Terrorism and Political Violence

ISSN: 0954-6553 (Print) 1556-1836 (Online) Journal homepage: http://www.tandfonline.com/loi/ftpv20

Exploring the Intersections of Technology, Crime, and Terror

Thomas J. Holt

To cite this article: Thomas J. Holt (2012) Exploring the Intersections of Technology, Crime, and Terror, Terrorism and Political Violence, 24:2, 337-354, DOI: 10.1080/09546553.2011.648350

To link to this article: http://dx.doi.org/10.1080/09546553.2011.648350

Published online: 14 Mar 2012.

Terrorism and Political Violence, 24:337–354, 2012

ISSN: 0954-6553 print/1556-1836 online
DOI: 10.1080/09546553.2011.648350

Routledge
Taylor & Francis Group

Exploring the Intersections of Technology, Crime, and Terror

THOMAS J. HOLT

School of Criminal Justice, Michigan State University, East Lansing, Michigan, USA

The Internet and computer-mediated communications (CMCs) have drastically changed the way that individuals communicate and share information across the globe. Over the last two decades, financial institutions, private industry, and governments have come to rely on technology in order to access sensitive data and manage critical infrastructure, such as electrical power grids. As a consequence, the threat posed by cybercriminals has increased dramatically and afforded significant opportunities for terrorist groups and extremist organizations to further their objectives. The complex and intersecting nature of both crime and terror make it difficult to clearly separate these issues, particularly in virtual environments, due to the anonymous nature of CMCs and challenges to actor attribution. Thus, this study examines the various definitions for physical and cyberterror and the ways that these activities intersect with cybercrime. In addition, the ways that terrorists and extremist groups use the Internet and CMCs to recruit individuals, spread misinformation, and gather intelligence on various targets are discussed. Finally, the uses of computer hacking tools and malware are explored as a way to better understand the relationship between cybercrime and terror.

Keywords cybercrime, cyberterror, hacking, hacktivism, malware

The emergence of the Internet and computer-mediated communications over the last three decades has revolutionized the ways that individuals share information and conduct business across the globe. As a result, there are now myriad opportunities for criminality and deviance in online environments, and to utilize technology as a means to facilitate off-line crime. Computer technologies have also spurred the development of cybercrimes, where technology plays a central role in the facilitation of the offense.[1] Criminal and deviant groups can now use computer-mediated communication (CMCs) technologies like forums and newsgroups to share information across great distances.[2] Furthermore, computer hackers have identified ways to exploit virtually all forms of computer software and hardware in order to obtain access to secured resources and steal information.[3]

Extremist and terror groups have also embraced technological innovations across the globe in order to gain advantage over their adversaries. In fact, the Internet and CMCs enable groups to engage in asymmetric attacks that far exceed their

Thomas J. Holt is an associate professor in the School of Criminal Justice at Michigan State University.

Address correspondence to Thomas J. Holt, School of Criminal Justice, Michigan State University, 434 Baker Hall, East Lansing, MI 48824, USA. E-mail: holtt@msu.edu

existing attack capabilities by leveraging rapid and decentralized communications systems.[4] Computers, cell phones, and technological equipment can be obtained at minimal cost and used with a high degree of anonymity. Additionally, blogs and video sharing sites can be used to deliver propaganda messages in support of an extremist group's position.[5] Such a campaign allows the group to control the delivery and management of their message to interested parties, while at the same time demoralizing and confounding their adversaries. Even more disconcerting is the fact that the Internet can be used as an attack vector to harm the underlying infrastructure that drives modern nation-states. Telecommunications, electrical grids, financial institutions, and governments depend on technology that can be harmed with greater secrecy and fewer resources than might otherwise be required in a traditional physical attack.[6]

The dynamic global online environment, coupled with constant changes in technology and offending techniques, make it exceedingly difficult to understand the nature and scope of extremist groups operating today. Thus, this study will consider the issues inherent in defining and separating cyberterror from physical terror and cybercrimes. Second, the ways that extremist and terror groups use existing technology to gather and disseminate information and recruit new members will be explored, followed by a discussion on the application of hacking techniques in support of extremist ideologies. Finally, the future of cyberterror and the challenges these activities pose for government policymakers, security organizations, and law enforcement agencies will be discussed. In turn, this study will provide a foundation for future research on the problem of cyberterror and its links to the broader community of cybercriminals.

Understanding Cybercrime, Cyberterror, and Physical Terror

In order to understand the phenomenon of cyberterror, it is first critical to understand its relationship to cybercrime and terrorism in general. There are multiple definitions and substantive debate over the nature of both cybercrime and terror, making it difficult to immediately distinguish these acts. In fact, scholars initially debated whether cybercrime should be conceived of as a traditional offense enabled by new tools and devices,[7] or a truly novel form of offending that has no previous parallel.[8] Both perspectives are supported by ample research data—most any existing form of crime can be assisted by technology in some way, while new categories of offenses have emerged that could not otherwise exist without computers, such as malicious software and computer hacking.[9]

As a consequence, there is no single accepted definition of cybercrime, though many argue that it involves criminal behaviors that incorporate cyberspace or computer technology in some fashion.[10] To help clarify what constitutes a cybercrime, David Wall developed one of the most comprehensive frameworks with four specific categories of offending: cyber-trespass; cyber-deception/theft; cyber-porn/obscenity; and cyber-violence.[11] Cyber-trespass concerns the crossing of invisible, yet salient boundaries of ownership online. Computer hackers typically engage in cyber-trespass due to their frequent participation in attacks against computer systems and networks that they do not own.[12] Breaches of computer networks and system boundaries are quite costly, and estimates suggest that U.S. businesses lose millions of dollars annually due to attempts to gain unauthorized access.[13]

The second and related category within this typology is cyber-deception and theft. Computer intrusions and hacking techniques can be used to steal sensitive

information from various targets, including intellectual property, state secrets, and money. For instance, businesses reported average losses of $500,000 in 2008 due to financial fraud incidents,[14] while individual consumers lost an average of $575 to various types of fraud in 2009.[15] Similarly, music and media piracy through computer outlets have caused billions of dollars in losses through lost revenue and jobs.[16] As a consequence, the Internet presents a clear opportunity for theft from literally millions of targets across the globe.

The remaining categories within this typology are related in that they may not necessarily violate laws within a given nation. The third category includes cyber-porn and obscenity, reflecting the availability of sexually expressive or explicit materials across the World Wide Web. The final category, cyber-violence, represents the distribution of injurious, hurtful, or dangerous materials online. This category references two forms of violence, the first of which includes behaviors that cause emotional harm to individuals through online environments. For example, individuals have begun to use the Internet as a means to send threatening or harassing messages to others via e-mail, instant messaging services, or social networking sites like Facebook.[17] The second form of violence involves the distribution of materials online that can be used to cause harm in the real or virtual world. The Internet enables individuals to spread bomb-making manuals, guides on guerrilla warfare strategies, and information to facilitate hacking and fraud in a distributed fashion.[18] The publication of such information may not pose a substantive risk to any single individual or group, though the availability of this information can be misused in the wrong hands. Additionally, free speech laws in the United States and elsewhere may actually protect radical positions or ideological documents. In fact, anecdotal evidence indicates that Muslim extremists are increasingly using website hosting services in the United States because of the protections afforded to individual civil liberties.[19]

The wide range of acts that may be viewed as cybercrimes pose a significant challenge to any definition of cyberterror, since many extremist groups may engage in the same activities as non-ideological criminals. This problem is compounded by the fact that most nations treat acts of terror as criminal offenses.[20] There are, however, substantive differences between crime and terror based on motive and the scope of harm caused. For instance, criminal acts often target single individuals and may be motivated by economic or other objectives, while terrorist attacks are often driven by a political motive and are designed to not only hurt or kill innocents but to also strike fear into the larger population.[21]

In order to better understand the complexities of cyberterror, it is first necessary to understand physical terror. There is generally little consensus across governments as to what constitutes an act of physical terror, due to variations in cultural norms, political and religious ideologies, and political relationships.[22] Schmid and Jongman examined over 100 definitions for terror across the world and found few common characteristics across these terms.[23] The most prevalent elements include: the use of violence, political motivations, fear, threats, and psychological effects and reactions.[24] Similarly, Hoffman compared terrorist behavior to criminals and other irregular war-fighters to consider what constitutes terror.[25] He identified terrorism as the "deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change" in order to intimidate and generate fear in the psyche of the population targeted and obtain leverage and power to cause political change.[26] This definition argues that acts of terror are performed by subnational groups or non-state entities regardless of the ideological or political motives of the

actors. Thus, though there is no single definition for terror, a common framework can be developed to identify these acts.

The lack of consistency is also present in definitions for "cyberterror," a term which emerged in the mid-1990s as the World Wide Web became an integral component of business and citizen communications.[27] The challenge in defining cyberterror lies in differentiating these acts from cybercrimes. For example, the interconnectivity afforded by the Internet enables attackers to target military systems containing sensitive information, financial service systems that engender commerce, and power grids, switching stations, and other critical infrastructure necessary to maintain basic services.[28] At the same time, these resources can be targeted by hackers, identity thieves, foreign nationals, or other criminal entities with differing motives and ideologies. One way researchers have separated these incidents is through the use of the term "hacktivism," recognizing the use of hacking techniques to promote an activist agenda or express an opinion.[29] Politically-driven groups employ hacking techniques to engage in more serious strikes against governments and political organizations. These attacks may violate the law though not necessarily produce fear or concern among the general population.[30]

As a result, hacktivism is similar to certain forms of real world protest actions, such as vandalism and destruction of private property in furtherance of a political agenda.[31] For instance, a group utilizing hacking techniques to disrupt or otherwise hinder the ability of government agencies to communicate may serve the same function as members of the Earth Liberation Front lashing themselves to trees or buildings in an attempt to reduce the operability of a logging company.[32] These actions may be illegal, though they may not be designed to spur fear in the target or a broader populace. As a result, hacktivism provides a means to identify criminal acts of protest involving hacking techniques which may have some analogue to off-line political action.[33] The use of this term does not, however, help to refine our understanding of cybercrimes generally since it only adds to the jargon of investigators and researchers.

In order to further separate cyberterror from hacktivism and physical terror, some argue that an act of cyberterror must be motivated by a political or ideological agenda and seek to produce fear, coerce, or otherwise intimidate a government or its people.[34] Some have also argued that cyberterror incidents must result in a loss of life or physical harm in the real world, since the concept of physical harm plays a key role in the operationalization of traditional terror incidents.[35] For instance, Pollitt defined cyberterror as "the premeditated, politically motivated attack against information, computer systems, and data which result in violence against noncombatant targets by subnational groups."[36]

Physical violence may not, however, be necessary in online environments due to the increasing dependence on the Internet as both a conduit for service and a medium for expression. For instance, a virtual attack against financial institutions or power systems that produces a loss of service could hinder the ability of a population to engage in commerce or communicate with others. In fact, posts from Islamist extremist websites have noted the value of attacking financial services online, stating that disrupting these resources "for a few days or even for a few hours . . . will cause millions of dollars worth of damage."[37] The economic harm produced by a cyberattack, coupled with fear over the likelihood that it may occur again, could be equal to a physical attack. To that end, some definitions of cyberterror recognize the disruptive effect of virtual attacks against information or infrastructure. Foltz suggested that cyberterrorism involved "an attack or threat of an attack, politically motivated, intended to: interfere with the political, social, or economic functioning of a group organization or

country."[38] A similar definition was used by Stambaugh and colleagues, defining cyberterror as a "premeditated, politically motivated attack against information systems, computer programs and data . . . to disrupt the political, social, or physical infrastructure of the target."[39] As a result, physical harm may be less pertinent relative to the production of fear in defining an incident as an act of cyberterror.

At the same time, terror and extremist groups have not engaged in attacks that conform to these existing definitions of cyberterror, particularly those that incorporate physical harm or the production of fear. For instance, terror groups' use of forums and CMCs to communicate and provide targeting information would largely be excluded from other definitions of cyberterror that emphasize violence or physical harm only. Instead extremist groups utilize the Internet in ways that more closely resemble the characteristics of cybercrimes including the dissemination of information to incite violence and harm. In order to capture this variation, Foltz's definition also recognizes acts which "induce either physical violence or the unjust use of power."[40] A recent definition provided by Britz also includes the "dissemination of information, facilitation of communication, or, attack against physical targets, digital information, computer systems, and/or computer programs . . . or any utilization of digital communication or information which facilitates such actions directly or indirectly."[41] Thus, while there is no single agreed upon definition for cyberterror, it is clear that this term must encapsulate a greater range of behavior than physical terror due to the dichotomous nature of cyberspace as a vehicle for communications as well as a medium for attacks. More expansive definitions, such as those provided by Britz and Foltz, provide a much more comprehensive framework for exploring the ways that extremist groups utilize technology in support of their various agendas.

Cyberspace as a Medium for Communication and Image Management

Over the last two decades, extremist and terror groups have used the Internet for recruitment, fundraising, and the dissemination and acquisition of attack information. The Internet has also provided criminals and terrorists with new capabilities for clandestine communications between operatives, including through free e-mail accounts, message drop boxes, encrypted messaging, steganography, and other tools. Most all nations have some form of Internet connectivity, thus extremist groups can communicate their messages to the world with ease, and often tailored to specific audiences. Multimedia creation software like Adobe Photoshop enables individuals to develop videos, photos, and stylized text in an easy-to-read and professional manner. These tools can also be acquired with minimal economic investment through pirated software channels.[42] In addition, cell phone cameras and web cams allow individuals to create training videos and share these resources with others through video sharing sites at no cost.[43]

The most significant benefit of the Internet lies in the fact that extremist groups can directly control the way that their message is delivered to the general public. Blogs and social networking sites enable individuals to post and re-post text, videos, and web links so that they spread rapidly across the globe. In turn, a group can influence how they are portrayed in both underground and popular media, rather than waiting for mainstream press to handle the story.[44] Further, extremist groups can directly refute claims made by law enforcement, governments, and the media as part of their overall effort to control their public perception. As James Forest and other terrorism scholars have noted, controlling perceptions is central to what terrorists hope to accomplish.[45] Additionally, these online materials can contribute to the

radicalization process by repeatedly exposing individuals to messages that may elicit rage and frustration over oppression or injustices.[46]

There are multiple examples of extremist group utilization of technology for recruitment and message distribution. Web forums like Stormfront.org are extremely popular among the neo-Nazi movement as a means to debate issues publicly and promote their agenda.[47] The forums on this site have over 100,000 members and thousands of new posts made daily. In addition, the Stormfront website maintains pages on a number of social networking sites like Facebook as a means to help recruit and connect members.[48] Hate groups are even creating their own social networking sites, such as "New Saxon," which is a "Social Networking site for people of European descent" produced by the neo-Nazi group the National Socialist Movement.[49] This site enables members to create profiles, blog, post pictures, videos, and even send cards to other members. In turn, this helps to provide a mechanism to connect those in the movement with others despite any geographic boundaries.

The jihad movement has also begun to produce highly stylized websites, videos, and magazines to promote their message as a lifestyle rather than as a marginalized position. In fact, a message posted on the website www.azzam.com stated that "the more Web sites, the better it is for us. We must make the Internet our tool."[50] These pages are often written in multiple languages to communicate their messages across multiple groups, and focus on justifications for resisting foreign occupation or Western ideals rather than on the use of violence. For example, anti-American extremist groups utilized the images of prisoner mistreatment by U.S. soldiers in Abu Ghraib to demonstrate a lack of respect for Islamic value systems.[51] In addition, Al Qaeda operatives have begun to use the Internet as a means to communicate with established media outlets. For example, Al Qaeda agents posted a video ending with a statement welcoming questions from the media that could be posted and answered via web forums online.[52] Thus, they would be able to directly control their responses through the use of new media, rather than traditional dealings with media outlets.

The web also enables the distribution of multi-media resources that help to promote specific agendas. For example, the white supremacist group, the National Alliance, operates a record label called Resistance Records which sells over 1,000 CDs, as well as magazines, books, and clothing via their website.[53] The various items sold enable the spread of hate messages through popular media, introducing individuals to these messages in a way that speaks directly to generational interests. In addition, they have created sophisticated computer games aimed at attracting teenagers to their movement. For instance, the game *Ethnic Cleansing* is a first-person shooting game centered around players killing blacks, Jews, and Hispanics as they run through urban ghettos and subway environments.[54] Other terrorist groups have created video games, like Hizbollah's *Special Force*, that have become wildly popular among supporters and potential new recruits.[55]

Extremist groups can also utilize the Internet as a critical resource for the dissemination of attack information. For example, the jihadi movement has developed various videos and documents on bomb making, developing improvised explosive devices, and conducting suicide bombing operations.[56] Eco-terrorist groups have also provided resources online to enable individuals to engage in attacks on their behalf. For instance, the Earth Liberation Front published its *Ozymandius* manual online, a several-hundred-page resource providing tactical and strategic information on the ways to affect job sites and heavy equipment used in construction and logging industries. These manuals have been used in various bombings by ELF actors, such

as the burning of a Vale, Colorado ski resort using a device with the same design as one found on an ELF website.[57]

The amount of data available online can also be used by terrorist and extremist groups to acquire information on prospective targets and to develop pre-mission strategies. For example, satellite images from Google Earth and the street view function of Google Maps provide relatively up-to-date, real-world images of the topography and detail of most major cities throughout the world. This information can be used to develop tactical plans for the execution of an attack against various targets. In fact, one of the conspirators in the 2008 terror attacks in Mumbai, India claimed that Google Earth images were used to plan the attacks.[58] Similarly, information on the physical and virtual topography of public utilities, telephone systems, and other critical infrastructure can be obtained from various public and private websites.[59] As a consequence, attackers can readily obtain tactical and strategic information through online sources with ease.

Overall, the Internet offers many information assets for terrorist and criminal activity, including covert messaging among members of decentralized networks, multimedia communications between organizations and its supporters or potential recruits, and surveillance or operational intelligence gathering, to name just a few. As a result, the technology offers extremist groups unparalleled opportunities to promote their agenda and increase membership.

The Intersection of Hacking and Cyberterror

The Internet also provides a platform for potentially lethal attacks against civilian and government targets. There are myriad sensitive systems now connected to the Internet that act as high-value targets for extremist groups due to the amount of economic and/or physical harm that could be produced, as well as extremely high levels of fear among civilian populations. Such attacks require the use of tools and techniques developed by a hacker community that has evolved considerably over the last three decades.

In the 1980s and early 1990s, would-be hackers needed to develop a sophisticated understanding of technology in order to engage in an attack.[60] The hacker community was also regionally bound, with groups forming in cities or suburbs based on friendship circles.[61] Individuals communicated and shared information via Bulletin Board Systems (BBS) and party lines, and often had to demonstrate their skill in order to gain access to these resources. In addition, hackers would often barter for new resources, whether through trading stolen information or credentials, BBS access, or other valuable resources.[62] In turn, the primary targets of attacks were often corporate entities or telecommunications due to a small proportion of the population with networked computers.

The advent of the World Wide Web and its rapid adoption across the globe in the mid-1990s, coupled with a substantive decrease in the cost of computer technology, forced a significant shift in the hacker community and the ways in which individuals engaged in attacks. Computer technology became increasingly easy to use, requiring hackers to spend less time learning how software and hardware functioned in order to engage in attacks.[63] Additionally, hacker tools became more readily accessible through forums and downloadable files that could be obtained from various websites.[64] The global connectivity afforded by the adoption of technology engendered the formation of hacker communities and collectives that were not bound by geography or region. Individuals could develop a reputation based on their ability,

which could extend beyond their location and generate status in the international community. In addition, the development of weaponized malicious software—including viruses, worms, and Trojan horses—enabled individuals to engage in damaging attacks with global impact.[65] At the same time, the availability of these tools allowed attackers with minimal knowledge to carry out attacks previously beyond their level of skill.

As hacking became a global phenomenon in the late 1990s and early 2000s, the mechanics of the hacker community changed. Though tools could still be developed and released as a means of garnering status, a burgeoning marketplace for malicious software and hacker tools on a fee-for-service basis emerged.[66] The development of sophisticated attack tools like botnet malware, which combines the functionality of a virus with the capability to remotely control infected machines through a single Internet Relay Chat (IRC) channel, enabled hackers to establish stable networks of infected computers around the world.[67] These tools can be used for multiple attack strategies, such as the distribution of spam, network scanning, or direct attacks against other networks. The small proportion of skilled hackers with the capability to develop these tools have begun to recognize the monetary value of their products, and now lease out their infrastructure to the larger population of semi-skilled hackers for a fee to engage in attacks.[68] In addition, individuals sell custom builds of malicious software directly to interested parties, enabling semi-skilled hackers to access high quality tools that substantially increase their attack capabilities. Thus, the market for malicious software has changed the process of hacking and created significant opportunities to engage in cyber-attacks that were not previously possible.

The global reach of the Internet also allows attackers to monitor and identify useful tools regardless of the region in which they were created. For instance, a recent study found that the distribution patterns of free-to-use malware often starts in Europe, and circulates through the Middle East, South America, and Asia within a six- to eight-month window.[69] The tools can be identified by a local actor via web forums, and reposted with a new language pack reflecting the regional dialect or preferences.[70] This distribution chain not only allows hackers to identify easy-to-use or high quality tools, but also to obfuscate the creation of malware by taking credit for a tool that was created by someone else. Thus, the international dynamics of the hacker community engender access to tools and attack techniques that may be unique to a specific region or group.

The historic changes in the hacker community provide important context for the current methods and tactics for cyberattacks from extremist communities around the world. For example, the Turkish hacker community, which is driven in part by religious and nationalist agendas, regularly posts videos and tutorials on various types of cyberattacks in order to facilitate learning and attacks by less skilled actors.[71] In addition, Turkish hackers use various social media sites like YouTube and Facebook to draw attention to their attacks against government and private industry targets.[72] Various groups in support of Al-Qaeda also operate web forums to distribute hacker tools and coordinate attacks. Most notably, the hacker Younis Tsoulis promoted the use of hacking tools against various targets in support of global jihad. Using the handle Irhabi 007, or Terrorist 007, he published a manual entitled "The Encyclopedia of Hacking the Zionist and Crusader Websites," which detailed various attack methodologies and a list of vulnerable targets online.[73]

In light of the diverse nature of vulnerable systems and points of attack for hackers, it is critical to identify the most common attack vectors for extremist groups

online. One of the most common tactics involves the use of Denial of Service attacks in order to keep individuals from using certain services or resources.[74] In fact, Denial of Service tools have been a part of the arsenal of activists and extremists since the mid-1990s. For example, members of a hacktivist group called the Electronic Disturbance Theater developed an attack tool called FloodNet that overloaded web servers and kept others from being able to access their services.[75] Hackers used this tool in attacks against the U.S. Pentagon, Mexican government websites, and various business targets as a means of protest against their activities and policies. Recently, the al-Jinan forum has been noted for its role in distributing a tool called "Electronic Jihad."[76] This stand-alone Denial of Service tool can be used to attack servers without a great deal of skill on the part of the attacker. In turn, this enables anyone to play an active role in the facilitation of cyberattacks on behalf of their beliefs. Similar tools have been used by members of a group called Anonymous in a series of attacks against government and private industry targets in order to protest attempts to reduce the distribution of pirated media.[77] The group believes that intellectual property laws are unfair, and that governments are stifling the activities of consumers, requiring a direct response from the general public to stand up against this supposed tyranny.

Another valuable attack method in support of political or ideological agendas is web defacements, where an actor replaces the normal html code with an image and message of their choosing.[78] Defacements are particularly valuable as they allow an actor to express their opinions or beliefs, and attribute the attack to themselves or their cause. In addition, the defacer can also choose to simply replace the initial page or cause more substantive harm by deleting the original content. Initially, web defacements served as a way to garner attention and status within the hacker community.[79] Over the last decade, however, an increasing proportion of these attacks are used to express a political or patriotic message.[80] For instance, the Turkish hacker community began a widespread campaign of web defacements after the publication of a cartoon featuring an image of the prophet Mohammed with a bomb in his turban.[81] Many Muslims were deeply offended by this image, and Turkish hackers began to deface websites owned by the Danish newspaper that published the cartoon along with any other site that reposted the image. Hackers defaced thousands of websites in support of their faith, believing this to be their duty on behalf of the Islamic community.[82]

Hacker groups have also used e-mail spam campaigns with some success in order to hamper communications by government and industry. In fact, one of the earliest incidents that may be defined as an act of cyberterrorism occurred in 1998 in Sri Lanka. A group called the Internet Black Tigers, tied to the Liberation Tigers of Tamil Eelam (LTTE), engaged in a series of "suicide email bombings" against Sri Lankan embassies.[83] The group sent over 800 e-mails a day for a two-week period in order to disrupt communications and voice dissent against the government and their actions.[84] Similar tactics were observed in the course of attacks between Russian and Estonian hackers in 2007 as a consequence of real-world protests over the removal of a Russian statue from an Estonian cemetery.[85] Thus, e-mail can be used not only as a communications method but as an inexpensive and uncomplicated attack vehicle as well.

Forecasting the Future of Cyberterror

Given the rapid evolution of technology and the unintended changes they force in human behavior, it is difficult to predict the ways that extremist group behaviors

will evolve over time.[86] For example, there have been relatively few incidents of cyberterror across the globe and virtually none within the United States despite the explosion in attacks against sensitive government networks and the financial sector over the last decade.[87] In addition, experts argue that the general cyberattack capabilities of extremist groups like Al-Qaeda are relatively limited by comparison to the larger hacker community.[88] In fact, jihadi hackers attempted to engage in a series of attacks against the U.S. stock exchange and financial institutions. The so-called "Electronic Battle of Guantanamo" did not come to fruition due to bank notifications by law enforcement and preparation against the attacks.[89] The failure of that effort, however, should not be construed as a success for government agencies, but rather act as a warning that Al-Qaeda and other extremist groups are becoming cognizant of various vulnerabilities and identifying techniques to exploit these flaws.

With this in mind, it is necessary to consider the various ways that cyberspace may be used for either communications or as an attack mechanism in the immediate future, and the challenges these threats pose for law enforcement and policy makers. One of the key developments lies in the recent release of the malware program Stuxnet. In late 2010, a flurry of media coverage described a new malware program that appeared to target nuclear power plants in Iran.[90] It is not clear what its true functionality and purpose was, though analyses of the program indicate it was clearly designed to affect a specific Siemens brand control system used in the Natanz nuclear enrichment plant in Iran.[91] By degrading the functionality of this system, it is possible that the program could have caused substantive harm to the functions of the facility. In addition, computer control systems are often segmented from publicly connected computer networks in order to reduce the risk of compromise.[92] The Stuxnet malware however, was initially spread via flash drives, indicating that the creators clearly understood how to affect their target.[93] The code also replicated itself in an extremely limited and cautious fashion in order to minimize its likelihood of detection. Finally, the malware utilized several previously unknown exploits in various computer programs to affect system functionality, suggesting the creators were extremely skilled in computer software and hardware exploitation.[94]

The emergence of Stuxnet clearly demonstrates the potential vulnerabilities that can be exploited in critical infrastructure across the globe. Most power grid technologies, water, sewer, and other critical infrastructure are managed via Supervisory Control and Data Acquisition (SCADA) systems that communicate via hardened or defended networks.[95] Though security researchers regularly attempt to identify and secure SCADA systems from attack, the perception of the likelihood of attack has always been largely antecedent to questions about their overall reliability. As a consequence, Stuxnet clearly demonstrates the need to carefully secure these systems from multiple forms of cyberattack. Though the development and release of this sort of program may be beyond the existing skills of extremist groups, widespread access to this code may encourage attackers to develop similar resources that may be made available through the malicious software market.[96] In fact, the U.S. Department of Homeland Security recently reported concerns over this same sort of code being used as the basis for attacks against U.S. power installations.[97] Thus, Stuxnet represents one of the first true examples of a cyberattack that could directly cause physical harm in the real world.

The problem of Stuxnet also highlights a significant issue in any discussion of cyberterror and cybercrime: attribution.[98] Despite investigations by a number of computer security researchers, it is unclear who created this code. The complex nature

of Stuxnet suggests that multiple highly skilled programmers developed the code, most likely in the employ of a nation-state or military entity.[99] No nation or entity however, has come forward to claim responsibility for the program. The lack of attribution here is common among other kinds of crime—both physical and online—although terrorists generally seek public attention through their attacks. Skilled offenders can carefully conceal or obfuscate their identity to reduce the likelihood of detection. This problem is compounded in virtual environments due to various tools that can shield an individual's physical location, such as anonymizers and proxy servers.[100] In addition, skilled actors can use compromised computer systems to obfuscate their location and the actual identity of the attacker. For instance, a botnet can be used to route attack traffic through multiple unsuspecting victim machines across the world.[101] As a consequence, malicious traffic may appear to come from individual systems in the United States or other countries. In addition, attackers can acquire tools from hacker communities across the globe in an attempt to confound actor attribution. For instance, using tools common to Chinese hackers may add a layer of complexity to the investigation of the origins of an attack.[102]

It is also difficult to truly discern whether an extremist group engaging in cyberattacks is acting independently from a nation-state or criminal entity. The complexity of an attack may give some insight into the skill and knowledge of the attackers, but does not provide any information on their sources for funding or training, or any connections they may have to other groups.[103] In particular, the hacker community engenders a horizontal organizational structure, where individuals are judged based on skill and ability. As a consequence, when groups form they are generally short-lived, have minimal leadership, and are structured based on skills.[104] This is different from the general cell-based structure of traditional terror groups off-line that work through intermediaries.[105] As a consequence, virtual terror attacks can occur more quickly and with fewer trails to identify funding and tool acquisition sources than traditional terror groups.

In addition, the nature of virtual attacks may reduce the likelihood of attribution in general. Terrorists and extremists may claim responsibility after an attack in order to garner attention and demonstrate their power and capability in physical attacks. For instance, suicide bombers often post videos online or distribute pre-recorded messages to the media in order to ensure that their justification for an attack is clearly known.[106] The need for attribution in the course of a cyberattack may not be pivotal until well after the act is completed since initial actions to survey and access a virtual target must be kept silent in order to minimize the likelihood of detection. The final attack or outcome produced from initial intrusions may, however, lead the group to take responsibility in order to garner attention for their cause. Thus, the variation in group ideologies, coupled with the anonymity afforded by virtual environments, make attribution an exceedingly difficult challenge for policy makers and law enforcement to appropriately respond to cyberattacks.

A final concern related to attribution is the increasing incorporation of civilian participants in various cyberattacks. For instance, recent attacks by the group Anonymous and its offshoot LulzSec were facilitated in part by tools that could be downloaded for free by interested parties to perform denial of service attacks.[107] In addition, the group provided information on prospective targets and asked participants to rate who they most wanted to attack, and utilized the web to coordinate attacks. As a consequence, the ability for an extremist group to rapidly recruit and radicalize sympathetic individuals, or employ their technical skills on a temporary

basis without the need for complete indoctrination or membership into their organization, should not be ignored in light of the worldwide spread of the Internet and computer technology.

The continuous and varied threats posed by cyberattacks from cybercriminals, extremist groups, and nation-states require a substantive retooling of U.S. policies toward cyberspace and cybersecurity in general. While the past few presidential administrations established roadmaps to improve the governmental response to cybercrime and prospective attacks,[108] there have been few unclassified policy responses to potential attacks, making it difficult to understand the true posture toward cyberattacks. In July 2011, the Department of Defense released a policy document detailing their view of cyberspace as a protected domain in much the same way as the physical environments of sea, air, and land.[109] The report recognizes that the current defensive measures used to protect critical infrastructure and the defense industrial base against cyberattacks are ineffective and require significant expansion. In addition, the Department of Defense is now placing a specific emphasis on the need for careful responses to theft of data, destructive attacks to degrade network functionality, and denial of service attacks due to the direct threat they pose to the communications capabilities of the nation, and the maintenance of secrecy and intellectual property.[110] In order to reduce the risks posed by malicious actors and attacks, the report calls for improved relationships with private industry in order to develop an improved total government response and an expanded workforce focusing on cybersecurity.[111]

The issue of collaboration between governmental agencies, public and private companies, and law enforcement is critical, but presents one of the greatest challenges to securing cyberspace. Multiple presidential administrations have made similar policy recommendations, though they have generally failed to produce lasting innovations or strategic change due to the difficulty in linking all necessary groups. For instance, a substantive majority of the power plants, telecommunications equipment, and processing facilities that constitute critical infrastructure are owned by private industry using software and hardware from multiple vendors.[112] As a consequence, it is extremely difficult to develop standards that can be readily adopted across industries in order to effectively reduce the risk of cyberattacks. The creation of initiatives like the Department of Homeland Security's Control Systems Security Program helps to identify general vulnerabilities and improve security standards across all vendors and owners, though their true impact is hard to assess in light of the proprietary nature of private industry practices.[113]

In much the same way, there is a need to more clearly integrate state and local law enforcement agencies into the response to cyberterror attacks. There has been a marked increase in funding for training and equipment to prepare local responders to handle physical terror incidents since 9/11. The same attention has not been given to cyberattacks due to the jurisdictional dynamics that arise in inter-state or international offenses.[114] This perception may, however, unnecessarily diminish the response capability of local law enforcement and hinder investigations which may otherwise reduce some forms of online extremism. In particular, domestic terror groups often emerge as a direct result of conditions within a given region or locale, though they may communicate and share information with others through online networks. Thus, there must be an increase in the training and investigative tools available to state and local police agencies to improve their overall ability to investigate cyberterror incidents and generally improve cybersecurity practices.

Policymakers must also give greater consideration to the integration of individual citizens into the defense of cyberspace. The average computer user can pose a substantive threat to the larger security of private industry and government targets because of their potential to mismanage technological resources or be used as a launch point by attackers. Individuals who do not regularly update their computer software or utilize anti-virus and other security tools face an increased risk of compromise from criminal or extremist groups.[115] Those who engage in media or software piracy or view pornography are also susceptible to attacks since malware is often spread through these vectors.[116] Thus, individuals who act without regard for ethical behavior online or utilize minimal standards for computer security present a substantive opportunity for attackers to gain a foothold into larger networks.

As a consequence, hardening end users from all manner of attacks may greatly improve the total security of the nations' computer systems. This is a substantive challenge given the variations in end users' skill with technology and overall recognition of basic security strategies. Multiple strategies must be employed to effectively target individuals regardless of age, technological skill, or access to technology. National programs that promote awareness of computer security issues, such as October's National Cybersecurity Awareness Month, are useful in communicating the problem of cybercrime and harm to a wide audience.[117] Targeted programs are also necessary at all phases of the educational system to ensure that youth are exposed to proper online conduct and computer security principles from an early age.[118] Adult education programs must also be employed in order to ensure that users are frequently reminded of their role in securing their system and various techniques they can employ to reduce their vulnerability to compromise. For instance, Internet Service Providers could communicate these messages to their customers via e-mail and during login periods in order to constantly expose users to computer security issues. In turn, these measures may help to reduce the overall efficacy of attacks by both extremists and criminal entities against individuals and government targets alike.

Finally, it is critical that national policies toward cyberspace develop in tandem with—and to the extent possible, in advance of—prospective strategies employed by cyberattackers. In fact, there is a need for strategic policy initiatives that carefully consider global variations in law enforcement and governmental policies toward cyberattacks. Most developed nations have laws against certain forms of cybercrime,[119] though there are substantive variations in the ways that they may deal with criminal actors. For instance, there is some evidence that Russian and Chinese law enforcement agencies investigate those individuals who target systems within their national borders.[120] Meanwhile, individuals who attack foreign civilian, business, or government entities may be ignored or under-investigated, creating a sort of tacit approval for certain types of cyberattack. As a consequence, there is a need for clearly defined national polices related to threats from cybercriminals, extremists, and nation-states in order to better protect and defend U.S. critical infrastructure.

In addition to policy responses, there is a clear need for research from both the technical and social sciences in order to better understand the tactical and strategic practices of extremist and terror groups online. For instance, social science research utilizing web forums, blogs, and other online data sources can provide a substantive understanding of the activities of terrorist and extremist groups in their own words.[121] Such data sources can be developed with minimal interaction or penetration into these communities, reducing the risk of researcher contamination or harm.[122] Additionally, these data can be used for both qualitative and quantitative analyses

to provide significant insights into the changing dynamics of extremist communities on both the left and right.

Online data sources can also be used to identify the ways that extremist groups are adapting tools and tactics from the hacker community in order to engage in attacks against critical infrastructure and other targets. For example, investigations of the market for malicious software and stolen data across the globe can be useful to identify prospective trends in attack tools and vectors that may be used by an extremist group.[123] Evidence suggests that an Al-Qaeda cell used credit card numbers purchased from an online data market to obtain web hosting services, phones, and engage in fraudulent charges.[124] Thus, explorations of the activities of cybercriminals can be used to expand our understanding of how extremists may utilize these resources. Combining this research with technical analyses of cyberattacks in general can help to better understand the dynamics of the current and future cyber threat worldwide.

Finally, there is a need to identify the behavioral and attitudinal factors that affect participation in politically motivated cyberattacks. The increasing incorporation of citizens into attacks against government targets online may reflect a difference in the nature of extremism on and off-line. For instance, radicalization may not be necessary in order to lead individuals to engage in attacks against targets online since they do not face the same risk of detection or loss of life in support of a cause as in real-world attacks. Instead, they may only need to share a certain outlook on a social or political issue, or hold antagonistic views against a target group. Research utilizing demographically diverse samples can help to determine the influence of nationalism, political beliefs, technological skills, and ethnic antagonism on individual willingness to engage in cyberterror attacks. In turn, we may better understand the relationship between extremist behaviors on- and off-line.

Notes

1. Steven Furnell, *Cybercrime: Vandalizing the Information Society* (Boston: Addison-Wesley, 2002); David S. Wall, "Cybercrimes and the Internet," in *Crime and the Internet*, ed. David S. Wall (New York: Routledge, 2001), 1–17.

2. Heather DiMarco, "The Electronic Cloak: Secret Sexual Deviance in Cybersociety," in *Dot.cons: Crime, Deviance, and Identity on the Internet*, ed. Yvonne Jewkes (Portland, OR: Willan Publishing), 53–67.

3. Jake Brodscky and Robert Radvanovsky, "Control Systems Security," in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, ed. Thomas J. Holt and Bernadette Schell (Hershey, PA: IGI-Global, 2011), 187–204; Dorothy E. Denning, "Cyber-conflict as an Emergent Social Problem," in *Corporate Hacking and Technology-Driven Crime* (see previous), 170–186; Thomas J. Holt, "Subcultural Evolution? Examining the Influence of On- and Off-line Experiences on Deviant Subcultures," *Deviant Behavior* 28 (2007): 171-198.

4. Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2008); Dorothy E. Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," in *Networks and Netwars: The Future of Terror, Crime, and Militancy*, ed. John Arquilla and David F. Ronfeldt (Santa Monica, CA: RAND, 2001), 239–288; Jerrold M. Post, Keven G. Ruby, and Eric D. Shaw, "From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism," *Terrorism and Political Violence 12* (2000): 97–122.

5. Brenner, *Cyberthreats* (see note 4 above); Bruce Hoffman, *Inside Terrorism,* 2nd ed. (New York: Columbia University Press, 2006); Manuel Soriano, "The Road to Media Jihad: The Propaganda Actions of Al Qaeda in the Islamic Maghreb," *Terrorism and Political Violence 23* (2010): 72–88.

6. Brodscky and Radvanovsky, "Control Systems Security" (see note 3 above); Dorothy Denning, "A View of Cyberterrorism Five Years Later," in *Internet Security: Hacking, Counterhacking, and Society*, ed. Kenneth Himmaed (Sudbury, MA: Jones and Bartlett, 2006), 123–139; Irving Lachow, "Cyber Terrorism: Menace or Myth?," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington DC: National Defense University, 2009), 123–139.

7. Peter N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?," *Social and Legal Studies* 10 (2001): 243–249.

8. David S. Wall, "Catching Cybercriminals: Policing the Internet," *Computers & Technology* 12 (1998): 201–218.

9. See Thomas J. Holt, ed., *Crime On-line: Correlates, Causes, and Context* (Raleigh, NC: Carolina Academic Press, 2010).

10. Furnell, *Cybercrime* (see note 1 above); Wall, "Cybercrimes and the Internet" (see note 1 above).

11. Furnell, *Cybercrime* (see note 1 above); Wall, "Cybercrimes and the Internet" (see note 1 above).

12. Holt, "Subcultural Evolution?" (see note 3 above); Bernadette H. Schell and John L. Dodge, *The Hacking of America: Who's Doing it, Why, and How* (Westport, CT: Quorum Books, 2002).

13. Computer Security Institute, *Computer Crime and Security Survey,* 2010, http://www.cybercrime.gov/FBI2010.pdf.

14. Computer Security Institute, *Computer Crime and Security Survey, 2008*, http://www.cybercrime.gov/FBI2008.pdf.

15. Internet Crime Complaint Center, *IC3 2009 Internet Crime Report*, http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf.

16. IDATE, *Taking Advantage of Peer-to-Peer: What Is at Stake for the Content Industry?* (2009), http://www.idate.fr/an/_qdn/an-03/IF282/index_a.htm.

17. Thomas J. Holt and Adam M. Bossler, "Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization," *Deviant Behavior* 30 (2009): 1–25.

18. Wall, "Cybercrimes and the Internet" (see note 1 above).

19. Niv Ahituv, *Old Threats, New Channels: The Internet as a Tool for Terrorists* (Berlin: NATO Workshop, (2008); Hoffman, *Inside Terrorism* (see note 5 above).

20. Brenner, *Cyberthreats* (see note 4 above).

21. Ibid.

22. Marjie T. Britz, "Terrorism and Technology: Operationalizing Cyberterrorism and Identifying Concepts," in *Crime On-Line: Correlates, Causes, and Context*, ed. Thomas J. Holt (Raleigh, NC: Carolina Academic Press, 2010), 193–220; Hoffman, *Inside Terrorism* (see note 5 above); Gus Martin, *Understanding Terrorism: Challenges, Perspectives and Issues,* 2nd ed. (Thousand Oaks, CA: Sage, 2006); Alex P. Schmid and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, & Literature* (New Brunswick, NJ: Transaction Publishers, 2005).

23. Ibid., Schmid and Jongman, *Political Terrorism*.

24. Ibid.

25. Hoffman, *Inside Terrorism* (see note 5 above).

26. Ibid.

27. Ibid. Denning, "Activism, Hacktivism, and Cyberterror" (see note 4 above).

28. Ibid.

29. Furnell, *Cybercrime* (see note 1 above); Tim Jordan and Paul Taylor, *Hacktivism and Cyberwars: Rebels With a Cause* (New York: Routledge, 2004).

30. Ibid.

31. Alex P. Schmid, "Frameworks for Conceptualising Terrorism," *Terrorism and Political Violence* 16 (2004): 197–221.

32. Stefan H. Leader and Peter Probst, "The Earth Liberation Front and Environmental Terrorism," *Terrorism and Political Violence* 15 (2003): 37–58.

33. Jordan and Taylor, *Hacktivism and Cyberwars* (see note 29 above).

34. Britz, "Terrorism and Technology" (see note 22 above); Dorothy E. Denning, *Cyberterrorism*. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, May 23, 2000, http://www.cs.georgetown.

edu/~denning/infosec/cyberterror.html; Bryan C. Foltz, "Cyberterrorism, Computer Crime, and Reality" *Information Management & Computer Security 12* (2004): 154–166; Mark M. Pollitt, "Cyberterrorism—Fact or Fancy?" *Computer Fraud & Security* 2 (1998): 8–10.

35. Ibid.

36. Pollitt, "Cyberterrorism—Fact or Fancy?" (see note 34 above).

37. Denning, "Cyberconflict" (see note 3 above), p. 178; E. Alshech, "Cyberspace as a Combat Zone: The Phenomenon of Electronic Jihad," *MEMRI Inquiry and Analysis Series* 329 (Washington, DC: The Middle East Media Research Institute, 2007).

38. Foltz, "Cyberterrorism, Computer Crime, and Reality" (see note 34 above).

39. Hollis Stambaugh, David S. Beaupre, David J. Icove, Richard Baker, Wayne Cassady, Wayne P. Williams, *Electronic Crime Needs Assessment For State And Local Law Enforcement* (Washington, DC: National Institute of Justice, 2001).

40. Foltz, "Cyberterrorism, Computer Crime, and Reality" (see note 34 above).

41. Marjie T. Britz, *Computer Forensics and Cybercrime,* 2nd ed. (Upper Saddle River, NJ: Prentice-Hall, 2009).

42. Thomas J. Holt and Heith Copes, "Transferring Subcultural Knowledge Online: Practices and Beliefs of Persistent Digital Pirates," *Deviant Behavior* 31 (2010): 625–654.

43. Gary Bunt, *Islam in the Digital Age: E-jihad, Online Fatwas and Cyber Islamic Environments* (London: Pluto Books, 2003); Lachow, "Cyber Terrorism" (see note 6 above).

44. Ibid.; Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty First Century*, (Philadelphia: University of Pennsylvania Press, 2008).

45. James J. F. Forest, ed., *Influence Warfare: How Terrorists and Governments Struggle to Shape Perceptions in a War of Ideas* (Westport, CT: Praeger, 2009); and James J. F. Forest, "Influence Warfare and Modern Terrorism," *Georgetown Journal of International Affairs* 10, no. 1 (2009): 81–90.

46. Ibid.

47. Tammy Castle, "The Women of Stormfront: An Examination of White Nationalist Discussion Threads on the Internet," *Internet Journal of Criminology* (2011), http://www.internetjournalofcriminology.com/Castle_Chevalier_The_Women_of_Stormfront_An_Examination_of_White_Nationalist_Discussion_Threads.pdf; Stormfront website. www.stormfront.org; Robert W. Taylor, Eric J. Fritsch, John Liederbach, and Thomas J. Holt, *Digital Crime and Digital Terrorism,* 2nd ed. (Upper Saddle River, NJ: Pearson Prentice Hall, 2010).

48. Taylor et al., *Digital Crime and Digital Terrorism* (see note 47 above).

49. See the website http://www.newsaxon.com for details.

50. Gabriel Weimann and Katharina Von Knop, "Applying the Notion of Noise to Countering Online Terrorism," *Studies in Conflict and Terrorism* 23 (2009): 883–902.

51. Britz, "Terrorism and Technology" (see note 22 above); Lachow, "Cyber Terror" (see note 6 above); Sageman, *Leaderless Jihad* (see note 44 above).

52. Vivian Salma, "Ask a Terrorist," *Newsweek,* 19 December 2007, http://www.newsweek.com/2007/12/19/as-a-terrorist.html.

53. See http://www.resistancerecords.com for details.

54. Taylor et al., *Digital Crime and Digital Terror* (see note 47 above).

55. For a description of this and several other terrorist-created video games, see Madeline Gruen, "Innovative Recruitment and Indoctrination Tactics by Extremists: Video Games, Hip Hop, and the World Wide Web," in *The Making of a Terrorist,* ed. James J.F. Forest (Westport, CT: Praeger, 2005).

56. Britz, "Terrorism and Technology" (see note 22 above); Lachow, "Cyber Terror" (see note 6 above); Sageman, *Leaderless Jihad* (see note 44 above).

57. Taylor et al., *Digital Crime and Digital Terrorism* (see note 47 above).

58. Britz, "Terrorism and Technology" (see note 22 above); Max Kilger, "Social Dynamics and the Future of Technology-Driven Crime," in *Corporate Hacking and Technology Driven Crime: Social Dynamics and Implications*, ed.Thomas J. Holt and Bernadette Schell (Hershey PA: IGI-Global, 2010), 205–227.

59. Kilger, "Social Dynamics and the Future of Technology-Driven Crime" (see note 58 above).

60. Paul A. Taylor, *Hackers: Crime in the Digital Sublime* (New York: Routledge, 1999).

61. Gordon R. Meyer, *The Social Organization of the Computer Underground* (Master's thesis, Northern Illinois University, 1989).
62. Ibid.
63. Taylor, *Hackers* (see note 60 above).
64. Ibid.
65. Taylor et al., *Digital Crime and Digital Terrorism* (see note 47 above).
66. Bill Chu, Thomas J. Holt, and Gail Joon Ahn, *Examining the Creation, Distribution, and Function of Malware On-Line* (Washington, DC, National Institute of Justice, 2010), http://www.ncjrs.gov./pdffiles1/nij/grants/230112.pdf.
67. Ibid.
68. Ibid.
69. Thomas J. Holt, "Examining the Origins of Malware," Paper presented at the Department of Defense Cyber Crime Conference, Saint Louis, MO, January 2008.
70. Ibid.; Thomas J. Holt, Joshua B. Soles, and Ludmilla Leslie, "Characterizing Malware Writers and Computer Attackers in Their Own Words," Paper presented at the International Conference on Information Warfare and Security, Peter Kiewit Institute, University of Nebraska Omaha, April 2008.
71. Thomas J. Holt, "The Attack Dynamics of Political and Religiously Motivated Hackers," in *Cyber Infrastructure Protection*, ed. Tarek Saadawi and Louis Jordan (New York: Strategic Studies Institute, 2009), 161–182.
72. Ibid.
73. Denning, "Cyberconflict as an Emergent Social Phenomenon" (see note 3 above).
74. Ibid.; Taylor, *Hackers* (see note 60 above).
75. Ibid.
76. Denning, "Cyberconflict as an Emergent Social Phenomenon" (see note 3 above).
77. Sean Paul Correll, "An Interview with Anonymous," PandaLabs Blog, 29 September, 2010, http://pandalabs.pandasecurity.com/an-interview-with-anonymous/.
78. Taylor et al., *Digital Crime and Digital Terrorism* (see note 47 above); Denning, "Cyberconflict as an Emergent Social Phenomenon" (see note 3 above).
79. Ibid.; Kilger, "Social Dynamics and the Future of Technology-Driven Crime" (see note 58 above).
80. Denning, "Cyberconflict as an Emergent Social Phenomenon" (see note 3 above).
81. Holt, "The Attack Dynamics of Political and Religiously Motivated Hackers" (see note 71 above); Michael Ward, "Anti-Cartoon Protests Go Online," *BBC News*, 8 February 8, 2006, http://news.bbc.co.uk/2/hi/technology/4691518.stm.
82. Ibid.
83. Denning, "Cyber Conflict as an Emergent Social Phenomenon" (see note 3 above).
84. Dorothy E. Denning, *Information Warfare and Security* (Reading, MA: Addison-Wesley, 1999).
85. Ryan Naraine and Dancho Danchev, "Zero Day: Coordinated Russia vs Georgia cyber attack in progress," *ZDNet*, 11 August 2008, http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670.
86. Taylor et al., *Digital Crime and Digital Terrorism* (see note 47 above).
87. Britz, "Terrorism and Technology" (see note 22 above); Denning, "Cyber Conflict as an Emergent Social Phenomenon" (see note 3 above); Lachow, "Cyber Terror" (see note 6 above).
88. Ibid.
89. Ibid.
90. See Paul K. Kerr, John Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Washington, DC: Congressional Research Service, 2010).
91. Mark Clayton, "Stuxnet Malware is 'Weapon' out to Destroy . . . Iran's Bushehr Nuclear Plant," *Christian Science Monitor*, 21 September, 2010, http://www.csmonitor.com/USA/2010/0921/Stuxnet-malware-is-weapon-out-to-destroy-Iran-s-Bushehr-nuclear-plant.
92. Brodscky and Radvanovsky, "Control Systems Security" (see note 3 above); Denning, "A View of Cyberterrorism Five Years Later" (see note 6 above).
93. Clayton, "Stuxnet Malware is 'Weapon' out to Destroy . . . Iran's Bushehr Nuclear Plant" (see note 91 above).
94. Ibid.

95. Brodscky and Radvanovsky, "Control Systems Security" (see note 3 above); Kilger, "Social Dynamics and the Future of Technology-Driven Crime" (see note 58 above).

96. Clayton, "Stuxnet Malware is 'Weapon' out to Destroy . . . Iran's Bushehr Nuclear Plant" (see note 91 above).

97. Kim Zetter, "DHS Fears a Modified Stuxnet Could Attack US Infrastructure," *Wired Threat Level*, 20 July, 2011, http://www.wired.com/threatlevel/2011/07/dhs-fears-stuxnet-attacks/.

98. Brenner, *Cyberthreats* (see note 4 above).

99. Clayton, "Stuxnet Malware is 'Weapon' out to Destroy . . . Iran's Bushehr Nuclear Plant" (see note 91 above); Kerr et al., *The Stuxnet Computer Worm* (see note 90 above).

100. Brenner, *Cyberthreats* (see note 4 above); Chu et al., *Examining the Creation, Distribution, and Function of Malware On-line* (see note 66 above); Kilger, "Social Dynamics and the Future of Technology-Driven Crime" (see note 58 above).

101. Chu et al., *Examining the Creation, Distribution, and Function of Malware On-line* (see note 66 above); Taylor et al., *Digital Crime and Digital Terror* (see note 47 above).

102. Holt, "Examining the Origins of Malware" (see note 69 above).

103. Brenner, *Cyberthreats* (see note 4 above); Kilger, "Social Dynamics and the Future of Technology-Driven Crime" (see note 58 above).

104. Holt et al., "Characterizing Malware Writers and Computer Attackers in Their Own Words" (see note 70 above).

105. Britz, "Terrorism and Technology" (see note 22 above).

106. Brenner, *Cyberthreats* (see note 4 above).

107. Correll, "An Interview with Anonymous" (see note 77 above); Kevin Poulsen, "In 'Anonymous' Raids, Feds Work From List of Top 1,000 Protesters," *Wired*, 26 July, 2011, http://www.wired.com/threatlevel/2011/07/op_payback/.

108. Brenner, *Cyberthreats* (see note 4 above); Taylor et al., *Digital Crime and Digital Terror* (see note 47 above).

109. Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*, (Washington DC: Department of Defense, 2011), http://www.defense.gov/news/d20110714cyber.pdf.

110. Ibid.

111. Ibid.

112. Brodscky and Radvanovsky, "Control Systems Security" (see note 3 above); Kilger, "Social Dynamics and the Future of Technology-Driven Crime" (see note 58 above).

113. Ibid.

114. Ibid.

115. Adam M. Bossler and Thomas J. Holt, "On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory," *International Journal of Cyber Criminology* 3 (2010): 400–420; Chu et al., *Examining the Creation, Distribution, and Function of Malware On-line* (see note 66 above).

116. Ibid.

117. Taylor et al., *Digital Crime and Digital Terrorism* (see note 47 above).

118. Bossler and Holt, "On-line Activities, Guardianship, and Malware Infection" (see note 115 above).

119. Brenner, *Cyberthreats* (see note 4 above).

120. Chu et al., *Examining the Creation, Distribution, and Function of Malware On-line* (see note 66 above).

121. Joshua Sinai, "Using the Internet to Uncover Terrorism's Root Causes," in *Influence Warfare,* ed. James J. F. Forest (Westport, CT: Praeger, 2009).

122. Thomas J. Holt, "Exploring Strategies for Qualitative Criminological and Criminal Justice Inquiry Using Online Data," *Journal of Criminal Justice Education*, 21 (2010): 300–321.

123. Chu et al., *Examining the Creation, Distribution, and Function of Malware On-line* (see note 66 above); Thomas J. Holt and Eric Lampke, "Exploring Stolen Data Markets On-line: Products and Market Forces," *Criminal Justice Studies* 23 (2010): 33–50.

124. Brian Krebs, "Terror Webmaster Sentenced in Britain," *Washington Post*, 5 July 2007; Kimberly Kiefer Peretti, "Data Breaches: What the Underground World of "Carding" Reveals," *Santa Clara Computer and High Technology Law Journal* 25 (2009): 375–413.