THE PROBLEM WITH CYBER TERRORISM[1]

Elina Noor

ABSTRACT

The alarm of cyber terrorism has been raised for more than a decade and yet the world has still not witnessed any crippling effects of a so-called "logic bomb" to date. Cyber terrorism holds promise as a cheaper option to physical terrorism and offers the veil of anonymity and maximum destruction to its perpetrator(s). As technical knowledge and expertise advance, cyber attacks continue to rise, and terrorists increasingly demonstrate a keenness to engage in cyberspace, the barriers to cyber terror will eventually be significantly lowered. While the risk of cyber terrorism is not at present imminent, its execution in conjunction with a well-planned physical act of terror is a serious potential threat that should not be ignored.

Keywords: *Cyber terrorism; terrorism; critical infrastructure*

Introduction

As rush hour hits another weekday in City X and businesses begin trading, a worm commanded to infect and incapacitate the electricity grid of City X is released from halfway across the world. Blackout. Minutes later, as the city reels in puzzlement and back-up generators are fired up, five explosions simultaneously rock the financial district, a major hospital, a mass transit station, a cell phone tower, and a five-star hotel. Communication lines stutter and emergency services scramble. Carnage and chaos ensue.

It would be tempting to dismiss the above scenario as hyperbole. There have, after all, been no deaths directly caused by terrorists manipulating computer networks nor have there, so far, been any critical infrastructure meltdowns paralysing whole communities due to malware infection. Yet, as the 2010 Stuxnet target-specific worm and the 2000

[1] The views expressed herein are personal to the author.

[2] Stuxnet infects Windows systems in searching for industrial control systems. It has targeted critical infrastructure, notably infecting computers at the Bushehr power plant in Iran. Stuxnet's infection rate has been highest in Iran at 58.8 per cent followed by 18.2 per cent in Indonesia, 8.3 per cent in India, 2.6 per cent in Azerbaijan and 1.6 per cent in the United States.

hacking of a waste management control system in Australia have shown,[3] a pseudo-apocalyptic consequence of a cyber attack may not completely be out of the question in the near future.

This article will consider the prospect of cyber terrorism in light of its many ambiguities. It will firstly parse the various references to the term "cyber terrorism" and argue that shorthand equations of it to terrorists' use of computers or networks to plan, organise, and coordinate physical acts of terrorism are misleading and erroneous. Secondly, this article will discuss why cyber terrorism would even be an option, specifically considering cost, anonymity, and target and effect maximisation as influencing factors of decision. Thirdly, this article will assess the charge that cyber terrorism is an exaggerated threat, particularly given security measures surrounding Supervisory Control and Data Acquisition Systems (SCADA) systems. Fourthly, this article will discuss the likely perpetrators of cyber terrorism before concluding with a brief outlook of the threat of cyber terrorism in the future. This article will not consider preventive measures against cyber terrorism or engage in a discussion of legal measures that are or should be available to combat a threat and/or actual act of cyber terrorism.

Defining the Boundaries of Cyber Terrorism

Given the lack of a universal accord on the definition of terrorism despite the decades, perhaps even centuries, of recorded acts of terrorism, it is unsurprising that there has been just as much irresolution surrounding cyber terrorism as a newer sub-phenomenon. If terrorism can generally be accepted to be the means through which the use of force is carried out to intimidate or cause fear and to elicit a political or ideological change, then cyber terrorism marks the convergence of cyber space and terrorism (Denning, 2000). An actual use of force executed through and against information or computer systems and networks resulting in fear, violence and physical destruction of property or persons to coerce a political or ideological change would therefore qualify as an act of cyber terrorism.

Cyber terrorism should not be confused with the use of the Internet by parties communicating, coordinating, or plotting physical acts of terrorism to bring about political or ideological change. It is not networked groups of individuals transferring funds across borders to

[3] In 2000, Vitek Boden, hacked into the computerised waste management system of Maroochy Shire Council, Queensland, Australia releasing millions of litres of raw sewage into local parks, rivers and the grounds of a hotel. At the time, he was an employee of the company which had installed the system and had had his job application to the Council rejected.

finance physical acts of terrorism. Nor is it the spread of propaganda to threaten, encourage or launch mass destruction in the name of an ideological belief.

In the same manner that chemical, biological, radiological, and nuclear (CBRN) weapons provide a tactical means of delivering terror, cyber space affords the terrorist yet another delivery system for real world devastation. Cyber terrorism offers the projection of an unparalleled dimension in which the virtual and physical realms can collide in damaging proportions and through which no cross-border laws have yet adequately transcend. It represents an extension of the *tactic* of terrorism driven to manipulate change through the threat or use of violence. It is precisely because of this that cyber terrorism is to be treated as a crime, not an act of war, and like terrorism in general is to be combated through legal rather than military means.

Crucially, cyber terrorism distinguishes itself from a "regular" (cyber) crime in that it is not motivated by a desire to effect political or ideological change. Thus a disgruntled former employee's disabling of a company's alert network to incapacitate response in an emergency as happened to Chevron in 1992, while serious, inconvenient, and criminal would not count as cyber terrorism for lack of a political or ideological motive. On the other hand, the same act would be considered cyber terrorism if done by an individual with the criminal subjective element – or, *mens rea* – of causing widespread fear, panic and possibly destruction to pressure a change in a system of government.

The Appeal of Cyber Terrorism

The value of cyber terrorism lies in its premise that it is relatively cheap; that it offers the perpetrator(s) anonymity; and that with a certain level of skill, high value targets could be crashed, affecting large masses of people and generating a substantial amount of publicity. Each of these claims will be assessed.

Cost. In 1999, a virus named for a Miami stripper, Melissa, exploited the power of social engineering and mass mailed itself to the first 50 addresses in a user's Microsoft Outlook address book. Although more of an inconvenience rather than a security threat, it resulted in more than $80 million in damage to North American businesses and provided the blueprint for subsequent mass email worms including The Love Bug, Anna Kournikova, and MyDoom (U.S. Department of Justice, 2002). A year later, a similar self-propagating but far more destructive virus, ILOVEYOU, shut down email for millions of computers worldwide in a

matter of hours and cost businesses between $6 and $10 billion in estimated damages. This eclipsed the $12.1 billion total cost for all computer viruses in 1999 (Kirschner, 2000).

While huge financial damages were amassed from both these viruses, their scripts were written by lone individuals for a negligible amount. The ILOVEYOU virus, for example, bore distinct similarities to its author's rejected proposed college thesis (BBC News, 2000) and did not require any structured fund-raising for its creation or release. In fact, individuals motivated by either one or a combination of ego, thrill, revenge, greed have long been hacking systems at relatively minimal financial cost. Contrast, for example, the cost of setting up and maintaining an Internet connection to the alleged US$74,000 transferred for the purchase of three tonnes of explosives used in the 2002 Bali bombing (Fielding, Campbell, and Rufford, 2002). Or the roughly US$100,000 spent on purchasing the rifles, electronic devices, and ammunition used by the Mumbai attackers in 2008, excluding payments made to each of the 10 terrorists (Nanjappa, 2008). Or the estimated US$400,000 to US$500,000 it took to execute the attacks against the World Trade Centre on 11 September 2001 as well as the expenses associated with the network of support it took to plan, train, and launch the attacks (National Commission on Terrorist Attacks upon the United States, 2004).

Remote execution of a cyber attack renders it far cheaper than the travel and preparatory expenses inevitably incurred with physical acts of terror. With increasing nodes of Internet penetration through WiFi and mobile signals as well as faster connection speeds, cyber space also provides the flexibility and mobility in deployment of attacks or perpetrators that physical terrorism cannot necessarily compete with. Additionally, the proliferation of malware-and botnets-for-sale, and hacker-for-hire rings as burgeoning businesses on the Internet as well as the many hacking tools available for free or cheap download make cyber attacks an increasingly cost-effective option for contemplation. For $150, neophytes can be self-taught in hacking through an online purchase of various hacking modules. Tutors are also available via instant messaging and interactive tutorials (Lee and Hornby, 2010).

Yet the estimated $3 million building cost of the target-specific Stuxnet worm shows that not all cyber attacks come cheap (Hesseldahl, 2010; Schneier, 2010). The sophistication and size of Stuxnet and Conficker, which still remain active and infectious, lend belief that these malware were designed and tested for several months by a team of highly skilled programmers able to mask the worms' origin and as in the case of Conficker, trigger variant spawns to continually confound experts. As malware becomes increasingly complex, deceptive, and therefore costly,

the perception of cyber terrorism being a cheaper option than physical terrorism will need to be re-evaluated from time to time. As the case of the "underwear bomber" who, last year, tried to blow up an international flight to Detroit on Christmas Day demonstrates, the trend may be for terrorists to optimise maximum impact through smaller – and cheaper – scales of physical attacks.

Anonymity. The phenomenal growth of the Internet that saw only 16 million (0.4 per cent) of the world's population connected in 1995 to nearly 2 billion (28.8 per cent) connected in the third quarter of 2010 coupled with gaping legal lacunae within and across jurisdictions to regulate conduct on the Internet have led to criticisms of the Internet as the wild, wild web (Internet World Stats, 2010; ITU, 2010).

The protection of privacy – and by implication, anonymity – on the Internet has its champions. However, unlike in the real world where geographical borders are monitored and enforced through customs, immigration, and patrols, the virtual world has no comparable equivalent, thus, making identification, verification, and attribution a challenge. That difficulty is only compounded by the sheer size and traffic of information that flows through the networks. As with any double-edged sword, anonymity on the Internet provides a user not only the luxury – but some would say, the right – to free speech and a measure of privacy but it also facilitates service disruption, site vandalism, and data theft, among others and masks the offender(s) by various means available, such as by hiding or changing an IP address. For the publicity-shy terrorist, Internet anonymity provides a perfect cover for identity without masking the results of a cyber terror attack.

Target and effect maximisation. In October 2010, Symantec released a report of its survey of 1,580 private businesses in six critical infrastructure industries from 15 countries worldwide. The six industries were energy, banking and finance, communications, information technology, healthcare, and emergency services. More than half (53 per cent) of businesses surveyed said they "suspected or were pretty sure they had experienced an attack waged with a specific political goal in mind" with three in five respondents convinced that the attacks were "somewhat to extremely effective" (Symantec, 2010). Banking and finance topped the list and expected to continue being hit by politically-minded attacks in the future. Energy industry respondents reported they were best prepared for such attacks.

This accords with a January 2010 McAfee and the Centre for Strategic and International Studies report identifying the oil and gas sector as a priority target for cyber attacks. The sector reported more Ghostnet-

style infiltration,[4] more large-scale DDOS attacks, more extortion attacks, and more theft of service attacks than any other sector. Attackers were also more likely to target the sector's SCADA system than for financial information in other sectors (Baker & Waterman, 2010).

The vulnerability of critical infrastructure industries as a collective target lies in the industries' function as public sector service providers and the backbone of a nation's economy. Unlike military installations, they straddle the public and the private spheres making them especially valuable, strategic targets. As shown in the opening example, assuming inadequate back-up measures, a blow on the energy or emergency services industry by disabling its network could have the very real, chilling, and public effect of bringing a nation to its knees. A mass and subtly-executed shutdown of critical infrastructure would provide optimum visibility, propaganda, and glory at minimum cost to the terrorist and maximum cost to society.

An exaggerated threat?

By its very nature, terrorism provokes anxiety, fear, desperation, maybe even paranoia. Technology, because of its novelty and dynamism, inspires a milder sense of incertitude, apprehension, maybe even concern about its reach to those unfamiliar with it. As cyber terrorism merges these two formidable spheres, the charge is that it creates an alarmist policy reaction because people – in this case, policy-makers and government officials – fear what they do not understand (Green, 2002).

While sceptics maintain that cyber terrorism's barriers to entry remain ridiculously high,[5] the constant dread that looms large in the minds of those concerned is the vulnerability – real or perceived – of key installations such as nuclear power plants, military and intelligence infrastructure, utility grids, as well as air traffic control and other SCADA systems. In theory and to a large extent, in practice, many of these systems

[4] Ghostnet refers to a 10-month investigation by the Information Warfare Monitor into alleged Chinese cyber espionage against Tibetan institutions. The study revealed a network of over 1,295 infected hosts in 103 countries. For more, see Information Warfare Monitor. (2009, March 29). Tracking *Ghostnet*: Investigating a Cyber Espionage Network. JR02-2009. Retrieved from http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

[5] For example, a 2002 article debunking the cyber terror threat to water utilities, in general, and the Massachusetts Water Resource Authority (MWRA), in particular, asserts that three hacks into very narrow access points would need to be committed before the MWRA's IT and SCADA systems could be corrupted and threatened (Berinato, 2002).

especially the most sensitive ones are air-gapped. This means they are secured and kept separate from other local networks or the Internet and operate on specially-designed software for their unique purposes. The implied conclusion from air-gapping is that these systems are safe from, and invincible to, computer network attacks. In the case of the US nuclear weapons system, extra layers of security such as "permissive action links" or codes are required to be separately inputted by the president (Green, 2002).

In truth, however, air-gapping can be breached through numerous uncontrolled interconnects, the use of mass storage devices, or roaming notebooks. In 2006, Internet Security Systems researchers detailed how back-end networks controlling power, oil and gas, manufacturing, water, and transportation systems have "no security". They found that in most cases, the systems themselves did not support authentication, encryption, or even the most basic validation protocols. The few systems that did have these protocols usually ran with security features disabled. Thus, all that was required to gain access to controlled networks that appeared to be secure were "average" hacking skills (Maynor and Graham, 2006).

Moreover, air-gapping SCADA systems do not always make cost-effective business sense particularly in profit-generating critical infrastructure industries. To air-gap SCADA systems would foster huge inefficiencies for a supply chain that depends on a seamless flow of information. It would also prove costly due to the development of specialised software it would require. Furthermore, data generated through SCADA systems can provide invaluable information for real-time business analysis and be fed to other systems outside the SCADA realm (Schneier, 2010).

It also bears reminder that while air-gapping protects against leaked data, it is not impervious to infection. System updates that are performed using CDs or USB sticks may be a vector of infection on even air-gapped SCADA systems. Stuxnet relied on a USB mass storage device as just such a vector.

It is worth pausing here to consider (i) the advanced nature of Stuxnet and (ii) how, despite its complexity, it overcame perimeter defences through a simple and single USB stick on a host computer in Iran before going on to infect approximately 45,000 computers around the world. Stuxnet takes advantage of four zero-day vulnerabilities. This, according to experts, is itself remarkable given that threat using one zero-day vulnerability is already "quite an event" (O'Murchu, 2010). Stuxnet uses two different stolen but valid digital certificates, contains dozens of encrypted code blocks, hides itself, uses peer-to-peer capabilities for remote command and control, and alters its behaviour based on the

systems it infects (Sverdlove, 2010). Stuxnet was written using multiple languages, is notable for its complexity *and* stability, and utilises detailed knowledge of anti-virus technologies and their vulnerabilities (Kaplan, 2010). Significantly, unlike Melissa, ILOVEYOU, or Conficker, Stuxnet specifically targets industrial control systems.

For all its impressive attributes, however, Stuxnet's initial infection was delivered directly to an end point simply by plugging in a compromised USB device. It was also the end point of a US military laptop at a Middle East base that proved to be the Department of Defense's Achilles' heel in a 2008 malware attack delivered by an infected USB stick. That infection which spread through US Central Command's classified and unclassified network systems took 14 months to clean up under Operation Buckshot Yankee (Shachtman, 2010; Lynn III, 2010).

Perpetrator(s)

If, therefore, even secure and air-gapped networks can be penetrated for infection as a preliminary step towards cyber terrorism, the question arises as to the type(s) of perpetrators such an act would draw. In 1999, the Centre for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California analysed the "demand" for cyber terror capability by terrorist groups based on their goals, ideology, and psychology. The study considered five terrorist group types: religious, New Age, ethno-nationalist separatist, revolutionary, and far-right extremist and concluded that of the five, only religious groups were likely to seek the most damaging capability level consistent with their propensity for indiscriminate violence. The most immediate threat, however, came from New Age or single-issue terrorist groups although they were most likely to accept disruption as a substitute for destruction. Both groups had, by far, the best match in desire, ideology and environment to support a near term "advanced-structured" attack threat. In other words, they possessed the capability to conduct sophisticated attacks against multiple systems or networks (Arquilla & Tucker, 1999).

The 1999 report is for its detailed framework on cyber terrorism. Developments since then – and instructive particularly since the 11 September attacks – have appeared to confirm the study's conclusion regarding religious groups. In January 2002, the U.S. National Infrastructure Protection System (NIPC) reported interest by al-Qaeda members in SCADA systems, specifically seeking information on "water supply and wastewater management practices in the U.S. and abroad" (NIPC, 2002). A few months later, Sheikh Omar Bakri Muhammad,

radical cleric and founder of the now disbanded London-based group Jama'at Al-Muhajirun, warned of "attacks on the stock market" in "a matter of time", stating that Osama bin Laden himself had propagated the use of technology to "destroy the economy of the capitalist states" (Verton, 2002).

In 2000, the Centre followed up in a second report by suggesting that terrorists have not yet integrated IT into their overall strategy and that the psychological and organisational ill-conformity of hackers to cyber terrorism make an alliance with terrorists unlikely (Weimann, 2004; Conway, 2003). However, two developments call into question the strict veracity of this a decade on. First, since March 2000 there has been the very real possibility of terrorists infiltrating government systems as evidenced by Aum Shirinkyo's supply of software to Japan's Metropolitan Police Department's system to track classified police vehicle data. This, coupled with documented interest and agitation for cyber attacks against several Western governments by groups or individuals affiliated with al-Qaeda over the years, hint at a more comprehensive strategy including the use of IT of terror by these groups (Denning, 2007). Second, the proposition assumes that terrorists are non-state actors without the financial wherewithal of governments. Finally, while experts are doubtful of the rise of an unholy alliance between professional e-mercenaries and terrorists because of the closed nature distinctive of many modern terrorist groups, the possibility is not altogether to be precluded particularly if there is a convergence of interests and timing. In 2002, the US Central Intelligence Agency, in fact, revised its assessment of al-Qaeda's interest in cyber terrorism and asserted that the group had contemplated the use of hackers for hire to accelerate its capabilities acquisition. This contrasted its judgment of the group only a year earlier as posing "only a limited cyber-threat" (Gellman, 2002).

Conclusion: Future trends

Currently, while the threat of cyber terrorism is still secondary to that of physical terrorism, it is real and extant. It holds specific appeal if executed ancillary to, and in combination with, physical resources in order to extract maximum amplification of a devastating one-two blow. And while a city-wide blackout may not be as visually searing as body parts exploding into pieces of blood and gore, the uptrend in actual cyber attacks suggests that the scale and complexity of the digital option may only escalate. The threat landscape, for example, evinces significant growth in both the volume and sophistication of cyber crime attacks, with malicious

code appearing more rampant than ever.[6]

Notwithstanding its outstanding conceptual ambiguities, cyber terrorism as a not-too-distant possibility should be taken seriously. It is submitted that as terrorists bide their time to build, advance, and improve their capabilities, the prospect of a cyber terror attack also lies in wait. It would seem folly to deny, dismiss, or ignore it as societies become increasingly networked and whole economies and nations grow more reliant on technology. To do so would only invite regret.

References

____. (2010, October 19). ITU estimates two billion people online by end 2010. *ITU Press Release.* Retrieved from http://www.itu.int/net/pressoffice/press_releases/2010/39.aspx.

____. (2010, October). Symantec 2010 Critical Infrastructure Protection Study: Global Results. Symantec. Retrieved from http://www.symantec.com/content/en/us/about/presskits/Symantec_2010_CIP_Study_Global_Data.pdf.

____. (2010, April). Symantec Global Internet Security Threat Report: Trends for 2009. *XV*. Symantec. Retrieved from http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf.

____. (2010). Internet Growth Statistics. *Internet World Stats*. Retrieved from http://www.internetworldstats.com/emarketing.htm.

____. (2004, August 21). National Commission on Terrorist Attacks upon the United States. *Final Report of the National Commission on Terrorist Attacks upon the United States.*

____. (2000, September 26). Suspected creator of "ILOVEYOU" virus chats online. *CNN online chat transcript*. Retrieved from http://archives.cnn.com/2000/TECH/computing/09/26/guzman.chat/.

[6] The security firm, Symantec, recorded more than 240 million distinct new malicious programmes in 2009 representing a 100 per cent increase from 2008 (Symantec, 2010).

____. (2000, May 10). Love Bug Revenge Theory. *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/science/nature/743082.stm.

____. (2000, May 10). Melissa Virus Creator Jailed. *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/americas/1963371.stm.

____. (1999, December 19). Melissa Virus Creator Pleads Guilty. *BBC News*. Retrieved from http://news.bbc.co.uk/2/hi/science/nature/557605.stm.

_____. (1999, December 9). Creator of "Melissa" Computer Virus Pleads Guilty to State and Federal Charges. *U.S. Department of Justice Press Release*. Retrieved from http://www.justice.gov/criminal/cybercrime/melissa.htm.

Baker, S. and Waterman, S. (2010, January 28). In the Crossfire: Critical Infrastructure in the Age of Cyber War. McAfee and Centre for Strategic and International Studies. Retrieved from http://csis.org/files/attachments/100128_mcafee_CSIS.pdf.

Berinato, S. (2002, March 15). Cybersecurity – The Truth about Cyberterrorism. *CIO*. Retrieved from http://www.cio.com/article/30933/CYBERSECURITY_The_Truth_About_Cyberterrorism.

Conway, M. (2003). Hackers as Terrorists? Why it doesn't Compute. *Computer Fraud and Security,* 12, 10-13.

Denning, D. E. (2007). A View of Cyberterrorism Five Years Later. In Himma, K. (ed.), *Internet Security: Hacking, Counterhacking, and Society*. Boston: Jones and Bartlett.

Denning, D. E. (2000, May 23). *Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives*. Retrieved from http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html.

Fielding, N., Campbell, M., Rufford, N. (2002, October 20). Bin Laden paid for Bali bombing. *The Sunday Times*. Retrieved from http://www.timesonline.co.uk/tol/news/uk/article815606.ece.

Frauenheim, E. (2002, December 12). IDC: Cyberterror and other prophecies. *CNET News*. Retrieved from http://news.cnet.com/2100-1001-977780.html?tag=fd_top.

Gellman, B. (2002, June 27). Cyber-Attacks by Al Qaeda Feared. *The Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html.

Green, J. (2002, November). The Myth of Cyberterrorism. *Washington Monthly*. Retrieved from http://www.washingtonmonthly.com/features/2001/0211.green.html.

Hesseldahl, A. (2010, September 25). Computer Worm May Be Targeting Iranian Nuclear Sites. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2010-09-24/stuxnet-computer-worm-may-be-aimed-at-iran-nuclear-sites-researcher-says.html.

Kaplan, D. (2010, September 14). Microsoft fixes another Stuxnet-related bug, 10 others. *SC Magazine US*. Retrieved from http://www.scmagazineus.com/microsoft-fixes-another-stuxnet-related-bug-10-others/article/178903/.

Kirschner, S.K. (2000, July). I Love You…Not. *Popular Science*. 48-49.

Lee, M., Hornby, L. (2010, January 20). Google attack puts spotlight on China's "red" hackers. *Reuters*. Retrieved from http://www.reuters.com/article/idUSTRE60J20820100120.

Lynn III, William J. (2010, September/October). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

Maynor, D., Graham, R. (2006). Scada Security and Terrorism: We're Not Crying Wolf! Blackhat Federal 2006. Retrieved from http://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

Nanjappa, V. (2008, December 26). Mumbai attacks cost Lashkar Rs 4 crore. *Rediff.com.* Retrieved from http://www.hvk.org/articles/1208/344.html.

National Infrastructure Protection Centre. (2002, January 30). Terrorist Interest in Water Supply and SCADA Systems. *Information Bulletin 01-001.*

O'Murchu, L. (2010, September 14). Stuxnet Using Three Additional Zero-Day Vulnerabilities. *Symantec Connect.* Retrieved from http://www.symantec.com/connect/blogs/stuxnet-using-three-additional-zero-day-vulnerabilities.

Schneier, B. (2010, July 23). Internet worm targets SCADA. *Schneier on Security*. Retrieved from http://www.schneier.com/blog/archives/2010/07/internet_worm_t.html.

Schneier, B. (2010, October 7). Stuxnet. *Schneier on Security*. Retrieved from http://www.schneier.com/blog/archives/2010/10/stuxnet.html.

Shachtman, N. (2010, August 25). Insiders Doubt 2008 Pentagon Hack Was Foreign Spy Attack (Updated). *Wired.* Retrieved from http://www.wired.com/dangerroom/2010/08/insiders-doubt-2008-pentagon-hack-was-foreign-spy-attack/#more-29819#ixzz12ldznbc5.

Sverdlove, H. (2010, October 18). Stuxnet worm shows critical infrastructure attacks no longer just Hollywood hype. *SC Magazine US*. Retrieved from http://www.scmagazineus.com/stuxnet-worm-shows-critical-infrastructure-attacks-no-longer-just-hollywood-hype/article/181212/.

Verton, D. (2002, November 18). Bin Laden Cohort Warns of Cyberattacks. *Computerworld.* Retrieved from http://www.pcworld.com/article/107052/bin_laden_cohort_warns_of_cyberattacks.html.