) sites. "It hasn't been determined which agency will protect the actual intelligence community," says Steven Bucci, a well-known cyber security expert from IBM, but he feels it will likely be the Department of Defense.

Congress also seems desirous of passing what they call "comprehensive cyber security" legislation. Bills in both the House of Representatives and Senate are being looked at more seriously. The goal is to modernize the government's ability to safeguard the nation's cyber networks from attack. The Act affords the president, in coordination with the private sector, the power to authorize emergency measures if a cyber-vulnerability is being exploited or is about to be exploited. It's doubtful that the president will have the time to "... notify Congress in advance about the threat," but that is the goal. Some argue that that may be a mistake. Patricia Titus, vice president and global chief information security manager for Unisys says that "The president needs to be able to lower the boom, and stop business on this or that IP, and shut it down." She adds that "he has the power under the War Powers Act, which is still valid, but since our critical infrastructure rests on the dot-com world, it belongs to DHS to protect."

Whatever "comprehensive" legislation may come out of Congress the consensus viewpoint is that the government cannot and should not reflexively lock down the flow of commerce and think that this is the best possible way of addressing the cyber security issue. Nor can the private sector just shrug its shoulders and say "well, that is just the way it is." The government must lead, not dictate from a closed-minded position of isolation, and industry must offer alternatives that are affordable and workable. If there is a lack of transparency and openness, the overarching problems will go unsolved.

Workforce Warriors

The House companion version of the Senate bill, H.R. 4061 indicates recognition of another vexing problem in the cyber security battle. The desperate need for cyber expertise. It reauthorizes cyber security workforce and traineeship programs at the National Science Foundation including the Scholarship for Service Program, the Integrative Graduate Education and Research Traineeship program and the Graduate Research Fellowship program.

The importance of personnel in cyber security cannot be overstated. If our people are poorly trained, or unaware of the possible effects of their actions, our nation is infinitely more vulnerable. Actions (or inaction) by individuals – be them simple mistakes or malicious acts – account for the vast majority of cyber breaches. We can develop and deploy the best technological cyber security systems available, but if we fail to recognize that a worker is behaving in a peculiar or inappropriate manner, a competitor or enemy can penetrate the system.

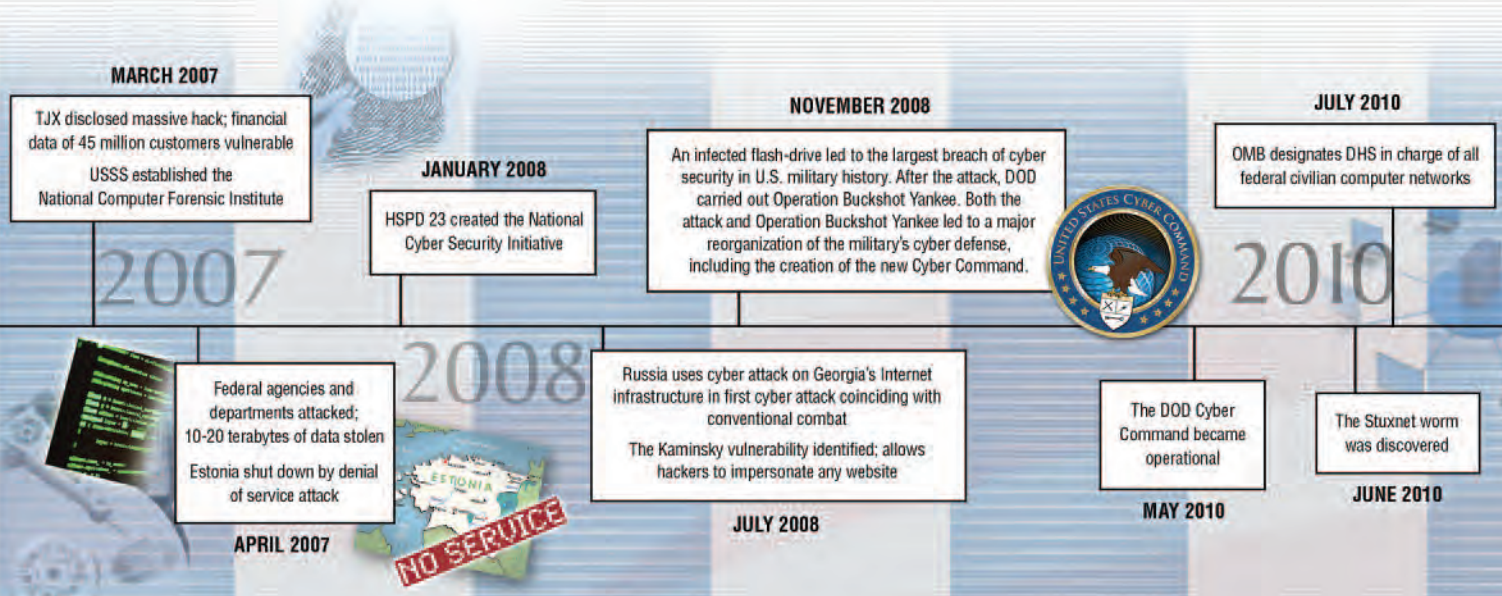
Ongoing Attacks

From DHS' perspective, it has worked diligently on its intrusion-detection system, Einstein, which is a group of DHS-created digital sensors that detect malicious activity in federal computer networks and tries to develop more information that displays patterns and gives actionable data to deal with attacks that have been repeated.

But in an August 2010 article in *Congressional Quarterly*, it was revealed that the DHS' own office in charge of building a federal cyber security response capability missed 1,085 security holes in its Virginia computers, 202 of which were deemed high-risk. The issues existed within systems the U.S. Computer Emergency Readiness Team, (U.S.-CERT), uses for email service and to access data gathered by Einstein. The programs were missing timely patches for Microsoft applications, Adobe Acrobat and Sun Java; operating systems affected included Windows and Redhat Linux.

Sounds easy enough to repair, but the real problem is that many government systems use legacy equipment and patches for PCs might interfere with their operation, so a universal patch is not going to work; all updating must be done manually.

The good news was that the audit found no vulnerabilities in the Einstein sys-



tem of two other U.S.-CERT cyber-security programs. The Einstein program also has proper security agreements in place with participating agencies, and NCSA has implemented adequate physical security — including “smart card” access and fingerprint scanners — at its cyber security offices, including the Virginia computer facility. DHS will eventually move to Einstein III, going from an intrusion-detection system to a full-on intrusion-prevention system, but of course, that will take time, and we simply do not have it.

Next Moves

On September 22, 2010 General Keith B. Alexander, who heads the U.S. Cyber Command and directs the NSA, testified before the House Armed Services Committee, and discussed the idea of creating a “secure” network for government computer systems and those of critical industries, such as power and water. The strategy of walling off critical computer networks from the rest of the Internet has been discussed for a while now, and although it may sound simple, nothing is easy in cyber world.

Creating a virtual moat would be expensive and difficult, if only because of the problems inherent with interconnecting a myriad of different companies and industries, including the government, to all the neighboring utilities necessary. With the “smart grid” every home-owner might have to be included, too. At least Alexander realizes that whatever initiative moves forward, private-sector companies will have to be involved. They do, after all, own and protect about 90% of our country’s critical infrastructure. As Alexander said, “If we’re going to defend networks that are owned and operated in part by industry, the solution can’t be a government-only solution,” he said. “It has to be joint. How do you do that? That’s the key issue.” He added, “There is a real probability that in the future this country will get hit with a destructive attack, and we need to be ready for it.”

If a worm or an army of zombie computers operated by a nation state or a well-financed group of terrorists can literally take down a building-sized generator and hobble our electric grid, or, if a person’s identity can be stolen along with their personal information and money, why haven’t we secured our networks more vigilantly?

There are many answers, and one is actually fairly simple and understandable. While these attacks are potentially catastrophic, they simply haven’t gotten the emotional response needed to incentivize people—yet. “If you have a data breach, and even though it’s possibly more harmful, and has latent threats, it’s not so emotional, and so you don’t get a reaction,” says Scott Price, vice president and general manager for General Dynamics IT. “You can’t get people motivated without that emotional response. It’s the same reason people don’t turn on their firewalls until they’ve had an intrusion.”

Technology isn’t the only answer – but it’s an important part. Addressing these problems will require a mix of some newer technologies, such as data loss prevention and computer forensics, as well as a stronger emphasis on the use of some mature security tools that have new relevancy, such as strong authentication for email and identity validation, encryption, intrusion detection and prevention systems and vulnerability assessment.

Beyond technology, we must, in clear and concise detail, define who is in charge of national cyber assurance and what their specific authorities, roles, and responsibilities are inside and outside the government. We must also create an effective public/private partnership with a twofold purpose. First, ensure that industries receive timely information that will enable them to react to attacks. Secondly, provide industry with protection when it reveals proprietary and sensitive information to government and competitors about attacks, penetrations and their infrastructure. Finally, the government must aggressively take on the role of educator, standard setter, compliance auditor, and law enforcer.

Today the world faces a wide array of cyber threats. The majority of these threats are aimed at the Western democracies, and the commercial entities that power them. These countries and businesses are highly dependent, almost completely in some cases, on cyber means for every significant societal interaction. They seek the speed, accuracy, efficiency, and ease that a “wired” system of systems brings, and all its benefits.

The danger we face is that there are many individuals, groups, and states that desire to exploit those same systems for their own purposes. Our collective and individual intellectual property and infrastructure are at risk, every day.

As we move further away from 9/11, we tend to forget that there are real threats out there. In the cyber realm, it is more than terrorism. The ubiquitous nature of cyber, the fact that it touches all sectors of commercial, social, and security environments, makes it critical that our nation – at all levels: individual citizens, communities, businesses, and government – stay vigilant and prepared for the day after tomorrow.

The Homeland Security & Defense Business Council (HSDBC) works to ensure that the perspective, innovation, expertise and capabilities of the private sector are recognized, respected and integrated with the public sector. The 9/10/11 Project has called upon critical thought leaders and subject matter experts, including our chief writer, Vicki Contavespi. For more information on the Council’s 9/10/11 Project visit: www.homelandcouncil.org/91011-Project.html

For a more complete timeline, visit the Council’s website

For more information on the Homeland Security & Defense Business Council visit: www.homelandcouncil.org

Homeland Security & Defense Business Council • 1140 Connecticut Avenue Suite 1008 • Washington, D.C. 20036 • (202) 470-6440

Marc A. Pearl, *President/CEO* • Kristina Tanasichuk, *Vice President & Project Director*



Bringing Together Mission Experience and Domain Expertise

General Dynamics works in partnership with customers to solve their top priorities. We bring original thinking to their most pressing challenges and combine innovation, resourcefulness and intellect to deliver the right solution.

Based on our experience, we are uniquely qualified to deliver proven cyber solutions.

- Prime contractor for US-CERT since its launch in 2003
- Prime contractor for the DHS OneNet Security Operations Center
- Directly servicing the IT needs of DHS at 300 sites nationwide
- Running over 22 security operations centers and incident response teams across government and industry
- Provider of 85% of NSA-approved security solutions to the federal government
- Large employee base with clearances and cross-clearances giving us the unique ability to address challenges with an interdisciplinary team
- ITIL-based managed services tightly integrates cyber security services within overall enterprise support model

Our solutions include:

- Security Operations and Services
- Intelligence and Analysis Support
- Information Assurance Products and Services
- Computer and Digital Forensics
- Cyber Incident Response
- Information Operations and Computer Network Exploitation
- Systems Engineering Development and Integration