Industrial Control Systems and Cybercrime

Aunshul Rege

Critical infrastructures are socio-economic entities that are vital to the day-to-day functioning of a society. Some of these include transportation, banking and finance, telecommunications, emergency services, electricity, and water supply systems (Blane 2002; DHS 2008; Verton 2003). Over the years, these infrastructures have started relying on industrial control systems (ICS), which are computer systems that oversee operations, improve efficiency, and provide early warning of possible disaster situations (Blane 2002; Fogarty 2011; NCS 2004; Rossignol 2001). These systems range in their complexity; some can be relatively simple, monitoring environmental conditions of a small office building, or very intricate, monitoring all the activity in a nuclear power plant or the activity of a municipal water system (NCS 2004). Furthermore, ICS have embraced the continually changing face of technology to improve critical infrastructure monitoring, control, and operations.

This technological dependency, however, increases their online exposure and susceptibility to cybercrime. In 2005 alone, approximately 2,700 businesses detected 13 million incidents, suffered $288 million in monetary losses, and experienced 152,200 hours of system downtime (Rantala 2008). Indeed, these systems are attractive targets and incapacitating them could have detrimental effects on everyday operations, the economy, and national security.

Given the importance of these systems, it is not surprising that a considerable amount of research has been conducted in the ICS area. Research includes descriptive accounts of ICS (DPS Telecom 2011a; Ezell 1998; Luiijf 2008); ICS functionality (Scadasystems.net 201; Stouffer, Falco, and Scarfone 2011); ICS threats, vulnerabilities, consequences, and risks (Lemos 2000; Luiijf 2008; Nicholson 2008; Oman, Schweitzer, and Robert 2001; Poulsen 2003; SANS 2001); ICS disruption simulations (GAO 2003); and ICS cybercrime case studies (Kuvshinkova 2003; Morain 2001; NSTAC 2000; ZDNN 2001). This literature, while important, is limited to industry and security sectors or media accounts, and is, therefore, technical or sensationalized (respectively) in nature. Furthermore, the studies on critical infrastructure and cybercrime are found in isolation; this disconnect hinders a thorough understanding of critical infrastructure cyberattacks.

More importantly, existing ICS research has minimally addressed the *human* component in cybercrimes, such as the organization and operation of offenders, the factors that influence offender decision-making, and how the cybercrime process is carried out. The discipline of criminology is thus highly beneficial as it offers yet another, important, perspective on the phenomenon of ICS cybercrimes. Despite the importance of these systems, criminological research is scarce. Some reasons for this paucity may be due to the lack of public disclosure and underreporting; the difficulty in accessing confidential and sensitive national security infrastructure data; and the methodological limitations in researching the ICS attackers, their modus operandi, and their organizational dynamics.

This chapter reviews the abundant technical literature, media cases, and the brief criminological research in the ICS area. First, the ICS literature is reviewed, which provides information on ICS components, their functions, and inter-relationships that can be targeted by cybercriminals. Second, the literature on ICS vulnerabilities is examined, which offers insight into system design or architecture flaws that make them suitable targets. Third, the literature on ICS threats is reviewed, which identifies the assortment of cybercriminals that may target these systems. Next, six case studies of ICS cyberattacks are listed to illustrate the varying nature and intensity of attack strategies and cybercriminal skills. Finally, the case is made for expanding criminological research inquiry using alternate methodologies, applying the rational choice perspective and situational crime prevention principles, employing simulation studies and agent-based modeling, and exploring the physical-cyber relationships in ICS cybercrimes.

Industrial Control Systems

Industrial Control Systems (ICS) gained prevalence in the 1960s, when the need to monitor and regulate remote infrastructure equipment and processes increased (DPS Telecom 2011a). Early ICS required human operators to make decisions and were therefore very expensive to maintain; these systems are more automated today and hence cost-efficient (DPS Telecom 2011a). "ICS" is a general term, which covers an assortment of control systems, including

Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), and Supervisory Control and Data Acquisition (SCADA) systems.

SCADA systems are highly distributed systems, which are used to control geographically dispersed assets, often scattered over vast distances, where centralized data acquisition and control are critical to system operation (Stouffer et al. 2011). SCADA systems are designed to collect field data and transfer it to a central computer facility. This data is displayed graphically or textually to the plant operator, who can then monitor or control an entire system from the centralized location in real time (Stouffer et al. 2011). SCADA systems thus control *and* monitor plant operations and processes. A DCS is responsible for controlling production systems within the same geographic locations for industries (Stouffer et al. 2011). There is often confusion over the differences between SCADA and DCS. SCADA systems, as the acronym implies, includes data acquisition *and* control, while DCS is purely control oriented (DPS Telecom 2011b). Before the introduction of computer networks, a SCADA system was the top-level controller for lower-level systems, as it was impractical for SCADA to control every minute aspect of a system (DPS Telecom 2011b). Here, DCS did most of the lower level detail work and reported back to, and took orders from, the SCADA system (DPS Telecom 2011b). With the growth of fast computer systems, however, SCADA and DCS have blurred together into a single monitoring and control system (DPS Telecom 2011b).

PLCs are control systems that are typically used throughout SCADA and DCS systems to provide local management of processes (Stouffer et al. 2011). Data acquisition starts at the PLC level, which includes equipment status reports and meter readings, which are then communicated to the SCADA system (Scadasystems.net 2011). Based on the data collected from the stations, automated or operator-driven supervisory commands are sent back to the PLCs, which in turn control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions (Stouffer et al. 2011).

Consider the utilities industry, where ICS encompass data transfers between SCADA systems and PLCs. Here, PLCs are connected directly to geographically scattered field devices, such as reservoir level meters, water flow meters, temperature transmitters, and power consumption meters (NCS 2004). This information is relayed back to SCADA systems, enabling facility operators to determine utilities systems performance. Based on this data, operators can send commands back to the PLCs that, for instance, change the set points for temperature settings, open or close valves that regulate water flow, and enable alarm conditions, such as loss of flow and high temperature (NCS 2004).

Most ICS in use today were developed years before public and private networks or the internet were commonplace in business operations. These systems were designed to meet performance, reliability, safety, and flexibility requirements (Stouffer et al. 2011). They were physically isolated from outside networks and based on proprietary software, hardware, and communication protocols that included basic error identification and correction capabilities, but lacked the secure communication capabilities needed in today's interconnected systems (Stouffer et al. 2011). Information and communication technologies started making their way into ICS designs in the late 1990s, exposing them to new types of threats and significantly increasing their vulnerability (Stouffer et al. 2011). The US critical infrastructure is highly interconnected and mutually dependent through a host of technologies; an incident in one infrastructure can directly, or indirectly, impact other infrastructures through cascading and escalating failures (Stouffer et al. 2011).

While this literature identifies the different types of ICS and their uses in critical infrastructure, it does not shed light on their vulnerabilities. As such, the next section examines the types of vulnerabilities that are present in ICS and how they can be exploited by cybercriminals to conduct their attacks.

Industrial Control System Vulnerabilities

ICS were designed and implemented in an era when network trespass and data manipulation were not relevant. Information security was not built into these systems because there was "no public information on how SCADA worked, … no connections to the [internet], … the environment was assumed to be hacker-free, [and that the systems operated in] totally controlled and closed secure environments" (Luiijf 2008, 11; Nicholson 2008; Stamp et al. 2003).

Today, ICS use cost-cutting technology and non-proprietary software, which offers convenience and efficiency; these advancements have also resulted in several built-in vulnerabilities that increase the likelihood of ICS cybercrimes. Several overlapping definitions of vulnerabilities are found in the literature. Vulnerabilities are any weaknesses that can be exploited by an adversary to gain access to an asset (Byres and Hoffman 2004). Vulnerabilities have also been defined as any characteristics pertaining to the installation, system, asset, application, or its dependencies that could result in loss of functionality when subjected to a threat (Robles et al. 2008). The Department of Homeland Security's Risk Lexicon (DHS 2010) defines vulnerability as "a physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard." The National Institute of Standards and Technology (NIST) Guide to Industrial Control Systems Security categorizes ICS vulnerabilities into three groups: Policy and Procedure, Platform, and Network categories. There is no pecking order of vulnerabilities with regards to the likelihood of occurrence or severity of impact (Stouffer et al. 2011).

Policy and procedure vulnerabilities are often introduced into ICS because of incomplete, inappropriate, or nonexistent security policy documentation. This documentation identifies safe user practices, such as regular password updates, and network connection requirements (Stouffer et al. 2011). The lack or paucity of security audits is also problematic as this process typically determines the adequacy of system controls and ensures compliance standards are met (Stouffer et al. 2011). To make matters worse, ICS information, such as proprietary protocols, reports, and specifications, are made available online by industry and ICS vendors to facilitate employee education and enable third-party manufacturers to build compatible accessories (GAO 2003; Luiijf 2008; Stouffer et al. 2011). Furthermore, SCADA tutorials are easily available online as downloadable white papers, YouTube videos, and 'ask SCADA experts' websites (DPS Telecom 2011a; YouTube 2009; Zintro 2011). Thus, the internet serves as an extensive knowledge base documenting system blueprints, tutorials, expert advice, and vulnerability details which cybercriminals can use to research their targets and design corresponding attack techniques.

The next type of vulnerability occurs due to flaws, misconfigurations, or poor maintenance of ICS platforms (Stouffer et al. 2011). Platform vulnerabilities can be configuration-based (patches implemented without exhaustive testing), hardware-based (insecure remote access), software-based (buffer overflow), and malware-based (malware protection software not installed, not current, or implemented without exhaustive testing) (Stouffer et al. 2011). ICS also utilize user-friendly browser applications that can be easily understood and employed by anyone, and thus little technical expertise is required to operate these systems (Luiijf 2008). Furthermore, organizations are transitioning from proprietary systems to less expensive, standardized technologies, such as commercial—off-the-shelf (COTS) SCADA systems and software. COTS software, however, has publicly known design errors and bugs which can be easily exploited using tools that are widely available online (Luiijf 2008; Stouffer et al. 2011).

A third source of ICS vulnerabilities occur from flaws, misconfigurations, or poor administration of ICS networks and their connections with other networks (Jordan and Taylor 1998; Stouffer et al. 2011). ICS are remotely accessible to plant operators for maintenance and to corporations for assistance with business decisions (Luiijf 2008; Stouffer et al. 2011). This integration of

ICS networks with remote and corporate networks increases ICS accessibility to both legitimate and illegitimate users (Stouffer et al. 2011). Another problem is that unencrypted and/or static passwords are often used in ICS environments, which are assumed to be secure (Luiijf 2008; Nicholson 2008). Adversaries with password cracking software can easily gain access via remote connections and obtain administrator access without supervision (Luiijf 2008; Stouffer et al. 2011). Finally, technical protection is often lacking, with **virus** scans rarely being performed and security patches not being installed regularly and rigorously. Insufficient quality control for SCADA software, poor or improper usage of **firewalls**, lack of individual authentication and poor **intrusion detection systems** collectively increase the likelihood of ICS cybercrimes (Luiijf 2008; Nicholson 2008).

These three types of vulnerabilities can be abused individually but are more likely to be exploited in combination. Cybercriminals get the necessary access and information, while facing little resistance. Different types of cybercriminals may use these vulnerabilities in different ways. It is, therefore, important to identify the types of attackers that pose a threat to ICS, as well as their expertise and modus operandi.

Industrial Control System Threats

There are several definitions of threats found in the literature, which share common components. Threat is defined as any indication, circumstance, or event with the potential to cause the loss of, or damage to an asset (Byres and Hoffman 2004; Moteff 2005). Threat is also defined as the intent and capability to adversely affect (cause harm or damage to) the system by changing its state and function (Haimes 2006). The DHS Risk Lexicon (2010) defines threat as a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/ or property.

Nine threat sources may attack critical infrastructures. First, *leisure cybercriminals* break into networks for thrill, challenge, curiosity, or bragging rights in the cybercriminal community (Holt and Kilger, 2012a; Krone 2005; Weaver et al. 2003). These attackers do not have to be technically knowledgeable; they can now download pre-written attack scripts to target ICS, thereby increasing the possible pool of attackers (McAfee 2005; Souffer et al. 2011). Second, *industrial spies* seek to acquire intellectual property, personnel files, or monitor proprietary activities through covert and illegitimate methods (Holt and Kilger 2012a; Stouffer et al. 2011; Taylor et al. 2010; Williams 2006). Third, *for-*

eign intelligence services, or *nation-states*, are developing information warfare doctrines, programs, and capabilities, which can disrupt ICS supply and communication functionalities in several infrastructures (Holt and Kilger 2012a; Stouffer et al. 2011). Fourth, *terrorists* seek to disrupt, debilitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence (Stouffer et al. 2011; Weaver et al. 2003).

Fifth, *disgruntled insiders* possess ICS knowledge and unrestricted access to cause system damage or steal sensitive information; they may be current or past employees, contractors, or business partners (Datz 2004; Shaw and Stock 2011; Moore et al. 2011; Shaw and Stock 2011; Stouffer et al. 2011). Sixth, *criminal groups* attack ICS for monetary gain and use spam, phishing, and malware to conduct their attacks; they hire or develop cybercriminal talent to target ICS (Krone 2005; McAfee 2005; McMullan and Rege 2007).

Phishers are the seventh threat source to ICS. These are individual or small groups of cybercriminals that execute online schemes, via spam, spyware, and malware, to steal ICS operators' identities or ICS information for monetary gain (Stouffer et al. 2011). Eighth, *spammers* are cybercriminals that distribute unsolicited email with hidden or false information to sell ICS-related products, conduct phishing schemes, or distribute spyware and malware (Stouffer et al. 2011). Finally, *spyware authors* are individuals or organizations with malicious intent that carry out attacks against users by producing and disseminating spyware to gather specific intelligence data and assets from ICS vendors, which is then used to design tailor-made cyber-attacks (Stouffer et al. 2011).

Table 1 summarizes the preceding technical discussion of ICS components, threats, and vulnerabilities. There is, however, limited publicly-available information on ICS cybercrime consequences. As such, a review of a few, well-known critical infrastructure cybercrimes are offered next to capture not only the consequences, but also the different threat agents and their attack techniques.

Critical Infrastructure Cybercrime Cases

Several publicly known critical infrastructure cybercrime cases have been documented in both technical literature and media cases. These cases cannot be covered extensively here, and as such this section discusses six cybercrime events to demonstrate that ICS cybercrimes can occur across different critical infrastructures: transportation, sewage, power, finance, and communication infrastructures. These cases offer preliminary insights into the history of ICS cyberattacks and the range of cybercriminal skills, techniques, and organization.

Table 1. Summary of Industrial Control Systems, Vulnerabilities and Threats

Item	Details
Types	
Supervisory Control and Data Acquisition (SCADA)	Control geographically dispersed assets from centralized location
Programmable Logic Controllers (PLC)	Provide local management of processes based on SCADA commands
Vulnerabilities	
Policy and Procedure	Incomplete, inappropriate, or nonexistent security policy documentation
Platform	Flaws, misconfigurations, or poor maintenance of configuration, hardware, software and anti-malware elements
Network	Remote access, poor password practices, poor authentication, inadequate intrusion detection
Threats	
Leisure Cybercriminals	Thrill, challenge, curiosity, or bragging rights
Industrial Spies	Acquire intellectual property, personnel files, or monitor proprietary activities
Foreign Intelligence Services	Develop programs to disrupt ICS supply and communications
Terrorists	Threaten national security, cause mass casualties, weaken the U.S. economy, damage public morale and confidence
Disgruntled Insiders	Possess ICS knowledge and unrestricted access to cause damage or steal sensitive information
Criminal Groups	Hire or develop cybercriminal talent to target ICS for monetary gain
Phishers	Use spam and malware to steal ICS information and operators' identities
Spammers	Distribute unsolicited email with hidden or false information to sell ICS-related products
Spyware Authors	Produce and disseminate spyware to gather specific intelligence data and assets from ICS vendors

Oil and Gas Infrastructure

One of the earliest documented cyber attacks occurred during the Cold War, when US President Reagan approved a SCADA attack on the Russian pipeline system in Siberia. To automate the operation of valves, compressors, and storage facilities on such a large scale, the Russians needed sophisticated ICS software (Crowell 2010). They approached the United States for the necessary automation software but were turned down, and so sought to steal the necessary code from a Canadian firm. US Intelligence, however, was tipped off of the impending theft, and in cooperation with the Canadian firm, **modified** the software before it was stolen (*The Economist* 2010, Crowell 2010). The pipeline software, which ran the pumps, turbines, and valves, was reprogrammed to go haywire and "reset pump seeds and valve settings to produce pressures far beyond those acceptable to pipeline jolts and welds," resulting in a large blast in Siberia (Cornish et al. 2010; The Economist 2010). This attack was an indirect effort to disrupt Russia's technological capabilities and military industrial base; it was specifically designed to tamper with Russia's gas supply system, harm the Russian economy, and decrease its gas revenues from the West, which ultimately undermined its power (Cornish et al. 2010).

Transportation Infrastructure

In March 1997, a teenager hacked into the Worcester, Massachusetts, airport, resulting in the shutdown of communication services at the airport's Federal Aviation Administration Tower, fire department, airport security, weather service, and several private airfreight companies for over six hours (Lewis 2004; Taylor et al. 2010). Furthermore, the main radio transmitter and the circuitry activating runway lights were disabled. The hacker changed the system identification to "Jester," demonstrating his actions were driven by thrill (Rindskopf 1998). This attack caused flight delays and cancellations and major financial losses to the airport and numerous airlines. He received two years' probation, during which he could not access any computers or digital networks, paid restitution to the phone company, and forfeited all computer equipment used in the attack (Lewis 2004).

Another transportation sector cybercrime was the 2008 Polish tram system hack. A juvenile hacked into the tram system, using it like a "giant train set" (Baker 2008, 1). He visited tram depots to study the trams and tracks thoroughly and then built a remote control device to manipulate the trams and tracks and change signals (Baker 2008). While this attack did not result in any deaths, it did cause serious harm: four vehicles were derailed, others made emergency stops, and 12 people were injured (Baker 2008). The boy faced charges of endangering public safety in juvenile court.

Sewage Infrastructure

In 2000, the sewage system in Queensland, Australia, was hacked by Vitek Boden. He was a former temporary contractor with the company that installed a local computerized sewage system. Boden was angered after being denied a permanent job. He used his credentials to remotely access the sewage system and send commands to disrupt approximately 140 sewage pumping stations (Crawford 2006; Lewis 2004; Stamp et al. 2003; Verton 2003). This attack released up to one million liters of raw sewage into public parks, creeks, and a hotel, severely polluting the environment and killing numerous marine life (Lewis 2004; Verton 2003). Boden was found guilty on 30 charges of computer hacking, theft, and causing environmental damage; he was sentenced to two years in jail and fined 13,000AUD for his crime (Crawford 2006; Lewis 2004).

Finance and Communication Infrastructure

On April 26, 2007, Estonia suffered a massive cyberattack, resulting from anger over the relocation of a World War II statue. The country experienced approximately 128 unique crippling **Distributed Denial of Service (DDoS)** attacks. A DDoS attack occurs when several compromised computers attack a targeted system by flooding it with data. The target uses up all of its resources to manage this data, which forces it to shut down, thereby denying service to legitimate users. The Estonian DDoS attack disrupted the country's prime minister website functionality, financial transactions, telephone communications, and media transmissions (Davis 2007; Evron 2008). The cyberattacks ranged in duration, with some lasting for less than an hour and others for over 10 hours (Brenner 2007; Davis 2007; Evron 2008). Online Russian discussion boards had detailed instructions on cyberattack preparation, target selection, and response strategies to Estonia's defense, indicating that these attacks were organized and adaptive (Evron 2008). A conglomeration of several tactics were used, such as **website defacements**, using pre-written programs to overwhelm Estonian web servers, and herding **botnet armies**. Botnets comprise numerous malware-infected computers that are remotely controlled by a cybercriminal unbeknownst to their legitimate users. The computers used in the attacks were located in the USA, Brazil, Canada, Egypt, Peru, and Vietnam, which made tracing the attack source problematic (Brenner 2007; Davis 2007).

Power Infrastructure

The notorious Stuxnet **worm** first appeared in July 2010 and targeted PLCs made by Siemens, which were used in Iran's Bushehr nuclear facility (BBC 2011). The worm only activated when it detected the presence of a specific configuration of controllers, running a particular set of processes that only existed in a centrifuge plant (Broad, Markoff and Williams 2011). The worm was a "dual warhead" as it had two major components (Broad et al. 2011, 5). The first was designed to lie dormant for long periods, then sped up the machines to "send Iran's nuclear centrifuges spinning wildly out of control," leading to their eventual destruction (Broad et al. 2011, 2). The second component, the "man in the middle," was a computer program that secretly recorded normal plant operations, then played those readings back to plant operators, "like a pre-recorded security tape in a bank heist," to make it appear that everything was operating normally, when in fact, the "centrifuges were actually tearing themselves apart" (Broad et al. 2011, 2). This program appears to have been created as part of top secret program by the US government titled "Operation Olympic Games" (Sanger 2012). The code was actually ordered for use in the field under President Obama, but developed under then-President Bush. As a result, Stuxnet appears to be a nation-state driven attack in the same fashion as the Reagan-ordered attack against Russia discussed earlier, rather than a random attack by sophisticated cybercriminals.

Table 2 summarizes the cases discussed above. These cases demonstrate the broad spectrum of critical infrastructure that has been targeted by cybercriminals, and provides insight into the attack vectors and the attackers, their organizational dynamics and modus operandi. Thus, different types of critical infrastructures relying on ICS are equally likely to be targeted using an assortment of techniques that range in their technical sophistication, planning, and duration.

The Brief Criminological Industrial Control System Cybercrime Research

The above discussion demonstrates that there is no shortage of ICS research in the technical domain, nor is there paucity in media accounts of critical infrastructure attacks. However, both these domains have shortcomings. The technical studies on infrastructure cybercrime are found in isolation, which does not offer a thorough understanding of ICS cyberattack techniques, frequency, duration, intensity, and patterns. While technical research is undoubtedly crucial, it primarily focuses on ICS vulnerabilities and prevention

Table 2. Summary of Industrial Control System Cybercrime Incidents

Infrastructure	Year	Target	Technique	Damage	Organizational Dynamics
Oil and Gas	1982	Serbia Pipeline	Modification	Disruption of operations of valves, compressors, and storage facilities	Associates
Transportation	1997	Massachusetts Airport Polish Tram System	Modification	Flight delays, communication delays	Loner
Sewage	2000	Queensland Sewage System	Exploitation	Environmental pollution	Loner
Finance and Communication	2007	Estonia	Modification; DDoS	Disruption of website functionality, financial transactions, phone communications, media transmission	Network
Transportation	2008	Polish Tram System	Modification	Vehicle derailment, passenger injuries	Loner
Power	2011	Iran's Bushehr Nuclear Facility	Worm	Disruption of operations of nuclear centrifuges	Network

measures from the industry's perspective and is, therefore, limited in scope. Media accounts of infrastructure cyberattacks are sensationalized, skewed, and result in myth-based thinking (Dubois 2002; Finckenauer 2010). Furthermore, they lack scholarly rigor and are descriptive in nature.

The criminological discipline has just started addressing critical infrastructure cybercrimes, focusing on the type of attackers, their organizational characteristics, the nature and properties of cyberattacks, and industry executive perception studies of infrastructure cybercrimes. First, criminological research on critical infrastructure cybercrimes involves cybercriminal taxonomies. Vatis

(2002) offers a typology of critical infrastructure cybercriminals, which includes disgruntled insiders, criminal groups, virus writers, foreign intelligence services, state-sponsored cybercriminals, terrorists, and recreational hackers. Similarly, Cornish et al. (2010) focus on cyber warfare and identify four cyber threat domains: state-sponsored cyber-attacks, ideological and political extremism, serious organized crime, and lower-level/individual crime. This typology parallels those identified in the technical domains discussed above (Krone 2005; Stouffer et al. 2011; Weaver et al. 2003) as well as other general hacker taxonomies (Holt and Kilger 2012a; Jordan and Taylor 1998; Rogers 2005).

The second form of criminological research on ICS cybercrimes involves the organizational dynamics of attackers. Using documents from government agencies, security firms, media sites, and hacker forums, Rege-Patwardhan's (2009) research offers a cybercriminal organization taxonomy. Hackers often engage in solo operations; these loners use technology and automated techniques that enable them to bypass digital defenses, and hence operate alone. Loners vary with respect to their technical skills. Cybercriminals often work together and engage in a minimal division of labor. These alliances are transient in nature, allowing deviant associates to unite for specific crimes and disband upon their completion, once again becoming free agents to form new alliances. Some cybercrimes, however, are conducted by online crime networks with sophisticated organization, extensive group membership, elaborate divisions of labor, and networked group structure. Each player brings specific skill—sets to the operation, making the organization's expertise broad and diverse. Like associates, these organizations coalesce for the sole purpose of executing the attack, resulting in criminal organizations that are temporary, flexible, and networked. These organizational dynamics can also be found in McMullan and Rege's (2010) study on online gambling crimes and Rege's (2009) work on internet dating scams.

Third, criminological research on critical infrastructure cyberattacks also examine attack techniques. Some of these techniques include website defacements, **Domain Name Server (DNS) attacks**, DDoS attacks, viruses, worms, and **Trojan** horses, and **routing attacks** (Vatis 2002). Cybercriminals can also **exploit** bugs or loopholes in infrastructure programs, utilize their technical and programming skills to modify the actual infrastructure systems, and use **rootkits** and **toolkits** to conduct their attacks (Rege-Patwardhan 2009). These techniques have also been identified in the technical ICS research (Byres and Hoffman 2004; Luiijf 2008; Nicholson 2008; Souffer et al. 2011) and in criminological research addressing other cybercrimes (Holt and Kilger 2012a; Jordan and Taylor 1998). While certain techniques require greater expertise than others, the lack of technical knowledge does not imply attack failure. The techniques themselves vary with respect to their organizational dynamics. Some techniques are simpler in their organization, others require intricate preparation, scheduling, and sophistication, and some attacks are adaptive in nature (Rege-Patwardhan 2009). Finally, these criminal techniques can be used individually or in combination to create endless, unique, sophisticated, and damaging attack possibilities that are difficult to track (Rege-Patwardhan 2009; Vatis 2002).

More importantly, Rege-Patwardhan (2009) investigates the link between the organization of criminal techniques and the organization of criminals in cyberspace. The sophistication of criminal organization is not always directly proportional to the sophistication of criminal technique. Some loners conduct sophisticated attacks, while some associates and criminal organizations use simpler techniques (website defacements and toolkit-based attacks). Another important finding is that while cybercrimes involve digital attacks, traditional techniques are also used; this marriage of traditional/physical and technical tactics results in the successful execution of cybercrimes against critical infrastructures that can have more devastating impacts than when orchestrated in isolation (Rege-Patwardhan 2009; Vatis 2002).

Finally, industry perception studies offer an alternate perspective of ICS cybercrimes. Baker et al. (2010) survey 600 information technology and security executives from seven critical infrastructure sectors in 14 countries. These respondents are questioned about their practices, attitudes, and security policies, and the types of attacks they have faced. Executives fear that recession-driven cuts may affect their security practices and are concerned about how well-prepared critical infrastructure is to deal with large-scale attacks. Chinese executives report the highest rates of adoption of security measures, such as encryption and strong user authentication. Approximately 54 percent of the executives experience attacks from high-level adversaries, such as organized crime groups, terrorists, or nation states, as well as stealthy infiltration from large-scale spy rings. Roughly 59 percent believe that foreign governments are already involved in such cyber-attacks and infiltrations.

Baker et al. (2010) also identify the types of attacks faced by critical infrastructures. Nearly one-third of the respondents report suffering large-scale DDoS attacks multiple times per month, and two-thirds of these report that such attacks impact operations in some manner. However, DDoS attacks are not the most common type of attack; 89 percent experience attacks resulting from virus or malware infections. More than half experience DNS poisoning and **SQL injection attacks.**

Attacks against the utilities sector are aimed at SCADA systems roughly 55 percent of the time. Of the 600 respondents, only 143 have ICS responsibilities. Of these, China has the highest SCADA security measure adoption rate of 74 percent, followed by Australia and Brazil at 57 and 54 percent, respectively. The United States and Japan have rates of 50 percent each, with France, Russia, Germany, Saudi Arabia, Italy and Mexico in the 35 to 40 percent range. Adoption rates of these measures are lowest in India and Spain, at 29 percent each and the UK at 31 percent. Seventy-six percent of the 143 respondents have their networks connected to an IP network or the Internet, with nearly half of them knowing the risks involved with such online exposure. Ninety-two percent of the executives responsible for SCADA report monitoring them in some way, either using network behavior analysis tools (62 percent) or audit logs (59 percent). Thus, Baker et al. (2010) demonstrate that critical infrastructures, including ICS, are operating in a high-threat environment and face a number of risks.

Despite the importance of these systems, the criminological research on ICS cybercrimes is still in its infancy. One reason for this paucity of research may be due to the sensitive nature of the topic. Gaining access to information on cyberattacks against critical infrastructure faces several barriers, such as confidentiality and privacy issues, liability issues, access to classified national security information, and reservations about sharing information with the academic community. An equally important reason for the lack of research is methodological limitations. Data on the phenomenon of critical infrastructure cybercrimes are not easily available. Finding cybercriminals to interview or survey is nearly impossible because they belong to an underground culture that is unknown or inaccessible. Acquiring access to online deviance requires technical expertise and covert observation, which are difficult given the sensitive, national-security nature of the problem. Interviewing security experts and critical infrastructure personnel is equally challenging. The former are often hesitant to disclose confidential incident information, which may include up-to-date counter strategies, digital evidence and equipment, and the implementation of social control efforts. Industry representatives are reluctant to disclose incidents for fear of being perceived as vulnerable to such attacks, which, in turn, encourages further cybercrimes. Additionally, open knowledge of critical infrastructure attacks generates fear and uncertainty in the public.

Expanding the Criminological Lines of Inquiry

The limitations discussed above should not deter criminologists from research inquiry. Researchers can use existing criminological studies and schools of thought to study ICS cybercrimes from multiple perspectives. Using alternate modes of inquiry to study the same phenomenon of ICS cybercrimes may offer greater insights into the phenomenon of ICS cybercrimes.

Primary Data Collection

The criminological research discussed earlier is descriptive and rudimentary in nature. They rely on case studies and document analysis. Obtaining data on actual critical infrastructure cybercrime incidents is difficult, and accessing ICS attackers is problematic because they belong to an underground culture that is unknown, inaccessible, and geographically dispersed. However, future research can follow Baker et al.'s (2010) global study which surveyed information technology and security executives from various critical infrastructure sectors. Perception surveys can also be done using ICS vendors, infrastructure executives, and ethical hackers to identify how each domain views ICS threats, vulnerabilities, and consequences (TVCs). Vignettes detailing hypothetical critical infrastructure cyberattacks and mixed focus groups can also be used to get a more qualitative and in-depth understanding, stimulate alternate interpretations, and offer more in-depth information resulting from greater response clarity in group discussions (Holt and Kilger 2012b).

Interviews, vignettes, and mixed focus groups have already been successfully used in studying other cybercrimes, such as online child sexual abuse (Martellozzo, Nehring and Taylor 2010), youth victimization by online harassment (Moore, Guntupalli, and Lee 2010), online child pornography behavior (Seigfried, Lovely, and Rogers 2008), and identifying the risk propensity of hackers (Bachman 2010). These methods can be used in ICS cybercrime studies to explore offender decision-making, organizational dynamics, and the structural features, such as criminal roles, group dynamics, criminal expertise, and the characteristics of the offense and offender.

Offender Decision-Making, Crime Scripts, and Situational Crime Prevention

The rational choice perspective (RCP) views criminality as an outcome of the continual interaction between a criminal's desires and preferences and the opportunities and constraints to commit crime (Cornish and Clarke 2008). RCP therefore portrays offenders as active decision makers who perform a cost-benefit analysis of presenting crime opportunities; offenders are reasoning criminals who use cues from the potential crime environment in deciding whether to commit crimes and how best to commit them (Cornish and Clarke 2008). Crime scripts systematically partition the modus operandi of simple and complex crimes into discrete, standardized stages or units of action (Smith 2003). Thus, crime scripts identify every stage of the crime-commission process and the decisions and actions that are needed at each stage. Understanding offender crime scripts and the corresponding decision-making process are crucial in designing prevention measures using situational crime prevention (SCP) principles. These measures can impact the offender's cost-benefit analysis by increasing the effort required by the offender, increasing the risks of detection, reducing the rewards, removing excuses, and reducing provocations (Clarke 2008).

Crime scripts have been examined rudimentarily for cybercrimes such as online dating crimes (Rege 2009), cyberextortion (McMullan and Rege 2007), and cybercrimes at gambling websites (McMullan and Rege 2010). SCP has also been applied to cybercrimes, such as online frauds (Newman and Clarke 2003), cyberstalking (Reyns 2010), information systems security (Beebe and Rao 2005), and insider threats to systems security (Theoharidou et al. 2005). Using these studies as a guide, future research should use offender decision-making, crime scripts, and SCP to examine ICS cybercrimes. This school of thought can help identify a thorough set of factors that influence offender decision-making and examine whether these factors have a temporal sequence in crime scripts. For instance, one rudimentary crime script for critical infrastructure cyberattacks may involve five stages, such as preparation, entry, initiation, attack dynamics, and exit. It would be invaluable to determine how offenders make decisions at each of these stages in the crime script. Once this intricate working is understood, SCP principles can be used to implement appropriate ICS protection strategies at each stage of the crime script.

Furthermore, understanding the degree to which factors influencing offender decision—making vary across different infrastructure sectors can also be useful. This research can shed light on whether different infrastructures experience different types of attacks (frequency, duration, intensity) from different threat agents (terrorists, organized crime groups, nation states, individuals). This would improve our understanding of critical infrastructure attacks and offender decision-making, help develop an offender-technique profile matrix, and offer insight into the effective application of situational crime prevention principles. These future studies can move *beyond* existing technical research on infrastructure vulnerabilities, by including the human element in ICS cybercrimes

Simulation Studies and Agent-Based Modeling

As noted earlier, access to "real-time" data or observing an ICS cybercrime unfold is problematic. This data can be useful in understanding the crime process. Simulation studies can provide a viable alternative for researchers to replicate environments that are hard to study. In fact, simulation studies have already been used in criminal justice research to simulate large-scale drug-distribution networks (Dombey-Moore et al. 1994) and estimate the impacts of California's three strikes law on elderly prison populations (Auerhahn 2002). Following suit, ICS environments, their vulnerabilities, prevention measures, and accessibility points can be replicated (and modified) to examine how cybercrimes are executed in a variety of settings. Such studies can shed light on offender decision-making processes at each stage of the crime process.

Simulation studies can be supplemented by using agent-based-modeling (ABM) systems, which are modeled as a collection of autonomous decision-making entities (agents). ABM has also been used in criminological research to model civil violence (Epstein 2002), street robbery (Groff 2007), and crime simulations (Wang, Liu and Eck 2008). In ICS cybercrime research, for example, each agent can individually assess its situation and can make decisions accordingly. This interaction between simulated environments and agents can be extremely useful. By altering any single element (vulnerabilities, prevention measures, access points, agent decision rules), a rigorous analysis of numerous crime processes can be obtained.

Trend Analysis

Trend analysis is a form of comparative analysis that is often employed to identify current movements or trends in a particular area of interest. Trend analysis has been used in criminological research, some of which include domestic abuse (Roy 1982), sexual offenses (Veysey, Zgoba, and Dalessandro 2008), and relationships between alcohol and crime (Greenfeld 1998). The process of trend analysis for critical infrastructure cybercrimes can be conducted along six dimensions: criminal organization, division of labor, attack properties, alliances, communication, and physical elements. Comprehending how each of these dimensions has evolved over the years not only offers a more plausible and thorough picture of critical infrastructure cybercrimes, but also sheds light on the changing nature of these crimes, techniques, and threat agents.

Physical Components of Industrial Control System Cyberattacks

Exploring the physical and cyber relationships of crime is not new to criminological research. Studies exist about online dating scams (Rege 2009), cybercrimes at gambling sites (McMullan and Rege 2010), online child pornography (Marcum et al. 2010), deviant peer associations (Holt, Bossler and May 2011) and cybercrimes against critical infrastructures (Rege-Patwardhan 2009). The above cases suggest that ICS cybercrimes can have a physical component to them, either as **social engineering** strategies or when digital attacks are combined with physical attacks. Thus, understanding the physical-cyber relationship is also a useful and relevant research area.

Researching ICS cybercrimes is an important endeavor, as technologically-dependent societies are negatively affected by them. It is, therefore, imperative to understand cybercriminals and how they operate. As noted earlier, there is simply not enough data to study this area. Critical infrastructures cybercrimes are not reported frequently because they are a matter of national security, a public display of inadequate security measures, and likely to cause fear in the public and industry embarrassment. Furthermore, ICS cybercrimes are clandestine; they are not easy to access as they occur and oftentimes, the attacks go unnoticed. Finally, the topic is relatively new in the criminological discipline, which further hinders researchers in establishing rapport and access to the ICS industry and security sectors.

Initiating a discussion across multiple arenas, including the ethical hacking community, infrastructure industry, and criminal justice community, is crucial. Hackers share the same skill set as cybercriminals and therefore offer relevant insight into exploitable infrastructure vulnerabilities (Holt and Kilger 2012a). Industry experts have insider information on (undisclosed) infrastructure cybercrime, which sheds light on system weaknesses and cybercrime prevention measures. Offender decision-making, crime scripts, organizational dynamics, and modus operandi, however, are multi-faceted phenomena. Drawing on various criminological theories that account for these areas offers a more plausible take on critical infrastructure cybercrime. Thus, a collaborative effort is necessary to bring together a diverse set of people with different views, objectives, and knowledge to address a common problem. This collaborative approach expands existing studies, draws them together to make new points of contact, and enables "big picture" thinking about critical infrastructure ICS cybercrimes.

Glossary

Botnet armies: Computers that are compromised after hackers install malware that gives them complete control over the infected machine.

Distributed Denial of Service (DDoS) Attack: An attack created by amassing a botnet army to disrupt a targeted site's traffic band width capability and consume all disk space or CPU time. The site is thus overwhelmed with requests and is slowed down to a crawl, resulting in a DDoS attack.

Domain Name Server (DNS) Attack: An attack where internet data traffic intended for one website is redirected to the cybercriminal's service. Neither the intended website nor the internet user who seeks to access it is aware of this redirection. This attack is also known as DNS Spoofing or DNS Cache Poisoning.

Exploitation: Hackers study, note, and link software bugs and loopholes in order to achieve optimal exploitation of computer systems.

Firewall: Device that permits or denies network data transmissions based on preset rules. It protects networks from unauthorized access while allowing legitimate network traffic to pass.

Intrusion Detection System: Device that monitors network and system activities for malicious activity, identifies possible incidents, documents incident information in logs, and reports unauthorized access attempts.

Modification: Cybercriminals utilize their technical and programming skills to modify critical infrastructure/Industrial Control Systems.

Rootkits: Collections of computer programs that give hackers administrator-level, or "root," access to computer systems. Rootkits incorporate malware (malicious code), such as Trojans, worms, and viruses, which conceal their presence and activity from users and other system processes.

Routing attacks: Routers, which ensure that information packets travel successfully from their source to destination, are also targeted, resulting in massive routing attacks.

Social engineering: A strategy used to trick individuals, such as ICS vendors and/or operators, into divulging sensitive information by obtaining their trust. These techniques can be both physical and digital in form.

SQL injection attacks: An attack that targets databases through web-based forms. Database programming code (SQL) is inserted into the online form input fields, which are thus injected into the database. This SQL code may change database content or dump the database content, such as customer credit card numbers, passwords, and social security numbers, to the attacker.

Toolkits: Collections of computer programs and/or user manuals that are designed by hackers and sold to technically challenged cybercriminals to commit cybercrimes.

Trojans: Programs that appear benign on the surface, but harbor malicious code within.

Virus: Malicious software spread through human actions, such as running an infected program or opening a malicious email attachment, which steals confidential information, blocks system resources, or tampers with system data.

Website defacement: A website is maliciously altered by inserting or substituting provocative and offending data. Defacing the target's website exposes visitors to misleading, embarrassing, or revealing information that damages the target's security, functionality, productivity, and reputation.

Worms: Malicious software that replicates by spreading copies of itself through shared networks autonomously, without any human intervention.

References

Auerhahn, Kathleen. "Selective incapacitation, three strikes, and the problem of aging prison populations: Using simulation modeling to see the future," *Criminology and Public Policy*, 1 (2002), 353–388.

Bachman, Michael. "The Risk Propensity and Rationality of Computer Hackers," *International Journal of Cyber Criminology*, 4 (2010), 643–656.

Baker, Graeme. "Schoolboy hacks into city's tram system," *The Telegraph*, January 11, 2008. Accessed November 20, 2008. http://www.telegraph.co.uk/news/worldnews/1575293/Schoolbo-y-hacks-into-city's-tramsystem.html.

Baker, Stewart, Shaun Waterman, and George Ivanov. "In the Crossfire: Critical Infrastructures in the Age of Cyber War." *McAfee,* 2010. Accessed August 2012. http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf.

BBC (British Broadcasting Corporation). "US and Israel were behind Stuxnet claims Researcher." 2011. Accessed August 17, 2011. http://www.bbc.co.uk/news/technology-12633240.

Beebe, Nicole and Srinivasan Rao. "Using Situational Crime Prevention Theory to Explain the Effectiveness of Information Systems Security." Proceedings of the 2005 SoftWars Conference, Las Vegas, NV, Dec 2005.

Blane, John. V. *Cyberwarfare: Terror at a Click*. New York: Novinka Books, 2002.

Brenner, Bill. "Experts doubt Russian government launched DDoS attacks." *Search Security*, May 18, 2007. Accessed November 21, 2008. http://searchsecurity.techtarget.com/originalContent/0,281942,sid14_gcil2555548,00.html.

Broad, William, John Markoff, and David E. Sanger. "Israeli Test on Worm Called Crucial in Iran Nuclear Delay." *The New York Times*, January 15, 2011. Accessed August 17, 2011. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html.

Byres, Eric,and Dan Hoffman. "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems" Paper presented at VDE 2004 Congress, VDE, Berlin, October 2004.

Clarke, Ronald. "Situational Crime Prevention." In *Environmental Criminology and Crime Analysis*, edited by Richard Wortley, and Lorraine Mazerolle, 178–194. Oregon: Willan Publishing, 2008.

Cornish, Derek, and Ronald Clarke. "The Rational Choice Perspective." In R. Wortley and L. Mazerolle. (Eds.), *Environmental Criminology and Crime Analysis* (pp. 21–47). Oregon: Willan Publishing, 2008.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. "On Cyber Warfare." *Chatham House*. Accessed January 5, 2012. http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf.

Crawford, Michael. "Utility hack led to security overhaul." *ComputerWorld*, February 16, 2006. Accessed November 20, 2008. http://www.computerworld.com/securitytopics/security/story/0,10801,108735,00.html.

Crowell, Richard. "War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare." *U.S. Naval War College*. Accessed January 5, 2012. http://www.usnwc.edu/getattachment/01f666f2-40a6-4875-88a7-df65d53147d0/War-in-the-Information-Age-A-Primer-for-Cyberspace.

Datz, Todd. "Out of Control." *CSO Security and Risk*, August 2004. Accessed March 8, 2006. http://www.csoonline.com/read/080104/control.html.

Davis, Joshua. "Hackers take down the most wired country in Europe." *Wired Magazine*, August 21, 2007. Accessed November 21, 2008. http://www.wired.com/print/politics/security/magazine/15-09/ff_estoni.

DHS (Department of Homeland Security). "Infrastructure Taxonomy, Version 3: November 1, 2008." Infrastructure Information Collection Division (IICD). Office of Infrastructure Protection.

DHS. *Risk Steering Committee DHS Risk Lexicon—2010 Edition.* September 2010. Accessed August 1, 2011. http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf.

Dombey-Moore, Bonnie, Susan Resetar, and Michael Childress. *A system description of the cocaine trade.* Santa Monica, CA: Rand, 1994.

DPS Telecom. *SCADA Knowledge Base*. Fresno, CA: DPS Telecom 2011a. Accessed August 5, 2011. http://www.dpstele.com/dpsnews/techinfo/scada/scada_knowledge_base.php.

DPS Telecom. *DCS vs. SCADA in Modern Environments*. Fresno, CA: DPS Telecom 2011b Accessed August 9, 2011. http://www.dpstele.com/dpsnews/techinfo/scada/dcs_vs_scada.php.

Dubois, Judith. "Media Coverage of Organized Crime: Impact on Public Opinion?" Research & Evaluation Branch Community, Contract and Aboriginal Policing Services Directorate. Royal Canadian Mounted Police, 2002.

Epstein, Joshua. "Modeling Civil Violence: An Agent-Based Computational Approach," *Proceedings of the National Academy of Sciences of the United States of America*, 99 (2002), 7243–7250.

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Science & Technology,* Winter/Spring 2008: 121–126.

Ezell, Barry. "Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply." MSc diss., University of Virginia, 1998.

Falliere, Nicolas, Murchu, Liam., and Eric Chien. "W32.Stuxnet Dossier, Version 1.4." *Symantec*, February 2011. Accessed August 18, 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Finckenauer, James. *Mafia and Organized Crime: A Beginner's Guide*. Oxford: Oneworld Publications, 2007.

Fogarty, Kevin. "U.S. power grid is a big, soft target for cyberattack, MIT study shows." *IT World*, December 5, 2011. Accessed December 7, 2011.http://www.itworld.com/security/230469/us-power-grid-big-soft-target-cyberattack-mit-study-shows.

Gabor, T. "Armed Robbery Overseas: Highlights of a Canadian Study." In: D. Challenger (ed.), *Armed Robbery.* Canberra, AU: Australian Institute of Criminology, 1988. (Seminar Proceedings No. 26.)

GAO (General Accounting Office). "Critical Infrastructure Protection: Challenges in Securing Control Systems." Washington DC: General Accounting Office, 2003. Accessed March 20, 2010. http://www.gao.gov/new.items/d04140t.pdf.

Greenfeld, Lawrence. *Alcohol and Crime: An Analysis of National Data on the Prevalence of Alcohol Involvement in Crime.* Washington, DC: Bureau of Justice Statistics, 1998.

Groff, Elizabeth. "Simulation for Theory Testing and Experimentation: An Example Using Routine Activity Theory and Street Robbery." Journal of Quantitative Criminology 23 (2007), 75–103.

Haimes, Yacov. "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures." *Risk Analysis,* 26 (2006), 293–296.

Holt, Thomas, Adam Bossler, and David May. "Low Self-Control, Deviant Peer Associations, and Juvenile Cyberdeviance." *American Journal of Criminal Justice, Online First, June 2011*

Holt, Thomas and Max Kilger. "Know Your Enemy: The Social Dynamics of Hacking." The Honeynet Project, 2012a. Accessed June 10, 2012. https://honeynet.org/files/Holt%20and%20Kilger%20-%20KYE%20-%20The%20Social%20Dynamics%20of%20Hacking.pdf.

Holt, Thomas and Max Kilger. "Examining Willingness to Attack Critical Infrastructure On and Off-line," *Crime and Delinquency* 58 (2012b).

Jordan, Tim and Paul Taylor. "A Sociology of Hackers." *The Sociological Review,* 46 (1998), 757–780.

Krone, Tony. "Hacking Motives." Australian Institute of Criminology. High tech crime brief no. 6 (2005).

Kuvshinkova, Svetlana. "SQL SLAMMER worm lessons learned for consideration by the electricity sector." My IT Forum, September 5, 2003. Accessed September 21, 2011. http://www.myitforum.com/articles/15/view.asp?id=5985.

Lemos, Robert. "Power play: Electric company hacked." *ZDNet*, December 15, 2000. Accessed September 20, 2011. http://www.zdnet.co.uk/news/emerging-tech/2000/12/15/power-play-electric-company-hacked-2083210/.

Lewis, James. "Cyber terror: Missing in action." In *Technology and Terrorism*, edited by David Clarke, 145–153. New Jersey: Transaction, 2004.

Luiijf, Eric. "SCADA Security Good Practices for the Drinking Water Sector." TNO: Netherlands Organization for Applied Scientific Research, 2008.

Marcum, Catherine, George Higgins, Tina Freiburger, and Melissa Ricketts. "Policing Possession of Child Pornography Online: Investigating the Training and Resources Dedicated to the Investigation of Cyber Crime," *International Journal of Police Science & Management*, 12 (2010), 516–525.

Martellozzo, Elena, Daniel Nehring, and Helen Taylor. "Online Child Sexual Abuse by Female Offenders: An Exploratory Study." *International Journal of Cyber Criminology*, 4 (2010), 592–609.

McAfee. *McAfee Virtual Criminology Report: North American Study into Organized Crime and the Internet.* San Francisco, CA: McAfee, 2005. Accessed October 20, 2005. http://www.mcafee.com/us/local_content/misc/mcafee_na_ virtual_ criminology_report.pdf.

McMullan, John, and Aunshul Rege. "Cyberextortion at Online Gambling Sites: Criminal Organization and Legal Challenges." *Gaming Law Review*, 11 (2007), 648–665.

McMullan, John and Aunshul Rege. "Online crime and internet gambling." *Journal of Gambling Issues.* Issue 24, July 2010.

Moore, Andrew, Dawn Cappelli, Thomas Caron, Eric Shaw, Derrick Spooner, and Randall Trzeciak. *A Preliminary Model of Insider Theft of Intellectual Property.* Pittsburg, PA: Computer Emergency Response Team 2011. Accessed June 10, 2012. http://www.cert.org/archive/pdf/11tn013.pdf.

Moore, Robert, Naga Tarun Guntupalli, and Tina Lee "Parental Regulation and Online Activities: Examining factors that influence a Youth's potential to become a Victim of Online Harassment." *International Journal of Cyber Criminology*, 4 (2010), 685–698.

Morain, Dan. "Hackers Victimize Cal-ISO." *Los Angeles Times*, June 9, 2001. Accessed August 18, 2011. http://articles.latimes.com/2001/jun/09/news/mn-8294.

Moteff, John. *Risk Management and Critical Infrastructure Protection: Assessing, Integrating, and Managing Threats, Vulnerabilities and Consequences.* CRS Report for Congress, Order Code RL32561, 2005.

NCS (National Communication System). *Supervisory Control and Data Acquisition (SCADA) Systems.* Washington DC: National Communication System, 2004. Accessed May 31, 2012. http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf.

Newman, Graeme and Ronald Clarke. *Superhighway Robbery: Preventing e-commerce crime.* Oregon: Willan Publishing, 2003.

Nicholson, Rick. "Critical Infrastructure Cybersecurity: Survey Findings and Analysis." Energy Insights, an IDC company. White Paper sponsored by Secure Computing, November 2008.

NSTAC (National Security Telecommunications Advisory Committee). *Information Assurance Task Force: Electric Power Risk Assessment—Executive Summary.* Washington DC: National Security Telecommunications Advisory Committee, 2000. Accessed August 17, 2011. http://www.solarstorms.org/ElectricAssessment.html.

Oman, Paul, Edmund Schweitzer III, and Jeff Robert. "Safeguarding IEDS, Substations, and SCADA Systems Against Electronic Intrusions." *Schweitzer*

Engineering Laboratories 2001. Accessed August 11, 2011. http://www2.selinc.com/techpprs/6118.pdf.

Poulsen, Kevin. "Slammer worm crashed Ohio nuke plant network." *Security Focus,* August 19, 2003. Accessed August 10, 2011. http://www.securityfocus.com/news/6767.

Rantala, Ramona. "Cybercrimes Against Businesses, 2005." *Bureau of Justice Statistics*, October 27, 2008. Accessed February 19, 2009. http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf.

Rege, Aunshul. "What's Love Got to Do With It? Exploring Online Dating Scams and Identity Fraud." *International Journal of Cybercriminology*, 3 (2009), 494–512.

Rege-Patwardhan, Aunshul. "Cybercrimes against critical infrastructures: a study of online criminal organization and techniques." *Criminal Justice Studies, 22* (2009), 261–271.

Reyns, Bradford. "A situational crime prevention approach to cyberstalking victimization: Preventive tactics for Internet users and online place managers." *Crime Prevention and Community Safety*, 12, (2010) 99–118.

Rindskopf, Amy. "Juvenile computer hacker cuts off FAA tower at regional airport: First federal charges brought against a juvenile for computer crime." *Department of Justice*, March 18, 1998. Accessed November 20, 2008. http://ncsi-net.ncsi.iisc.ernet.in/cyberspace/law/responsibility/cybercrime/www.usdoj.gov/criminal/cybercrime/juvenile.htm.

Robles, Rosslin, Min-kyu Choi, Eun-suk Cho, Seok-soo Kim, Gil-cheol Park, and Jang-Hee Lee. "Common Threats and Vulnerabilities of Critical Infrastructures." *International Journal of Control and Automation, 1* (2008), 17–22.

Rogers, Marcus. *The Development of a Meaningful Hacker Taxonomy: A Two Dimensional Approach.* Accessed January 23, 2007. https://www.cerias.pur due.edu/tools_and_resources/bibtex_archive/ar-chive/2005-43.pdf.

Rossignol, Michael. "Critical Infrastructure Protection and Emergency Preparedness." *Government of Canada Publications*, June 2001. Accessed August 27, 2007. http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/BP/prb017-e.htm.

Roy, Maria. *Abusive Partner—An Analysis of Domestic Battering.* New York: Van Nostrand Reinhold, 1982.

SANS (System Administration, Networking, and Security Institute). *Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack.* Chicago, IL: SANS Institute, 2001. Accessed August 30, 2011. http://www.sans.org/reading_room/whitepapers/hackers/hackers-turn-lights-off-vulnerability-power-grid-electronic-attack_606.

Scadasystems.net. “SCADA systems.” Accessed August 9, 2011. http://www.scadasystems.net/.

Seigfried, Kathryn, Richard Lovely, and Marcus Rogers. “Self-Reported Online Child Pornography Behavior: A Psychological Analysis.” *International Journal of Cyber Criminology*, 2 (2008), 286–297.

Shaw, Eric and Harley Stock. “Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall.” 2011. Accessed June 10, 2012. https://www4.symantec.com/mktginfo/whitepaper/21220067_GA_WP_Malicious_Insider_12_11_dai81510_cta56681.pdf.

Smith, Martha. “Introduction.” *Crime Prevention Studies*, 16 (2003), 1–5.

Stamp, Jason, John Dillinger, William Young, and Jennifer DePoy. “Common Vulnerabilities in Critical Infrastructure Control Systems.” *Energy.gov*, May 22, 2003. Accessed August 27, 2007. http://www.oe.netl.doe.gov/docs/prepare/vulnerabilities.pdf.

Stouffer, Keith, Joe Falco, and Karen Scarfone. “NIST Guide to Industrial Control Systems (ICS) Security.” *National Institute of Standards and Technology*. Computer Security Division, Computer Security Resource Center, June 2011. Accessed August 5, 2011. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

Taylor, Robert, Eric Fritsch, John Liederbach, and Thomas Holt. *Digital Crime and Digital Terrorism, 2nd Edition*. NJ: Pearson Education, Inc, 2010.

The Economist. “Cyberwar: War in the Fifth Domain.” *The Economist*, 2010. Accessed January 5, 2012. http://www.economist.com/node/16478792.

Theoharidoua, Marianthi, Spyros Kokolakisb, Maria Karydaa, and Evangelos Kiountouzis. “The insider threat to information systems and the effectiveness of ISO17799.” *Computers & Security*, 24 (2005), 472–484.

Vatis, Michael. “Cyber Attacks: Protecting America’s Security Against Digital Threats.” Executive Session on Domestic Preparedness, 2002. Accessed January 20, 2012. http://belfercenter.ksg.harvard.edu/files/vam02.pdf.

Verton, Dan. *Black Ice: The Invisible Threat of Cyber-Terrorism*. CA: McGraw-Hill, 2003.

Veysey, Bonita, Kristen Zgoba, and Melissa Dalessandro. “Preliminary Step Towards Evaluating the Impact of Megan’s Law: A Trend Analysis of Sexual Offenses in New Jersey from 1985 to 2005.” *Justice Research and Policy*, 10 (2008), 1–18.

Wang, Xuguang, Lin Liu, and John Eck. “Crime Simulation Using GIS and Artificial Intelligent Agents.” In J. E. Eck & L. Liu (Eds.), *Artificial Crime Analysis Systems: Using Computer Simulations and Geographic Information* Systems (pp. 209–224). Hershey, PA: IGI Global, 2008.

Weaver, Nicholas, Vern Paxson, Stuart Staniford, and Robert Cunningham. *A Taxonomy of Computer Worms*. International Computer Science Institute, 2003. Accessed March 8, 2006. http://www.icir.org/vern/papers/taxonomy.pdf.

Williams, Dan. “Israel holds couple in corporate espionage case.” *Computer World*, January 31, 2006. Accessed March 8, 2006. http://www.computerworld.com/s/article/108225/Israel_holds_couple_in_corporate_espionage_case.

YouTube. “SCADA Tutorial.” Accessed August 5, 2011. http://www.youtube.com/watch?v=tIU_wDVoEVE.

ZDNN. “Humans opened the door for power hack.” *ZDNet*, November 7, 2001. Accessed August 18, 2011. http://www.zdnet.com/news/humans-opened-the-door-for-calif-power-hack/117607.

Zintro. *SCADA Experts—Find SCADA Consultants, Expert Witnesses & More*. Zintro, 2011. Accessed August 5, 2011. https://www.zintro.com/area/scada.