

CHAPTER 10

Emerging Technologies and the Human Rights Challenge of Rapidly Expanding State Surveillance Capacities

Mohammad Dastbaz, Edward Halpin, Steve Wright

They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety...

Benjamin Franklin (1759)

INTRODUCTION

We live in the shadow of rapidly developing and converging technologies, from the humble beginnings when the Internet and the World Wide Web emerged, out of developing network technologies and hypertext, to today's connected world where from the comfort of our laptops we have access to terabytes of data that up until recently were reserved exclusively for large corporations. We are living in the era of “smart devices” that we trust with our most intimate personal and financial information and carry with us wherever we go. The integration and embedding of these technologies in our daily routines are such that life without our smart devices is unimaginable, and a world without them looks something like a postapocalyptic Hollywood blockbuster.

The use of these technologies informs every dimension of modern lives. From learning and training, to commerce and re-engineering our business processes, these tools facilitate communication between governments and their citizens and even the way we are made aware of social and political issues. Yet we are only exploring the tip of the iceberg in terms of the width and breadth of second- and third-order impacts from the application of these technologies.

Typically such rapid growth and advancements in mobile information communication technology (mICT) and its “uses and misuse” have received wide and varied treatment in the literature. Perhaps one of the current, controversial, and most talked about aspects of the use or misuse is the unprecedented application of these technologies in state surveillance versus citizens' rights in the emerging world.

Jacques Ellul, in *The Technological Society* (Ellul, 1964), considered the emergence of technology philosophically before concluding “..... What good is it to pose questions of motives? Of Why? All that must be the work of some miserable intellectual who balks at technological progress.” While we do not balk at technological progress of the expanding state surveillance technologies in this chapter, we do try to pose questions of motive and of “why?”.

There is a well-trodden history to the development of the surveillance capacities within the state; however, for the purposes of this chapter we will attempt to look at what might be described as the new era of intelligence gathering and security. It might be easy to pick the post-9/11 period as the significant point of change, although the origins of the response to 9/11 pre-existed the tragedy that occurred. A large range of public domain U.S. military thinking predates 9/11 and shows the need for, and use of, advanced information-gathering techniques, including Vision for 2020 (United States Space Command, 1997), and Information Operations (U.S. Air Force, 1998). In Information Operations the question of why is answered clearly and resolutely:

Today, information systems are part of larger information infrastructures. These infrastructures link individual information systems through numerous and redundant direct and indirect paths, including space-based systems. There is a growing information infrastructure that transcends industry, the media, and the military and includes both government and nongovernment entities. It is characterized by a merging of civilian and military information networks and technologies. Collecting, processing, and disseminating information by individuals and organizations comprise an important human dynamic, which is an integral part of the information infrastructure.

U.S. Air Force, 1998

In a special issue of *TIME* magazine (Thornburgh, 2005), Massimo Calabresi poses an interesting thought about the nature of the technology and how it's used these days. He stated:

If anybody wanted to develop a global system for tracking human beings and collecting information about them, it would look a lot like the digital mobile device networks. It knows where you are, and—the more you text, tweet, shop, take pictures and navigate your surroundings using a smart phone—it knows an awful lot about what you are doing...

He goes on to highlight the growing issue of U.S. federal and local law enforcement agencies requesting mobile providers to hand over their data for various requests. According to Calabresi, such cases are now very common.

Ed Markey, major U.S. cell carrier and provider, states that they received 1.3 million requests for cell-phone tracking data from federal, state, and local law enforcement officials in 2011. This, compared to the 3,000 wiretap warrants issued in the United States in 2010, shows the growing problems and issues related to the private and personal data held by mobile carriers.

While there could be justifications made about the use of these technologies and data in tracking criminals and bringing them to justice, there is very little doubt that such data can also be easily used to violate individual's rights and freedoms. The images of societies where the state is constantly tracking its citizen's personal and quite often very private data can be used to change people's behavior is nothing short of the 1984 Orwellian nightmarish society where everybody is watched by “big brother.” Yet our current surveillance capability so far exceeds Orwell's nightmare dystopia; in 1984 there were no computers, no “dataveillance,” no geolocation, and no communication, command, and control based on algorithmic rather than human intervention.

A BRIEF SURVEY OF EMERGING SURVEILLANCE TECHNOLOGIES

While it is outside the scope of this chapter to review all emerging surveillance technologies, we felt it would be appropriate to highlight some of the emerging key technologies.

Naomi Wolf (2012), in an article in the *Guardian* (August 15, 2012) titled “The New Totalitarianism of Surveillance Technology,” quoting a software engineer from her Facebook community, highlights an interesting case on surveillance technologies that affects our day-to-day activities. She stated that, while visiting Disneyland with his partner, the software engineer goes on a number of rides and later notices that the theme park is offering him photos of him and his partner, with his credit card information already linked to the offer. He is baffled as he had not entered his name or any other information into anything in the theme park or indicated that he was interested in photos or had informed anybody from the theme park who his partner was. He then comments that on closer inspection this scenario could have only happened if Disney was using advanced facial recognition technology. He then went on to claim that Disney had recently shared data from facial recognition technology with the U.S. Army. Wolf (2012) further stated that News21 supported by the Carnegie and Knight foundations recently reported that the Disney sites are indeed controlled by the same facial recognition software in which the U.S. military is interested.

Biometric Technologies

Biometric technologies generally refer to the use of technology to identify a person based on some aspect of their biology. Fingerprint recognition is one of the first and original biometric technologies that have been grouped loosely under digital forensics. With the ever-growing number of video surveillance cameras mushrooming in large cities, the use of the data captured by these cameras has been at the center of a number of privacy and human rights storms. Following the 9/11 terrorist attack, the use of facial recognition, especially in crowded places, as a means of detecting possible threats has been debated widely. The way the technology works is straightforward. CCTVs in streets, public places, and office buildings record images 24/7, sophisticated algorithms then carry out a matching exercise with an existing database of images of potential “villains” or

“targets.” A match will trigger enhanced surveillance and possible future and further action. For the system to be effective, the matching database should be as wide and comprehensive as possible. It is not surprising to note that to put such a database together security agencies never (at least we cannot identify any evidence) consult or seek permission to keep people's records in their data centers. Furthermore routine phishing activities through the Internet and social networks provide a fertile ground for not only a simple one-dimensional set of data (photos and other personal data) but potentially three-dimensional datasets of associated friends, links, habits, and quite often current location. In early August 2012, Michael Bloomberg, Mayor of New York, and Ray Kelly (NYPD Commissioner) unveiled a new police surveillance infrastructure developed by Microsoft called the Domain Awareness System, which links existing police databases with live video feeds from a variety of different sources.

Furthermore, according to a Homeland Security newswire in the United States, billions of dollars are being invested in the development of various biometric technologies capable of identifying anyone anywhere in the world. These include iris-scanning and foot-scanning technology, and voice pattern ID, as well as facial recognition technologies (Wolf, 2012).

Location-based and Tracking Technologies

In a recent visit to Prague, in the city's main square, I decided to find a restaurant called Bily Konichcek, about which I had read good reviews. After several attempts at finding the restaurant through asking people failed, I decided to use Google Map to find it. The search result was quite interesting. Not only did Google map find the restaurant for me, it also found a person called Bily Konichcek, which was within the search parameters I had given. Was Bily Konichcek aware that his location was being broadcast to a total stranger looking for a restaurant? I doubt it.

Wang and Loui (2009) defined the working of the GPS systems as using constellations of GPS

satellites that orbit the earth. These satellites then broadcast signals on radio frequencies that consist of the time of the message and orbital information. A receiver measures the transit times of messages from four satellites to determine its distance from each satellite, and thereby calculate its location. They further noted that

In the United States, law enforcement officials use GPS technology to track criminal suspects and parolees without their awareness. For example, they may attach to the individual's car a device such as Trackstick,™ which is a GPS data logger integrated with GoogleEarth. Law enforcement officials argue that GPS devices fall outside the scope of laws regulating wiretaps and similar forms of electronic surveillance because they do not record conversations.

Wang and Loui (2009)

As well as GPS systems, we also now have a Global System for Mobile Communications (GSM), which provides a wealth of data including locations to mobile operators and providers. For example, GSM signals transmitted from mobile devices can be used to monitor a traveling car and its passengers.

Through-the-wall Surveillance Technology

In the early years following the turn of the millennium, military and law enforcement agencies began developing technologies that were capable of detecting human movements and positioning behind enclosed spaces and solid walls. The technology, loosely termed through-the-wall surveillance, used radar technologies aimed at providing vital information to security forces dealing with difficult emergency situations. The more peaceful version of the same technology can be usefully deployed in natural disasters to detect victims of earthquakes buried beneath rubble. The main drive behind the development of this technology was for “safe” surveillance of potential criminals and threats to state security. In defining the possible application areas of such technologies, each year correctional and law enforcement

officers are injured because they lack the ability to detect and track offenders through building walls. While the early versions of this technology were not able to map building or room interiors or could not tell how many walls are between the user and monitor, the later development of the same idea now provides quiet sophisticated three-dimensional mapping of buildings using building blueprints.

Mobile Surveillance and Wireless Sensor Systems

Tseng et al. (2005) explored the possibility of incorporating the environment sensing capabilities of wireless sensors with video-based surveillance systems. The result is an Integrated Mobile Surveillance and Wireless Sensor System (iMouse) capable of detecting and analyzing unusual events.

The proposers of this system believed that such a surveillance system could enhance human life in areas such as healthcare, building monitoring, and home security, but clearly one can see security agencies and the military could also be interested in the mobile capabilities of such sensors, which are versatile and battery operated.

Virtual Reality, Surveillance, and Security Systems

Another technology having a major impact in the development of surveillance and security applications is virtual reality (VR). VR technology is used to provide a state-of-the-art training environment for key decision makers and people dealing with national emergencies, is capable of receiving data from a variety of different sources (including GPS, live news feed, and direct agent communications; see FP7 PANDORA project, Dastbaz and Cesta, 2011), and has been used to create surveillance and security systems.

Ott et al. (2006) stated that

Virtual Reality (VR) can become a key component of future surveillance and security systems, being used in a number of tasks such as: teleoperation of the actual

data acquisition systems (cameras, vehicles, etc); providing multimodal interfaces for control rooms where information is analyzed; and empowering on-field agents with multimedia information to ease their tasks of localizing problematic zones, etc.

According to Ott et al. (2006), a general surveillance and security system typically has three key components: data acquisition, information analysis, and on-field operation.

Typically a VR device can be used to improve the ergonomics of existing systems. Today, visualization systems for video surveillance based on an augmented virtual environment (AVE) are also an important topic. AVE fuses dynamic imagery with three-dimensional models in a real-time display to help observers comprehend multiple streams of temporal data and imagery from arbitrary views of the scene.

NONGOVERNMENTAL ORGANIZATION POLICY RESEARCH: INTERVENTION AND ACCOUNTABILITY ON SURVEILLANCE

Over the last 30 years, surveillance studies has become a respectable academic field with a *Handbook of Surveillance* studies published by Routledge in 2012 (Ball et al., 2012). There is also a worldwide security and surveillance network run by academics to exchange views, sponsor publications, organize conferences, and build a critical community of academics to understand this burgeoning field and its associated industries (<http://www.surveillance-studies.net/>).

While academics ponder the adequacy of legally controlling the surveillance of mICT and associated proliferation, a number of nongovernmental organizations (NGOs) have systematically studied the changing state of the art and the need for intervention and if and when this goes beyond the limits of the law. Early work was accomplished by the British Society for Social Responsibility in Science, which controversially viewed much of what was being

developed as a “technology of political control.” This perspective was taken up by the Omega Foundation in a policy report titled *An Appraisal of the Technology of Political Control* for the European Parliament.

This Science and Technology Options Assessment (STOA) report called for a European Commission (EC)-wide oversight of interception procedures and activities after revealing that millions of e-mails, telephone calls, and faxes were routinely intercepted each hour by the secretive U.S. National Security Agency—often in direct contravention of privacy guarantees enshrined in individual Member State's national legislation. This exposure of a secretive global telecommunications system, known as Echelon, generated worldwide awareness of a new capability of mICT interception. The STOA report also revealed a new European Union (EU)–Federal Bureau of Investigation surveillance agreement researched by the NGO Statewatch. This plan was introduced to force service providers to make all of their traffic transparent via a document known as “the requirements,” largely demanded because privatization had led to piecemeal evolution of systems that were opaque to the authorities. These measures were adopted by “written procedure”—literally 15 faxes sent to Member States—without any parliamentary scrutiny or debate and adopted “on the nod” by the EU Fisheries Council on December 20, 1996.

Since then, the EC has funded a number of research projects studying security and surveillance technologies. These include a number of projects concerned with taxonomic classification of surveillance systems such as the Stakeholders Platform For Supply Chain Mapping, Market Condition Analysis and Technologies Opportunities (STACCATO); Security technology Active Watch (STRAW); Supporting Fundamental Rights, Privacy and Ethics in Surveillance Technologies (SAPIENT); Security Impact Assessment Measures (SIAM); and Public Perception of Security and Privacy: Assessing Knowledge, Collecting Evidence, Translating Research into Action (PACT; see <http://www.projectpact.eu/>).

These substantial research projects are assembling a significant body of knowledge regarding the state of the art as well as policy impacts on areas such as privacy and human rights. However, the recent experience of the EU security research expenditure has suggested that there has been a process of bureaucratic capture by the military, industrial, security, and media entertainment industrial complex (Statewatch, 2009). In response to such perceptions, the EC set up a Societal Impacts of Security Panel that looked to create measures that would rebalance the mutual dependency of the triangle of research investments in security, freedom, and justice. This was a useful exercise since the sunset report from that panel made a recommendation, which has been largely accepted, that all future EU-funded research on security must have a core element devoted to a formal study of its anticipated societal impacts.

Some of these EC-funded security projects explore the different perceptions between experts, stakeholders, and citizens on such matters as the potential trade-offs of privacy and security (e.g., PACT). But is this merely an exercise in liberalism in which security is seen as one set of competing values that must be fairly balanced against others?

Are the checks and balances adequate? For example, there may be a formal body charged with ensuring surveillance activity operates within the rule of law, but if that body has a workload that massively exceeds its resource capacity, oversight becomes tokenistic rather than effective. How has this revolution in surveillance come about so quickly that the evolution of capacity appears to have outstripped controls?

Digitalization and Dataveillance

The need to increase bureaucratic efficiency necessitated by shrinking budgets proved a powerful imperative for improved identification and monitoring of individuals. Fingerprints, ID cards, data matching, and other privacy-invading techniques were originally fielded on populations

with little political power such as immigrants, welfare recipients, criminals, and members of the military.

Older surveillance systems were slow, used film or tape, and were static. Now the content of the surveillance can be transmitted to other places by microwave links or through the Web. Many of the innovations owe their existence to the rapid increases in processing power now possible with digital technology. Modern systems can “piggyback” on other forms of telecommunications infrastructure such as the mobile phone network and associate satellites.

By the 1980s new forms of electronic surveillance were emerging, many of these directed toward the automation of telecommunications interception. The interconnection of visual and audio surveillance into networks of storage and data processing has enabled a new era of mass supervision and tracking, so-called dataveillance, initially pioneered in the UK.

We are only at the beginning of this era, but since it is happening within a specific sociopolitical context, that is, “the war on terror,” we can anticipate that military communication command and control systems will become amalgamated with civilian systems of monitoring and management.

Surveillance Flows and Dataveillance Networks

Surveillance versus privacy is not some zero sum game, it is more complex than that. Modern surveillance no longer just stakes out individuals but looks at “flows” of information; in many senses we are always shadowed by a body of data that somehow “represents us,” not all of which we can check for veracity.

Network is the operative term here since systems can be requested to record, “hunt,” track, and alert. Emerging ID systems, for example, are networks reliant on more than one mode of tracking technology, such as facial recognition with an electronic card. This is already leading to a massive accumulation of personal data that cannot be kept secure. It is

also leading to the evolution of a powerful architecture of surveillance that can sense, record, and identify specific individuals entering a designated surveillance zone. Privacy and surveillance now exist in a world of data flows, with modern surveillance offering increasing capacities to track mobility, whether it is physical or virtual.

Algorithmic Surveillance and Geolocation

Introna and Wood (2004) argued that when surveillance is digitized there is a step change in power; for example, so-called algorithmic surveillance, which has some intelligent reasoning and learning attributes. Algorithmic surveillance can be defined as the move toward smart semi-intelligent monitoring both at borders, on the Internet at strategic gateways and highways, and via mobile phones. There is a link between information gathering and assembly from information to intelligence, especially in times of national crisis such as the war against terror.

The software or mathematical instructions or “algorithm” enables the technology to scan unobtrusively without any need for cooperation from the target. Such algorithmic systems use neural networks to discover otherwise hidden patterns. Wikipedia defines a neural network as nonlinear statistical data modeling or decision-making tools. They can be used to model complex relationships between inputs and outputs in order to find patterns in data.

Graham and Wood (2003) argued that the silent nature of this technology makes it difficult for society to scrutinize it. Such lack of accountability enables the micro politics of surveillance to become pervasive. Although we have extensive community consultation and impact studies for motorway development, this is not done when CCTV systems are installed, and customers of mobile phones asked their permission to collect geolocation data. Every mobile phone routinely generates a host of data including its approximate geographical location. Mobile phone location

data are typically based on the nearest mast from which the handset receives a network signal. Location data, together with other data about communications, are stored by mobile phone service providers for billing and legal purposes (Gorra, 2007). These data are used regularly in court cases and by the intelligence services, because they provide a rich picture about a mobile phone user's actions.

Accountability

The Surveillance Studies Network has raised concerns that the routine tracking and information-gathering mechanisms used in today's society are often not obvious to citizens. The complexity of the interconnections between surveillance devices and processing capacities makes it difficult to ask meaningful questions to the public about these capacities if only individual components of just some of the technologies are explored.

This makes it important to incorporate checks and safeguards when collecting data to ensure accountability. The retention of mobile phone communications data especially bears the potential for identifying patterns in the collected data. It is possible to analyze the behavior of particular groups of people or of mobile phone users located in a particular area without identifying specific individuals (Marx, 2002). A key question is the extent to which bodies charged with the responsibility to monitor the monitors have the access, staff, and resources to practically oversee such huge surveillance enterprises.

These capacities and their potential role and functions can only be truly comprehended as systems within an entire political and social context. For example, Western companies provided mobile surveillance technologies used to track down dissidents during the Arab Spring, including Syria (<http://topics.bloomberg.com/wired-for-repression/>).

President Obama recently introduced new export controls to prevent such proliferation of U.S. surveillance technologies to authoritarian regimes in the future, but EU countries have continued to do so. Companies such as ISS

bring together suppliers and buyers at specialist conferences/expos such as that in Prague in June 2012. Are EU citizens comfortable with such prioritization of profit over principle? NGO's like Privacy International have made it a priority to gather evidence to link security company's mICT and related training with subsequent human rights abuse. They are currently saying companies that supply surveillance technologies to the likes of Syria must cease or face legal action.

NGO's such as Witness are now using satellite technology to monitor suspected human rights violations. Similarly, some protestors are beginning to adopt cheap unmanned aerial vehicle surveillance cameras to monitor community safety when riot squads are at work. What are the implications of such mICT-driven approaches to protect human rights defenders? What if they initiate response and counter-response arms races between the controllers and those who challenge that control? The next section explores some of the core issues in light of recent experience, especially during the so-called Arab Spring.

HUMAN RIGHTS AND SURVEILLANCE TECHNOLOGIES

Lannon and Halpin (2012) discussed the application of technology in the human rights world in *Human Rights and Information Communication Technologies: Trends and Consequences of Use* describing the innovation that has transformed the use of ICT as

...(having) helped enormously to move the promotion and protection of human rights forward...They (ICT) have transformed the capacity of the human rights community to highlight human rights abuse and to advocate for causes and victims of oppression. They have made it easier to access and share information, to facilitate human rights data aggregation and analysis, to offer new tactical approaches to campaigning, and to precipitate real-world activities ranging from local demonstration to inter-governmental agency lobbying.

In 2000 there was no YouTube for video sharing. Social networking with Facebook or Twitter was still half a decade away, and blogging had not yet become mainstream. Web mashups were nonexistent, and wireless devices were still only emerging technologies. The World Wide Web was still relatively young at that time, and was all about read-only content and hyperlinked Web pages designed to be read by humans. The bursting of the dot com bubble in 2001 led many people to believe that this Web was overhyped, but organizations like O'Reilly Media (formerly O'Reilly & Associates) had a different view. They recognized that the Web was becoming more important than ever and exciting new applications and sites were popping up with surprising regularity (O'Reilly, 2005). To highlight these innovations they organized a conference in 2004 at which the term Web 2.0 was born.

Web 2.0 applications that facilitate participatory online information sharing and collaboration have transformed the human rights community. Blogging in particular has become a vitally important tool for individuals and organizations that want to keep the public or the human rights community informed about human rights issues. Very often the first people to present evidence of human rights violations publicly today are “frontline” bloggers who are either witnessing and documenting the violations themselves or posting someone else's information. Aggregation bloggers like Global Voices Online (<http://globalvoicesonline.org>) amplify this information so that it is more accessible. International human rights NGOs and libraries also publish and translate selected blogs, and sometimes editorialize what they consider to be the “good sources”.

The value of Twitter, Facebook, YouTube, and other social media tools of the Web 2.0 era was demonstrated during the pro-democracy protests in Iran in June 2009 and in the Arab Spring uprisings in Tunisia and Egypt in January 2011. Real-time reports on what was happening on the streets went out on these social networks, as did calls to rally. Poignant images of

suffering—a video recording of the death of Neda Agha-Soltan who was shot on her way to the election protests in Iran, or photographs of Mohamed Bouazizi, a street vendor who burned himself to death to protest harassment by the Tunisian authorities—were seen by millions of people around the world.

Today the Web is used by large groups of people to create collective works whose value far exceeds that provided by any of the individual participants. In 2009, Tim O'Reilly and John Battelle wrote that it

...is no longer a collection of static pages of HTML that describe something in the world. Increasingly, the Web is the world—everything and everyone in the world casts an “information shadow,” an aura of data which, when captured and processed intelligently, offers extraordinary opportunity and mind-bending implications.

O'Reilly and Battelle, 2009

We are now in the era of Web 3.0, which is all about personalization, intelligent searching, and the Semantic Web. The latter links up information on a global scale and has the potential to provide powerful data organization and query capabilities. These enable machines to understand the meaning of information on the Web through the addition of machine-readable metadata about pages and how they are related to each other. Resources can be aggregated, shared, and accessed from many different places, and users can choose the appropriate presentation for the tasks they need to accomplish (Hendler and Goldbeck, 2008). As a result we are crossing into a new learning paradigm, which offers a qualitative change in the way people think of interacting on the Web. With Web 2.0, interaction treats the Web as an information source and we learn by browsing, searching, and monitoring it. But with Web 3.0 the Web will be understood as an active human-computer system, and we will learn by telling it what we are interested in, asking it what we collectively know, and using it to apply our collective knowledge to address our collective needs (Gruber, 2008, p. 12).

An important factor in achieving this is to be able to draw on domain knowledge in areas where searches are difficult (Hendler and Goldbeck, 2008). One of the key challenges, therefore, for the human rights community is to bring human rights experts, information scientists, and technologists together to ensure that the necessary semantic linkages exist between the vast array of human rights-related information that is published online.

The human rights world has always been early adopters and adapters of emerging technology. In the days of the early Internet and Web organizations such as Amnesty International used bulletin boards to cut the time in transmission of their rapid response interventions for human rights defense, as reported to the European Parliament study on The Use of the Internet for the European Parliament's Activities for the Promotion and Protection of Human Rights (Halpin and Fisher, 1998). Throughout the period and since this trend has been continued with the use of GPS, crowd sourcing, blogs, and tweets, all playing a part in the repertoire of the modern human rights activist.

An examination of some evidence about current uses of mICT in human rights protection provides an interesting insight. If we look at the work of Ushahidi, who uses crowdsourcing, and the work by Douai on the Arab Spring, we can quickly view a small selection of these technologies in action (Lannon and Halpin 2012).

Douai, in Lannon and Halpin (2012), described research undertaken during the Arab Spring into the use of YouTube as a human rights advocacy resource. The “Arab Democracy Spring” has promised to end the entrenched history of human rights violations in Egypt, Libya, Syria, and Tunisia, among other Arab authoritarian states. However, the long fight against these abuses commenced years prior to the 2011 mass protests as an unprecedented era of virtual politics and activism took shape within Arab societies. At the forefront of these shifts, the Internet and other new communication technologies have been central forces for change. A few years after its inception, YouTube soon became an important tool for publicizing

Arab regimes' human rights abuses both locally and globally. Preliminary evidence suggests that YouTube has been effective in highlighting police abuse cases and prosecuting perpetrators. This work thus contributes to a growing body of research that underscores the vital role of communication and information technologies in promoting human rights worldwide.

Within the above framework, Arab citizens have similarly harnessed the site's video exchange capabilities to expose political corruption, police brutality, and demand political reform in the same way bloggers have countered official narratives and/or media blackouts on local events. YouTube and the new breed of social media have grown more effective as favorite political instruments for several reasons: high levels of anonymity, global reach, technical simplicity, absence of professional prerequisites, and local/global-organizing tool capabilities. Significantly, YouTube is hosting and abetting a new political discourse in which readers vent their frustrations and heap their scorn online before moving offline. The first tremors of this movement toward harnessing YouTube's social networking and video exchange capabilities appeared in 2007, as videos of police brutality and corruption in Egypt and Morocco were posted online.

Rosneau (2003, p. 149) argued that the twin forces of globalization of communication technologies mean that "the misdeeds of human rights violators no longer pass from human kind's conscience." For example, YouTube videos, in publicizing police abuse, corruption, and other human rights violations in Egypt and Morocco, have been a major factor in publicizing "misdeeds" by the abovementioned governments.

For activists, YouTube's repository and exchange capabilities provide audiovisual evidence for the excesses of the state. The more shocking the video evidence is, the louder the public and global outcry against those excesses will be. Also, the "permanent campaign" implies that the more "permanent" the record is, the more salient and constant the fight becomes. Permanent campaigning means constant surveillance of authoritarians' violations. Internationalization of human rights abuses builds on a well-proven record of transna-

tional solidarity movements, similar to the movements behind publicizing human rights abuses in Latin America (Keck and Sikkink, 1998). In their campaign, these "activists without borders" are wielding cameras and low-tech skills whether they post amateurish videos showing police abuse or they construct highly edited videos.

Another interesting use of social media and emerging mICT is the use of technology to develop human rights organizations and campaigns. The Ushahidi organization developed in Kenya and describes itself as a "non-profit tech company that specializes in developing free and open source software for information collection, visualization and interactive mapping" (the word Ushahidi means testimony in Swahili). Their work developed from engagement in the 2008 post-election period in Kenya, when they produced a Web site to map the violence that was occurring, working alongside Kenyan citizen journalists. In the short period since then Ushahidi the Web site mapped incidents of violence using reports submitted via mobile phones and the Web, accumulating approximately 45,000 users who provided evidence of the violence. Ushahidi stated that

Since early 2008 we have grown from an ad hoc group of volunteers to a focused organization. Our current team is comprised of individuals with a wide span of experience ranging from human rights work to software development. We have also built a strong team of volunteer developers primarily in Africa, but also Europe, South America and the US.

The technology for communication is low tech, mobile phones are sufficient, particularly where Internet coverage or accessibility is difficult, and the free open source software used for creating the mapping provides an information and content management system that allows analysis of complex and dangerous events as they happen, which it is argued allows for early warning and visualization for response and recovery. These tools, along with others provided as open source resources by Ushahidi, help human rights activists hold perpetrators of human rights abuses accountable. Using

these low-tech tools to achieve a high level of data gathering and analysis is vital in the very quickly changing world in which they work.

There are numerous other examples of the use of mICT, but there is also an alternative position, of which the human rights activist and citizens in general need to be aware. Reports indicate that governments do not stand idly by and watch their legitimacy challenged. In particular, Privacy International draws attention to the role that states take in repressive action of surveillance and monitoring of citizens and human rights activists. There is evidence of this from many sources, including the countries of the Arab Spring. They also report the exporting of these technologies by American and European companies to regimes known to be repressive and abusing human rights.

CONCLUSIONS

We started this chapter by stating that emerging technologies are creating fundamental changes to our daily lives and explored the role of these technologies in rapidly growing state surveillance capabilities. It is clearly obvious that the advent of the technology has had a tremendous impact in helping human society be better informed and hopefully better equipped to deal with natural and social ills. It is heartwarming to see how emerging technologies have helped human rights campaigners across the world to highlight state cruelty and suppression and how they have been able to mobilize public opinion in defense of peoples' rights in various countries. We are also very conscious and anxious that states across the world are using emerging surveillance technologies as an

integrated part of their suppressive apparatus and citizens' right to privacy and their human rights are increasingly threatened and violated.

Borrowing from Charles Dickens (1859) it might be said that the world of human rights and the impact of mICT on it is a little like the introduction to his work, *A Tale of Two Cities*:

It was the best of times, it was the worst of times, it was the age of wisdom, it was the age of foolishness, it was the epoch of belief, it was the epoch of incredulity, it was the season of Light, it was the season of Darkness, it was the spring of hope, it was the winter of despair, we had everything before us, we had nothing before us, we were all going direct to Heaven, we were all going direct the other way—in short, the period was so far like the present period, that some of its noisiest authorities insisted on its being received, for good or for evil, in the superlative degree of comparison only.

While technology marches on and surveillance capabilities are developing it is also important to recognize that the human rights of citizens should also be recognized as part and parcel of the national security of a country. It is the ethics of development and the ethics of practical application mICT that we need to balk at and rigorously, to ensure that they are justified within a democratic and free society. Everyone is responsible to ensure that they enhance human dignity rather than diminish it. The human rights community, which will always be an active stakeholder in mICT policies and possibilities, must also ensure that this is so.

Securing Cyberspace: Strategic Responses for a Digital Age

Andrew Staniforth

CYBER TERROR

When Metropolitan Police officers raided a flat in West London in October 2005, they arrested a young man, Younes Tsouli. The significance of this arrest was not immediately clear, but an investigation soon revealed that the Moroccan born Tsouli was the world's most wanted "cyber terrorist." In his activities Tsouli adopted the user name "Irhabi 007," (Irhabi means terrorist in Arabic), and his activities grew from posting advice on the Internet on how to hack into main-frame computer systems to assisting those planning terrorist attacks. Tsouli trawled the Internet searching for home movies made by U.S. soldiers in the theaters of conflict in Iraq and Afghanistan that would reveal the inside layout of U.S. military bases. Over time these small pieces of information were collated and passed to those planning attacks against armed forces bases. This virtual hostile reconnaissance provided insider data illustrating how it was no longer necessary for terrorists to conduct physical reconnaissance if relevant information could be captured and meticulously pieced together from the Internet.

Police investigations subsequently revealed that Tsouli had €2.5million worth of fraudulent transactions passing through his accounts,

which he used to support and finance terrorist activity. Pleading guilty to charges of incitement to commit acts of terrorism, Tsouli received a 16 year custodial sentence to be served at Belmarsh High Security Prison in London where, perhaps unsurprisingly, he has been denied access to the Internet. The then National Coordinator of Terrorist Investigations, Deputy Assistant Commissioner Peter Clarke, said that Tsouli "provided a link to core al-Qaeda, to the heart of al-Qaeda and the wider network that he was linking into through the Internet," going on to say: "what it did show us was the extent to which they could conduct operational planning on the Internet. It was the first virtual conspiracy to murder that we had seen."

The case against Tsouli was the first seen in the UK, and it quickly brought about the realization that cyber terrorism presented a real and present danger to its national security. Law enforcement practitioners understood that the Internet clearly provided positive opportunities for global information exchange, communication, networking, education, and as a major tool in the fight against crime, but a new and emerging contemporary threat had appeared within the communities they sought to protect. The Internet had been hijacked and exploited by terrorists not

only to progress attack planning but to radicalize and recruit new operatives to their cause. It was also the core and affiliated networks of al-Qaeda that were quick to realize the full potential of the global platform provided by the Internet.

It is now clear to Western national security intelligence practitioners that al-Qaeda and its global network of affiliated groups is resilient, becoming increasingly independent, mobile, and unpredictable. Of critical concern for the security of the Western world remains the way in which individuals from our own communities are being influenced by the single narrative and extreme version of religious ideology promoted by al-Qaeda. This narrative, when combined with a complex array of social, political, and economic factors set within the specific environment of each nation, has served to manipulate individuals toward extremist perspectives cultivating a home-grown terrorist threat, which presents security concerns to the free and democratic way of life enjoyed in the West. The way in which the recruiters and radicalizers of al-Qaeda have influenced and indoctrinated the young and vulnerable across the world has alarmed national security professionals. The direct impact they have made upon impressionable members of our communities who require safeguarding from this terrorist tactic continues to damage the confidence of our communities in the ability of the state's security apparatus to police the Internet and protect their online experience. Al-Qaeda has also preyed upon school-age individuals, which reveals the extent they are prepared to go to progress their cause. During June of 2006, Hammad Munshi, a 16-year-old school boy from Dewsbury in Leeds of West Yorkshire, was arrested and charged on suspicion of committing terrorism-related offenses. Following his arrest, searches were conducted at his family home where his wallet was recovered from his bedroom. It was found to contain handwritten dimensions of a sub machine gun, taken from a book titled *Expedient Homemade Firearm*. At the time Munshi had excellent information technology skills and had registered and run his own Web site on which he sold knives

and other extremist material passing on information on how to make napalm as well as how to make detonators for improvised explosive devices. While the online rhetoric of al-Qaeda cyber recruiters reached the computer in the bedroom of Hammad Munshi, authorities on this occasion were able to intervene before any critical security risks to citizens were realized. But not all individuals being recruited online would be prevented from carrying out attack planning by UK security forces.

On May 22, 2008, Nicky Reilly, aged 22, left his home in Plymouth with a rucksack containing six bottles full of nails and home-made explosives. His target was the Giraffe restaurant in Exeter, a popular place for shoppers to lunch. Reilly, who has Asperger's syndrome and a mental age of 10, was a suicide bomber, recruited online in local Internet cafes by extremists in chat rooms who had fueled a hatred of the West. Extremists had molded a home-grown terrorist and had directed him to bomb-making Web sites discussing what his target should be. As Reilly was seated in the restaurant, 44 customers had also sat down to dine. One of the eleven members of the staff working that day brought Reilly a drink, and he sat for 10 minutes before making his way to the lavatory taking his rucksack with him. Once inside a cubicle the device detonated prematurely causing injury to Reilly and damage to the restaurant. No other person was injured in the blast. A note left at his home revealed the motivation for his actions in which he paid tribute to Osama bin Laden and called on the British and U.S. governments to leave Muslim countries. The note declared that Western states must withdraw their support of Israel and that violence would continue until "the wrongs have been righted." Reilly, appearing in court as Mohammed Abdulaziz Rashid Saeed, pleaded guilty to offenses of attempted murder and preparing for acts of terrorism. At the Old Bailey on January 30, he was sentenced to life imprisonment. Mr. Justice Calvert-Smith said that "I am quite satisfied that these offences are so serious that only a life sentence is appropriate. This defendant currently represents a significant

risk of serious harm to the public.” He went on to say that “The offence of attempted murder is aggravated by the fact that it was long planned, that it had multiple intended victims and was intended to terrorize the population of this country. It was sheer luck or chance that it did not succeed.” Defense counsel, Kerim Fraud, representing Reilly stated that “He may comfortably be deemed to be the least cunning person ever to have come before this court for this type of offence.” The threat from cyber terrorism in all of its forms continues to represent a serious risk to the national security of many nations, but other criminals, extremists, agitators, and states themselves also have come to understand the unique potential of the Internet, presenting a complex malaise of new cyber-based threats to Western democracies and their citizens.

CYBER THREATS

The Internet and digital technologies continue to transform our societies by driving economic growth, connecting people, and providing new ways to communicate and cooperate with one another. The World Wide Web only began in 1991, but today 2 billion people are online—almost one-third of the world's population. Billions more are set to join them over the next decade, and there are over 5 billion Internet-connected devices with \$8 trillion changing hands each year in online commerce. As a direct result the Internet is already having a profound impact on the way citizens across the globe live their lives. This social change is only set to grow and gather pace as the number of users increases. Already it appears the phenomenal growth of Internet use will be on the scale of the very largest shifts in human history, such as the coming of the railways, or even the learning to smelt metals. Real Gross Domestic Product per capita has risen by \$500 over the last 15 years in mature countries enabled by the Internet. By comparison, it took 50 years for the industrial revolution to have the same effect. Given this context it is understandable why the growth of the Internet has had such a dramatic impact upon societies across the world.

Cyberspace is transforming business, making it more efficient and effective. It is opening up markets, allowing commerce to take place at lower cost and enabling people to do business on the move. It has promoted fresh thinking, innovative business models, and new sources of growth. It enables companies to provide better, cheaper, and more convenient service to customers, and it helps individuals to shop around, compare prices, and find what they want. Cyberspace is an interactive domain made up of digital networks that is used to store, modify, and communicate information. It includes the Internet, but also the other information systems that support businesses, infrastructure, and critical services. Digital networks already underpin the supply of electricity and water to our homes, help organize the delivery of food and other goods to stores, and act as an essential tool for businesses. And their reach is increasing as we connect our TVs, game consoles, and even domestic appliances. In summary, the development and use of the Internet by advances in smart mobile technology is accelerating Western society's dependence upon cyberspace. Developing countries in particular stand to benefit as increasing interconnectivity makes commerce easier and allows access to information, knowledge, and education, enabling people to innovate, collaborate, and compete in global marketplaces.

The UK, like many nations in the Western world, has positively adopted cyberspace as a means of doing business. In 2009, 608 million card payments were made online in the UK, with a total spent of £47.2 billion, and in 2011 90% of high street purchases were being made using electronic transactions with ~52% of UK consumers having direct access to broadband using online shopping as an opportunity to save money. The Internet will become increasingly central to national economies, but the growing role of cyberspace has also opened up new threats as well as new opportunities. The national security machinery of governments has no choice but to find ways to confront and overcome these threats if they are to flourish in an increasingly competitive and globalized world. The digital architecture

on which we now rely was built to be efficient and interoperable. When the Internet first started to grow, security was less of a consideration. However, as we put more of our lives online, security matters more and more. People want to be confident that the networks that support our national security, our economic prosperity, and our own private lives as individuals are safe and resilient. Unfortunately a growing number of adversaries are looking to use cyberspace to steal, compromise, or destroy critical data. The scale of our dependence means that our prosperity, our key infrastructure, and our places of work and our homes can all be affected. For this reason the British government's 2010 national security strategy—*A Strong Britain in an Age of Uncertainty: The National Security Strategy*—identified cyber attacks on the UK as a “Tier 1” threat; one of its highest priorities for action stating that “hostile attacks upon UK cyber space by other states and large scale cyber crime” presented a primary risk to national security and economic well-being.

Criminals from all corners of the globe are already exploiting the Internet to target Western democracies in a variety of ways. There are crimes that only exist in the digital world, in particular those that target the integrity of computer networks and online services. But cyberspace is also being used as a platform for committing crimes such as fraud, and on an industrial scale. Identity theft and fraud online now dwarf their offline equivalents. The Internet has provided new opportunities for those who seek to exploit children and those who are vulnerable. Cyberspace allows criminals to target countries from other jurisdictions across the world, making it harder to enforce the law. As businesses and government services move more of their operations online, the scope of potential targets will continue to grow. Some of the most sophisticated threats to cyberspace come from other states that seek to conduct espionage with the aim of spying on or compromising government, military, industrial, and economic assets, as well as monitoring opponents of their own regimes. “Patriotic” hackers can act upon a state's behalf to spread disinformation, disrupt

critical services, or seek advantage during times of increased tension. In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce the technological advantage of a nation's military or to reach past it to attack domestic critical infrastructures.

The threat to Western democracies from politically motivated activist groups operating in cyberspace is also very real. Attacks on public and private sector Web sites and online services in the UK in particular orchestrated by “hacktivists” are becoming more common, aimed at causing disruption, reputational and financial damage, and gaining publicity. All of these different groups—criminals, terrorists, foreign intelligence services, and militaries—are active today against countries' interests in cyberspace. With the borderless and anonymous nature of the Internet, precise attribution is often difficult and the distinction between adversaries is increasingly blurred. Assessing the actual level of threat from cybercrime is a major challenge. Law enforcement statistics are generally considered to be a poor indication of the actual level and trends. Many cyber deceptions go unreported to the authorities so the scale of cybercrime is very difficult to measure, and there are challenges in gathering accurate data because the victims have not discovered that they are the subject of a criminal act or the victims report the offense to a providing company rather than the police, while the companies tend not to disclose their levels of loss or attack to avoid loss of reputation and custom.

As the actual threat from cybercrime may be proving difficult to measure accurately, organizations also are not always aware of the new vulnerabilities that dependence on cyberspace can bring. Intellectual property and other commercially sensitive information such as business strategies and research and development data can be attractive targets. This risks undermining the strengths of countries' innovative research base, investment, and intellectual property as important drivers of economic growth leading to improved prosperity. Services relying on, or delivered via, cyberspace can be taken offline by

criminals or others, damaging revenue and reputations. Cyberspace has now grown to become a domain where strategic advantage, industrial or military, can be won or lost. The Internet underpins the complex systems used by commerce and the military. The growing use of cyberspace means that its disruption can affect a nation's ability to function effectively in a crisis. Nearly two-thirds of critical infrastructure companies report regularly finding software designed to sabotage their systems. Some states also regard cyberspace as providing a way to commit hostile acts "deniably." Alongside existing defense and security capabilities, nations must be capable of protecting their national interests in cyberspace. Iain Lobban, Director of the Government Communications Headquarters (GCHQ), stated that "There are over 20,000 malicious emails on UK government networks each month, 1,000 of which are deliberately targeting them." These kinds of attack are increasing; the number of e-mails with malicious content detected by government networks in the whole of 2010 was double the number seen in 2009 and law enforcement agencies are even being targeted.

During 2012 a UK-based hacker posted online what appeared to be authentic login information for police officers in the Hertfordshire and Nottinghamshire constabularies.

The usernames, passwords, and personal identification numbers were posted to a "Pastebin" Web site along with the banner "OpFreeAssange" and a quote from WikiLeaks founder Julian Assange. In a statement, Hertfordshire Constabulary said it was investigating the breach of security and confirmed that the information had been stored on a database linked to its public facing Safer Neighborhoods pages of an external Constabulary Web site. The police force said the database was externally hosted and they were forced to disable part of its Web site as a precaution reassuring their personnel and the wider communities they served that there was "absolutely no suggestion that any personal data relating to officers or members of the public has been, or could have been compromised." With the increase in unlawful and illegitimate activity in cyberspace over the past decade, a dedicated response was required

by governments to counter all cyber-related threats; a response that continues to be the greatest contemporary challenge to national security policy and practice.

STRATEGIC RESPONSES

The threat from all manner of cyber hazards was recognized by the British government as presenting a primary risk to its security and economic prosperity. As a direct result it published its first ever cyber security strategy on June 25, 2009. The strategy, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyberspace*, acknowledged the UK's growing dependence on cyberspace revealing that modern globalized lifestyles become increasingly dependent upon information communications technology, and that cyberspace provided a new arena in which hostile states, terrorists, and conventional criminals can threaten UK security interests. Upon announcing the launch of the strategy, then Prime Minister Gordon Brown stated that

Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyberspace in order to give people and businesses the confidence they need to operate safely there.

To deliver the strategic aim of the new strategy designed to "reduce risk from the UK's use of cyberspace and exploiting opportunities in cyberspace through improving knowledge, capabilities and decision-making," a new cyber security architecture had to be constructed. The Office of Cyber Security and Information Assurance (OCSIA) was established, tasked with driving forward a cross-government program of work supporting the Minister for the Cabinet Office, the Rt. Hon. Francis Maude MP and the National Security Council in determining priorities in relation to securing cyberspace. The unit provides strategic direction and coordinates action relating to enhancing cyber security and information assurance in the UK, while a new

Cyber Security Operations Center (CSOC) based at GCHQ in Cheltenham, Gloucestershire, provides the coordinated protection of the UK's critical information technology systems. The OCSIA, alongside the CSOC, works with lead government departments and agencies such as the Home Office, Ministry of Defence, GCHQ, Communications-Electronics Security Group, the Center for the Protection of National Infrastructure, and the Department for Business, Innovation and Skills in driving forward the cyber security program for the UK government, which seeks to provide the UK with the balance of advantage in cyberspace.

Law enforcement agencies across the UK government also have their part to play in providing safety and security online to UK citizens and business users. The police service, under the auspices of the Association of Chief Police Officers (ACPO), developed a new E-Crime initiative to provide the strategic foundation and direction to ensure UK police services were alert to cybercrime and cyber terrorism activities and that any suspected activity, no matter how small, was encouraged to be reported by the public and commerce and recorded. This policing initiative was supported by others under the leadership of the Office of Security and Counter Terrorism at the Home Office. With primary responsibility for the cross-government strategy on tackling terrorist use of the Internet, the Home Office published guidance for those citizens who are responsible for vulnerable individuals and work within communities to help ensure that the Internet is an environment where terrorist and violent extremist messages are challenged. As part of their wider efforts to counter the threat of radicalization on the Internet, a public facing Web page was launched in February 2010 to encourage the public to take action against unacceptable violent extremist and hate Web sites and other online content. Where individuals believed that material they have located is potentially unlawful they are provided with the opportunity to complete a form on the Web page and refer it to the Counter Terrorism Internet Referral Unit (CTIRU), established by ACPO during 2010. The CTIRU provides a national coordinated response to referrals from the

public as well as from government and industry. It also acts as a central, dedicated source of advice for the police service. The CTIRU initiative supports two key strands of the UK's Counter Terrorism Strategy "CONTEST" as follows:

- **PREVENT:** This seeks to stop people from becoming terrorists or supporting violent extremism by taking action against material that encourages radicalization through the glorification of violent extremism.
- **PURSUE:** This aims to stop terrorist attacks by taking action against material useful for acts of terrorism.

The CTIRU provides the UK police service with a unit of experts who can carry out an initial assessment of material located on the Internet. It is also responsible for alerting forces and the units of the UK Police Counter Terrorism Network to online terrorist offenses that may fall within their jurisdiction. Powers under UK terrorism legislation provide for the CTIRU to take a national lead in serving notices on Web site administrators, Web hosting companies, Internet Service providers, and other relevant parties within the UK, to modify or remove any unlawful content.

The CTIRU also focuses on developing and maintaining relationships with the Internet industry, an important part of ensuring the delivery of a safer and more secure online experience for its citizens. A further challenge given the global scope of cyberspace for UK law enforcement was the majority of terrorist content online being hosted in other countries outside UK jurisdiction. To counter this challenge the CTIRU continues to forge links with law enforcement counterparts abroad to help target those Web sites hosted overseas. UK Counter Terrorism and Extremism Liaison Officers based in countries around the world have a key role in supporting this work. The ACPO national coordinator for PREVENT, Assistant Chief Constable John Wright, described the role of CTIRU as

providing the opportunity to effectively enforce, and control, access to material believed to be extreme. In addition, the CTIRU will help to develop a culture of

collaboration between police, partners and service providers dedicated to making the internet a safer place, particularly for young people.

The tools to tackle cyber terrorism and the criminal use of the Internet to recruit and radicalize potentially vulnerable individuals online are an important aspect of combating contemporary terrorism. Professor Sir David Omand GCB, former Director of GCHQ and UK Security and Intelligence Coordinator in the Cabinet Office under Prime Minister Tony Blair, believes that “the cyber dimension is likely to become a means for terrorists to try to cause disruption and to score propaganda points.” He went on to reveal that the UK has “many cyber vulnerabilities.” Such vulnerabilities include the growing threat of fraud. The British government has now come together with leading industry players to help people better protect themselves. In the first campaign of its kind involving both the private and public sectors, “The Devil’s in Your Details” campaign brings together Action Fraud, Telecommunications UK Fraud Forum and the Financial Fraud Action UK—the name under which the financial services industry coordinates its fraud prevention activity—in a powerful demonstration of what can be achieved when industry and government work together. The National Fraud Authority-backed campaign is raising awareness of the importance of protecting personal information and aims to remind the public to check and make sure that who they share their details with is genuine, whether on the phone, in person, or online. The Devil’s In Your Details campaign encourages consumers to suspect anyone or anything they are uncertain about, to keep asking questions, and to challenge or end an engagement if it feels uncomfortable. As an introduction to a wider campaign against fraud, this awareness activity aims to increase reporting of fraud, making it harder for fraudsters to target consumers and in the future providing evidence of the new and innovative ways in which governments must now inform and support their citizens to protect them from specific cyber-related threats.

A NEW APPROACH

In order to maximize the potential of the Internet, it is important that people feel confident that it can be used safely. As all of us make more use of the Internet in our work and private lives, it makes for a more attractive target for criminals or others. Any reduction in trust toward online communications can now cause serious economic and social harm to Western democracies. Beyond the impact upon individual citizens, the scale of the use of cyberspace means that it can now also affect society more broadly. Western governments have a strong tradition of protecting its citizens in ways that are guided by the core values of liberty, fairness, transparency, and the rule of law. These values help define who we are and what we do. The interconnected nature of cyberspace and its expansion mean that it has developed to promote many of these values, but the conventions and norms covering conduct within the cyber domain are still developing. While this helps make it the vibrant domain that it is today, it can also cause instability and uncertainty about accountability. The blurring of boundaries in cyberspace increases the risk of actions affecting larger numbers of people and organizations unintentionally. At its most serious, this leads to the potential for unpredictable and large-scale shocks.

Actions to strengthen national security must therefore also be consistent with states’ obligations, such as those concerning freedom of expression; the right to seek, receive, and impart ideas; and the right to privacy. Defending security should be consistent with the commitment to uphold civil liberties. Of course, these are well-established and ongoing debates, but cyberspace can bring them into focus in new ways, and more quickly than in other areas. These changes do not affect single nations alone. The global reach of the Internet and digital technologies can provide an important means for the spread of ideas, with profound implications for societies across the globe. But like any communications medium, cyberspace can also potentially be used to restrict liberty and undermine freedoms. Some states

and organizations are already seeking to control and restrict the future development of the cyber domain. These attempts are ultimately doomed to fail. But for as long as they last they are holding back progress and reducing social benefit. It is important that Western democracies continue to work with like-minded states around the world to maximize the extent to which the world can fully realize and enjoy the benefits that cyberspace will offer.

To secure the vast economic and social opportunities that cyberspace has to offer, the newly elected British coalition government under Prime Minister David Cameron during 2010 transformed its approach to cyber security, setting out a new vision toward 2015 in its cyber strategy, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*. The new strategy revealed that the British government believed that there was no such thing as “absolute security,” indicating that its strategy to counter cyber threats was to apply a risk-based approach to prioritizing its

response. The new strategic vision for the strategy was for the UK in 2015 to derive huge economic and social value from a vibrant, resilient, and secure cyberspace, where its actions, guided by its core values of liberty, fairness, transparency, and the rule of law, enhance prosperity, national security, and a strong society. To counter all cyber challenges the new strategy was divided into four strategic objectives as shown in [Figure 17.1](#).

To tackle cyber crime the British government will work to reduce online vulnerability and restrict criminal activity online while promoting more effective partnerships. To make it safer to do business in cyberspace the strategy reveals that efforts will be made to increase awareness and visibility of threats, improving incident response and further protect information and services by fostering a culture that manages cyber risks serving to promote confidence in cyberspace. This strategy also seeks way in which to defend UK national infrastructures by strengthening defenses in cyberspace, improving

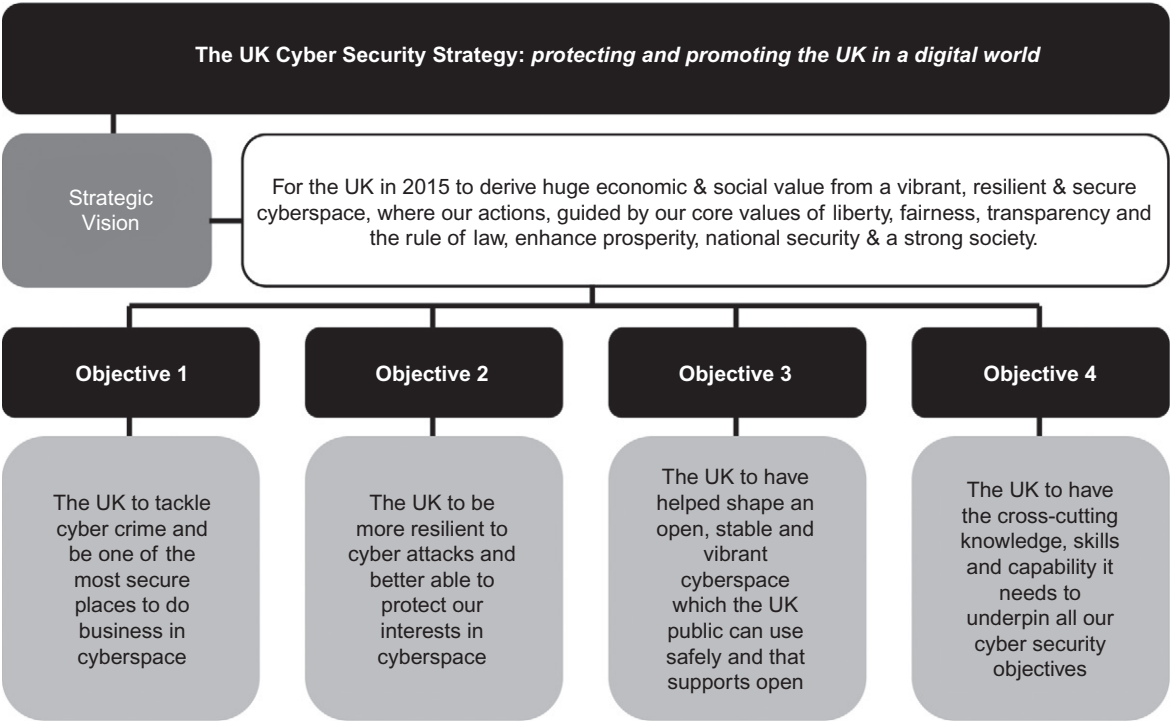


FIGURE 17.1 The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.

resilience and diminishing the impact of cyber attacks and countering the terrorist use of the Internet. Ensuring that the UK has the capability to protect its interests in cyberspace, national security policy makers in government ensured that the new strategic approach is set to improve the UK's ability to detect threats in cyberspace by expanding its capabilities to deter and disrupt attacks. The UK cyber strategy provides an “all hazards” approach to cyber security ensuring that all of its efforts are coordinated in a detailed program of work across the full operating landscape of government. It specifically highlights the important need to help to shape the development of cyberspace by promoting an open and interoperable environment while promoting the fundamental freedoms and rights that British citizens enjoy. This particular element ensures that the UK will pursue cyber security policies that enhance individual and collective security while preserving UK citizens' right to privacy and other fundamental values and freedoms. The strategy also reveals that internationally the UK will continue to pursue the development of norms of acceptable behavior in cyberspace, starting from the belief that behavior that is unacceptable offline should also be unacceptable online. The UK governments' position on cyber security is guided by seven principles proposed by the Foreign Secretary, Rt. Hon. William Hague MP, during February 2011.

UK CYBER SECURITY GUIDING PRINCIPLES

1. The need for governments to act proportionately in cyberspace and in accordance with national and international law
2. The need for everyone to have the ability—in terms of skills, technology, confidence, and opportunity—to access cyberspace
3. The need for users of cyberspace to show tolerance and respect for diversity of language, culture, and ideas
4. The need to ensure that cyberspace remains open to innovation and the free flow of ideas, information, and expression
5. The need to respect individual rights of privacy and to provide proper protection to intellectual property
6. The need for us all to work collectively to tackle the threat from criminals acting online.
7. The promotion of a competitive environment that ensures a fair return on investment in network, services, and content.

The British government understands that achieving its vision for cyber security for 2015 within the framework of its guiding principles will require everybody—the private sector, individuals, and government—to work together. Just as all citizens from all countries benefit from the use of cyberspace, all have a responsibility to help protect it. Therefore ordinary citizens have an important role to play in keeping cyberspace as a safe place to do business and live our lives. By 2015 the new approach by the British government will seek to ensure that its citizens know how to ensure a basic level of protection against threats online and that they have ready access to accurate and up-to-date information on the online threats that they face together with the techniques and practices they can employ to guard against them. If citizens are careful about putting personal or sensitive information on the Internet, are wary of e-mail attachments or links from unrecognized senders, and are cautious about downloading files from Web sites they know little about then they can significantly assist in countering the cyber security challenge making cyberspace increasingly resilient to all types of cyber threats posed to individual citizens. It is essential therefore that everyone, in their homes, at their place of work, and on the move can help identify threats in cyberspace and report possible offenses that make cyberspace a hostile environment for those seeking to unlawfully exploit its potential.

The private sector also has a crucial role to play in strengthening cyber security. Much of cyberspace is owned and used by private companies and it is therefore businesses that will drive the innovation required to keep pace with security challenges. By 2015 the British government

will seek to ensure that companies are aware of the threat and use cyberspace in a way that protects commercially sensitive information, intellectual property, and customer data. It will also work to protect private organizations by working in closer and increasingly integrated partnerships to share best practice supported by government and law enforcement agencies. These partnerships will share information and resources to transform the response to a common challenge and actively deter the threats faced in cyberspace. The role of government will underpin the efforts of citizens and the private sector to help reduce the risk from cyber threats, and the British government has now committed to playing its full part in achieving these aims by seeking to amplify its capacity to detect and defeat high-end threats by 2015. In addition, the British government is committed to investing in the growth of a cadre of cyber security professionals and strengthening law enforcement to tackle cybercrime. One such development is already in action—the introduction of a new National Crime Agency (NCA). The NCA will be a powerful body of operational crime fighters with a clear focus on public protection with a federal approach. The NCA receives its legal footings from the Crime and Courts Bill, which was introduced into the House of Lords on May 10, 2012. Subject to Parliamentary processes, the government's ambition is that the new NCA will be fully operational by December 2013. Its mission will include tackling organized crime, strengthening borders, fighting fraud and cybercrime, and protecting children and young people.

The creation of the NCA marks a significant shift in the UK's approach to tackling serious, organized, and complex crime, with an emphasis on greater collaboration across the whole law enforcement landscape. The NCA will build effective two-way relationships with police forces, law enforcement agencies, and other partners, and will be made up of four commands including the Economic Crime Command, providing an innovative and improved capability to deal with fraud and economic crimes, including those carried out by organized criminals, and the Child Exploitation and Online Protection

Centre, which will work with industry, government, children's charities, and law enforcement to protect children from sexual abuse and to bring offenders to account. Both of these primary arms of the NCA will work to significantly reduce the cyber-based risks to British citizens and protect the broader security of the nation. The NCA will also benefit from an intelligence hub, which will build and maintain a comprehensive picture of the threats to the UK from organized criminality and a national cybercrime center, providing expertise, support, intelligence, and guidance to police forces and the commands of the NCA. The new organization will confront some of the most risky and dangerous people that affect UK communities and will be one that is unequivocally focused on keeping the public safe. The British government has gone even further to ensure that all police forces efforts are marshaled to augment the NCA lead role in tackling cyber-related crime. During November 2011 Home Secretary, Theresa May, presented the shadow Strategic Policing Requirement (SPR) to Parliament. The publication of the shadow SPR set out what the Home Secretary views as the national threats the police services must address providing the appropriate national capabilities to do so. These threats included terrorism, civil emergencies, organized crime, public order, and a large-scale cyber incident. The shadow SPR received statutory effect during November 2012 and now empowers the newly democratically elected police and crime commissioners to deliver their important role of holding their Chief Constable to account for the totality of policing, both locally and nationally. The police and crime commissioners are expected to drive collaboration between police forces and to ensure that forces can work effectively together and with their partners. The SPR now provides a statutory obligation on police forces to provide the necessary resources and commitment to effectively tackle a large-scale cyber incident. It provides evidence of the commitment of the British government to focus its assets on countering cyber threats and the seriousness in which they assess the phenomenon of cyber-related threats to its national security.

CYBER COLLABORATION

Although the scale of the cyber security challenge requires strong national leadership, governments cannot act alone as they must recognize the limits of their competence in cyberspace. Much of the infrastructure that countries need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business driven. Similarly, although individual nations can improve their own defenses domestically, the Internet is fundamentally transnational and threats are cross-border. A global threat requires a global response. Not all the infrastructure on which countries rely is based within their own boundaries. So many nations of the Western world, like the UK, cannot make all the progress it needs to on its own. Therefore collaboration is the key to success in cyberspace, and the British government has committed to building strong partnerships with other countries that share its views and reach out to other nations where they can to those who do not.

On May 25, 2011, President Obama and Prime Minister David Cameron reaffirmed their close bilateral cooperation, and charted important new steps forward for cyber security. The United States and the UK share unparalleled bilateral cooperation and both leaders agreed on a shared vision for cyberspace, which places at its heart fundamental freedoms privacy and the free flow of information in a secure and reliable manner. Prime Minister Cameron stated:

Our goal is to nurture and accelerate the progress that these technologies have enabled in our economies and societies; we will continually work, individually and as partners to ensure they create jobs, enrich lives, and provide return on the sound investments we make in them today.

Both leaders acknowledged that building consensus on responsible online behavior was an important role for their governments to tackle, recognizing that the same kinds of “rules of the road” that help maintain peace, security, and respect for individual rights internationally must equally apply in cyberspace. Through its deposit of instruments of accession in Strasbourg, during May 2011, the UK has now joined the United States and 30 other states as parties to the Budapest Convention on Cybercrime, the world's foremost treaty to combat cybercrime internationally. The Convention sets standards for national laws in dealing with online fraud and abuse, but even more importantly it permits effective cooperation between nations—a crucial tool since so many cybercrimes cross national boundaries. Noting this landmark achievement, President Obama and Prime Minister Cameron agreed to continue work to expand the reach of this important treaty.

The collaboration between the United States and the UK provides both governments with an opportunity to share experiences and develop effective countermeasures together, ensuring they are doing all they can to stay one step ahead of those who wish to unlawfully exploit and misuse the freedom offered in cyberspace. While governments across the world seek to define and then address their cyber security concerns, the technological advances of the Internet and the phenomenon of social media networks, smart mobile communications devices present both future challenges to, and opportunities for, the national security apparatus of states. By simply increasing collaborative approaches to all types of cyber threats will ensure that individually and collectively, governments are better prepared today to meet the cyber security challenges of tomorrow.



CHAPTER 18

National Cyber Defense Strategy

Paul de Souza

*In trying to defend everything he defended nothing.
Frederick the Great, (Frederick II)*

INTRODUCTION

A solid national cyber defense strategy must be based on the understanding that although risk can be minimized, the threat can never be completely eliminated. The attack surface will always be present no matter how many layers of defense one implements. Defense in depth in conjunction with situational awareness (SA) and active defense when properly implemented can take any nation from being reactive to proactive.

Defense in depth is nothing but the active deployment of Computer Network Defense (CND). According to the U.S. Joint Chiefs publication “Joint Pub 3-13, Information Operations” CND involves actions taken via computer networks to protect, monitor, analyze, detect, and respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems and networks. According to the U.S. Department of Defense (DoD), defense in depth is also “the siting of mutually supporting defense positions designed to absorb and progressively weaken attack, prevent initial observations of the whole position by the enemy, and to allow the commander to maneuver the reserve.”

In today's technology field and cyber domain, Chief Technology Officers (CTOs), cyber commanders, strategists, or even network engineers commonly add more and more of the same when it comes to implementing security. Many believe that complexity is a negative trait of systems when, in reality, complexity and variety can add real defense in depth and “progressively weakens the attack” of the adversary. The fact most users employ the same operating systems (Windows 7 and XP are the most popular operating systems in the United States) naturally gives the adversary the advantage when attacking networks running those systems. Adding less popular systems to a network will lessen the attack surface and increase the complexity of one's network.

Any nation must ensure it has the necessary capabilities to operate effectively in all domains, such as air, land, sea, space, and cyberspace. A well-developed cyber-defense strategy must cover the necessary areas that enable a nation to operate in a degraded environment. Unplugging systems from cyberspace is no longer acceptable, but fighting through and in cyberspace under attack is the key to success.

A natural overlap occurs within the realms of Information Assurance (IA) and CND. The National Security Agency defines IA as “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.” While CND naturally focuses on systems, IA focuses on data. However, one must protect both systems and data. A healthy cyber-defense strategy will heavily target both of these.

Cyberspace now spans all other war-fighting domains, such as land, sea, air, and space. A stable national cyber defense strategy must take into consideration the enormity of cyberspace and the need to operate through and in cyberspace as a way to keep order and peace. The current national threat environment is a convergence of traditional sources of power with new social sources of power to include non-nation state actors armed with highly technological capabilities. These technological threats can and do affect physical domains. We can see the natural course being the intensification of cyber conflict from data exploitation to data disruption and to data destruction.

When designing a cyber defense strategy, one must take into consideration the operational construct of cyberspace: man-made, global, complex, contested, and mostly privately owned. The U.S. DoD released its cyberspace strategy named “Department of Defense for Operating in Cyberspace” in July 2011. Strategic Initiative Two from this strategy reads: “Employ new defense operating concepts to protect DoD networks and systems.” Staying current on new concepts for operational defense is no easy task, but it is essential in order to have an effective approach in cyberspace. The DoD strategy itself states that “the implementation of constantly evolving defense operating concepts is required to achieve DoD’s cyberspace mission today and in the future.”

Solid defense operating concepts in the cyber domain will take into consideration the fluid nature of cyberspace and keep up with its rapid pace of change. When speaking about

defense, a phrase often heard from cyber security professionals is “in near-real time” or even defense “in real time.” What does it mean to be able to defend one’s systems and data in real time? Is it even possible? Most cyber security vendors want potential clients to believe that such capabilities rest upon their technological solutions, when in reality the solution is a combination of technologies and human capabilities. The gap found in most cyber defense strategies is the lack of human capabilities, the lack of proper trained cyber security professionals, and the lack of SA.

TRAINING CYBER DEFENSE PROFESSIONALS

A current global trend is for cyber security professionals, so-called cyber warriors, to have their training focus on specific technologies, tools, and segmented methodologies that apply only to defensive matters. In the physical domain, soldiers are trained to both defend and attack; the same reality must be applied in cyberspace by training our cyber warriors to be battle focused.

To be battle focused in cyberspace means to be able to be cross-trained to operate in both offensive and defensive environments. In order to deploy “active defense” strategies in the cyber domain, one must fully comprehend what it means to deploy full-spectrum cyber operations. The objective of this chapter is not to delve into authorities and how the law would treat “active defense,” but to give the reader the understanding of the need for a shift in thinking when approaching defensive strategies. A well-rounded cyber security professional aspiring to become well versed in Defensive Cyberspace Operations (DCO) should also be trained to create exploits and payloads, work on cyber weapons development, find new attack vectors and techniques, and finally to plan and execute Offensive Cyberspace Operations. The DCO professional of today must be able to defend his domain by understanding the mind of the adversary.

What would a national cyber defense strategy look like? The DoD’s definition of strategy from the DoD dictionary of military and

associated terms (US—JP 1-02) can be applied to cyberspace: “A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives.” The following are core elements that might constitute a framework that could be used to create a national cyber defense strategy:

1. Set of ideas
2. Instruments of power (including well-trained people, the right technologies and processes)
3. Synchronized efforts
4. Objectives and direction

With that framework in mind, how is a solid cyber defense strategy created and maintained? The following are steps to a practical and objective approach to creating a cyber defense strategy that could be applied at both organizational and national levels.

1. Understand what cyber strategy is not.
2. Understand and accept the unique threats that apply to you—Know Your Enemy! (CyberINT, Attack Analysis and Strategy Analysis) CyberINT means collecting data on the Internet, before the attacks take place. It is a form of trying to predict what form of cyber attack will take place by studying online communications and connecting the dots.
3. Know yourself and how vulnerable you are. Understand your capabilities.
 - Applying actionable intelligence to the process of developing a cyber defense strategy framework can give one a better understanding of the current threat landscape. Sun Tzu, the great Chinese military strategist stated, “It is said that if you know your enemies and know yourself, you will not be imperiled in a hundred battles.” The following are two main approaches to understanding your enemy.
 - Cyber attack analysis: Reactive Approach
 - Cyber intel collection: Proactive Approach
 - Define what is critical.

- Understand what is wanted by your adversary.
 - Understand your vulnerabilities by running vulnerability assessments.
 - Engage trusted but external partners to test your systems.
4. Create a set of ideas (the WHAT of things and not necessary the HOW of things).
 - Now that I know the unique threats that apply to my organization and I know my capabilities, WHAT do I do?
 - Write down your set of ideas, much like a “risk Assessment procedure.”
 - What security controls are needed to appropriately protect the information systems that support the operations and assets of the organization so that organization can accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals?
 5. Develop your instruments of power (set of skills, technology, knowledge, etc.) to counter the threat and minimize the risk (the HOW of things).
 - HOW do I develop and deploy people, technology, and processes to create “risk mitigation”?
 6. Synchronize, collaborate, integrate, and coordinate.
 - A cyber strategy must keep security events in sync with time.
 7. A cyber strategy must cover collaboration, integration, and coordination efforts with other cyber entities of interest. List objectives and expand on direction.
 - Strategy goals must be well defined.
 - Define success and appropriate metrics.
 - Create a strategy forecast and future direction.
 8. Write down the strategy.
 - A cyber strategy is a sensitive living document that is dynamic and ever changing.
 9. Repeat the cycle.

Do not rely only on third-party companies to protect your cyber assets; you create your strategy based on the level of threat you face and based on your cyber combat zone. You can use

their know-how, but this is not a cookie-cutter process. It is about connections and who you know and how fast you can share knowledge and collaborate. Connect the dots in the present to understand the future and learn from the past.

The Center for Strategic and International Studies, using open-source literature, has reviewed policies and organizations in 133 states to determine how these organizations deal with cyber security and whether they have a military command or doctrine for cyber activities. The Center for Strategic and International Studies identified 33 nations with cyber warfare capabilities and strategies that directly relate to full-spectrum cyber capabilities. It is worth noting the fast advancement in acquiring such capabilities and the need to develop national cyber strategies to address such needs.

Another point to consider is the classified side of each strategy in use today by state actors. Almost every strategy has a nonpublic side, which reinforces secrecy. Most of these national cyber strategies identify the threats that directly affect their respective national security and way of life, along with initiatives to help minimize the threat surface in cyberspace.

Every nation and organization should develop a cyber defense strategy in order to help guarantee the freedom to maneuver in cyberspace, to move data through the network without being compromised, and the ability of business to thrive in modern economies. A safer cyberspace is one of the key elements for the healthy economic growth of a nation and a good indicator of an unyielding cyber defense strategy.

TYPES OF CYBER WARRIOR

At the core, it is essential that a cyber warrior be driven by a sense of patriotism or zealotry that forges unyielding vigilance. Moreover, linking this conviction to a "higher calling" or sense of purpose ties people to a set of universal ideals that focuses their energies on protecting the home front, and on constantly moving forward. A driving force must exist to motivate an individual to become a lifelong student of cyber

warfare and to enter into a process of continuous self-improvement. Consistently, if one were to ask a deployed Marine if he/she were happy out in the operating environment, the response would be a resounding "Yes!" Quite simply, this is because persons with a warrior mindset yearn to answer that call to employ their special set of skills in support of the mission. The various skill sets and expertise at all levels of command (tactical, operational, strategic, etc.) each have their own unique requirements.

The first level of cyber warrior is the generalist, which is similar to the infantryman who knows how to use a rifle, basic demo, basic navigation, and so forth. At this level (Cyber Warrior—Generalist), the basic cyber warrior should have at least a simple understanding of the following concepts: hardware, networking (wired and wireless), penetration, defense, exploitation, and cryptography. Basic certifications for this level might include those such as A+, Security+, Microsoft Certified IT Professional (MCIPT), Juniper or Cisco, Certified Ethical Hacker (CEH), and Computer Hacking Forensic Investigator (CHFI).

After the Generalist comes the Cyber Warrior—Specialist. These cyber warriors have a mastery of the basics and then continue to develop their skill sets, proving mastery to a specialty. Three main specialties are computer network exploitation (CNE), computer network attack (CNA), and CND.

Cyber warriors who specialize in CNE are comparable to the Armor Scouts and Scout CAV (Cavalry Scout). These are people who know how to infiltrate networks to collect information through hardware, network, malware, and so forth. In addition to the basic education, they would have specialized training and have a deeper capacity in understanding the "big picture" of combine arms combat, such as how to envision the way little pieces fit into the whole, how to inject misinformation, how to alter in very subtle ways targeting information, and so forth. They do not disrupt networks; instead, they remain hidden like traditional Scouts to "spy" and report.

Next are the cyber warriors who specialize in attack (CNA). These are like Special Forces; they exist for the sole purpose of destroying networks, denying networks, and causing total collapse of communications. Unlike the exploitation specialist, they will further their training in penetration and disruption tools.

Then there are the cyber warriors who specialize in defense (CND). This has been argued that a CND cyber warrior knows all CNA methods and works to defeat CNA attacks. This indicates an understanding of attacks and how to perform countermeasures. This is a major difference from what is traditionally considered to be CND today. Many people, even those in the field, think that CND is little more than implementing a Security Technical Implementation Guide (STIG), maybe retina scans, but the bar must be raised when discussing what CND means as a cyber warrior.

ACKNOWLEDGMENTS

I would like to dedicate this chapter to The Cyber Security Forum Initiative members and to my close friends who support my mission "to provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the U.S. Government, U.S. Military, Commercial Interests, and International Partners."

I would also like to recognize the insights of USMC Sgt. Nicholas Andersen, U.S. Army Major Alexander Tambascia, U.S. Army Lt. Col. Mark Coffin, USMC Major Anthony Guess Johnson, USAF Col. (Ret.) Jeffrey Caton, and USAF Major General (Ret.) Harold W. "Punch" Moulton II.

CHAPTER 19

From Cyber Terrorism to State Actors' Covert Cyber Operations

Jan Kallberg, Bhavani Thuraisingham

INTRODUCTION

During the first 20 years of the Internet era there was a widespread fear of threats from the Internet, but in reality it was fairly secure. The limited abilities and resources of the early attackers contained the threat to criminal activity and marginal damage. Recent advancements in client computer security, in conjunction with the impact of time and Internet maturity, have created a population at ease and with and trusting of the Internet. In reality, the Internet has a reverse trajectory for its security, where the Internet has become more unsafe over time. The threat no longer engulfs just individuals and businesses, but also the nation state. In almost 20 years concerns have been raised about what single hackers and cyber terrorists can do to a targeted society or individual. In the mainstream media, and our collective weltanschauung, hackers and cyber terrorists have been credited with the ability to create a digital Armageddon or, in American terms, a digital Pearl Harbor. Naturally, the loudest and most graphic contributions to the public sphere have been either news media trying to get our

attention or computer software companies in pursuit of marketing their security software. Fear has been the main driving source.

In reality, hackers have not achieved any significant national disturbance or damage to the nation state in the last 20 years. Successful hacker attacks mainly stole information that affected a number of individuals or companies. The few events that targeted the government, such as the highly publicized Wikileaks incident, a massive theft of federal information and communications, did not have any significant long-term impact on the targeted society. The nation state stood unaffected.

Traditionally hackers had little or no interest in destabilizing or challenging the state. The reasoning behind this could be as simple as there is no monetary gain for such activity. Cyber criminality is an enterprise that seeks to earn money through illegal activities and defraud others. That is one reason why fighting cybercrime has had such a low priority as measured by the number of prosecutions. The traditional cybercrime does not threaten the state, the government, or the societal order, and there is no sizeable harm to the general population.

Low Incentive to Attack the State

Cyber criminals are instead avoiding a state confrontation for a simple set of reasons: prosecution, forensics, and ability to extradite. For example, a criminal activity that steals \$5 from 100,000 individuals worldwide by using their credit card numbers benefits from the fact that the \$5 is still \$5 for each victim. Only a few of these 100,000 victims will take their time to fill in a police report or report the crime to federal authorities, because they realize that they probably will not get their \$5 back. Unless the federal authorities or credit card companies organize a legal counter activity, the theft of \$500,000 goes unpunished. The perpetrators can increase the likelihood that they are never prosecuted or extradited overseas, because the victims are not organized and have no resourceful institutional body to take counteraction. If the cyber criminals instead attack a state, for example, the UK, United States, or France, and create significant damage, the cyber criminals face a forceful counteraction and law enforcement. Until now the aggressors on the Internet have been of minor size and limited resources, but this is changing as states become involved in a militarized cyberspace.

The Militarized Cyberspace

The militarized cyberspace becomes a contested domain when state actors enter in pursuit of an intelligence objective, power maximization, and national security concerns. The main difference now is that there are massive resources available for state actors compared to the earlier generations of independent hackers. States can engage knowledge and ability generation through the defense industry, academic research centers, and covert operations, and outsource the cyber warfare to industrial contractors.

This represents a major shift in the threats. The hackers are no longer a few people operating with a marginal budget in their spare time. Cyber attacks are becoming a well-funded operation, sanctioned from within the defense and intelligence establishment of the attacking

country, using allocated resources equal to any military and intelligence operation. This serves as the argument for the comparison, and contrary to the common belief, that the first 20 years of the Internet were more secure than the cyber environment of the future.

The entrance of state actors and the creation of a militarized Internet used as a contested space for intelligence, economic espionage, information operations, and to destabilize adversarial states has radically changed the fundamentals for security in cyberspace. The state actor seeks to exploit weaknesses in the critical national infrastructure and information systems, and take advantage of the fact that our populations rely heavily on the Internet.

One major weakness in the advanced societies is the overemphasis in cyber security training and research on information assurance and the hardening of systems when the paradigm has changed toward full-spectrum cyber operations (Kallberg and Thuraishingham, 2012). By continuously hardening systems a false sense of control and security is maintained, mainly based on the earlier attacker profile with single individual or small criminal efforts to penetrate the system. Other security concerns related to cyberspace such as influencing population sentiment, information operations, and destabilizing governments by systematic attack are unaddressed. Cyber security now consists of tools and the implementation of those tools and lacks abstract theory, therefore, becoming incoherent and lacking a strategic societal system approach. This gap of consistency is an inlet for attacks.

The Growing Cyber Opportunity

The state acts in the state's best interest, unless it is confused by media. In the last decade the national security debate has oftentimes missed the distinction between national security and individual security. The attack on the World Trade Center in New York added fuel to an already established popular notion that attacks on a number of individuals are an attack on the state. Terrorism is a menace and it is the state's

responsibility, as the state claims the right to maintain the monopoly on violence, to protect the citizens of the state. The blurred demarcation between national security and individual security becomes apparent for a cyber-defending nation. Cyber attacks, seen from a state perspective, are annoying and a threat to the economy until it reaches a point when it becomes a national security concern. The United States considers an attack on military networks, critical infrastructure, and main industries as an attack on the state itself.

As cyberspace matures, states are able to define their reasoning and level of thresholds for national security response. Over the last few years there has been a shift in cyber strategy focusing on the national security. During the next decade the national security concerns in cyberspace are likely to override the earlier paradigm of focusing on securing individuals and single corporations. The attacks on individuals and corporations have become solely a criminalized act; meanwhile, the state considers attacks on the national critical infrastructure, the state's core function, the state's legitimacy and authority, and its military complex as attacks on the state itself.

The increased reliance on computer networks, changes in societal sentiment influenced by the Internet, and the increased complexity create opportunities for an aggressor and terrorists. It is unlikely that terrorists will be able to represent a permanent cyber threat to a nation due to the cost and infrastructure needed. The combination of a covert state actor and terrorists as executors of attacks creates a different more likely scenario for the future.

Covert Operations by Proxies

The scenario becomes more complex if a state actor gathers information about cyber vulnerabilities in the networks of a targeted organization or other nation and then outsources the attack to a criminal or terrorist network. This innovative *modus operandi* creates numerous obstacles and considerations for the targeted organization. First, the attribution problem is highlighted,

because even if the executing criminal network is identified, it is still unclear which actor initiated the attack. Criminal networks are enterprises and the compensation could be a range of illicit goods (Kan, 2009). States can pay to get things done. If necessary, a covert operating state can pay criminal networks cash, drugs, weapons, or any currency to act as a proxy. Terrorist organizations can finance their operation through cyber terrorism "entrepreneurship" instead of engaging in other forms of financing that are far riskier for detection such as drug dealing and credit card fraud. Second, the lack of attribution evaporates the option to initiate retribution against the initial attacker. Third, it is likely that the vehicles for the attack are dismantled directly after the attack. The computers and networks that were used for the attack are no longer in use afterward. The lack of attribution removes the risk to engage and the fundamentals of state-to-state deterrence are no longer in place (Reed, 1975).

Cyber terrorists can be a national security threat, and create significant damage to critical infrastructure and national assets for the targeted state, if the terrorists are given the toolset and pre-attack intelligence from a state actor. The covert warfare in cyberspace in many cases resembles the covert operations in the Cold War. The targeted country, or organization, could assume where the attack is coming from but attribution is not strong enough for retribution. A state engaging in retribution toward another state could face other grave unanticipated political consequences, which pose uncertainty and generate a risk-averse state actor.

The aggressor's risk is lowered if the state actor collects vulnerabilities in the opposing state's networks, builds cyber weapons, and creates a strategy to create disruption and destabilization in the opponent's networks, but uses a proxy to carry out the actual attack. In this case the aggressor is unlikely to be held accountable for its actions. The opportunity not to be held accountable is extremely inviting for countries that are covert adversaries.

If the adversary is skilled, it is more likely the attribution investigation will end with a set of

spoofed innocent actors whose digital identities have been exploited in the attack rather than attribution to the real perpetrator. A strong suspicion would impact interstate relations, but full attribution and traceability are needed to create a case for reprisal and retaliation. Attribution can be graduated, and the level varies as to what would be accepted as an "attributed" attack. The national leadership can accept a lower level of tangible attribution, based on earlier intelligence reports and adversarial *modus operandi*, than the international community might demand, but it is restrained in taking action.

La Raison d'état

Cyberspace is already by definitions and doctrine a war-fighting domain even if only a few states are able to do any offensive cyber operations, but the strategic abilities will grow in the next decade. There are several reasons why cyber weapons are inviting.

In an era of austerity countries seek alternatives to traditional military policy options that are better suited for future conflicts, but also reduce the collateral damage that a kinetic operations creates. The pursuit of cyber abilities also drills down to pure financial numbers (Kallberg and Lowther, 2012). Militaries are expensive and require a standing force to ensure ability and deterrence. If the force is a professional army it will cost to recruit, train, pay, and pension its soldiers. In modern state reasoning, cyber warfare is a cheaper option for both covert operations and to engage and destabilize an adversary (Kallberg and Lowther, 2012).

States act in their own self-interest; therefore, it is questionable if a regulated cyberspace is in the long-term interest of the major powers, as a restrictive use of cyberspace would undermine their dominant status. Earlier efforts to create a uniform approach toward information technology security on a global scale have shown marginal progress. One example is the global standard for security certification of hardware, "Common Criteria," that has been hindered by the lack of unrestricted trust between nations

(Kallberg, 2012a). If any international effort fails to create a uniform approach to securing the Internet domain we can assume by logic that major actors prefer the anarchy before order because there is a perceived opportunity and potential future gain for these powers.

Expanded Reach for Cyber Conflicts

State actors will implement cyber conflict at all levels that benefit the state. As an example, targets that had limited value for cyber criminals, such as the global space-borne information grid, are a prime target for a state actor (Kallberg, 2012b). Satellites are a major concern for any state or nonstate actor who intends to conduct operations in secrecy. Satellites gather intelligence, provide surveillance, and perform reconnaissance (Moltz, 2011). This can be extremely annoying to states that seek to avoid transparency between their international commitments, their public posture, and their actions behind the scenes.

Terrestrial cyber attacks are a single exploit on thousands, if not millions, of identical systems, and the exploit will be eliminated afterward by updates or upgrades. The difference between satellites and terrestrial cyber exploits is that a satellite is often custom made, whereas the computing design is proprietary. Cyber attacks in space exploit a single system, or limited group of systems, within a larger group of satellites (*Wired*, 2011). These space-borne assets have a variety of operating systems, embedded software, and designs from disparate technological legacies. As more nations engage in launching satellites with a variety of technical sophistication, the risk for hijacking and manipulation through covert activity increases. A satellite's onboard computer can allow reconfiguration and software updates, which increase its vulnerability to cyber attacks. The attack on the satellite is tailored, one shot, and unique.

An attributed cyber attack on the global information grid would be considered an act of war, and provide the targeted state with at least a theoretical *casus belli*, a risk that the aggressor would

seek to avoid. An act of war is a tangible security risk that can have catastrophic consequences for an aggressor nation. Are attacks on the global information grid ideal for being outsourced from the aggressive state actor to terrorists and criminal network to avoid attribution? The symbiosis between a state actor and cyber terrorist can provide an ability that makes cyber terrorism a tangible national security threat at the strategic level.

CONCLUSION

The threat from cyber operations will increase in the next decade, even if we have implemented extensive information security. The Internet and the application layer become a globally contested domain where the entrance of state actors as contestants and aggressors create a radical shift. The early hackers and information thieves had limited resources and mainly a financial goal. State-run operations have a complete different set of targets and goals.

If states collect vulnerabilities in targeted systems, utilize the whole covert spectrum, and

instead of attacking themselves uses terrorist groups as proxies, then cyber terrorism is a tangible and relevant national security threat.

The digital environment where critical assets can be copied, sent, and forwarded within seconds, ushers in a symbiosis between aggressive adversarial state actors and terrorist networks when the state actor can produce military-grade cyber weapons for the terrorists to use. Waltz (1990) argued that the power embedded in nuclear arms is not what you do but what you can do. The outsourced proxy cyber war from state actor to cyber terrorists operates along the same lines as military-grade cyber weapons dispersed to violent groups and militant political groups create extensive uncertainty. This uncertainty is based on what an aggressor can do—not what they actually do.

This development creates an asymmetric covert conflict with an anonymous aggressor and a reactive targeted society. Terrorists can reach their objectives, create damage, influence policy, and leverage the disproportional power relation between terrorists and the defending state.



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 Survey™, 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 Abujihad 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). Abujihad 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 honeypots 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 accidentally), 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 sites 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 through 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 threats 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.

Langner 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 hacktivism, 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 19080s (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 (Birmingham 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.



CHAPTER 21

Developing a Model to Reduce and/or Prevent Cybercrime Victimization among the User Individuals

Hamid Jahankhani

INTRODUCTION

It appears that the current thinking in cybercrime prevention puts the technology first and concentrates on protecting computers and devices with the hope that the users will not fall victim to cybercrime and forget about the human element in crime.

Unlike traditional crime, which is committed in one geographical location, cybercrime is committed online and it is often not clearly linked to any geographical location. Therefore, a coordinated global response to the problem of cybercrime is required. This is largely because there are a number of problems that pose a hindrance to the effective reduction in cybercrime. Some of the main problems arise as a result of the shortcomings of the technology, legislation, and cyber criminology.

This research is primarily based on the hypothesis that understanding the characteristics of the users of the computer systems will allow for the creation of more effective cybercrime prevention strategies, which will also result in reduced impact on the users as compared to a

more broad-brush approach to crime prevention. A secondary hypothesis of the research is that the particular characteristics of the users have an impact on their vulnerability to cybercrime. A consequence of this hypothesis is that if this is true, then it is important to identify the relationship between the particular characteristics of the users and its linkage to the type and severity of cybercrime. This kind of linkage will allow for the development of more effective crime prevention techniques, which will be tailored to the type of user. The entire population of users of the Internet can then be classified on the basis of the particular characteristics and the appropriate techniques deployed for the particular class of users. This will, in turn, serve to increase the effectiveness of these crime prevention programs further, as they will enable the more efficient use of resources.

CRIME PREVENTION THEORIES

The theories of crime prevention are distinguished from theories of crime causation, and while the two may be linked in some cases in the

literature; however, they are seen as rightfully being regarded as distinct because of the following:

1. There is no established theory of crime causation that can be accepted and used as a basis for preventative theories.
2. The issue of crime prevention is not a theoretical pursuit at all. While criminality theory focuses on causality, prevention, and transcends etiology, it proceeds into the field of strategy and tactics.

Therefore, while theories of criminality are abstract, and based on deduction and observation, prevention is practical and must seek methods of controlling human behavior in practice. The two fields, therefore, differ substantially at a theoretical level.

It is widely argued that many of the conclusions reached from a theoretical approach to criminology had failed when applied to practical scenarios, both due to the difficulties experienced when attempting to put theory into practice and also because in the sociological field society constantly changes during the period between the development of a theory and the time of its practical application. Therefore any consideration of the theory of criminology must be conducted with a view to the strategy and tactics that would be used to put that theory into practice in the field. Crime prevention theory must focus on its goals of preventing crime before it occurs, and preventing persons who have committed crimes from re-offending. Therefore, application of theory that does not focus on this goal would result in fruitless efforts.

The two factors that are generally used to explain the causes of crime are environment and personality.

Looking first at environment, Lunden (1962) argued that attributing crime to environment would deny the social reality that there is very little meaningful community existence in modern society. Therefore, any criminological theory that concludes that the community must adapt to prevent crime, in Lunden's view, is useless; because, in the field, working with criminals and working in areas of high crime, there is no distinct

and specific community with which to work. It was noted that a crime prevention theory implies some kind of social reform that would be implemented in favor of the status quo. Therefore, theory comes up against resistance in practice, as most people distrust reform. The theories must, therefore, be willing and able to overcome such resistance to any type of change in the social sphere if they are to have any chance of making a difference in practice.

The second common theoretical approach views crime as the result of complex internal and emotional reactions to the environment. Another criticism Lunden made of criminological theory is that it tends to view crime as a pathological or abnormal behavioral trait, rather than as a fairly normal aspect of human behavior. Lunden went on to conclude that it is impossible to prevent all crime, although it is possible to decrease the amount of it. It was also noted that there are and have been in the past, societies with only a minimal level of crime. However, not many people would choose to live in such societies. As long as there are human beings, there will be crime. Therefore, criminological theory must deal with this fact as it applies to today's society, one that has little and weakening community.

Geason and Wilson (1988) examined a number of criminological theories including rational choice theory, which portrays criminals as economic decision makers who make conscious choices to commit crimes because the benefits outweigh the costs or are perceived as such. Situational crime prevention, which entails "the use of measures directed at highly specific forms of crime," was also examined by Geason and Wilson (1988). This involves the management, design, or manipulation of the immediate environment in as systematic and permanent a way as possible. This system, often referred to as primary prevention, seeks to reduce the chances of committing crime. Situational approaches to crime prevention are based on rational choice theory in that they view the crime as the result of a conscious decision that the perpetrator of the crime was able to make, in response to the circumstances and environment they are presented with. This assumes that

the motivation to commit crime is not beyond control. Geason and Wilson (1988) suggested a link between situational factors and personal internal factors. That is, the decision to consider committing a crime in the first place would depend on the personal characteristics of the individual, while the final decision on whether or not to commit the crime in this particular context, and in this particular moment, would depend on the situation.

Geason and Wilson (1988) went on to discuss the issue of displacement, which is a major criticism of situational crime prevention. This argument holds that situational preventive measures do not prevent the crime from occurring absolutely, but merely force the criminal to reconsider the options. For example, the installation of a house alarm is a situational preventive measure but if the burglar simply decides to burgle a neighbor's house instead, then it cannot really be claimed that a crime has been prevented, it has simply been moved to another more accommodating location.

Situational Crime Prevention Theory

Beebe and Rao (2005) looked at the application of situational crime prevention theory as a means of explaining information systems security and its effectiveness. The value of information as an asset in today's economy and the role that information systems security technologies could play in protecting such assets were noted. They argued that it would be necessary to understand the factors that could contribute to the effectiveness of such security systems. What Beebe and Rao (2005) achieved is an extension of the theoretical study of security in relation to computer data, using situational crime prevention theory. The issue of extending a criminal justice theory designed to cover physical crimes to computer-based crimes was addressed, and a conclusion was made that situational crime prevention theory may be nonetheless effective, and that there are opportunities for the theory to improve the effectiveness of information systems security approaches by reducing the anticipated amount of crime.

Lifestyle Routine Activity Theory

According to Cohen and Felson (1979) the lifestyle routine activity theory (LRAT) suggests that crime is likely to occur when the following factors converge:

1. Motivated offenders
2. Suitable targets
3. The absence of capable guardians against violation

Cohen et al. (1981) tested the effect of LRAT variables (exposure, proximity, and guardianship) on criminal incidents (burglary, assault, and personal larceny). Using National Crime Survey statistics of U.S. households, they found that LRAT variables have a significant effect on predatory victimization.

LRAT would suggest that all criminal events occur in a particular place at a particular time. Cohen and Felson (1979; cited in Kyung, 2008) asserted that "the synchronization of a perpetrator's rhythms with those of a victim's" facilitate a convergence of a potential offender and a target. Cohen and Felson (1979) also believed that examining how and why criminal offenses occur in particular places may be useful and important to a study of cybercrime victimization. This argument relies on the notion that cybercriminals often search for suitable and valuable targets in specific types of social arenas (Piazza, 2006).

However, the Internet as a part of human environment and the physical measures taken to prevent the traditional crime are similar to those used to increase cyber security. The software, such as antivirus and firewalls, should not be ignored by anyone as a part of the cybercrime prevention strategy, especially if the computer is part of the network. As the physical prevention measures, the software is protecting and guarding the user devices (PCs) in the Internet.

Jahankhani and Al-Nemrat (2010, 2011) have tested the LRAT and identified the importance of three elements of LRAT, in particular the discussion of the three subelements of capable guardianships. It can be concluded that none of the strategies can play an effective role in reducing

cybercrime victimization or can guard against cybercriminal activities when operating in isolation.

Furthermore Jahankhani and Al-Nemrat (2010, 2011) recognized the importance of awareness as an element in reducing cybercrime victimization in the society. It therefore seems appropriate to introduce “user awareness” as a new category within theoretical capable guardianship, accompanying formal social control, informal social control, and target hardening.

This new pillar will strengthen the guardianship discourse in its fight to reduce cybercrime victimization. In order to support the argument that “user awareness” is a crucial key element that needs to be added to the capable guardian, it must work in coalition with other elements. The model of Jahankhani and Al-Nemrat (2010, 2011) shows how user awareness may play a vital role in reducing cybercrime victimization in light of LRAT (Figure 21.1).

CRIME PREVENTION MODELS

Cyber Terrorism Prevention Model

Fiore and Francois (2010) developed a cyber terrorism prevention checklist for use by organizations. This model consists of actionable steps that management and information technology (IT) security departments could put in place to prevent an organization from becoming a victim of or its infrastructure being unwittingly used for cyber terrorism. The model comprises actions

that relate to intelligence gathering, an area that was claimed to include three possible security lapses that would lead to penetration of an organization's system and loss of confidential or sensitive data. Strategies include the avoidance and actionable prevention steps of identity impersonation or identity theft and Spyware. Some of the preventive steps include access controls, document controls, information procedures that will protect data and identities, scanning programs, the installation and maintenance of firewalls, intrusion detection systems, and the use of third-party software audits.

To avoid internal threats from an organization's own employees, Fiore and Francois (2010) recommended carrying out stringent background checks. Also, policies and procedures are required to deal with disgruntled employees and to control any backdoor threats. The importance of testing all backup systems was also highlighted.

Within the area of systems damage, Fiore and Francois identified four areas of security lapse. The first is breakdown in the human firewall, which can be reduced by using inquiries, controlling points of contact, and ensuring awareness of people in the building or accessing IT equipment. Bounds checking and code reviews, system patches, and the use of alternative heterogeneous applications and platforms can reduce threats. The IT department can also be filtering any executable file attachments that are received from outside and taking steps to educate users on the methods that can be used to reduce the risks.

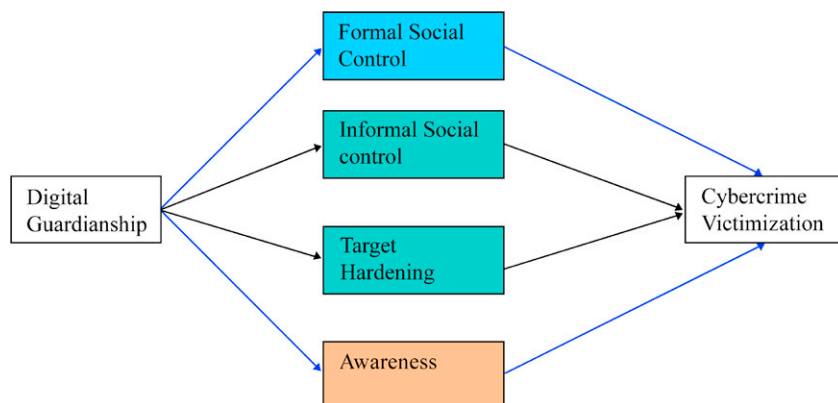


FIGURE 21.1 The structural model proposed by Jahankhani and Al-Nemrat (2010, 2011).

Wireless network strategy together with strong user authentication procedures is essential and must be in place. Organizations can also make use of Virtual Private Network (VPN) technology that makes encrypted data difficult to access. The use of Wireless LANs and wireless demilitarized zones can make wireless networks more secure. In order to reduce the risk from denial of service attacks, recommendations are to filter RFC 1918 addresses, controlling spoofed addresses, monitoring bandwidth usage, and scanning internal hosts and devices. System hijacking, which allows others to communicate securely using an organization's network, has been linked to steganography and can be controlled by checking for unauthorized software. Scanning both inbound and outbound e-mails to ensure that unusual files are not being attached is also essential.

Organizations often assume that using proxies or firewalls will prevent unauthorized Web surfing or unauthorized passing of information to external recipients. Using a SOCKS server or port mapping, HTTP tunneling can get around TCP and UDP. It is important to review logs of traffic to ensure that corporate espionage is not taking place. IT departments should monitor systems closely to ensure that corporate security policies are not being bypassed. Also, it should be ensured that unauthorized VPNs are not being used to mask unauthorized access to the system. Worms, Trojan horses, and viruses are becoming more prevalent, sophisticated, and capable of ever more intelligent attacks on systems. Scanning for unauthorized software is important in reducing the risk of such attacks, as is the use of up-to-date antivirus software, and perhaps considering the use of alternative heterogeneous applications or platforms that are less susceptible to attack. Educating users and ensuring proxies and firewall filters that are working effectively are also important steps.

Disinformation, which could include the dissemination of false information from an organization, or the insertion of false information into databases to reduce the effectiveness of such databases, is also potential threats. Such potential threats can be dealt with to reduce the risk of their occurrence.

DNS poisoning and domain hijacking involve falsifying IP addresses or stealing a domain from a registrar, and the risk of this can be reduced by using the latest security features of DNS, ensuring passwords are in use, and requiring SSL encrypted Web page or PGP signatures from e-mails.

DNS information should also be controlled and prevented from being taken from a system. In order to avoid Web site defacement, which is the unauthorized alteration of Web site content, staging servers should be read only, user authentication should be required for "sign-ons," software patches and security policies should be maintained and kept up to date, DNS should be hardened, and code should be reviewed to ensure weaknesses are weeded out of the system.

Cybercrime Execution and Analysis Model

Hunton (2009) demonstrated the opportunities for law enforcement when investigating the cybercriminal by defining an emerging cybercrime execution model.

Such models will allow for the transfer of conventional policing models into the cybercrime environment, which is often seen as being abstract and too technical for the application of such models. Before setting out the specific components and characteristics of this model, Hunton (2009) reviewed the background to the issue. The aim was to simplify cybercrime investigations so that investigators and analysts would cooperate and work together better when investigations are taking place. Such cooperation is currently hampered by the complexity of investigations. By providing specific points of reference, it is hoped that cooperation will be more practical. The components of cybercrimes that are in common with other crimes will be identified and this will provide areas of common ground upon which cooperation can be based.

Hunton's (2009) model aimed at assisting investigators in planning their investigations, regardless of the level of complexity of the investigations, with due regard to the techniques and technology that would be used, and in a manner

that would allow for a consistent examination of each element of the crime. The intention of developing the model was to provide a tool that could facilitate further innovation of both practices and policies in the field of cybercrime investigation. This involves breaking down the technical tasks that are required to be performed into more manageable and use of the Internet and other networks to facilitate the process. Given the difficulties of cybercrime that include both technical and technological complexities and legal issues surrounding the fact that there is no common legal system across the Internet, there is a growing urgency surrounding development of such models. Hunton's (2009) claim that the model proposed allows for specialist skills to be identified rapidly and ensure that the knowledge necessary to secure relevant and admissible, high-quality evidence is present at the stage that they are required. This will also facilitate more simple communication of the elements of the execution of the crime and its investigation, in courts and to juries, as well as to victims of cybercrime.

Virus Prevention Model

Wang et al. (2009) looked at the lack of effectiveness of traditional antivirus methods to prevent virus infection. They proposed a behavior-based virus prevention model. The behaviors are defined by observing dynamically linked libraries and application programming interfaces. Information was then filtered to ensure that redundant behavior attributes were identified and informative features for training a virus classifier were selected. The performance of the model on a database of 1,758 benign executable files and 846 viruses was measured. It was noted that the results of the experiment were promising with 99% of known viruses and 96.66% of previously unknown viruses detected.

Cybercrime Prevention and Detection Model

Shiva Kumar (2003) examined the types of cybercrime and identified the types of harm they caused. Shiva Kumar also discussed the

preventive steps that governments and organizations could take to reduce the risks from these harms. Provisions of cyber law were examined and the elementary problems associated with cybercrime were noted.

Cyber Trust and Crime Prevention Model

Collins and Mansell (2004) examined the issues of cyber trust and crime prevention. In a report commissioned by the UK government, they examined the position of crime prevention in this field by making reference to science journals. Their report stated:

provide a synthesis of theoretical and empirical work in the sciences and social sciences that indicates the drivers, opportunities, threats, and barriers to the future evolution of cyberspace and the feasibility of crime prevention measures. It was based on ten state-of-the-art science reviews commissioned by the Foresight Project. Each of the papers highlighted the current state of knowledge in selected areas as well as gaps in the evidence base needed to address issues of cyber trust and crime prevention in the future

Collins and Mansell (2004) examined the issues of complexity of system behavior, managing identities in cyberspace, cyberspace usability and risk management security, cyberspace and crime prevention strategies, building forensics into data management tools, and cyberspace market evolution.

Cybercrime Reduction and/or Prevention Model

Efforts to reduce and/or prevent cybercrime victimization among user individuals have put the technology first and concentrate on protecting computers and devices with the hope that the users will not fall victim to cybercrime. These technical interventions differ significantly from mainstream crime prevention models that focus on the human element in crime. The field of criminology is yet

to catch up with the explosion of the Internet and cybercrimes. Jahankhani and Askerniya recently proposed a grid model for classifying cybercrime prevention strategies along four different dimensions (Figure 21.2). These include (axis X) the level of “Tech-savviness,” (axis Y) individuals at different levels of risk, (axis Z) the cognitive developmental stages of the individuals, and (idea/theme axis) the prevention program goal.

This model considers social aspects as an important element within crime prevention techniques and link education and awareness as a key player in crime reduction.

The Level of Tech-savviness. The first dimension on the grid model represents the level of tech-savviness targeted by the intervention.

Strategies for reducing and or preventing cybercrime have been focused at risk and protective factors required for the different types of Internet activities in which individuals engage.

Specific activities included in the grid model are based on the most common habits/activities individuals’ exercise on the Internet. However,

this does not mean that the individual user is engaged with all the listed activities, but definitely with at least one of them. In order to reduce risk and improve protective factors, interventions have focused on improving participant’s awareness, education, and training with regard to specific skills related to the specific listed activities.

These interventions need to be implemented on different developmental stages of the individuals in an attempt to help the users not fall victim to cybercrime.

Risk Level of the Participants. The second dimension in the grid relates to the users’ levels of risk and the extent to which interventions need to concentrate on participants’ level of knowledge, awareness, and training.

Low risk is allocated to users who have extensive knowledge of technology and the Internet exposure risks. Medium risk is for users who do not know enough about Internet exposure risks and are above average risk of falling victim to cybercrimes, including online

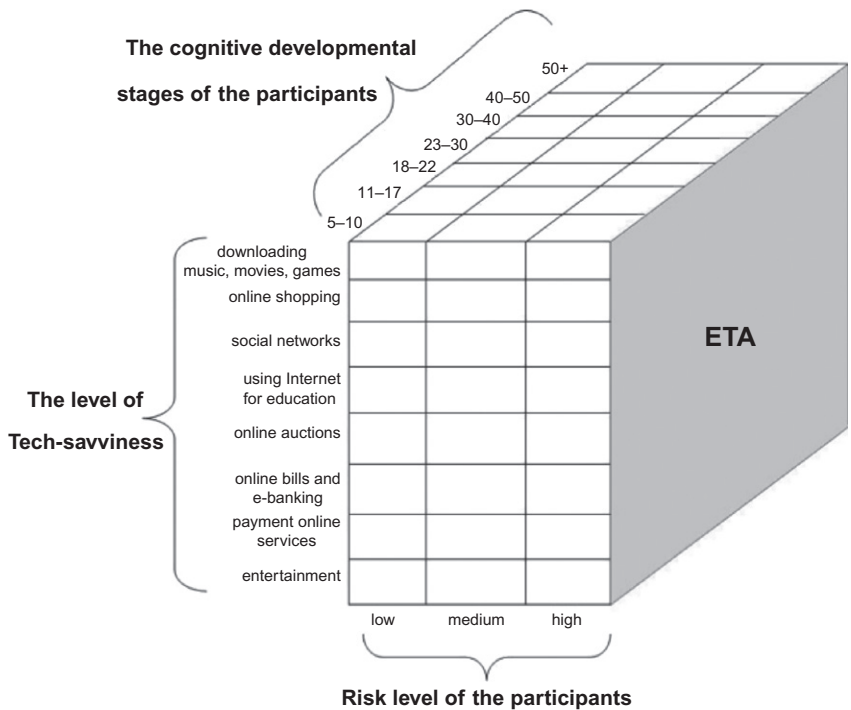


FIGURE 21.2 Cybercrime reduction and/or prevention model (Jahankhani and Askerniya, 2012).

credit card fraud, identity theft, and computer viruses. This group of users has an up-to-date knowledge of securing computers and devices, but they do not have a deep understanding of how to change their behavior when they are online. The high-risk users are the people who surf the net aggressively and continuously expose themselves to the elements. This group of users puts both themselves and the people around them at high risk.

Cognitive Developmental Stages. The stages of cognitive development are represented in the third dimension in the grid. Risk and protective factors have different effects at different developmental stages. Therefore, aim of the prevention would be different depending on the age of the user.

Prevention Program Goal. The fourth dimension in the grid model represents the prevention program goal.

The most effective strategy to reduce and/or prevent cybercrime victimization among user individuals is to improve on cognitive development and behavioral skills by developing a set of education, training, and awareness programs specific to Internet exposure risks and cyber behaviors.

The term “awareness” is very popular in the academia and the industry. It is used massively in different areas of computer science and Internet security.

Barney and Anselm (1964) singled out following four different classical types of awareness;

1. An open awareness means that each member of society is aware of the others’ true identity and his or her identity among the others.
2. A closed awareness refers to when someone does not know either the other's identity or the other's view of his identity.
3. Furthermore, we have suspicion awareness, which is a modification of the closed one. That is, someone suspects the true identity of the other or the other's view of his own identity, or both.
4. Pretence awareness is a modification of the open one. Here, both “interactants” are fully aware but pretend not to be (Barney and Anselm, 1964).

Liechti and Sumi (2002) in their research “Editorial: Awareness and the WWW,” formulated the definition of awareness on the Internet as:

True, awareness is often meant as awareness of other people, and refers to the ability to maintain some knowledge about the situation and activities of others. Having a general idea of what is happening, or merely that something is happening, is often already very valuable.

The model has a number of significant strengths. First, it is simple, and therefore easy to understand. It is important that a model is easily understood if it is to be applied widely and effectively. Second, the model is able to respond to changes in the external environment, such as changes in the nature of cybercrime. This is because the content of the education and training programs can be changed according to the new threats. Another advantage of the model arises from the reliance on situational crime theory. As highlighted earlier, situation crime theory does not have boundaries; this means that the theory develops with the manner in which the crime itself develops. If, for example, cybercrime turns out to become a major threat to users of tablets and smartphones, the training and awareness programs can be developed such that they educate users about how to guard against cybercrime on these platforms. This ability of the model to be relevant and adaptable to change in the external environment further lends to its practicability. Models that are highly specific may not be as flexible and able to respond to changes in the external environment. It would, therefore, be impractical to spend a significant amount of money in implementing models that might become obsolete and useless after a short period of time. This model, however, can be made to be relevant even when there are significant changes in the external environment. However, the unavoidable downside of this adaptability is that the implementation details of the model have to be regularly updated. That is, the contents of the training and awareness programs have to be continually updated for it to be effective and actually prevent and/or reduce cybercrime.

The situational crime prevention theory would require the use of measures directed at highly specific forms of crime, which should also be as permanent as possible. The three measures suggested by the model, namely education, training, and awareness, are all able to effect changes that are permanent in nature. The training and education of users to make them aware of the current threats and how they can protect themselves creates users who are more technically savvy. Hence, even if constant reinforcement training is not provided, the users will already have a basic amount of technical knowledge and are able to continue to keep themselves updated. This is a permanent change for the better.

Furthermore, the entire model is based on the adoption of preventive measures to deter crime. Educating users' results in them taking better precautions and also serves to make their systems better protected against attacks. Better protected systems are less likely to become targets. A large number of attacks are instituted on systems that have no protection.

CHALLENGES FACING PREVENTIVE MEASURES

Many computer systems are protected by the security mechanism of user accounts that can only be accessed with a valid username and password. The username and password combination method of securing user accounts and computer systems are one of the, if not the oldest, methods of providing security to a computer or a computer network. However, the username and password method is not a very secure method. Usernames and passwords can be easily guessed. Password-cracking programs, which run all permutations and combinations of the ASCII characters in order to guess the username and password of an account, are easily available. Furthermore, users often forget their passwords, which means the computer systems have to provide mechanisms by which the passwords of the user accounts can be reset. This provides opportunities for criminals to gain control of these accounts by posing

as legitimate users who have forgotten their login credentials. Clearly, more secure technology for regulating access to computer systems is required. Currently, more secure technology such as facial recognition and biometric identification systems are being developed. Many new computer systems already use these technologies to secure access. When these technologies mature and are used more widely, it can be expected that the traditional username and password login credentials will become obsolete. In addition to shortcomings with the technology for regulating access to computer systems, other shortcomings of technology exist, which allow attackers to gain control of a computer system. These are often called "zero day attacks." Therefore, attackers are continually looking for new vulnerabilities and take advantage of systems that have not been patched already.

Legislation is a major issue, but the attitude toward cybercrime and its victims needs to be addressed if we are to see an effectual clamp down on cyber villains and the like. Investment is essential, accurate recording of cybercrime does not exist, and international legislation and bureaucracy are major barriers for investigators.

There is no supreme regulatory body with adequate power to enforce the required regulations. In fact, the regulations do not really exist, other than those written on the statute books of individual countries. It seems therefore, that although certain jurisdictions are concentrating on resources to build an infrastructure around formalizing what constitutes cybercrime, little effort or funding is put into supporting law enforcement to tackle the proliferation of offenses committed.

Yar (2006) articulated the shortcomings of criminology in the arena of cybercrime as being the problem of where and who. Many criminological perspectives define crime on the social, cultural, and material characteristics, and view crimes as taking place at a specific geographic location. This definition of crime has allowed for the characterization of crime, and the subsequent tailoring of crime prevention, mapping, and measurement methods to the specific target audience.

However, this characterization cannot be carried over to cybercrime, because the environment in which cybercrime is committed cannot be pinpointed to a geographical location or distinctive social or cultural groups. For example, traditional crimes such as child abuse and rape allow for the characterization of the attacker based on the characteristics of the crime, including determination of the social status of the attacker; geographical location within country, state, district, urban, or rural residential areas; and so on. However, in the case of cybercrime, this characterization of the attacker cannot be made, because the Internet is “anti-spatial.” Yar (2006) explains that identifying location with distinctive crime-inducing characteristics is almost impossible in cybercrimes. This, in turn, serves to render the criminological perspectives based on spatial distinctions useless.

Criminology allows for the understanding of the motivations of the criminals by analyzing the social characteristics of the criminals and their spatial locations. For example, poverty may be considered to be a cause of crime if poor areas exhibit high crime rates, or a high percentage of criminals are found to come from poor backgrounds. According to Yar (2006) criminology helps to understand the reasons behind the preponderance of crimes committed by people with particular characteristics, such as the overrepresentation of offenders from groups of people who are socially, economically, or educationally marginalized. It was further explained that the association between geographical location and social characteristics has led to the association between crime and social exclusion in mainstream criminology.

However, in the case of cybercrime, such a correspondence appears to break down. One of the most important points to consider is that access to the Internet is disproportionately low among the marginalized sections of society who were considered to be socially excluded and therefore more likely to commit a crime. Furthermore, the execution of a cybercrime requires that the criminal have a degree of skill and knowledge that is greater than the level of skills and knowledge

possessed by the average computer user. It can, then, be said that cybercriminals are those who are relatively more privileged and who have access to the Internet, knowledge, and skills at a level above the average person. Therefore, the relationship between social exclusion and crime that had been widely accepted in traditional crime could not be true in the case of cybercrimes, and that cybercriminals are fairly “atypical” in terms of traditional criminological expectations. Hence, the current perspectives of criminology that link marginality and social exclusion to crime have no use in explaining the motivations behind cybercrimes. Without an understanding of motives, it is difficult for law enforcement agencies and government to take effective measures to tackle cybercrime.

Brenner (2010) also raised the important issue of privacy versus the need to prevent crimes and collect evidence of criminal activity in the digital world. In the real world, there are a number of safeguards against the infringement of personal privacy by law enforcement, such as laws regulating the tapping of phones and monitoring of digital communications such as e-mails and chats. Most people expect that their e-mail is private. However, the technological basis of e-mail is such that it is in fact not private. In normal letters, the information contained in the letter is transmitted in a sealed envelope. In order to access the information it is necessary for the carrier to gain access into the sealed envelope, which involves breaking the seal and perhaps re-sealing the envelope, and this can be classified as deception. However, in the case of e-mail, the information is not transmitted in a sealed envelope. It is transmitted in plain text, and therefore, can be intercepted.

The issue of privacy in the digital world is one that is becoming increasingly important with the rise of Web 2.0. Social networking Web sites such as Facebook and Twitter collect an enormous amount of personal information about the individual. Yet the privacy controls on these Web sites are often not easy to understand, making the less technologically savvy person a more likely candidate for attack.

CONCLUSION

The worldwide growth of personal and business use of the Internet over the past two decades has been almost exponential. Restrictions on the use of the Internet or how it is used is limited to how you access it, that is, how easily is the Internet accessible to an individual or business. The ability to be able to gain access 24/7 has presented untold opportunities for potential scammer, hacker, and identity thief or just about anybody in the World that has an unlawful intention to commit cybercrime.

The opportunity to generate income streams that were not previously possible combined with anonymity has increased the opportunity for crime.

Cybercrime offenses are crimes that have an underlying element of dishonesty that have been (or were) in existence before the Internet existed. What has changed is the following:

- Increased targeting of victims
- Cost reduction in targeting those victims
- Increased global capacity and the ability to cross international boundaries with ease
- Complete lack of legal process to deal with the issues

- Increased anonymity
- Extremely small chance of the crime being reported
- Lack of suitable international legislation to bring the suspect to justice

Total lack of understanding of the gravity of such offenses is as interpreted by the Courts of Justice.

Just as it is important to understand the characteristics of the criminals in order to understand the motivations behind the crime and subsequently develop and deploy crime prevention strategies, it is also important to understand the characteristics of the users of computer systems in order to understand the manner in which cybercrime makes these users victims, and also to develop and deploy effective crime prevention strategies at the user side.

ACKNOWLEDGMENTS

The author thanks Dr. Ameer Al-Nemrat and Dr. Imran Askerniya whose research helped to form the basis of the material here.



CHAPTER 22

Conclusion: National Security in the Networked Society

Simeon Yates

We argued in Chapter 1 that the current constellation of digital media and networks; networks of regular international trade and travel; and the complex networks of global political, economic, and social systems provide a new context for the formation of National Security Strategy. Key to this new context are the opportunities, threats, and challenges this new constellation provides. In the rest of the book we tried to explore specific aspects of these challenges.

NATIONAL SECURITY TODAY AND IN THE FUTURE

Section 1 explored current thinking on national security and contemporary threats to that security. Importantly, a key theme in this section was the interdependence of nation states regarding both the prevention of and vulnerability to security threats. As we noted in the introduction, a model of national security based on “unit level” and anthropomorphic model of nation states as actors on a global stage cannot hold in the age of the networked society. As Buzan (2009) noted, the interconnectedness of contemporary global societies requires that security be looked at via the lens of systems, networks, and institutions that function within, between, and among nation

states; this point is reiterated by Stanniforth in Chapter 2. In Chapter 3 Saathoff et al. reminded us that threats to security may arise from inside the state. This does not mean they are disconnected from the networked world. Far from it, as the examples discussed by Saathoff et al. indicated, access to networks provided the information, knowledge, materials, and substances that influenced behavior, as well as being the target or vectors for auctioning threats. It is also notable that failures to communicate between law enforcement networks may play a role in such insider threats going undetected.

Chapters 4 and 5 counterpoint the argument that nation states may be of less relevance in a networked age. In Chapter 4 Lehr focused on the response to asymmetric threats in a naval context, for example, the rise in piracy off the horn of Africa. This chapter strongly argued that such challenges to security fit a networked or “post-modern” view of our global world, and that ironically, this represents a very Western cosmopolitan view of global politics. Lehr concluded with the concern that other nations may not share this view and that Western nations may have underestimated the old-fashioned national security threat posed by direct action by other nation states. Stanniforth reminded us in Chapter 5 that nations

remain and that a key feature of the preservation and functioning of modern nation states lies in the policing and security of borders. Stanniforth noted that these borders are ever more difficult to police, whether through transnational agreements such as Schengen or through their penetrations by ever-growing “network flows,” to use Castells’ term. The need to police, protect, and derive intelligence from the people, goods, and information crossing borders will remain as long as there is a need to secure the nation state.

THE PUBLIC, THREATS, AND NEW MEDIA

Section 2 examined the issues and challenges facing citizens in a networked society. In Chapter 6 Rogers and Pearce clearly articulated the case for robust risk communication strategies. As is noted in many chapters, the networks in which many citizens now live their daily lives can provide access to ever-greater levels of information. Ensuring that risks are proportionately communicated and that policy makers have a good understanding of the levels of panic or compliance during moments of crisis is key to the operationalization of strategies. In Chapter 7 Krieger and Rogers applied the ideas of Chapter 6 to the case of a CBRN incident. A key feature of their discussion is the importance of citizens trusting the information they are provided, the institutions interacting with them, and the nature of the communication. Networks are not just made of communications channels, incidences of economic exchange, or of social interaction. They are also strongly influenced by our perceptions of those links. Such perceptions are closely tied to how we value the link itself, the channel, the persons or organizations involved, and the form of the message. Strategies to support the resilience of citizens at such challenging times need to be based on a deep understanding of these issues. Chapter 8 builds on this issue of trust. It notes that in the UK there is a key idea of “policing by consent” that builds upon a historical approach dating back to Saxon times. In this context the current PREVENT strategy for addressing

terrorist threats builds upon this community-based approach. Yet the Internet and digital media open up citizens to networked flows from beyond the confines of their local communities. A key part of ensuring trust- and consent-based policing of potential terrorist threats must entail understanding how these “dark” flows can be countered in a community context.

In Chapter 9 Manso and Manso developed the themes of this section further by exploring the possibilities provided by networked digital media to support both citizens and intuitions to respond to threats and crises. In this case it is the ability to deploy ubiquitous mobile and social media in response to crises. In this chapter it is shown that the networked society provides a resource to support the resilience sought in Chapter 7. There are often complexities and compromises in technology implementations, and in Chapter 10 Dastbaz et al. reminded us that many new media are “Janus faced.” Although Manso and Manso made the merits of mobile information communication technologies (ICT) clear, these media can compromise many of the rights Western citizens take for granted. In embracing digital media as tools for communication and potentially to provide resilience in crises, citizens may also open them up to greater surveillance by the state. Networked media, especially mobile ICT and social networking, are challenging both legal and cultural assumptions of public and private. The balance point between freedom, privacy, personal and public safety, and the role of the state in a networked age is clearly something still up for debate.

DEPLOYING NETWORK TECHNOLOGIES FOR NATIONAL SECURITY

Section 3 marked a change in focus within the book. Here we explored the use of new technologies in strategic responses to national security threats. Importantly, we have explored how current and future ICT tools might be developed and deployed. In Chapter 11 Stedmon et al. provided a very strong case for the use of user-centered methods in the elicitation and implementation of

security system requirements. This is an argument that has been made recently in many areas of ICT development and product design, yet is still often overlooked in major national and public sector system development. National security “users” are of course often the citizens the state wishes to protect. Koraeus and Stern reminded us in Chapter 12 that although we may exist today in a mass of information flows, it is the extraction of learning from prior experience (knowledge) and the management of it that is key to improving responses to potential and actual threats.

Although many new technologies support processes of knowledge extraction, storage, and management; for example, see Launder and Polovina's discussion of semantic tools in Chapter 13, the key task remains making this knowledge effectively available to managers, policy makers, and practitioners. As Saathoff et al. noted, actual examples of many types of security threats or crises may in fact be quite rare. Capturing the key learning from such events is therefore essential, whether it is through the use of ICT or through appropriate networks of experts. In Chapters 14 and 15 Andrews et al. and Pavlin explored how the huge flows of information within networked societies might be deployed both operationally and in the development of strategy. Here again we find that ICT tools and solutions may both create these flows and allow us to extract key knowledge and information in ways not previously possible. Rein reminded us in Chapter 16 that actually implementing such systems is challenging. Despite the large amounts of data collected in key hubs by the institutions of nation states, generated and shared by citizens through their networks and produced in response to crises, there remains a need to find standardized ways to store and exchange this material within the networks of security agencies.

THREATS TO THE INFRASTRUCTURE OF THE NETWORKED SOCIETY

What then of the core infrastructure of the networked society itself, within national borders or external? Section 4 explored the issues of

national cyber security and the threats to nations and networks. Stanniforth provided an overview of the emerging challenges of cyber security in Chapter 17 while Chapter 18 laid out the current key strategic goals of the United States cyber security strategy. In both cases the recognition of this as a transnational threat that requires a transnational response is made clear. Kallberg and Thuraingham reminded us in Chapter 19 that as with conventional threats, asymmetric or state based, there are a variety of players within global networks and that individuals, groups, or even nations may act to threaten each other's cyber security.

MacKinnon et al. combined many of the issues discussed in this book, user needs, technological solutions, and implementation methods to build proposals for general cyber security strategies to be employed by end users, organizations, and institutions. A key feature of the argument in Chapter 20 is that in a networked society cyber security has to be a shared responsibility across a wide range of citizen, institutional, national, and international actors. Finally, but very importantly, Jahankhani asked us in Chapter 21 to reflect on both the criminal and citizen behavior in the context of cyber crime. This provides a basis for modeling behavior and looking to methods to prevent threats to citizen's networks and ICT systems.

CONCLUSION

In our introduction we set out three key issues:

1. The development of strategy in the context of national security driven by national interest
2. The importance of high-quality information and knowledge in the development of strategy—strategic intelligence
3. The nature of globalized networks based on ICT systems and people that are concurrently locations for threats to national and global security, tools to defend or to threaten national security, and sources of information for both nations and citizens about threats and events

In essence, the strategic intelligence management vision for national security is released through connection between national security and national interest, dynamic collaboration among stakeholders, and proactive communication strategies and enabling technologies. We

hope that in the four sections of this book we have provided examples of how current security practitioners, academic researchers, and ICT system developers have sought to address these issues at the citizen, organizational, and national levels.