CHAPTER 20

Cyber Security Countermeasures to Combat Cyber Terrorism

Lachlan MacKinnon, Liz Bacon, Diane Gan, Georgios Loukas, David Chadwick, Dimitrios Frangiskatos

INTRODUCTION

Any piece of work that seeks to discuss cyber terrorism must necessarily start with some definitions and descriptions to aid the reader to both differentiate and contextualize cyber terrorism from other areas of cyber security, such as cybercrime, malicious hacking, cyber fraud, and the numerous different types of system breaches, failures, and human error.

Most contemporary definitions of cyber terrorism focus on the following three aspects:

1. The motivation of the perpetrator(s)
2. The targeted cyber system
3. The impact on an identified population.

For example, the Federal Bureau of Investigation (FBI) definition (Pollitt, 2003) describes cyber terrorism as:

- Politically motivated subnational groups or clandestine agents
- Breaches in information, computer systems, computer programs, and data
- Violence against noncombatant targets

The National Infrastructure Protection Center (Garrison and Grand, 2001) defines cyber terrorism the following ways:

- As a criminal act seeking to influence a government or population to conform to a particular political, social, or ideological agenda
- To be by the use of computers and telecommunications capabilities
- To be violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population.

Denning (2000) defines cyber terrorism as:

- As an unlawful activity to intimidate or coerce a government or its people for a political or social objective
- As attacks and threats of attacks against computers, networks, and the information stored therein
- As an attack that results in violence against persons or property, or at least causes enough harm to generate fear

In a real sense, therefore, we can make the argument that the key issue in cyber terrorism is the motivation to carry out an activity in cyberspace that results in violence/harm or damage to individuals and/or their property. If considered in these terms, it becomes clear that a number of existing activities in cyberspace, which result in harm to individuals and/or their property, might be constituted as cyber terrorism simply on the basis of establishing the motivation for the activity. This leads us into a current debate as to whether cyber terrorism actually exists or is simply another manifestation of existing malicious and criminal activity in cyberspace. A number of commentators have sought to make the argument that there is neither evidence nor rationale to argue that cyber terrorism exists independent of existing cyber activities (Conway, 2011). However, we would support the view put forward by a number of other authors that there is sufficient evidence, highlighted in particular by events such as Stuxnet and others described later in this chapter, to justify a consideration of cyber terrorism as a separate entity within this space (Greengard, 2010). On the basis of this argument, we would also argue that existing tools, techniques, and approaches adopted by perpetrators of malicious and criminal cyberspace activities can and should relevantly be considered within cyber terrorism. Fundamentally, if the motivation behind any kind of cyber event fulfills the criteria of seeking to promote or impose political agenda or will upon a given population identified by the various authors above, then whatever techniques are used it qualifies as cyber terrorism. Clearly, the use of these techniques by technologically advanced nations in conflict with one another would constitute cyberwarfare, which would change the nature and impact of many of the events described in this chapter. However, our focus is not on explicit cyberwarfare, although a number of the events described later in this chapter are attributed to national agencies, which does represent an implicit form of cyberwarfare.

So, What Is the Difference between Cybercrime and Cyber Terrorism?

The majority of cyber attacks are launched by cybercriminal gangs determined to steal money, credit card information, bank accounts, or personal information. The intent is to make money. A general description of the dark side of the Internet can be found in the paper by Kim et al. (2009). On the other hand not all hackers are cybercriminals. Many hackers are computer enthusiasts who take pleasure in gaining access to computers and networks just to leave their "calling card." Defacing a Web site for political motives or simply to gain acclaim among their peers is their objective.

Attack patterns seen in criminal operations differ from incidents involving cyber terrorists. Cybercriminals typically use numerous targets and do not maintain prolonged control over servers, as the risk of detection increases proportionally (Krekel et al., 2012). However, the motives for a cyber attack are to some extent irrelevant. A criminal trying to steal money or a cyber terrorist trying to cause disruption, destruction, or steal secrets (cyber espionage), will both use the same methods. The main difference lies in the purpose of the covertness: the criminal stealing money or information would not want anyone to know what they were doing, to evade capture and prosecution; whereas, cyber espionage tries not to do damage to the attacked system so that information can continue to flow out (Saalbach, 2012).

As described previously, cyber terrorists would have a different agenda and their targets are likely to be a lot less secure. Currently, banks and credit card companies go to a lot of effort to secure customer information, but these are of limited interest to a cyber terrorist. In general, they are looking for softer targets with maximum public impact. The U.S. government is increasingly aware of government-run and -controlled cybergroups originating in China and Russia. It is not too far a step, and would seem to be only a matter of time, for a terrorist group to follow suit.

The main difference between cybercrime and cyber terrorism lies in the objective of the attack. Cybercriminals are predominantly out to make money, while cyber terrorists may have a range of motives and will often seek to have a destructive impact, particularly on critical infrastructure. Cyber terrorists also want to have maximum impact with the greatest stealth. Greengard (2010) identified a range of cyber attack methods that can be deployed by cyber terrorists, including "vandalism, spreading propaganda, gathering classified data, using distributed denial-of-service attacks to shut down systems, destroying equipment, attacking critical infrastructure, and planting malicious software."

Cyber weapons are software tools used by cyber terrorists. These tools can manipulate computers, intrude into systems, and perform espionage. They are essentially the same as those used by cybercriminals (Saalbach, 2012). There is currently no evidence to suggest that terrorists are using malware or hacking into systems. However, it seems unrealistic to think that they have not identified the potential for doing so. They may even be developing a Stuxnet equivalent (described later in the chapter) for military targets at this time.

Why Are the Risks Greater Today?

The cyber landscape is very different today from only a few years ago. Now most electronic devices can be connected to the Internet—phones (IP phones, smartphones, iPhones), TVs, computers, iPads, Nintendo Wii, MS Xbox, Sony Playstation, smart home equipment (sensors, cameras, and alarms), CCTV systems—the list goes on. All of these systems have IP addresses, so they are trackable and accessible through the Internet. Devices with radio frequency ID chips can communicate with other computers and devices (Saalbach, 2012). Even systems that were never supposed to be connected to the Internet sometimes are; for example, the Supervisory Control and Data Acquisition (SCADA) systems that control water treatment plants, power grids, nuclear reactors, and production lines. Many of these systems have the ability to allow engineers to remotely log in and make adjustments to the computers that control, for example, pumps and sluice gates. The complexity of the systems connected to the Internet increases each year and with this the opportunities for security breaches also increases. In October 2011 the highest number of vulnerabilities were reported and patched by all the big vendors, such as Apple, Microsoft, VMware and Oracle (VeriSign, 2012). This is an indication of the numbers of vulnerabilities that are being found each month. Each vulnerability is a potential breach in security for anyone using that particular system. These days remote access is expected by users. People log into work machines to read e-mail and to work from home. Secure links are often provided in the form of virtual private networks, but if the computer that is connecting goes through the link that is already infected with malware, then security is compromised and the bad guys have bypassed the defenses.

There have been incidents in the past where hacker groups have broken into American computer systems. The first one identified in 2003 was code-named "Titan Rain," which been associated with an Advanced Persistent Threat. Titan Rain was the code name given by the U.S. federal government to a long series of coordinated and very sophisticated cyber attacks primarily against American computer systems between 2003 and 2005. There were thousands of files downloaded from a large number of organizations, including Lockheed Martin, Redstone Arsenal, and NASA. Shawn Carpenter, a security expert, worked for the FBI to track down the origin of the attacks. Initially the files were downloaded to servers in South Korea, Hong Kong, and Taiwan before being transferred to the southern Chinese province of Guangdong. The suspicion was that this was Chinese government state-sponsored espionage, which China strongly denies (Thornburgh, 2005).

In mid-2009 there was a series of attacks over a 6 month period on Google, Adobe, and dozens of other high-profile companies. These attacks, code-named "Operation Aurora," used social engineering to encourage a victim to connect to a malicious Web site and then "combined encryption, stealth programming and an unknown hole in Internet Explorer" (Stamos, 2012) that enabled the attacker to escalate their privileges and gain access. Google claimed that the attacks originated in China and threatened to pull out of the country (Sood and Enbody, 2012).

Titan Rain and Operation Aurora are often provided as examples of state-sponsored cyber terrorism. While this is plausible, there are a number of analysts who reject the notion that a technologically advanced state, in this case the Chinese, would leave a trail of obvious footprints leading back to the country of origin. For example, Lewis (2005) claimed that it was likely that the perpetrators of the Titan Rain attacks used poorly secured Chinese networks and systems as intermediaries. At the time, China had a very insecure information technology (IT) infrastructure due to poor security practices and the widespread use of legacy and pirated operating systems.

Possibly more worrying is the threat from the "insider." This is someone who is already a user on the network under attack and is inside the security perimeter. The insider is especially dangerous because he is far more aware of the security in place on a network and the attached servers. Insiders know about the information stored on those servers and they also know about the security that surrounds it. This is described further in the section The Insider Threat.

CYBERPHYSICAL ATTACKS

Terrorist attacks have traditionally aimed to cause considerable human loss through physical means, such as armed assaults, explosives, and biochemical agents. However, as our societies are increasingly dependent on IT infrastructures and systems that are dependent on computers and networks, a new class of potential cyberphysical terrorist threats has emerged. For example, the control systems of the Thames barrier, the flight mechanism of an unmanned aerial vehicle, the operating room of a hospital, the unmanned Docklands Light Railway, and even the typical passenger elevator contain and rely heavily on computer software, hardware, and communications. As a result, these systems are vulnerable to both physical and cyber threats. A cyber attack may facilitate a physical terrorist attack by disabling monitoring and security equipment or may cause physical damage directly. Such an attack against a gas or water management facility may require considerably less planning and resources than a physical terrorist attack with the same aim. In fact, one can easily find on the Internet detailed guides, attack tools, and specialized search engines for exploiting the computer vulnerabilities of common industrial control systems used in such facilities.

Interestingly, the concept of cyberphysical crime has been utilized in popular culture since at least the 1960s. For example, in the film *The Italian Job*, a team of robbers employs a scientist to compromise the computers of Turin's traffic control systems and help the robbers escape thanks to the resulting traffic jam. Reliable reports on real cyberphysical security incidents are rare and, to the best of our knowledge, none has been openly linked to terrorism. Nevertheless, a brief history of representative incidents can illustrate the breadth of targets and the evolution of the attack mechanisms and their complexity. It is worth noting that several were unintended accidents or the result of a hacker's curiosity without malicious intent. Yet, they have exposed cyberphysical vulnerabilities in critical systems that do not require exceptional technical knowledge to be exploited maliciously.

Notable Cyberphysical Incidents

The earliest incident that is often linked to a cyberphysical attack is the 1982 Siberian Pipeline Explosion, which has been reported to be the result of intentionally flawed industrial control software altered by the Central Intelligence Agency (CIA) and sold indirectly to the Soviets (Reed, 2004). According to these reports, the software that controlled critical pressure valves increased the effect of a pressure test of the pipeline and caused a "monumental" explosion.

The "Farewell Dossier," which was declassified in 1996, does indeed indicate that the CIA routinely fed defective technologies to the Soviet Union, but does not confirm the specific incident (Weiss, 1996). A confirmed incident involving a gasoline pipeline explosion happened in Bellingham, Washington, in 1999. The explosion caused three deaths and considerable environmental damage and was attributed in part to the slow-down of the pipeline's control software. Although no evidence of intent was identified, the control systems were found to be connected directly to the network of the building without proper access monitoring or other security measures.

Since then, cyberphysical incidents in the energy sector have multiplied. In 2003, the Davis–Besse nuclear power plant was shut down after the SQL "Slammer" worm disabled its safety monitoring systems. In 2007, the U.S. Department of Homeland Security's "Aurora Experiment" at the Department of Energy's Idaho lab demonstrated a cyber attack that blew up a power generator typically used in the U.S. domestic electrical grid. While it is not clear what type of cyber attack was used in this case, by then it was already known that critical industrial control systems were vulnerable to the same threats as Web sites and personal computers, including port scanning, SQL injection, anonymous FTP, and simple password guessing. Two years later, senior U.S. officials reported that cyber spies from foreign states had been probing the U.S. electric grid's infrastructure and had planted suspicious software for possible future use (Gorman, 2009). With the cyberphysical security weaknesses of this sector already obvious by then, it is not surprising that the first major attack, often considered the beginning of cyberwarfare, was against a nuclear facility. On November 29, 2010, Iran's president confirmed that the controller handling the centrifuges at the Natanz Nuclear facilities had been damaged by Stuxnet, an exceptionally complex worm that was designed specifically to attack this target (Falliere et al., 2011). Its complexity, the presumably high cost of development and, of course, the target, have led most analysts to suggest the United States and Israel as the originators of this new cyber weapon. Since then, at least two other worms have appeared that are closely related to Stuxnet, although with clearly different targets, and may have been designed by the same team.

The water sector has also seen a number of cyberphysical attacks over the last two decades. In 1994, a hacker used a common dial-up modem to connect to the Salt River Project's network in Arizona, and gain access to water and power monitoring information. An investigation concluded that there was no major threat to Arizona's Roosevelt Dam and there was no intention to cause harm (Gleick, 2006). As usual, the hacker had done it primarily out of curiosity. Very different was the motivation and impact of an attack in Australia in 2000 (Turk, 2005). Vitek Boden was a 40-year old employee of a firm subcontracted to install wireless control equipment for the sewage systems of Queensland's Maroochy Shire Council. When he lost his job with the firm and was also denied a job with the Council, he decided to use his technical knowledge to take revenge. He used stolen radio equipment to issue rogue commands to the sewage pumping systems and released over 800,000 liters of raw sewage into parks, rivers, and property. Although the subcontracting firm had noticed the misbehavior of the pumping stations, and had concluded that only someone with detailed familiarity of the systems could be behind it, Boden managed to connect to the pumping stations at least 46 times over 3 months. He was caught only after the police pulled him over for a traffic violation and found the radio equipment in the car. He was sentenced to two years in jail and was ordered to reimburse the Council for the cleanup.

Two years later, U.S. authorities discovered instructions on poisoning water sources on a suspected terrorist. The FBI issued a bulletin indicating that al-Qaeda agents had been seeking information on the control systems of dams, water supplies, and wastewater management facilities in the United States and abroad. While awareness of these threats has been raised since then, due to the prohibitive cost of replacing industrial control equipment there are still several vulnerable pumping stations worldwide. In fact, it was demonstrated at a 2011 hacker conference that the Internet address of the IT units controlling them are easily discoverable via common search engines, such as Google. By knowing their address, a hacker can attempt a wide range of attacks to disable them or alter their behavior.

In the transport sector, cyberphysical incidents usually cause disruption in dispatching and signaling. In the 1990s they were related primarily to the lack of user authentication mechanisms. For example, a hacker would connect via a dial-up modem to an airport network pretending to be the legitimate system administrator and would alter critical information. Later, due to the increasing use of off-the-shelf computers running Microsoft Windows, a number of incidents in the transport sector were caused by common viruses and worms that spread via the Internet and infected computers indiscriminately. One such virus disabled air traffic control systems in Alaska in 2006. Yet, in most cases, there was no malicious intent and, more significantly, there was no damage beyond frustration and financial costs due to downtime. In 2008 though, a teenager managed to take control of the tram system in Lodz, Poland, and operated its track switches, eventually causing four trains to derail and 14 people to be injured.

Since then, researchers have demonstrated that even common production cars can be targets of cyberphysical attacks (Koscher et al., 2010). Today's cars depend heavily on a variety of sensing and computing equipment that are interconnected and can affect each other in unpredictable ways. One can infect a car's electronic systems through a manipulated audio file added to its MP3 playlist or can use an infected smartphone connected to the car through Bluetooth. A car interfered with in such a manner may be forced to veer toward one direction while driving at a fast speed. Another cyber weakness of vehicles is the use of satellite navigation. These devices can be fooled to display the wrong location and traffic information and direct the driver of the vehicle toward a terrorist ambush. Interference with the satellite navigation signals over an area could cause local traffic jams, for example, to delay the emergency services following an act of terrorism. Scenarios involving such interference are increasingly likely because of the recent proliferation in the black market of GPS jamming devices that are often used by thieves to prevent stolen trucks from being tracked by their owners.

Cyberphysical attacks involving satellite systems are also becoming common in the defense sector. In 2009, militants in Iraq used off-the-shelf software, costing just $29.99, to intercept live video feeds from unmanned aerial vehicles (UAV). The software, which is still sold commercially, had been developed by a Russian company to allow interception of satellite TV, but proved to work just as well for unencrypted military surveillance feeds (Gorman et al., 2009). Since then, the military affected aircraft have been retrofitted to encrypt the video they transmit. Two years later, the U.S. military found that a number of their frontline UAVs had been infected by viruses that were logging the keystrokes of the pilots who remotely controlled them during combat missions. It is most likely that the intention behind this attack was to reveal what signals transmitted by the pilot would operate what part of the vehicle. The same year, Iranian TV showed an American UAV claiming that the Iranian army's electronic warfare unit had electronically hijacked and landed it intact. If UAVs costing millions of dollars can be interfered with via cyber means, it is more than likely that smaller civilian unmanned aerial devices, such as police surveillance cameras in major events, which receive and transmit unencrypted signals can also be hijacked and flown into a crowd. In fact, researchers from the University of Texas recently used their own mini helicopter drone to demonstrate how such an attack can be performed. The cost of the equipment they used to build their proof of concept system did not exceed $1,000.

By now, it is obvious that cyberphysical attacks can affect practically every sector that relies on a computer infrastructure, from defense and food to home automation and emergency management. Of particular interest is the health sector. Terrorist attacks against the health sector have traditionally been rare, possibly due to the moral outrage that they would cause. However, the increasingly networked infrastructure of modern healthcare systems may present opportunities for terrorists to cause damage in a more covert manner. The potential of such an attack became clear in the 1980s when massive overdoses by the Therac-20 computerized radiation therapy machine caused four deaths (Leveson and Turner, 1993). The machine's designers had faith in the computer software's reliability without the necessary hardware safety mechanisms and interlocks that were found in previous versions of the machine. In 2008, scientists demonstrated that common cardiac devices could be operated remotely without authorization, allowing a malicious user to deliver remotely a life-threatening shock (Halperin et al., 2008). In 2009, 10% of Sweden's healthcare IT infrastructure, including MRI machines and heart monitors, were disabled by an Internet worm originally designed to affect normal personal computers. The same year, a medical clinic's security guard in the United States was arrested for cyber intrusions that intentionally tampered with the air conditioning systems putting patients and pharmaceuticals in danger (FBI, 2009). A terrorist organization could potentially adopt such approaches to impede the emergency response operations after a physical attack and thus cause maximum damage.

MALWARE CANDIDATES FOR CYBER TERRORISM

As hacker attacks are on the increase, it is not unreasonable to assume that terrorist groups around the world also have their eye on the "low hanging fruit" that litters the Internet and that can be accessed using current cyber attack tools. The creators of worms and viruses have not had specific targets in their sights when they released their malware into the wild. However, there have been reported incidents where malware has gained access to critical systems by accident. Such an event occurred when the MS SQL Slammer worm gained access to the Davis–Besse nuclear plant in Oak Harbor, Ohio. The worm bypassed the firewall that was in place and flooded the network with worm traffic, blocking the safety systems for nearly 5 hours and the computer that controls the processing plant for over 6 hours (Byres, 2004). The Slammer worm also got onto ATM machines and into airline reservation systems (Chen, 2010).

Critical infrastructure is defined as water treatment plants, oil refineries, power grids, gas pipelines, and so forth. These are considered by governments to be essential assets without which society cannot function. SCADA systems are used to gather data and control these systems, particularly where it is difficult or dangerous for humans. This is usually done in factories and industrial plants, where there may be production lines or for monitoring nuclear plants, gas pipelines, or water treatment facilities. SCADA systems were originally designed to be closed systems, that is, not connected to the Internet. However, it has been found that they are increasingly routinely connected to the Internet. Remote access by engineers to make minor adjustments does have some merit. However, security should be the top priority. It was found that a number of SCADA systems that could be accessed via the Internet still had the four-character default password in use. Many SCADA systems were also connected to a back office network (Ten et al., 2010). This was a recipe for disaster, as normal users on such a network are generally not security aware and may pose a particularly serious threat to this type of network. This also gives an idea of the scale of the threat and the exposure of these systems to attack from the Internet.

Currently, the main contenders for malware that could be used as a cyber weapon are Stuxnet, Duqu, Flame, and Shodan. An overview of each of these is presented below.

Stuxnet

The biggest threat to SCADA systems has been the Stuxnet worm. The earliest reported appearance of Stuxnet was in June 2009 (Falliere et al., 2011).

This version was relatively harmless, but Stuxnet rapidly evolved and the next variant reported early in 2010 was using a valid signed certificate obtained from Realtek Semiconductor Corps for a Stuxnet driver, which enabled it to trick users into downloading it as it appeared to be legitimate. Throughout 2010 Stuxnet continued to evolve until by mid-July it was able to exploit a Windows shell vulnerability (Exploit MS10-046) that permitted remote execution of code. The certificate from Realtek was quickly revoked by VeriSign, but Stuxnet replaced it with another valid one from JMicron Technology Corp. Within days reports began to come in of the first infections of WinCC and PCS 7 SCADA software running Siemens SIMATIC software that ran on a programmable logic controller (PLC). The time between each of these improvements in the malware's capability has been progressively shorter, from months between events at the start, down to days, as Stuxnet evolved.

From July to September 2010 Microsoft issued patches in an attempt to stop Stuxnet from spreading. Stuxnet exploited at least four zero day exploits (Chen, 2010), which is quite remarkable. Most malware writers would only have used one at a time, so as not to waste future opportunities. Analysis of the Stuxnet code revealed that it was attempting to inject and hide code in a PLC found in Siemens systems. These PLCs interface between the control systems and the equipment that is being controlled, such as robot arms or elevator doors. Stuxnet only infected specific systems and did not activate if the victim computer was not connected to a SCADA system. As Stuxnet is a worm, it can install itself in the operating system and travel between systems. The method of propagation used was via USB sticks, as not all these systems were connected to the Internet. To maintain stealth and avoid detection, after a number of successful infections it deletes itself. It used Siemens default passwords to gain control before injecting code into the PLC.

The aim was to find the right kind of system to infect, such as a nuclear power plant, and then to begin to slow down and speed up the centrifuges. Any engineer called out to diagnose this fault would find it very difficult to identify the problem. The aim was to cause physical damage to these systems (Chen, 2010). According to statistics collected, it was estimated that by September 2010 there were around 100,000 infected hosts around the world and the majority were in Iran. This indicated to many security experts that Iran was the primary target (Falliere et al., 2011).

The work done for Siemens by Langner (2011) to decompile the Stuxnet code was very revealing. The code was found to be well engineered and sophisticated. It was atypical in terms of malware code, as it was quite large and written in a number of different programming languages, which was unheard of in all previous worms and viruses. It also appears to have been written by a number of different individuals. The method Stuxnet uses to attack specific pieces of equipment shows that the writers of the code had detailed knowledge of these plants and the systems that control them. It is the view of Langner (2011) that Stuxnet was not the work of hackers, but of a government-funded team of programmers, and that the biggest cyber superpower was the prime candidate, that is, the United States. The prime motive appeared to have been to disrupt Iran's nuclear program.

Stuxnet continues to spread and infect computer systems via the Internet, although its power to do damage is now limited by effective antidotes, and a built-in expiration date of June 24, 2012 (Farwell and Rohozinski, 2011).

Using freely available search engines (see Shodan) it is relatively easy to find the IP addresses of the SCADA systems, which manage and control the critical infrastructure of almost every nation (Naraine, 2010). That leaves a number of critical infrastructures vulnerable to cyber attacks. The worry among the cyber security communities regarding Stuxnet was the level of sophistication and the types of systems targeted.

Duqu

Duqu is referred to as the son of Stuxnet. How does it differ from Stuxnet? It is clearly based on the Stuxnet code but Duqu does not contain any code that could affect industrial control systems. Its mission seems to be to collect information such as design documents from the same systems that Stuxnet attacked. The purpose is assumed to aid the development of the next version of the attack tool (Symantec, 2011).

Duqu used a different approach to Stuxnet. It was delivered via e-mail with a Word document, which contained a zero day exploit that enabled Duqu to install itself. The aim was to gather information on system configurations and also to collect the keystrokes of users with the use of a key logger. For SCADA systems that are connected to office systems this seems like a very efficient way for Duqu to propagate. There have been a number of variants and the code seems to still be evolving.

The Duqu code comprises a configuration file and a driver file (dll), which has a valid (although stolen) digital certificate. This is the same technique used by Stuxnet. Duqu also needs an installer to load the dll. Forensic analysis of the configuration file showed that the time and date of the infection is stored in the file. It appears that Duqu will only be active for 30 days and then it removes itself, presumably to reduce the chances of detection. Having installed and collected intelligence, Duqu then attempts to communicate with a number of command and control (C&C) centers. C&C centers have been identified in India, Belgium, and Vietnam. These centers are acting as proxies and merely forwarding the traffic on, so it is very difficult to identify the real C&C center. The files transferred look like jpg files but have the data collected appended and lightly encrypted and compressed within them. As of March 2010 there have been 15 variants of Duqu identified (Symantec, 2011).

Duqu has serious implications for any network that requires top security. It hides itself on the infected system. It has the ability to log everything that a user types. It also collects information about the network and the infrastructure. All of these data are then encrypted and sent out disguised as an image file, which is sent to a C&C center somewhere on the Internet.

Flame

The next contender in the cyber weapon arsenal is Flame. It is unclear how long Flame has been around and opinions differ. It was first identified by Kaspersky in 2010. However, there is evidence to suggest that Flame was operating as an espionage tool prior to this (Lee, 2012).

Flame used social engineering to trick people into downloading it by spoofing the Microsoft's Windows update service using fake certificates. Users would then click on the update link and become infected by Flame (Whitney, 2012).

Analysis by Kaspersky has shown that Flame is a sophisticated attack toolkit with cyber espionage capability. It is significantly larger than Stuxnet (20 times bigger) and more complex than Duqu. Flame is coded using the object-oriented language C++. This makes it difficult to analyze due to the compiler and the way the language is constructed. It also appears to have been written in such a way that it is difficult to follow the logic of the code (Matrosov and Rodionov, 2012). It is made up of a number of attack tools, which include taking screenshots at regular intervals, recording audio conversations, key logging, and packet sniffing on the network. Flame has many ways to steal data. It has no similarities with the Stuxnet/Duqu code, but it does use C&C servers to upload the stolen information. Once Flame has installed there are more modules that can be added to improve the data-stealing capability. It would appear that at this time Flame is still undergoing further development, although the authors are still to be identified. Interestingly, the files within the code have false creation dates (starting in 1992) to hide the actual "age" of Flame.

Flame was clearly designed to steal information and not money from banks, making it a prime candidate for the cyber weapon of choice (Gostev, 2012). The cyber security coordinator for the United Nation's Geneva-based International Telecommunications Union, Mr. Obiso, told Reuters in May 2012, that he considered Flame to be a “dangerous espionage tool that could potentially be used to attack critical infrastructure” (Bozorgmehr, 2012).

> *Flame can easily be described as one of the most complex threats ever discovered. It's big and incredibly sophisticated. It pretty much redefines the notion of cyberwar and cyberespionage.*
>
> ***Alexander Gostev (2012), Kaspersky Lab Expert***

Shodan

The Shodan search engine was launched in November 2009. Shodan, named after the Sentient Hyper-Optimized Data Access Network of science fiction, was developed by a teenager called John Matherly who wanted to see how much he could find out about devices connected to the Internet. He was surprised to find that a large number of industrial control computers were in fact accessible from the Internet. To make it worse, many of these systems had little or no security at all. These vulnerable systems controlled water plants and power grids around the world.

How is Shodan different from other search engines that crawl the Web looking for data in Web pages? Search engines such as Google and Bing search through the text on Web pages to find what the user is looking for. Shodan searches the World Wide Web interrogating ports and grabbing banners to identify vulnerable devices. It identifies the IP addresses of devices and then tries to connect to them, and if it succeeds it “fingerprints” that device. All of the information collected, including geographical location, software, and any banner information displayed is stored and then available for anyone to download. It also searches for default passwords or nonexistent security controls. It is estimated that information about 10 million devices was collected each month, which are then available for anyone to query in the same way that you would with Google. It is reported that a Shodan user “found and accessed the cyclotron at the Lawrence Berkeley National Laboratory” (O'Harrow, 2012). Other users have found thousands of unsecured Cisco routers. It is therefore not unexpected that hackers are using Shodan to search for SCADA systems that are connected to the Internet (Naraine, 2010).

While Shodan is not a cyber weapon on its own, it is certainly a facilitator for cyber terrorism.

THE INSIDER THREAT

A very serious threat to any network comes from the insider. Who is the insider? This is a person who is not affected by any security that keeps intruders out of a network, because they are already inside the perimeter. This could be someone who is permitted to access the network because they have a legitimate login and ID. They could be an employee or a contractor working for the company, or anyone who has a formal business relationship with the company. They could be a bank customer who can access their own account details or someone who has stolen the credentials of a user. They could be someone who is forced to aid an outsider to perform some action. They could be a former insider who has retained their login credentials (Bellovin, 2008).

Many organizations focus their security on addressing potential attacks from outside the organization and give insufficient consideration to threats from insiders. Statistics quoted publicly on insider threats vary significantly; however, there is no disagreement that the threat is very real. The 2007 E-Crime Watch SurveyTM, conducted by the United States Secret Service, the CERT Coordination Center (CERT/CC), Microsoft, and *CSO Magazine*, found that where the perpetrator could be identified, 31% of attacks were committed by insiders and 49% of their survey respondents (671 security executives and law enforcement officials) had experienced at least one deliberate insider attack in the previous year. It is, however, important to clarify what we mean by insider threats. Jones and Averbeck (2011) defined three types of insider threats:

1. **Trusted unwitting insider**: This is someone who has no malicious intent but accidentally, through an error of judgment, supports or initiates an attack. For example, by opening an inappropriate e-mail releasing malware or, more classically, opening up a USB stick, which they think has been lost. In reality it has been planted for them to find, and unwittingly open up with the best of intentions to try and find the owner, releasing malware into the system. Inadvertent threats are as real and as important to address through education and so forth, but are not the focus in this section. Attacks of this type are generally referred to as access control failure attacks.
2. **Trusted witting insider**: This is someone who has legitimate access to systems and makes a conscious decision to, for example, release unauthorized data to a third party. Attacks of this type are generally referred to as misuse of access attacks.
3. **Untrusted insider**: This is someone who has gained access illegally, for example, by fooling someone with a lost USB stick, who now has internal access and can now act as though they are a trusted employee. Attacks of this type are generally referred to as defense bypass attacks.

What motivates someone to spy and steal information that could potentially aid another country? This is a complex issue and there are numerous factors. The motivation could be money, revenge, blackmail, or even anger at not getting promoted. There could be divided loyalties or they may simply want the thrill of living a James Bond type fantasy (Moore, 2008). Insiders can be current or former employees, contractors, or other parties who have or have had access to privileged information and include business partners and employees from companies to whom work has been outsourced. Insiders have a huge advantage over outsiders in that they are aware of company policies and procedures, how they are applied, and where the vulnerabilities and weaknesses are in their setup and use. For those with more technical skills, they will know how the technology is used, the level of security, how firewalls are set up, and if they are programmers, they then may have access to directly edit code. All this makes combating attacks by insiders more challenging.

A study was performed by the U.S Secret Service and CERT in which cases of insider attacks on U.S. critical infrastructure sectors were analyzed. Of this group 54 cases were followed up by CERT. It was found that 86% of the subgroup held technical positions and 90% routinely had administrator system access as part of their job (Keeney et al., 2005). These people are in a position to compromise security either by setting up secret accounts or by abusing their login privileges to access confidential or top-secret information.

It has been found that attackers using identity theft to masquerade as valid users often exhibit abnormal behavior (Salem, 2008). This would be a possible method for use in the detection of masquerades on the network. However, the perpetrators of attacks such as Titan Rain did not make any mistakes or exhibit any unusual behavior as they covertly stole information and more important, no one even knew they were there.

Examples of Insider Attacks

There have been a number of high-profile insider attacks over the years where information had been stolen and delivered directly to foreign governments. In 2007, Chi Mak was convicted of stealing U.S. Naval secrets and delivering them to China using members of his family as couriers. He confessed that he had been sent to the United States in 1978, by the Chinese government, to work in the defense industry and to gain a position of trust (Claburn, 2008).

An engineer, named Greg Chung, who worked on the U.S. space shuttle and other sensitive projects, was found to have been spying for China from 1979 until 2006. Chung had the highest level of clearance and managed to remove more than 225,000 pages of documents relating to Boeing-developed aerospace and defense technologies. Some of these were extremely sensitive at the time. Greg Chung was arrested in February 2008 and convicted of spying (Scherer, 2009).

An American seaman called Hassan Abujihaad converted to Islam in 1995. He was serving on a missile destroyer deployed to the Gulf and was found to be sending classified documents to a London-based organization called Azzam Publications, which had links to terrorism activities via e-mail and Web sites (Former U.S. Navy Sailor, 2009). The FBI alleged that “the Azzam websites were among the first to successfully utilize the internet on a global scale to propagate the call to jihad” (Mahony, 2010). Abujihaad had leaked classified information to al-Qaeda, which included the vulnerabilities of a number of battleships and also their movements in the Gulf during that time.

The insider threat is not new as demonstrated by the case of Walter Kendall Myers and his wife Gwendolyn. Walter had worked at the Bureau of Intelligence and Research in the State Department where he had one of the highest security clearances. It came to light that he had spent 30 years spying. Both were arrested in June 2009 and subsequently convicted of supplying classified documents to the Republic of Cuba and of committing wire fraud (Wilber and Sheridan, 2009).

Elliot Doxer worked for Akamai and had been leaking the company's trade secrets for an 18 month period. Fortunately, the undercover Israeli intelligence officer that he thought he was dealing with turned out to be an undercover federal agent. He was arrested in 2010 and charged with foreign economic espionage (Bray, 2010).

In March 2011 the U.S. Department of Defense (DoD) announced that 24,000 files had been downloaded from military contractor systems. DoD Deputy Secretary William Lynn stated, “It is a significant concern that over the past decade, terabytes of data have been extracted by foreign intruders from corporate networks of defense companies. In a single intrusion this March, 24,000 files were taken.” The U.S. DoD has seven million computers located in hundreds of countries and operating over 15,000 networks. They are currently taking action to try to stem the massive leakage of information that is currently taking place (Dignan, 2011).

Research on Insider Threat

The research done by Moore et al. (2008) was based on 49 insider sabotage cases. They attempted to identify common patterns within these cases. Seven general observations to help to identify insiders were proposed as a result of this work. The main conclusion was that disgruntled employees were the most likely candidates, for whatever reason. But they were also facilitated by a general lack of access controls (Moore et al., 2008).

Detecting the insider is a challenging problem as these attacks are often very sophisticated. The insider's familiarity with the networks and systems of the company that they work for makes it easy for them to cover their tracks and very difficult to catch them. It is estimated that approximately one-third of all data theft is due to insiders (Pfleeger, 2008).

One of the leading authorities on insider threats is CERT, the Software Engineering Institute of Carnegie Mellon University. They have accumulated data on hundreds of cases of insider attacks over the years for analysis. As of 2011 (Cappelli, 2011), their database contained 123 cases of sabotage, 196 cases of fraud, 86 cases of intellectual property theft, and 43 miscellaneous cases. What follows is a discussion of the key findings from some of their recent work on financial fraud (Cummings et al., 2012) and intellectual property theft (Moore et al., 2012).

Motives for an attack vary. Cappelli et al. (2009) analyzed 196 cases of insider attacks that occurred in the United States and observed their cases falling into the following categories (noting that some cases fell in to more than one category):

1. **IT sabotage**: These occur through individuals who are motivated to harm the organization, its data, or an individual. They misuse their access to systems, data, or networks and account for 45% of cases. Attacks were primarily committed by former employees and males; however, the fact that males were the majority is unsurprising as 74% of employees in this field are males. Motives identified from this group were disgruntled employees and revenge for some negative event such as termination, disputes, new supervisors, transfers or demotions, and dissatisfaction with salary. The majority who committed this type of attack did not have authorized access at the time of the attack. Thirty percent used their own username and password, others used a compromised account, an unauthorized backdoor they had created, systems or database administrator accounts, and so forth. Attacks included logic bombs and sabotaging backups. Most attacks were carried out through remote access, out of normal working hours, and in most cases system logs were used to identify insiders.
2. **Theft or modification for financial gain**: These occur where insiders intentionally exceed their authorized levels of access with the intention of stealing confidential or proprietary information for financial gain and occurred in 44% of cases. Targets focused in the banking and financial sectors followed by the government sector and then the IT and telecoms sector. The vast majority of these crimes were committed by current, not former, employees working in lower level, nontechnical positions and split evenly between males and females. Collusion with other insiders and outsiders was high, a recurring pattern was an outsider recruiting an insider. Ninety-five percent stole or modified information during normal working hours and 75% used authorized access, with 85% using their own username and password. The majority of the cases were detected through nontechnical means such as data irregularities or customer alerts and were typically caught through system, database, and file access logs. Within the financial sector (Cummings et al., 2012), it was noted that:
   - Criminals who executed a "low and slow" approach accomplished more damage and escaped detection for longer: on average fraud started over 5 years after hiring and it took an average of 32 months to be detected.
   - Insiders' means were not very sophisticated; very few held a technical role or used technical means and in more than half the cases, authorized access was used in some form.
   - Fraud by managers differed substantially from fraud by non-managers by damage and duration. Fraud by managers caused nearly twice the financial damage than non-managers and lasted almost twice as long—33 months compared to 18 months.
   - Most cases do not involve collusion: 16% involved collusion and of those 69% involved outsiders.
   - Most incidents were detected through an audit, customer complaint, or coworker suspicion; routine or impromptu auditing was the most common route for detection.
3. **Theft or modification for business advantage**: This is where insiders intentionally exceed their authorized levels of access with the Intent to steal confidential or proprietary information for business advantage and occurred in 14% of cases. The vast majority of crimes were concentrated in the IT and telecoms sector; however, the banking and financial sectors, chemical and hazardous materials and the defense industrial-based sectors were also affected. All of the attacks analyzed were carried out by males, 71% in technical positions, 29% in sales, 25% former employees, and 75% current employees. Nearly 80% had accepted positions with another company or had already set up a competing company. In 25% of cases information was passed on to a foreign company

or government and 88% had authorized access to the information. The majority of the cases occurred within a one month period and in approximately half the cases the insider colluded with at least one other insider. Cases were detected through emergence of competing products, informant, and so forth, and were typically proven through system, database, and file logs.

4. **Miscellaneous:** This is where insiders intentionally exceed their authorized levels of access with the intention of stealing confidential or proprietary information for purposes other than financial or business advantage and occurred in approximately 9% of cases.

As identified earlier, many people relate insider attacks to a disgruntled employee; however, the CERT team has noticed the following recent trends and issues related to insider threats:

1. **Collusion with outsiders:** Half of the insiders who stole or modified information for financial gain colluded with outsiders.
2. **Business partners:** The number of insider attacks from trusted business partners who have been given authorized access is increasing.
3. **Merger and acquisitions:** There is an increased risk from employees who are working in an uncertain climate from both the acquiring and acquired organizations.
4. **Cultural issues:** It is important to recognize that cultural issues can influence employee behavior.

Clearly, the range and scope of the events described in this section demands that there must be equivalent levels of countermeasure, otherwise our existing systems might fail in the face of such pressure. The next section sets out a range of countermeasures that are currently in use to address these issues.

COUNTERMEASURES TO COMBAT CYBER TERRORISM

There are a number of standard computer security measures that have a significant effect in countering cyber terrorist activity, if they are properly implemented and maintained. These include properly installed, managed, and regularly updated firewalls; packet-sniffer software; virus checkers; access control lists; and user validation systems. However, by far the greatest threats to any security system are the human users, who accidentally, forgetfully, lazily, ignorantly, or maliciously breach the security of systems on a daily basis. For the vast majority of cybercriminals, and cyber terrorists, they do not need sophisticated software or hardware tools to break into systems, as long as the user issues remain unaddressed. Therefore, the establishment of good cyber hygiene must be a priority for every organization, together with clear, well-defined, standards-based policies and protocols, and training systems, aimed at every level of user, establishing security as central to organizational culture.

Once these issues are addressed, consideration can be given to software measures to address more sophisticated threats, including diversionary tools such as honeytraps and dummy sites for hackers, sandboxing to trap malware, and bounties to trap bugs and security holes.

Policy

"How many of the recent, high-profile data breaches at blue-chip companies could have been prevented with better governance? While corporate governance is common practice, often obligatory, in many aspects of business, governance is not always present in information security. Yet it plays a vital role in reducing risk and speeding response" (ISF, 2011).

It is not sufficient to deal with cyber security by *ad hoc* application of tools and procedures as and when problems arise; indeed, it is often then too late. An organization needs to be proactive and to be ready, organized with a set of controls, trained personnel, and a written security policy, known by all staff, with defined rules and roles. Such a management policy should be based upon principles of good IT governance and be based upon recognizable standards that give assurance to all stakeholder parties.

Standards bodies such as International Standards Organization (ISO), American National Standards Institute, and British Standards Institute devise formal sets of rules by which processes and activities should be undertaken to achieve optimum performance. Relevant standards for cyber security might be ISO27032 CyberSecurity (draft standard), which is to be the defining standard for cyber security requirements, ISO27033 Network Security (draft standard), ISO27034 Application Security, and ISO27035 Information Security Incident Management (draft standard), as well as the already well-established ISO27001.

The use of recognized standards to form a cyber security policy is important as standards give trustworthiness to other parties, such as supply-chain partners, regulators, and law makers. Supply-chain partners such as suppliers, clients, and other trading partners are reassured about using electronic business transactions. In fact, a further useful standard here might be ISO27036 Information Security for Supplier Relationships. Regulators, too, may require reassurance on the security of network/Internet transactions especially in certain industries such as finance; for example, in the United States the Securities and Exchange Commission and in the UK, the UK Financial Services Authority. Lastly, compliance to standards shows due diligence and commitment when possible litigation arises in such areas as data protection, copyright, and computer misuse.

It has to be acknowledged that cyber security is a moving target; hacktivism, fraud, and denial of service attacks are constantly changing their modus operandi. Controls should therefore be monitored regularly using audit techniques. Auditing assures that the requirements of a cyber security policy are being met in practice. In practice, controls, both technical and administrative, may be ignored (deliberately or accidently), totally removed, or adapted to be less effective. Auditing identifies the effectiveness of the controls in place (the right control doing the right thing?), how efficient they are (are they used properly and quickly in practice?), and how economic they are (cost-effective?). In addition, auditing identifies whether new controls may be required and whether there exists a gap between the reality and the requirements of the adopted standard. This gap analysis shows what and where the shortfalls are and indicates how far the standard is being met. The gap may be used to measure the extent of compliance to the standard, to reassure a regulator, as a benchmark to compare the organization with other organizations in the same industry, to reassure supply-chain partners, or simply as part of a calculation of return on investment to reassure the accountants.

Cyber security auditing is as much an art as a science and needs careful planning, execution, and reporting. Auditing standards, methods, and tools may be found at the Information Systems Audit and Control Association and the Institute of Internal Auditors.

Training

Cyber terrorism is considered a top-tier national risk for many governments given the potential harm and disruption it can cause due to the world's increasing dependency on IT systems. While the obvious targets might be governments, banks, and utilities (e.g. water, oil, electricity, gas, chemical, and communication infrastructure), as attacks on these have the ability to cause the most economic, political, and physical havoc and damage to the critical national infrastructure, cyber terrorism groups are becoming more coordinated and sophisticated in their attacks and will make use of any computer connected to the Internet to support an attack. Cyber terrorism therefore affects everyone from large organizations to all citizens who own or use a computer connected to the Internet. The following list provides a brief summary of the different categories of people involved and a brief analysis of their training needs.

1. **Members of the public:** The single definitive source of advice for UK Internet users is Get Safe Online, which is a Web site sponsored by a cross section of organizations including the UK government. In November

2011, their Get Safe Online Report (Get Safe Online, 2011) stated that 87% of users surveyed had virus protection software and 41% of them updated it every time they switched their computer on. Clearly a lot more is needed to educate the public with a growing trend in cybercriminals making use of a wide variety of techniques including the use of personal information from social media cites to tailor realistic information more able to fool people into allowing a variety of forms of malware into their computers to clickjacking, and so forth. Training needs to start at an early age and more work needs to be done in educating school-age users as well as adults.

2. **IT support personnel within organizations**: These are staff who are technically trained to deliver IT services to an organization. Many have not received the level of training in security required or have misunderstood the threat to their organization. Over 80% of attacks could be dealt with through basic cyber hygiene, such as patches, passwords, anti-malware, and firewalls; however, even when used, many do not keep them up to date. Relevant training through certifications and Chartered Status should be required and monitored by senior managers.
3. **IT developers**: Many developers write poor code through laziness or a lack of understanding of how to protect their code from things such as SQL injection attacks. Education and training programs need to provide more of a focus on security issues, and organizations need to invest in regular CPD for their developers in this area.
4. **IT project managers**: It is not uncommon for large organizations to use staff with good project management skills, but limited technical capability, to manage and take oversight of IT projects; however, they frequently lack the technical knowledge to ensure the systems they manage are developed and maintained in a secure manner. These staff need to be trained to understand the risks to the organization, the questions to ask, and how to ensure that their IT projects are providing the right level of security required.
5. **IT users within an organization:** Most IT users within an organization find security an irritation as it makes systems less usable. As a result, they invariably find workarounds, not understanding the potential risks that they may be introducing into their organization's systems. This includes issues related to the use of personal devices at work (Bring Your Own Device; BYOD), which can be used by the entire family at home, introducing malware and other assorted risks.
6. **CEOs, Senior Board-level personnel**: Organizations are spending millions on security yet many still end up in the media as a result of security breaches. Most CEOs and board-level directors do not understand the security risks, how to manage them, or the behavior of their employees, which may result in security breaches (Lumension, 2011). All CEOs and senior board-level directors need to understand as much about the dangers of IT as well as how to exploit IT for business purposes in addition to who in their organization needs what type of training. They need to be able to adequately assess their vulnerability to a cyber terrorist attack, understand how to assess their risk, and drive appropriate policies. Should an attack occur, they need to consider how they will deal with data losses, downtime, the impact on infrastructure, and their customers, including the loss of their information, costs, reputational damage, how to address future issues of security versus privacy, risks of outsourcing and off-shoring, and so forth. Depending on the potential impact, senior staff may need crisis management training to help them deal with the media and management of a breach, which may take months or years to fully uncover and resolve. Use of training systems such as Pandora (Bacon et al., 2012), which can simulate realistic crisis training using an event-based time line model to allow different scenarios to be explored, could prove particularly useful.

Cyberphysical Security Challenges

The vast majority of cyberphysical systems have been designed and tested with physical safety but not cyber security in mind. More significantly, computer-controlled equipment in our critical national infrastructure, such as dams and nuclear plants, usually have an expected lifetime of 30 years and are too expensive to replace. Also, they have not been designed with modularity and upgradability in mind. A modern personal computer can be protected against most cyber threats by upgrading its software and applying security patches. This is not straightforward for 20-year-old industrial control equipment. A system upgrade may need months of planning and may cause prohibitively long downtime. In addition, modern software security packages are usually too demanding for the large number of legacy components found in such systems (Cardenas et al., 2009).

Still, the fundamental difference between cyberphysical systems and conventional IT systems is the interaction of the former with the physical environment. Unavailability of a corporate network or individual computer may cause frustration and may delay operations, but is unlikely to cause lasting damage. Real-time availability is more important in cyberphysical control systems, as was demonstrated at the 1999 gasoline pipeline explosion in Bellingham, Washington. On the other hand, this interaction between the physical and cyber world may also provide opportunities, as otherwise undetectable cyber attacks may become detectable though their physical manifestation. Yet, scientists still have not taken advantage of these interactions and all current detection mechanisms take into account only cyber traces to determine whether a system is under cyber attack or not. We expect this to change thanks to new, dedicated cyberphysical test beds that are currently being built in research centers around the world in response to increasing governmental interest in cyber security. The focus of these test beds and corresponding research varies from power networks (Edgar et al., 2011) to aviation cyber security (De Cerchio and Riley, 2011) and emergency response infrastructure.

Cyberphysical attacks may be attractive particularly to state-backed terrorism, since they can cause significant physical damage in a more covert manner with less risk to one's own troops and diplomatic status. However, development of exceptionally potent cyber weapons like Stuxnet is unlikely to be within the technical reach of terrorist organizations. To put things into perspective, the scientific team behind the cyber attacks that compromised a production car in 2010 spent two years of world-class academic research to achieve it, and the Stuxnet attack against the Iranian nuclear facility was most probably organized by a technical superpower. For this reason, we do not believe that a cyberphysical attack alone will be used soon by terrorists to cause considerable human loss. It is more likely that a common cyber attack will be used to facilitate a traditional physical attack by disabling cameras and other security systems or to disrupt emergency response by causing an artificial traffic jam and interfering with local communications. In that sense, conventional cyber security mechanisms, such as antivirus software, intrusion detection systems, and firewalls, can protect to a certain extent against cyberphysical attacks too. More important, promoting a culture of cyber hygiene and vigilance, with people and organizations following security policies, using strong passwords, regularly applying security patches, and so forth, would make a cyber terrorist's work more difficult.

Insider Threat Countermeasures

CERT has identified some practical countermeasures against the insider from their Common Sense Guide to Prevention and Detection of Insider Threats (Cappelli et al., 2009).

In addition to analyzing employee behavior in order to develop counterstrategies, there is a body of research around counterproductive work behavior (CWB), which has been recognized as a key factor in helping to identify factors influencing an insider to commit an act, along with the indicators and precursors that lead to those malicious acts (Cummings et al., 2012). CWB covers a variety of behaviors, but specifically encompasses sabotage, stealing, fraud, and vandalism. Sackett (2002) categorized the antecedents of counterproductive work behavior into the following groups: personality, job characteristics, organizational culture, work group characteristics, control systems, and perceived injustices. The primary personality model used in CWB research is the Five Factor Model (Costa and McCrae, 1992), which analyzes people's personality on five dimensions: openness to experience, extraversion, conscientiousness, agreeableness, and emotional stability. Salgado (2002) showed that levels of conscientiousness and agreeableness were significant predictors of workplace deviance.

Computer simulations have been used to simulate insider activity and test different detection mechanisms; however, these cannot be relied on as in the case of financial fraud, only 6% of fraud cases were detected by software and systems and in only 20% of cases transaction, access, and database logs were useful for incident responses. It is therefore vital that all organizations implement policies and procedures covering all aspects of the organization. Sixteen best practice recommendations from CERT (Cappelli et al., 2009) are outlined below:

1. Consider threat s from insiders and business partners in an enterprise-wide risk assessment: A balance needs to be found between trusting employee and protecting assets.
2. Clearly document and consistently enforce policies and controls: Many of the cases analyzed by CERT could have been prevented through this approach.
3. Institute periodic security awareness training for all employees: Employees must understand that policies and procedures exist for a good reason and that they must be enforced.
4. Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process: This includes dealing appropriately with repeated policy violations (which could escalate) and the effect of personal and professional stress indicators.
5. Anticipate and manage negative workplace issues: This should run from pre-employment to termination, consequences of policy violations should be clearly communicated and enforced. Employees should be encouraged to discuss workplace issues without fear of reprisal and terminations should be handled with care as most insider IT attacks occur after termination.
6. Track and secure the physical environment: Access to physical and virtual areas should be restricted to those who need it and all attempted violations and so forth should be logged and monitored.
7. Implement strict password and account management policies and practices: Ensure all activity from an account is attributable and provide an anonymous reporting mechanism to report unauthorized access including social engineering attempts; perform audits regularly to ensure expired accounts are disabled.
8. Enforce separation of duties and least privilege: Train employees and ensure critical functions are divided across employees so collusion is required to carry out an attack. Authorize each individual only for the access they need and be sure to remove access when an individual's job changes.
9. Consider insider threats in the software development life cycle: Ensure an appropriate separation of duties; more insider threats occur during maintenance than system development. Be sure to protect and restrict access to backup systems and so on.
10. Use extra caution with system administrators and technical or privileged users: Technically competent individuals are more likely to use their technical knowledge to exact revenge for perceived wrongs. Employ techniques such as separation of duties, two-man rule for critical system administrator functions, and so forth, should be employed.

11. Implement system change controls: Unauthorized modifications were a key feature of insider compromises so employ stronger change control mechanisms and alerts.
12. Log, monitor, and audit employee online actions: Logging and periodic monitoring will help detect suspicious activity such as the downloading of confidential files.
13. Use layered defense against remote attacks: Insiders are more confident when not scrutinized by coworkers, so restrict access to work-based machines unless external access is required, in which case monitor logs closely.
14. Deactivate computer access following termination: Whether termination was favorable or not, have procedures and policies in place to ensure fast deactivation of accounts and access.
15. Implement secure backup and recovery processes: Ensure secure backup and recovery procedures are in place, single points of failure are eliminated, test processes regularly, and so on.
16. Develop an insider incident response plan: This is required to control the damage. Should an attack occur, it is important that robust evidence is appropriately gathered and not corrupted, and that lessons are learned.

Sandboxing

A sandbox is a security mechanism for separating running components of a system. It was described in 1996 but is now used more and more. It is worth mentioning that HTML5 has a "sandbox" attribute for use with iframes. A sandbox is often used to execute untrusted software from unverified, or even verified, sources. Sandboxing offers prevention of manipulation, reverse-engineering, and reprogramming of systems and components, and is usually a purely software-based protection. A sandbox can be a virtual machine (e.g., VMware based), which has been set to emulate a complete host computer, on which a conventional operating system may boot and run as on actual hardware or something more specialized. In a more advanced scenario multiple sandboxes can take the place of multiple parts of a system targeted by multiple threats. The large majority of Web sites today embed third-party JavaScript (in many cases obfuscated) into their pages, coming from external partners. Most of this is benign and comes from trusted sources, but it is not unlikely that these scripts could come under the control of an attacker. It is now usual practice for security researchers to run such scripts into a sandboxed environment to establish how an attacker can perform unwanted actions safely.

The easiest way to understand how sandboxing can be used is to think of an example where an e-mail sent to your inbox has an executable attached. Assuming that this is a malicious application, once run it could stealthily harm your system and potentially any other systems that you are connected with. This would happen in most cases in the background and would not be noticed until it is too late. To stop such a threat it is imperative to understand how it operates, but this is very difficult to do after it has completed its operation. If, however, we were able to run this attachment in a protected environment then we could examine how it attempts to access and harm our system and carry out a step-by-step dissection of its operation. Traditionally the tamper proofing of programs relied on tamper-resistant hardware, but this is not always easy to use due to cost limitations and complexity of the required underlying configuration (Goldberg et al., 1996). Sandboxing offers a lower cost option to tamper proofing, as long as it is applied properly.

Bug Bounties

In 2004, Mozilla started a bug bounty program. This offered money to anyone who discovered a new bug or security flaw in software. Since that time a number of companies have followed suit. In 2011, Facebook joined the bounty program and reported that the submissions they receive have enabled the social Web site to improve security (Robertson, 2012). Does this make the bad guys turn into "white hat" hackers? This is uncertain, but there is clearly money to be made by discovering bugs but not exploiting them. If money will motivate people to report bugs, and by inference security holes, then this can only help to secure the networks connected to the Internet.

THE FUTURE

In 2000, the threat to SCADA systems used by the North American electric power grid was clearly identified by the U.S. National Institute of Standards and Technology. If this was known then, one must ask why the Stuxnet attacks were able to succeed. The report cited a number of reasons for the increased vulnerability. Nine factors that influence the likelihood of a cyber attack were discussed. The first, and quite significant one mentioned, was the shift to open protocols and standards from proprietary mainframe-based computer control systems. Items 2 to 5 related to factors that increased the likelihood of insider attacks. Items 6 to 9 are of interest to this discussion and are quoted below (Oman, 2000):

1. Increasing incidents of international and domestic terrorism targeted against North America.
2. Increasing number of countries with government sponsored information warfare initiatives.
3. Rapid growth of a computer-literate population.
4. Widespread availability of hacker-tool libraries.

The conclusion was stated by Oman (2000):

> *Increasing reliance on automated control systems with remote access (via phone or internet) and the growing global economy have expanded the number of potential attackers with access to substation controllers and SCADA systems, and therefore magnified the risk electric utilities have from sabotage and espionage.*

This warning has clearly not been heeded.

The United States has tested its capability to respond to cyberwarfare. In 2002 the U.S. Navy conducted an exercise called electronic Pearl Harbor, in which a massive attack on critical infrastructure was simulated. Since then three more "Cyber Storm" exercises have been run. In 2010 a new tool that could shut down the Border Gateway Protocol was launched. This was known as the "kill switch" and was designed to be defensive by shutting down the Internet to prevent a terrorist type cyber attack. This has never been properly tested as at that time it was felt that the disruption to the Internet would be too great (Saalbach, 2012).

The evidence for government-sponsored cyber espionage points to China and Russia. "In an unusually blunt report issued last year by U.S. intelligence agencies, the Obama administration said that massive cyber espionage operations by China and Russia posed a 'significant and growing threat' to U.S. national security, yet other countries often view U.S. complaints as hypocritical given its own cyber activities" (Dyer, 2012). However, if the speculation regarding Stuxnet is true then the United States and Israel may also have a place in this line up.

Ralph Langner (2011) described Stuxnet as a military-grade cyber missile that was used to launch an "all-out cyber strike against the Iranian nuclear program."

> *What Stuxnet represents is a future in which people with the funds will be able to buy an attack like this on the black market. This is now a valid concern.*
>
> ***Lagner in Clayton, 2010***

While there is no doubt that Stuxnet did cause damage to equipment at the Iranian nuclear facilities, it is also clear that the disruption only temporarily delayed Iran's nuclear program, and was quickly repaired.

The United States considers the threat to their military operations from the Chinese very real. The Peoples Liberation Army (PLA) relies on the Chinese commercial sector research and development (R&D) that could be subverted for use in cyber terrorism. Foreign partners share the cost of the R&D of technology. Telecommunications hardware manufacturers based in China provide the PLA with access to cutting edge research. This means that microelectronics manufacture destined for the U.S. military, civilian government, defense, and telecommunications industry are potentially at risk from compromise even before they have been installed or exposed to the Internet. State-sponsored activities target data that do not translate into hard cash. The target is information that could be of use to a foreign power. This could be technical defense information or military data relating to ongoing operations. All United States businesses that have manufacturing partnerships with China are concerned about intellectual property theft, according to a survey conducted in 2011 by the United States–China Business Council. (Krekel et al., 2012)

As we move into an era of smart environments, smart homes, smart devices, and the Internet of Things, the level of interconnectedness of all our systems increases exponentially, and the threat of cyber terrorist attacks bringing these systems down increases at the same level. Perhaps the most worrying aspect of this is the number of developments that are taking place without appropriate regard for security, while critical infrastructure providers and military and financial organizations are now clearly aware of the need for better cyber hygiene and security standards; there are a large number of organizations that are softer targets. The fact that we would regard as anathema an attack on life-support services in hospital systems does not make them safe from attack, and from a cyber terrorist perspective the ensuing outrage would be a desired result.

The growth of hacktivisim, tracing its roots from groups such as the Chaos Computer Club and the Cult of the Dead Cow, and now allied to a number of widespread societal protest organizations, also presents a further problem here. Clearly, within free societies, the rights of citizens to protest and promulgate a point of view different to the government of the day, or the accepted norm, has to be protected. However, the point at which this infringes the rights of others, by damaging or bringing down systems of target organizations or bodies, means these have to be regarded as cyber terrorist activities. If not, they will rapidly become a front for more radical groups utilizing their activities to achieve their own ends, as indeed the Chaos Computer Club did in the late 19080 s (Anderson, 2006). However, the growth of such movements is also evidence of a growing radicalization of youth on a worldwide basis, and there has to be concern that terrorists will seek to establish a route into hacktivist groups, not just as a front for their activities, but also as a recruiting ground for even more radical political and religious ideologies.

So, we face a very uncertain future, with our growing societal dependence on advanced, interconnected technological solutions offering potentially both our greatest advances and our greatest threats. As the famous saying goes "there is no such thing as a free lunch," and the cost for our technological advances has to be paid in ever greater vigilance in the protection and management of our systems, and ever greater awareness by organizations and individuals of the need for good cyber security. Trustwave, in their 2012 Global Security report, identified the two most important security goals for organizations for 2012 as "Education of Employees" and "Identification of Users" (Trustwave, 2012)—we now need to make it happen.

KEY ISSUES

If we are to tackle the issues of cyber terrorism identified in this chapter, then we need to address these from several perspectives as seen in the following sections.

Political/Policy Issues

The issues of cyber terrorism are not limited by national boundaries, nor do they lend themselves to purely local solutions. In considering actions that will be effective, there is a need to address local legislation, to ensure that there is an appropriate response to local events, stunts, or attacks. However, since the majority of the events that we are concerned with have international, or at least cyberspace, links there is clearly a need for concerted and consistent international legislation and action. Clearly, in such a space, there is a need for action from an international coordinating body, to date there has been no such initiative from the United Nations, but NATO has developed tools and capabilities to support international action against cyber terrorism. NATO offers powerful tools in four key areas:

- Operational ability to monitor networks, in particular international Internet traffic
- Intelligence gathering and knowledge of a large number of world arenas, particularly conflict arenas
- Partnership of 69 countries (more than one-third of the world); it tries to integrate existing analytical capabilities to build cyber defenses.
- Operational capabilities, particularly in monitoring and analyzing groups and the impact of Web site information on the radicalization of youth on a worldwide basis

In a worldwide marketplace, where technology companies sell access and expertise in the use of their systems in huge numbers (Cisco issues over a million certifications per year for courses on their technologies), security can only be enforced by similar levels of international cooperation, legislation, and action. The use of NATO systems, and national engagement with the NATO agenda offers some potential for future coordinated international response to cyber terrorism activities.

Research Issues

While any improvement of our cyber defenses would be beneficial, there are a number of technological research challenges with increased focus on cyber terrorism. We have chosen one for each of the four strands of the UK government's Pursue, Prevent,. Protect, Prepare strategy (Home Office, 2011).

Pursue. Pursue refers to activities that can stop terrorist attacks. Most cyber attacks against critical national infrastructure need substantial online research and active probing for a considerable length of time to identify vulnerable components. The technological challenge is to develop early warning mechanisms that monitor a system and its cyber surroundings and spot signs of preparations for future attacks against it. A relevant project that targets specifically botnet attacks has been piloted with the Seattle, Washington, in the United States (DHS, 2011), and the European Commission has recently published an open call for feasibility studies on technologies toward a Europe-wide early warning system.

Prevent. Prevent refers to activities that can stop people from becoming terrorists or supporting terrorism. Research has shown that radicalization is increasingly facilitated through the use of mainstream online platforms, such as social networks, forums, and media-sharing Web sites (Bermingham et al., 2009). The challenge here is to develop technologies that can identify pockets of radicalization and relevant online material without infringing the privacy of individuals.

Protect. Protect refers to activities that strengthen our protection against a terrorist attack. In the context of cyber terrorism this may refer to authentication, detection, or response mechanisms against a range of possible attacks. Of particular interest are technological mechanisms that could identify the intended aim and ultimate target of an attack. For example, denial of service attacks are often launched indiscriminately by amateur hackers without a specific goal, but such an attack may also be the first step that blocks monitoring equipment before a coordinated act of cyber terrorism (Loukas and Oke, 2010). Being able to identify the real target of an attack in real time rather than forensically postmortem would be a significant step forward for the defense against cyber terrorism. Initial work in this area has focused primarily on prediction of the next step of an attack (Zhang et al., 2009).

Prepare. Prepare refers to activities that mitigate the impact of a terrorist attack. Rapid

TABLE 20.1 Cyber Security Framework

Issue	Action	Reference
Organizational policy	Develop a clear and well-defined organizational policy on all aspects of cyber security, and based on identified international standards.	ISO and ANSI standards on data and information security (see the section Policy)
Recruitment	Develop a recruitment policy that explicitly addresses issues of cyber activity, radicalization, and extreme views. Work out how you might exclude a radicalized individual from employment.	Rather worryingly, there are currently no national guidance reports on this issue. Develop your own, based on the models provided in this report.
Training	Create an institutional training program that promotes organizational awareness and support, and explicitly addresses issues of cyber security.	Build a program based on the advice given in the section Training.
Insider threat	Develop institutional policies and practices that address the issues of insider threat and can be validated to provide support for your policies, and management buy-in.	Use the CERT Common Sense Guide to Prevention and Detection of Insider Threats (Cappelli et al., 2009), described in the section Insider Threat Countermeasures.
Software/hardware tools	Ensure that systems are up to date and secure, and develop an update and replacement strategy that fits the organization.	Current virus checkers, packet-sniffers, network pattern identifiers, hardware detection tools, and a myriad of other tools can be utilized. Ensure systems are in keeping with organizational policy.
Cyber hygiene	Training staff and developing policies is insufficient, without the development of a cultural model of cyber hygiene, led from the top. This model has to clearly identify cyber security as a fundamental priority for the organization.	U.S. DoD has identified models of organizational structure and activity that constitute good cyber hygiene. http://www.defense.gov/news/d20110714cyber.pdf
Organizational risk appetite	Organizations have significantly different risk profiles, based on their sphere of operation. Develop a risk profile model and operational plan, based on your organizational requirements, but reflecting the national and international risks that you face. Identify the level of risk that your organization can comfortably accommodate.	Base your work on Neutze (2012)). Cybersecurity in Germany——Toward a Risk-based Approach. AICGS, Johns Hopkins University.

self-healing features have been developed and tested with success against attacks that target the underlying network infrastructure, both wired (Sakellari, 2010) and wireless (Gungor and Hancke, 2009). In such systems, the network infrastructure is able to monitor itself and adapt in a manner that minimizes the impact of the attack. The challenge is to extend the self-healing concept to include all components of the critical national infrastructure, from industrial control equipment to satellite navigation systems and medical devices.

Practitioner Issues

Perhaps the key argument to emerge from this chapter should be a framework of issues and remediating actions that can be undertaken by security practitioners, in any situation or role that can be utilized to address cyber security issues, whatever their source. In keeping with our introductory arguments that addressed the problem of distinguishing the rationale for a cyber attack, at the time of the attack, so the cyber hygiene and countermeasures we introduce should not concern themselves with the rationale for the attack, but rather with preventing, resolving, or mitigating the impact of the attack on the systems involved. Table 20.1 provides a framework, based on the information provided in this chapter, to address issues of cyber security, with specific reference to cyber terrorism, in any organizational system.

Above all else, we should understand and accept that cyber security is a common responsibility that needs to be fundamental to the culture of all organizations and activities utilizing this technology to further their aims; if this is not the case then the cyber terrorists will undoubtedly win.

References

Abrams, M. and Weiss, J., 2007. *Bellingham, Washington, Control System Cyber Security Case Study*, NIST workshop, 15 August.

Anderson, K., 2006. *Hacktivism and Politically Motivated Computer Crime*, http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf
retrieved 01/09/12

Bacon, L., MacKinnon L.. Cesta A., Cortellessa G.. "Developing a Smart Environment for Crisis Management Training". Special edition of the Journal of Ambient Intelligence and Humanized Computing, entitled Smart Environments and Collective Computational Intelligence for Disaster Management. Vol 3, No 2. 2012. DOI: 10.1007/s12652-012-0124-0. Available at: http://www.springerlink.com/content/r586h5354923/?MUD=MP

BBC, 2012. *Flame malware makers send 'suicide' code*, [online]
http://www.bbc.co.uk/news/technology-18365844, June 2012, (Accessed August 2012)

Bellovin, S.M., 2008. *The Insider Attack Problem Nature and Scope*, Insider Attack and Cyber Security - Beyond the Hacker, Series: Advances in Information Security, Vol. 39, 2008, XII, 223, Chapter 1, pp1 ISBN 978-0-387-77321-6

Bermingham, A., Conway, M., McInerney, L., O'Hare, N., & Smeaton, A.F., 2009. *Combining Social Network Analysis and Sentiment Analysis to Explore the Potential for Online Radicalisation*. Proceedings of the International Conference on Advances in Social Network Analysis and Mining, ISBN: 978-0-7695-3689-7, pp. 231 – 236, Athens, Greece, 20 - 22 July.

Bozorgmehr, N., 2012. *Iran Attacks Israel over Cyberattack*, Financial Times, [online] www.ft.com/cms/s/0/cb1326b0-a9a-11e1-9772-00144feabdc0.html, 20th May 2012 (Accessed July 2012)

Bray, H., 2010. *Akamai employee charged with trying to sell secrets to a foreign government*, The Boston Globe, October 6, 2010, http://www.boston.com/business/ticker/2010/10/akamai_employee.html

Byres, E., Eng, P. & Lowe, J., 2004. *The Myths and Facts behind Cyber Security Risks for Industrial Control Systems*, Proceedings of the VDE Congress, VDE Association for Electrical Electronic & Information Technologies (October 2004), [online] http://nealsystems.com/downloads/Myths%20and%20Facts%20for%20Control%20System%20Cyber-security.pdf (Accessed July 2012)

Cappelli, D., 2011. "Insider Threats: Actual Attacks by Current and Former Software Engineers", Presentation by CERT, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org

Cappelli, D., Moore, A., Trzeciak, R. & Shimeall, T., 2009. "Common Sense Guide to Prevention and Detection of insider threats 3rd Edition – version 3.1". Published by CERT, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A. and Sastry, S.S., 2009. *Challenges for Securing Cyber Physical Systems,* Workshop on Future Directions in Cyber-physical Systems Security, DHS, Newark, USA, 22-24 July.

Chen, T.M., 2010. *Stuxnet, the Real Start of Cyber Warefare?*, ieeexplore, Network November/December 2010, Volume: 24 , Issue: 6, Page(s): 2 - 3

Claburn, T., 2008. *Engineer Gets 24 Year Sentence For Trying To Steal Navy Secrets*, InformationWeek, March 25, 2008, http://www.informationweek.com/engineer-gets-24-year-sentence-for-tryin/206905727

Clarke, R. A. & Knake, R., 2010. *Cyber War: The Next Threat to National Security and What to Do About It*, Chapter 2, pp54-55, ISBN 978-0-06-196223-3

Clayton, M., 2010. *Stuxnet malware is 'weapon' out to destroy Iran's Bushehr nuclear plant?,* September 21, 2010, [online] http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant, (Accessed August 2012)

Conway, M., 2011. *Privacy and Security Against Cyberterrorism.* Communications of the ACM, V.54, N.2, pp.26-28, February 2011, ACM.

Costa, P. T., Jr., & McCrae, R. R., 1992. Revised NEO Personality Inventory (NEO PI–R) and NEO Five-Factor Inventory (NEO FFI) professional manual. *Odessa, FL: Psychological Assessment Resources*

Cummings, A., Lewellen, T., McIntire, D., Moore, A. & Trzeciak, R., 2012. "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector". Published by CERT, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org

De Cerchio, R. and Riley, C., 2011. *Aircraft systems cyber security*. 30th IEEE/AIAA Digital Avionics Systems Conference (DASC), pp. 1C3-1 - 1C3-7, Seattle, WA, USA, 16-20 October.

Denning, D.E., 2000. *Cyberterrorism.* Global Dialogue.

Denning, D.E., 2012. *Stuxnet: What Has Changed?*, Future Internet 2012, 4(3), 672-687; [online] http://www.mdpi.com/1999-5903/4/3/672/htm, doi:10.3390/fi4030672, (Accessed August 2012)

DHS, 2011. *Cyber Security Experiments and Pilots*, [online]
http://www.cyber.st.dhs.gov/experimentsandpilots, (Accessed September 2012)

Dignan, L. 2011. *DoD: 24,000 files swiped in March from military contractor systems, for Zero Day*, July 14, 2011, http://www.zdnet.com/blog/security/dod-24000-files-swiped-in-march-from-military-contractor-systems/9026

Dyer, G., Bozorgmehr, N. & Blitz, J., 2012. *Cyberattack Clouds US-Iran Nuclear Talks*, Financial Times, 1st June 2012, [online] www.ft.com/cms/s/0/08b8b06e-ac04-11e1-923a-00144feabdc0.html#ixzz207yv40FY, (Accessed August 2012)

Edgar, T., Manz, D. and Carroll, T., 2011. *Towards an experimental testbed facility for cyber-physical security research*. In Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '11),Frederick T. Sheldon, Robert Abercrombie, and Axel Krings (Eds.). ACM, New York, NY, USA, Article 53, 12 - 14 October.

Falliere, N., Murchu, L.O. & Chien, E., 2011. *W32.Stuxnet Dossier, Version 1.4 (February 2011)*, White paper, [online] http://www.symantec.com/security_response/whitepapers.jsp (Accessed July 2012)

Farwell, J.P. & Rohozinski, R., 2011. *Stuxnet and the Future of Cyber Wa*r, Survival: Global Politics and Strategy, Volume 53, Issue 1, pp 23-40, 2011, DOI:10.1080/00396338.2011.555586, 28 Jan 2011 [online] http://www.tandfonline.com/doi/abs/10.1080/00396338.2011.555586, (Accessed August 2012)

FBI, 2009. *Arlington Security Guard Arrested on Federal Charges for Hacking into Hospital's Computer System*, FBI Press release, 30 June. Available at: <http://www.fbi.gov/dallas/press-releases/2009/dl063009.htm>

Former U.S. Navy Sailor, 2009. *Former U.S. Navy Sailor Sentenced in Terror Case*, Posted: April 3, 2009, http://www.adl.org/main_Terrorism/abujihaad_sentenced.htm, Accessed 08/09/2012

Framingham, M.A., 2007. "Overconfidence Is Pervasive Amongst Security Professionals" 2007 E-Crime Watch Survey^{TM} conducted by the United States Secret Service, the CERT® Coordination Center (CERT/CC), Microsoft, and CSO Magazine.

Garrison, L. & Grand, M., 2001. *Cyberterrorism: An evolving concept.* NIPC Highlights.

Get Safe Online "UK Internet Security: State of the Nation Report", November 2011 http://www.getsafeonline.org/media/GSOL_2011_Annual_Report.pdf last checked 28/7/12.

Gleick, P.H., 2006. *Water and Terrorism*. Water Policy 8: 481-503.

Goldberg, I., Wagner, D., Thomas, R. & Brewer, E., 1996. *A Secure Environment for Untrusted Helper Applications (Confining the Wily Hacker)*. Proceedings of the Sixth USENIX UNIX Security Symposium.

Gorman, S., 2009. *Electricity Grid in U.S. Penetrated By Spies*. Wall Street Journal, Technology, 4 April. Available at: < http://online.wsj.com/article/SB123914805204099085.html>

Gorman, S., Dreazen, Y., and Cole, A., 2009. *Insurgents Hack U.S. Drones,* Wall Street Journal, 17 December.

Gostev, A., 2012. *The Flame: Questions and Answers*, May 2012 [online] https://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers, (Accessed August 2012)

Greengard, S., 2010. *The New Face of War.* Communications of the ACM, V.53, N.12, pp.20-22, December 2010, ACM.

Gungor, V.C. & Hancke, G.P., 2009. "Industrial Wireless Sensor Networks: Challenges, Design Principles, and Technical Approaches", IEEE Transactions on Industrial Electronics, 56(10), pp. 4258-4265, October.

Halperin, D., Heydt-Benjamin, T.S., Fu, K., Kohno, T. & Maisel, W.H., 2008. *Security and Privacy of Implantable Medical Devices. IEEE Pervasive Computing*, Vol. 7(1), pp. 30-39, January.

Home Office, 2011. *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, [online] http://www.homeoffice.gov.uk/counter-terrorism/uk-counter-terrorism-strat, July 2011 (Accessed September 2012)

InfoSecurity, 2010. *SCADA systems can be located via public search engine says CERT*, [online] http://www.infosecurity-magazine.com/view/13690/scada-systems-can-be-located-via-public-search-engine-says-cert, 03 November 2010, (Accessed July 2012)

ISF, 2011. *Information Security Governance: Raising the Game*. Informational document ISF 11 ISG (Marketing) 2011, Information Security Forum Limited

Jones, J. & Averbeck, R., 2011. "The 3 types of insider threat", CSO, May 2011. http://www.csoonline.com/article/682205/the-3-types-of-insider-threat?page=1 (Accessed August 2012)

Keeney, M.M., Kowalski, E.F., Cappelli, D.M., Moore, A.P., Shimeall, T.J. & Rogers, S.N., 2005. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors*, Joint SEI and U.S. Secret Service Report, Section 2, pp 11, May 2005. [online] http://www.cert.org/archive/pdf/insidercross051105.pdf (Accessed August 2012)

Kim, W., Jeong, O-R., Kim, C. & So, J., 2009. *The dark side of the Internet: Attacks, costs and responses*, Special Issue of WISE 2009 - Web Information Systems Engineering,
Information Systems, Volume 36, Issue 3, May 2011, Pages 675–705

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H. and Savage, S., 2010. *Experimental Security Analysis of a Modern Automobile.* Proceedings of the IEEE Symposium on Security and Privacy, pp. 447-462, Oakland, USA, May.

Krekel, B., Adams, P. & Bakos, G., 2012. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, March 2012, [online] http://www.uscc.gov/, (Accessed August 2012)

Langner, R., 2011. *Cracking Stuxnet, a 21st-century cyber weapon* - TED [online] www.ted.com/.../ralph_langner_cracking_stuxnet_a_2...1, Apr 2011 (Accessed Feb 2012)

Lee, D., 2012. *Flame: Attackers 'sought confidential Iran data'*, [online] http://www.bbc.co.uk/news/technology-18324234, June 2012 (Accessed August 2012)

Leveson, N.G. and Turner, *C.S.*, 1993. *An investigation of the Therac-25 accidents*. IEEE Computer, Vol. 26(7), pp. 18-41, July.

Lewis, J.A., 2005. *Computer Espionage, Titan Rain, and China*. Center for
Strategic and International Studies - Technology and Public Policy Program. December 2005

Loukas, G. & Oke, G., 2010. *Protection against Denial of Service Attacks: A Survey.* Computer Journal, 53(7), pp. 1020-1037, BCS.

Luiijfa, E., Alib, M. & Zielstrab, A., 2011. *Assessing and improving SCADA security in the Dutch drinking water sector*, International Journal of Critical Infrastructure Protection, Volume 4, Issues 3–4, December 2011, Pages 124–134

Lumension. 2011. What Every CEO should know about IT Security. http://www.lumension.com/eBook---What-Every-CEO-Should-Know-About-IT-Security.aspx last checked 28/7/12.

Mahony, E. H., 2010. *European Court Blocks Extradition Of Terror Suspects To Connecticut*, July 08, 2010

Matrosov, A., Rodionov, E. & Harley, D., 2011. *Win32/Duqu: It's A Date*, October 26, 2011, [online] http://blog.eset.com/2011/10/25/win32duqu-it%E2%80%99s-a-date, (Accessed July 2012)

Matrosov, A. & Rodionov, E., 2012. *Flame, Duqu and Stuxnet: in-depth code analysis of mssecmgr.ocx*, [online] http://blog.eset.com/2012/07/20/flame-in-depth-code-analysis-of-mssecmgr-ocx#.UBvIFiQdovg.email, July 20, 2012 (Accessed July 2012)

Matrosov, A., Rodionov, E., Harley, D. & Malcho, E., 2012. *Stuxnet Under the Microscope*, Revision 1.31, [online]
http://go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf,
(Accessed July 2012)

Moore, A., Cappelli, D., & Trzeciak, R., 2008. The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures (CMU/SEI-2008-TR-009). The Software Engineering Institute, Carnegie Mellon University
website: http://www.sei.cmu.edu/library/abstracts/reports/08tr009.cfm, Accessed September 2012

Moore, A., Hanley, M. & Mundle, D., 2012. “A Pattern for increased Monitoring for Intellectual Property Theft by Departing Insiders”. Published by CERT, Software Engineering Institute, Carnegie Mellon University, http://www.cert.org

Moscaritolo, A., 2010. *Stuxnet should serve as wake-up call, say experts,* SC Magazine > News > September 28, 2010, [online] (Accessed July 2012)

Naraine, R., 2010. *Shodan search exposes insecure SCADA systems*, [online] http://www.zdnet.com/blog/security/shodan-search-exposes-insecure-scada-systems/7611, November 2010 (Accessed August 2012)

O'Harrow, R. Jr., 2012. *Cyber search engine Shodan exposes industrial control systems to new risks*, [online] http://smartgridsecurity.blogspot.co.uk/2012/06/shodan-again-search-engine-you-need-to.html, June 2012 (Accessed August 2012)

Oman, P., Schweitzer, E.O. & Frincke, D., 2000. *Concerns About Intrusions into Remotely Accessible Substation Controllers and SCADA Systems*, 2000, [online] http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.20.6519, (Accessed August 2012)

Pfleeger, C. P., 2008. *Reflections on the Insider Threat, Insider Attack and Cyber Security*, Advances in Information Security, 2008, Volume 39, 5-16, DOI: 10.1007/978-0-387-77322-3_2

Pollitt, M.M., 2003. *Cyberterrorism – Fact or Fancy?* FBI Laboratory, http://www.cs.georgetown.edu/~denning/infosec/pollitt.html, Accessed 01/09/12.

Reed, T.C., 2004. *At the Abyss: An Insider's History of the Cold War*. ISBN 0-89141-821-0, Presidio Press, 15 April.

Robertson, J., 2012. *Facebook Widens 'Bug Bounty' Program to Combat Internal Breaches*
Jul 26, 2012, [online] http://www.bloomberg.com/news/2012-07-26/facebook-widens-bug-bounty-program-to-combat-internal-breaches.html, (Accessed August 2012)

Ruppert, B., 2009. *Protecting Against Insider Attacks*, Reading Room SANs, www.sans.org/reading_room/whitepapers/incident/protecting-insider-attacks_33168

Saalbach, K., 2012. *Cyber war Methods and Practice Version 4.0* – 25 Mar 2012, [online] http://ebookbrowse.com/saalbach-cyberwar-methods-and-practice-pdf-d47450965 (Accessed July 2012)

Sackett, P. R., 2002. “The Structure of Counterproductive Work Behaviors: Dimensionality and Relationships with Facets of Job Performance”. International Journal of Selection and Assessment, 10: 5–11.doi: 10.1111/1468-2389.00189
http://onlinelibrary.wiley.com/doi/10.1111/1468-2389.00189/abstract.

Sakellari, G., 2010. "The Cognitive Packet Network: A Survey", Computer Journal, 53(3), pp. 268-279, doi: 10.1093/comjnl/bxp053, BCS.

Salem, M.B., Hershkop, S. & Stolfo, S.J., 2008. *A Survey of Insider Attack Detection Research,* Insider Attack and Cyber Security - Beyond the Hacker, Series: Advances in Information Security, Vol. 39, 2008, XII, 223, Chapter 5, pp69 ISBN 978-0-387-77321-6

Salgado, J. F., 2002. "The Big Five Personality Dimensions and Counterproductive Behaviors". International Journal of Selection and Assessment, 10: 117–125. doi: 10.1111/1468-2389.00198
http://onlinelibrary.wiley.com/doi/10.1111/1468-2389.00198/abstract

Scherer, R., 2009. *Why did it take so long to catch spy for China?*, Christian Science Monitor, July 18, 2009, http://www.csmonitor.com/USA/Justice/2009/0718/p05s01-usju.html

Sood, A.K. & Enbody, R., 2012. *Targeted Cyber Attacks - A Superset of Advanced Persistent Threats,* IEEE Security & Privacy, ISSN: 1540-7993 [online]
DOI: http://doi.ieeecomputersociety.org/10.1109/MSP.2012.90 (Accessed August 2012)

Stamos, A., 2010. *"Aurora" Response Recommendations*, February 17th, 2010[online]
https://www.isecpartners.com/blog/2010/3/1/aurora-response-paper-released.html, (Accessed August 2012)

Symantec, 2011. *W32.Duqu The precursor to the next Stuxnet, Version 1.4* (November 23, 2011), [online] http://www.symantec.com/security_response/whitepapers.jsp (Accessed July 2012)

Ten, C.W., Manimaran, G. & Liu, C.C., 2010. *Cybersecurity for Critical Infrastructures: Attack and Defense Modeling*, IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans, July 2010, Volume: 40 , Issue: 4, Page(s): 853 – 865
DOI : 10.1109/TSMCA.2010.2048028

Thornburgh, N., 2005. *The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)*, Aug. 29, 2005 [online]
http://www.time.com/time/magazine/article/0,9171,1098961,00.html (Accessed August 2012)

Trustwave, 2012. *2012 Global Security Report.* https://www.trustwave.com (Accessed 01/09/12)

Turk, R.J., 2005. *Cyber Incidents Involving Control Systems*. US-CERT Control Systems Security Center, Idaho Falls, Idaho 83415, INL/EXT-05-00671, October.

Verisign, 2012. *iDefence Cyber Threats and Trends report 2012*, Verisign iDefense Security Intelligence Services White Paper.

Weiss, G.W., 1996. *The Farewell Dossier: Duping the Soviets*. CSI Publications, Studies in Intelligence. . Available at: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/96unclass/farewell.htm>.

Whitney, L., 2012. *Flame Virus can Hijack PCs by Spoofing Windows Updates*, June 2012, [online] http://news.cnet.com/8301-10805_3-57447277-75/flame-virus-can-hijack-pcs-by-spoofing-windows-update/, (Accessed August 2012)
Wilber, D. Q. and Sheridan, M. B., 2009. *State Dept. Retiree, Wife Accused of Spying for Cuba for Decades*, The Washington Post, June 6, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/06/05/AR2009060502359.html?hpid=topnews

Zhang, Q., Man, D. & Yang, W., 2009. *Using HMM for Intent Recognition in Cyber Security Situation Awareness.* Proceedings of the Second International Symposium on Knowledge Acquisition and Modeling, ISBN: 978-0-7695-3689-7, pp. 231 – 236, Wuhan, China, 30 November – 1 December.