Journal of Universal Computer Science, vol. 15, no. 12 (2009), 2373-2386
submitted: 15/12/08, accepted: 25/6/09, appeared: 28/6/09 © *J.UCS*

Next Generation of Terrorism: Ubiquitous Cyber Terrorism with the Accumulation of all Intangible Fears

Hai-Cheng Chu
(Department of Information Management / International Business Tunghai University, Taichung, Taiwan, R.O.C.
hcchu@thu.edu.tw)

Der-Jiunn Deng
(Department of Computer Science and Information Engineering National Changhua University of Education, Changhua, Taiwan, R.O.C.
djdeng@cc.ncue.edu.tw)

Han-Chieh Chao
(Institute of Computer Science & Information Engineering, and Department of Electronic Engineering National Ilan University, I-Lan, Taiwan, R.O.C.
Department of Electrical Engineering National Dong Hwa University, Hualien Taiwan, R.O.C.
hcc@niu.edu.tw)

Yueh-Min Huang
(Department of Engineering Science National Cheng Kung University, Tainan Taiwan, R.O.C.
huang@mail.ncku.edu.tw)

Abstract: It is an urgent, imminent and present danger that we have to focus on the traditional terrorists, who are transforming ICT into the modern attacking tools that can devastate the metropolitan areas with the deconstruction of critical infrastructures via the computer network using state-of-the-art hacking and cracking technologies. The cyber terrorists could inflict catastrophic loss or damage on civilians, corporations or the governments physically thousands of miles away and accomplish severe death polls than the traditional one. The government in the public sector or the private critical infrastructure administrators should not underestimate these potential cyber attacks. In this paper, we presented the cyber terrorism, the next generation of terrorism, to be a forthcoming and unavoidable threat to the global community as well as providing a potential rational cyber terrorist scenario, which could be the global cyber terrorism phenomena. This paper explicitly demonstrates the feasibility of launching cyber attacks toward critical infrastructures that might cause severe casualties.

Key Words: Cyber Terrorism; Hacktivism; Internet Vulnerability; Critical Infrastructure; Malicious Code; Process Control System (PCS)

Category: J.0

1 Introduction

Cyber terrorism becomes the new research topic in the past decades due to the convergence of computing power and communication functionality. Cyber terrorism is the use of computer network tools to harm or shut down critical infrastructures such as energy, transportation, and government operations [Weimann, 2005; Denning, 2000]. Traditionally, terrorists or extremists launched devastating attacks in a metropolitan area of a country with deadly explosive materials. Nowadays, they are capable of executing traditional terrorist behaviors via state-of-the-art Information Communication Technology (ICT), which changes the way we live and provides unprecedented opportunities for cyber crimes that we were not able to foresee two decades ago [Grabosky, 2007; Levi, 2008].

In other words, the cyber attack could inflict catastrophic loss or damage on civilians, corporations or the governments by just a keyboard punch in the public café and the cyber terrorists are actually and physically thousands of miles away. Critical infrastructure systems support our everyday lives ranging from nuclear power plants to water-treatment stations, which support the fundamental functionalities for government and industry operations in most cases. Protecting national critical infrastructure assets from cyber attack is an extraordinary challenge and it is a hotly debated issue.

Highly educated extremists are able to initiate deadly demolition on the other side of the earth with sophisticated ICT knowledge via destruction of the certain critical infrastructure like the malfunction of nuclear plants. From voluminous researches indicate that cyber terrorism is a clear and present danger with the sum of all fears to all the people worldwide [Stohl, 2006; Grabosky, 2004]. In the meanwhile, some terrorists or extremists believe that the Internet is a handy tool to influence foreign policies and it can be used as an instant messaging platform to connect all organizations that have the same belief regarding a certain holy religion. Hacktivists have become exploiters of the Internet beyond routine communication operations. Basically, the cyber terrorists are obviously different from the computer hooligan, swindler or hackers. The ultimate goal of cyber terrorists' tactics is to maximize the dangerous consequences and public resonance and create a terrible atmosphere of the terrorism without revealing a specific target to attack via the ubiquitous Internet, which global civilians heavily rely on from leisure activities to office errands in this digital age [Denning, 2004].

Within the United States, the critical infrastructures include approximately 28,600 networked Federal Deposit Insurance Corporation (FDIC) institutions, 2,800 power plants, 2 million miles of pipelines, 104 nuclear power plants, 80,000 dams, 1,600 water-treatment plants and 60,000 chemical plants [Miller, 2005].

Consequently, even a tiny damage or malfunction of a certain critical infrastructure could bring extremely inconvenient to human daily activities or take hundreds of thousands lives away in some cases. Hence, protecting national critical infrastructure assets from cyber attacks is an important challenge for many countries and this potential threatening is around the corner with the clock ticking. These critical infrastructure structure systems are so essential that the devastation of these systems would definitely have a debilitating impact on the national economic security, national public health or safety.

As ICT makes progress on a daily basis, critical infrastructures are vulnerable to modern activists, who are ICT savvy and take advantage of the emerging cracking tools to fulfill their activism or hacktivism. Under such circumstances, cyber terrorism is an imminent challenge to the associate agencies. According to the related researches indicate that thirty hackers with a budget of $10 million U.S. dollar could bring the United States to its knees [Dynes, Goetz & Freeman, 2008]. Hacktivism evolved from a diverse set of groups who are hackers or crackers. Most media is confused with the terms that are being used above. Basically, hackers are those people who have a deep understanding of computer systems and networks and they apply their skills to invent, modify and refine these systems, creatively using computers to achieve a goal that the system was not original intended. However, crackers are those ICT savvy who break into computers in order to achieve destructive ends [Levesque, 2006].

According to U.S. National Security for Homeland Security, the following areas are considered as the targets for critical infrastructure protections: telecommunications and National Information Infrastructure (NII), water treatment, food industry, energy facilities, public health systems, finance and banking services, chemical industry and hazardous material disposal, defense industrial bases, postal and shipping operations, and transportations, etc. In the past two decades, traditional terrorists or extremists were widely utilizing ICT to increase their capability to influence the outside world to fulfill their goals as well as stimulate martyrs to complete the mission as an ultimate honor via sacrificing their lives in the old days.

Due to the dramatic progress of Personal Computer (PC) since 1980, the PC that locates on a desktop at work or home is similar to the one that is being used to operate critical infrastructure components encompassing from oils and gas pipelines, power plants, banking systems to some other large infrastructures that once primarily employed legacy systems with proprietary technologies have adopted commodity computer systems, software and networking technologies, applications, and protocols including internet connectivity [Cassidy, Chavez, Trent & Urrea, 2008].

By the virtue of Internet, it costs relatively nothing to publish messages to a public online forum or website, compared to the considerable costs involved in operating a radio, television or printing a newspaper in the past [Zhou, *et al.*, 2005]. Cyber terrorist organizations are capable of destabilizing many critical infrastructure systems with ICT causing potential extreme angst or anxiety for countless innocent civilians [Chaikin, 2006; Innes, 2004]. In February, 2003, the President of the United State, Mr. Bush, demonstrated the great concern regarding the threat coming from the organized cyber attacks that will cause the debilitating disruption of the critical infrastructure systems that will have significant consequences for public health and safety [Dacey, 2004].

There are numerous activism or terrorism web sites representing Middle Eastern extremist organizations. In reality, those web sites do not have to be web hosting in the Middle Eastern region. On the contrary, it could be geographically independent due to the ubiquity of the Internet. Since "Digital Divide" is a phenomenon in this digital era, the terrorists are taking advantage of this and unfortunately some countries are unwittingly served as the paradises for those computer criminals. Those web sites would not be permanent hosted on a specific server. Actually, those web sites could suddenly emerge right before the dawn with the newest modification of the contents, which utilized dynamic URL (Universal Resource Locator) that will be announced later in some online forums or through the chatting room on the Internet. All of a sudden, those digital trails vanished with little possibility of their traceability. Consequently, it will be extremely hard for the anti-terrorism agencies to exactly pinpoint the web server and proceed counterterrorism operations. Exploitation of irregularly emerging and vanishing web hosting mechanism makes the accountability of those URL with additional overheads for special agencies to deal with.

In contrast, traditional terrorists or extremists utilize TV, radio, or print media to catch the attention and sustain publicity. With the advanced application of ICT, the terrorists or extremists no longer have to contact with the public media journalists face to face, which increases the possibility of being exposed concerning some secret operations.

Currently, they bypass the inconvenience and directly utilize ICT to reach hundreds of millions of people globally 24/7/365. With the emergence of web sites and sophisticated multimedia technology, they can undergo fundraising, announce propaganda, train dedicated staffs, and continue to recruit new blood with tremendously resourceful online libraries of speeches, video clips and training manuals. They are targeting on global media, diverse global visitors, sympathizers or even the enemies [Weimann, 2004]. With high pace of proliferation and refined multimedia of on-line forums, the publicity of current terrorist campaigns is an imminent and substantive danger in the global community.

It's not hard to find the related literatures concerning traditional terrorism in history or the consequences that cyber terrorism might devastate human lives. However, few of them will specifically identify the potential occurrence via exploiting ICT as an extremist conspiracy. In the paper, we identified the scenario of launching the cyber terrorist attack by means of the ubiquitous networks and vulnerabilities of existing ICT with less capital and thresholds to demonstrate that cyber terrorism is an imminent potential threatening to global civilians.

2 General Cyber Crime Terminologies and Their Threatening

As computer crime has no boundary by its nature. Some sophisticated computer savvy might abuse the poorly managed network systems in some developing countries, where loosely computer auditing frameworks are running. Those terrorists take advantage of those countries and exploit those locations as the heavens for committing computer crimes because the chance of being caught is quit low due to the network forensics or auditing is never emphasized in those areas. We provided the following general cyber crime terminologies, which could be the fundamental criminal ingredients when uptake the cyber terrorism by contemporary extremists.

As the ICT progresses on a daily basis, we categorized the following terminologies as utilizing the existing technologies.

Virus: It is a computer program that was deliberately designed to spread from computer to computer when contaminated files are accessed. Virus is capable of running out of available memory and causes the performance of the computer to be dramatically downgraded. It may also result in the loss of digital data in a computer or crash the operating system.

Worm: It is a computer program that is capable of reproducing itself and spreading through networks and exhausting obtainable memory. The way of being transmitted of *worm* is different from *virus*. It does not need computer users to actually access the infected files to be propagated.

Malicious Code: It is a piece of software code that is purposely designed to cause damage to computer related systems like *worm* or *virus*.

Trojan Horse: Any computer program that purports to have a useful function disguises as legitimate software, which is generically called *Trojan horse*, or simply *Trojan*. It will hamper the normal functions of the infected computer systems and may even facilitate remotely unauthorized access via network or provide administrator authority for hackers over the compromised computer without the awareness of the current computer users [Anson & Bunting, 2007].

Hacker: Hackers are those ICT savvy who have a deep understanding of networks and computers. Hackers apply their skills to invent or modify the system creatively using computers to achieve a goal for which the system was not originally designed [Levesque, 2006].

Cracker: Crackers are computer savvy who break into computer systems via ICT in order to achieve destructive ends fulfilling illegal conspiracy.

Furthermore, we categorized the following terminologies as utilizing the new technologies.

Zombie: The compromised host (or called *Agent*) is being manipulated by crackers through the network to follow the instruction from the *cracker* in the back end. The unsuspecting users are totally unaware regarding the computer hacking incident.

Distributed Denial of Service (DDoS) Attack: The *DDoS Attack* tries to exhaust the resources of the compromised computers and degrade the network performance, which winds up with the victims' system failing to provide services. The *DDoS* is a typical cyber crime, which depicts the situation that the attacker launches hundreds of thousands from compromised computers (*zombie hosts*) to send lots of requests simultaneously over the Internet and passes through the firewall in order to force the target servers to be down.

Spam: Unsolicited and voluminous e-mails that are transmitted over the networks pretend to provide legitimate commercial services in order to commit conspiracy for lucrative purposes.

Spoofing & *Phishing*: Unscrupulous syndicate utilizes *spam* mechanism to unsolicited or specific victims redirecting the users to a *spoofing* web site that is almost identical to the official one. After the victim opens the link and provides the associate personal data like username and password, the heinous mob will commit extortion toward the victim and the deception process is called *phishing*, which utilizes ephemeral life cycle web sites to dupe personal data and commit computer frauds [Oppliger & Gajek, 2005].

Spyware: Any software that runs on computers monitoring the users' computer activities and collecting the associate information is called *spyware*, which might encompass from keystrokes to data files of the current logon user. It can propagate to remote collectors without the awareness or consent of the users. In many cases, the spyware is bundled with other pieces of free software that can be downloaded and installed from the web sites. Without loss of generality, the main purpose of spyware is to collect information and send to the gatherer [Klang, 2004].

Digital technologies offer contemporary terrorist organizations an unprecedented opportunity to leverage their campaigns of violence exhaustively. Iraq has quietly been developing a cyber arsenal called *Iraq Net* since the mid-1990s. *Iraq Net*, which was designed to overwhelm cyber-based infrastructures by *DDoS* and other cyber attacks, consists of a cluster of more than 100 web sites located throughout the world [Stohl, 2006]. Voluminous web sites provide resourceful software tools, video clips and other components for the public to download and install. This phenomenon is undermining the computer security issues, especially for those computers being deployed to control the critical infrastructures. Spyware will be installed and resident in the victims' computer without the awareness of those users. Confidential information will be periodically sent to the information gatherer. The anathema is that cyber terrorists could be fully taking charge and administrating the critical infrastructures even thousands of miles away without physically present in the nearby of those facilities.

3 The Phobia of Cyber Terrorism - The Sum of All Intangible Fears

The unforgettable tragedy occurred on September 11, 2001. Nineteen terrorists hijacked four airlines loading with thousands of gallon of jet fuel and crashed them into highly visible targets, New York City's World Trade Center [Jones, *et al.*, 2006]. Collectively, the global anti-terrorism organizations really began to recognize the overt threatening of cyber terrorism that is a present danger in this digital age. In the post 9/11 world, global media and government officials often tied the potential cyber terrorism to Al Qaeda or other extremist organizations [Matusitz, 2006; Qin, *et al.*, 2007].

After 9/11, the most recent terrorist action was on March 11, 2004. The attack occurred on Madrid's commuter train, which was a traditional way of launching the attack. Invariably, from the past terrorist acts, it is obvious that urban centers are indeed the potential targets to such hideous retaliation, where severe casualties happened. Generally speaking, terrorist acts are aimed to create the most insidious and onerous of all disruptions. Similarly, terrorist or extremist can inflict massive harm toward critical infrastructures to fulfill the same goal in the short coming future. As we stated above, most of the critical infrastructures are controlled by commodity computer systems with Internet connection for the purpose of real-time monitoring and managing.

Although the cyber terrorism has not officially set the record in our history in terms of severe casualties or death poll, it does not mean that it will not occur in the coming future. Actually, some probative operations are already undermined the internet security in order to fulfill the cyber terrorism. Recently, the cyber terrorists have defaced over 500 Danish Websites on February 9, 2006 [Stohl, 2006]. The Danish Internet security companies were fighting back via networks winding up with victory. There is no doubt that cyberspace is a new front to attack, which is being utilized by global extremists or dissidents. Cyber terrorists can take advantage of the web sites as portals to execute serial attacks, which may cause unbelievable casualties with no time to response or escape from the nightmare. The above web site defacement is only a wake up call for what will happen in terms of large scale destruction in any moment. Hence, cyber terrorist attack was first suspected in the 2003 Northeast blackout. Fortunately, the real cause for the incident turned out to be the incompetence of the existing electricity power system and the falling trees.

It's a great pity that cyber criminals will become much more sophisticated due to the progressing ICT and their advanced educations. For all the alliances in this world, if they do not continue to invest considerable resources in cyber security, the potential damages in the near future will be worse and more conductive than we can imagine. We probably are unable to recover in a decade after cyber terrorism reaches its maturity or it extensively starts to launch the cyber attacks. Consequently, building defenses against cyber criminals or terrorists is essential and the government agencies are indispensable for these unscrupulous cyber extremists.

4 Vulnerability of Critical Infrastructures for Cyber Terrorists - The Process Control Systems (PCSs)

A Process Control System (PCS) frequently applies in industry or factory automation, which supervises the real-time operating status of the current systems. PCSs are responsible for the safe, reliable and efficient operations of many critical infrastructure components. Similarly, among these critical infrastructures, PCSs play a crucial mechanism for the proper execution for those critical infrastructures. The functionality of a PCS is to monitor the operation of a certain system, for example, the current status of a nuclear plant [Tang & McMillin, 2008]. Any feedback from the system will trigger specific operations based on the responding mechanism that was embedded in the PCS. PCSs require providing real-time or nearly real-time response for a certain critical infrastructures, which are expected to offer availability around the clock. Therefore, the security issue of PCSs can not be over emphasized. Demonstrably, once the PCS is compromised, the critical infrastructures will be in danger.

In other words, the PCS will monitor and respond to the attached devices according to the protocol between the PCS and the corresponding critical infrastructures. On the contrary, the unauthorized access and insidious manipulation of the PCS may result in the malfunction of a nuclear plant emitting radioactive materials. Current PCSs have utilized proprietary protocols, which have replaced Ethernet/IP-based protocols allowing for inexpensive and efficient solutions, which might cause network attack due to the exploited vulnerability.

November 9, 2008, an accident that killed 20 people on a new Russian nuclear submarine was caused by a malfunction of the fire safety system that spewed out chemicals. It was Russia's worst naval accident since the nuclear submarine Kursk sank after an onboard torpedo explosion on August 12, 2000, killing all 118 crew members (http://www.cnn.com). The incident indicated that the breakdown of the distinct PCS caused the disaster, which resulted in radioactive contamination to the environment. From the cyber terrorism point of view, the scenario can be duplicated just by triggering different causes right from the keyboard on the terrorist's PDA or smart phone, as long as the cyber terrorist has the access authority over the remote PC that controls the PCS.

From the safety point of view, the priority for the consideration of the critical infrastructures will be confidentiality, integrity and then availability although we know that the downtime of those facilities will cost tremendous financial overhead. The cyber extremism or hacktivism is relentlessly seeking the vulnerabilities of the existing critical infrastructures. The reality is that the activists are beginning to integrate ICT into their well-organized decentralized networks, which can be served as the avenue to remotely launch cyber attack targeting certain critical infrastructures. Undoubtedly, the activists are working on facilitating low-cost operations with complex ICT technologies to initiate potential catastrophic deconstruction of some vulnerable critical infrastructures.

Among those PCSs, the PLC (Programmable Logic Controller) is the critical component that enables those PCSs run properly and safely. A PLC is often connected to the I/O device that is being controlled. In this digital era, voluminous enterprises have deployed advanced information systems into their core operations. A PLC can control the production rate of assembly lines of a chemical manufacturer as soon as the quantities of e-procurement changes in an Enterprise Resource Planning (ERP) system, which is a horizontal information integration hub within the organization. The PLC in a PCS is capable of dynamically modifying the manufacturing processes according to the sensors that attached to the production devices with the goal of maximizing the yield. Most of the above systems are currently operated under the control of PCs. Consequently, if the cyber terrorists can insidiously manipulate the above PCs, then the process of extremely poisonous materials disposal could be controlled by the cyber terrorists remotely and anonymously. Many critical infrastructures are deployed with commodity computer systems, which are being considered as an efficient and effective solution for operating those critical infrastructure components. However, they might introduce vulnerabilities that were embedded within the operating systems, hardware manufacturers, or even through the downloading and installing some software tools, which were bundled with spyware from the Internet. All possible security breaches could lead to unexpected disasters in some PCSs.

5 A Possible Scenario of Launching a Cyber Terrorist Attack

Dated back to 1986, Chernobyl Nuclear Disaster, Russia, resulted in radioactive leakage while they were testing the reactor and ignored the safety procedures. A chain reaction caused the explosion and released high radioactive materials. Currently, as we stated above, most critical infrastructures are controlled by the PCS and PLC, which play essential roles in the working mechanism. As Figure 1 suggests that the remote nuclear plant is monitored and operated by the PLC embedded in the PCS. This Figure also demonstrated the possible scenarios that the contemporary terrorists launch the cyber terrorist attack. Generally speaking, nuclear plants are located in remote areas, which is often the case. Between the corporate Intranet and the operating site, there must have a certain telecommunication network that can be used to remotely control the PLCs, which are connected to the I/O devices of the nuclear plants. Definitely, the firewall is a common hardware and software device that filters the incoming and outgoing information between the corporate intranet and the operating site. However, the cyber terrorists or extremists can take advantage of the security leakage or the exploited vulnerabilities that reside in the commodity computer systems, which are being deployed in the corporate intranet or the remote operating sites.

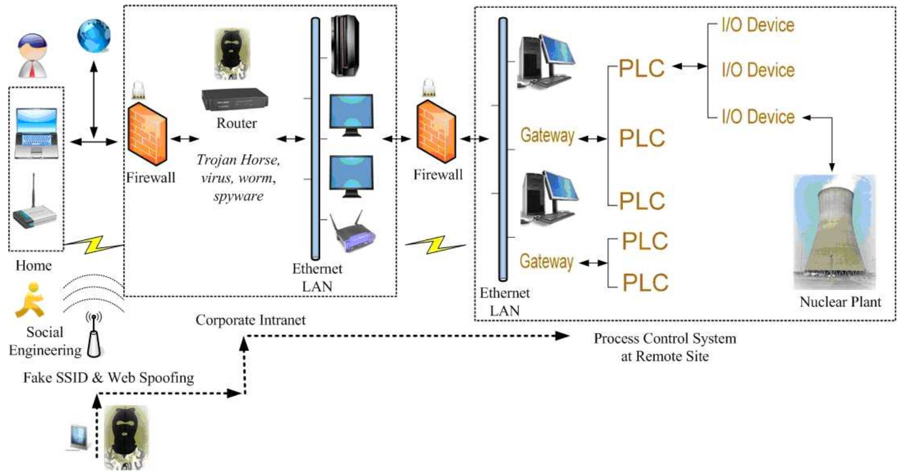

Figure 1: The possible scenarios that the contemporary terrorists launch a cyber terrorist attack

There are several ways for the cyber terrorists getting hold of the computers in the corporate intranet. As we stated above, *malicious code* is prevalent when the users download and install something from the web sites especially the *spyware*. Eventually, they can just use those computers as the *zombie hosts* to go through the firewall between the corporate intranet and the remote operating sites. In other words, the hidden cyber terrorists are capable of controlling the PCS in the remote operating sites, which means they might be able to manipulate the remote nuclear plants.

They can also use *zombie hosts* worldwide to launch *Distributed Denial of Service* (*DDoS*) *Attack* in order to shut down the service of a certain critical infrastructure. It is not a hard problem for them to crack into the corporate intranet. Applying the cracking techniques would not be obfuscated for those ICT savvy cyber terrorists. For example, a fake SSID (Service Set Identifier) for the wireless router is a way to collect the username and password that are being authenticated within the corporate. We have already seen that some fake SSID shows up in the airport or public access locations with the *spoofing* feature trying to record the existing users' username and password. The same scenario could happen in the corporate intranet as long as the signal of the wireless router of the *spoofing* SSID reaches.

Furthermore, through the social engineering methodology, the employee who may have to access the computers that reside in the corporate due to necessity during the severe weather condition in order to make sure that the critical infrastructures are properly operating 7/24/365. Consequently, cyber terrorists might apply social engineering techniques toward the employee and targeting his/her home computer as the stepping stone for furthermore access to the corporate Intranet. In other words, they may utilize social engineering method or fake SSID to obtain the username and password or even crack the confidential information that is being transmitted through the network. Undoubtedly, commercial sniffing tools can be applied to achieve the above goal.

The above scenario provides the possibility that as long as the cyber terrorists can access the corporate intranet, then they might be capable of remotely controlling the PCSs attached to the critical infrastructures. The extremists can be any place on earth: in the subways transportation system, public coffee shop, airport, or library where wireless access point is provided, especially the public accessible WLAN (Wireless Local Area Network) makes the traceability even harder for some cyber crime incidents. Hence, they can utilize any kind of mobile devices like 3G smart phone or PDA using WiMAX or Wi-Fi connection to get on the public network. Under such circumstances, the destruction of a remote nuclear plant could be triggered by just using one fingertip and causes tremendous disasters.

Although most PCSs are isolated in the proprietary network system, there is a high possibility that vulnerabilities are still exploited by heinous insiders or the employee accidentally introduce malicious code via downloading unauthenticated software or removable devices like USB thumb drives. *Spoofing* web site can ask the onsite employee to download the urgent service patches by *spam* mechanism. In the meanwhile, the *malicious code* includes *Trojan horse*, *virus*, *worm*, *spyware*, etc. Once the commodity computer system has been infected or compromised, the serious results will be extremely unpredictable. As Figure 1 indicates that the cyber terrorists can use diverse methods by using sophisticate ICT to get hold of the corporate intranet. Next, they can remotely manipulate the PCs that are being connected to the PLCs in the remote operating sites. The cyber terrorists can sit back and relax on the beach enjoying the sunshine, where is thousand miles away in the Middle Eastern. The cyber terrorists use the PDA to launch the terrorist attack across the time zone and the geographic boundary. There will be no need to commit suicide bombings in modern terrorist activities or extremist campaigns.

For all critical infrastructures, the SOP (Standard Operating Procedure) must be well documented and strictly enforced. Misconduct or violation of the SOP is not allowed to ensure the proper operation of those critical infrastructures. As we discussed above, PCS and PLC play essential role in this arena. However, from the counterterrorism point of view, all critical infrastructures must have the switching function between automatic and manual overriding operation. If the PCS is already controlled by the cyber terrorists, there is still a chance to stop the disaster by switching to manual operation of critical infrastructures.

The proposed scenario is a forthcoming public safety incident based on the vulnerabilities of current commodity computer system both from hardware and software aspects. In the proposed scenario, the ICT savvy can easily intercept or crack the wireless encryption, apply packet sniffing toolset, spoofing and phishing in the right place to obtain the confidential information. Some of the above scenarios already officially documented. Furthermore, if we ponder the above issue from existing schemes and the proposed scheme, we are able to clarify some blind spots. From existing schemes, we have seen many unaware victims lost their identities among cyber communities. Virus, worm, malicious code, or Trojan horse were widely exploited by heinous hackers. Endless computer incidents occurred from spam, spoofing & phishing have resulted in tremendous financial loss. The proposed scheme of the paper is the combination of the existing schemes to commit extremism. Especially the social engineering utilizes the sate-of-the-art technology in the proposed scheme and the naive victims are totally oblivious until the last minute. The academic theory behind the proposed scenario is the emphasis of computer auditing, especially for those of the critical infrastructures. Computer auditing encompasses the live applications, IT infrastructures, automation of auditing and the alert mechanism. It is never too late to thoroughly reflect those theories in real practices in order to alleviate the accumulation of all intangible fears from the cyber terrorists in our proposed scenario.

6 Conclusion

Demonstrably, cyber terrorists or extremists utilize sophisticated applications of ICT combining with voluminous content rich multimedia websites aiming to provide psychological warfare, fundraising, cooperation and distribution of propaganda materials through the Internet channels. Unfortunately, we have to face the reality that the contemporary terrorists or extremists already extensively utilized the Internet, which embodies ubiquitous access, anonymous posting, global reach and ambiguous regulations fostering the terrorists or extremists directly broadcast to the global audiences, supporters as well as adversaries, with little chance of being caught. The cyber terrorist or extremist organizations demonstrated sophisticated web knowledge as U.S. government agencies. The mushrooming cyber terrorism phenomena are well-organized, constructed and plotted in details. Although there is no instance so far resulting from cyber terrorism, which might cause a catastrophic loss of lives or physical destruction, no one can guarantee that the spectacular and deadly events will not occur. Frankly speaking, it's a matter of time instead of insufficient knowledge or skills. We have to improve the techniques to deal with the potential cyber attacks across the entire spectrum, from pre-attack warming, real-time responding mechanism to post-attack forensics in order to mitigate the anxiety from cyber threats. Cyber terrorism, next generation of terrorism, does pose an imminent threat to the world. Ubiquitous cyber terrorism will make the prevention even harder and sometimes the cyber forensics infeasible due to the prerequisite, which needs real time cooperation among global countries with different regulations, jurisdictions as well as political relationships. With sophisticated complication in its nature, this makes the civilians live in an atmosphere with the sum up of all intangible fears. The global responding agencies are indispensable and must develop cooperative and complementary research programs to come up with new principles, methodologies, tools, or mechanisms to design and construct more secure, reliable and robust commodity computer systems to face the challenge of global activism or extremism.

Acknowledgements

Authors would like to express their gratitude to Dr. Jong Hyuk Park for his valuable comments on this paper.

References

[Anson and Bunting 2007] Anson, S., Bunting, S.: "Windows Network Forensics and Investigation"; Wiley Publishing, Inc.

[Cassidy et al. 2008] Cassidy, R.F., Chavez, A., Trent, J., Urrea, J.: "Remote forensic analysis of process control systems"; IFIP International Federation for Information Processing, 253, critical infrastructure protection, (2008), 223-235.

[Chaikin 2006] Chaikin, D.: "Network investigations of cyber attacks"; The limit of digital evidence. Crime Law Social Change, 46, (2006), 239-256.

[Dacey 2004] Dacey, R.: "Critical infrastructure protection"; Challenges and efforts to secure control systems. Report GAO-04-628T, U.S. General Accounting Office, Washington, DC.

[Denning 2004] Denning, D.E.: "Information operations and terrorism"; Journal of Information Warfare, available and retrieved November 15, (2008), from `http://www.jinfowar.com`.

[Denning 2000] Denning, D.E.: "CyberTerrorism"; Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives, May 23, 2000. Retrieved November 21, (2008), from `http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html`.

[Dynes et al. 2008] Dynes, S., Goetz, E., Freeman, M.: "Cyber security: Are economic incentives adequate?"; IFIP International Federation for Information Processing, 253, critical infrastructure protection, (2008), 15-27.

[Innes 2004] Innes, M.: "Signal crimes and signal disorders"; Notes on deviance as communicative action. The British Journal of Sociology 55, 3, (2004), 335-355.

[Klang 2004] Klang, M.: "Spyware - the Ethics of Covert Software"; Ethics and Information Technology, 6, (2004), 193-202.

[Levi 2008] Levi, M.: "White-collar, organized and cyber crimes in the media: Some contrasts and similarities"; Crime Law Social Change, 49, (2008), 365-377.

[Grabosky 2004] Grabosky, P.: "The global dimension of cybercrime"; Global Crime, 6, 1, (2004), 146-157.

[Grabosky 2007] Grabosky, P.: "Requirements of prosecution services to deal with cyber crime"; Crime Law Social Change, 47, (2007), 201-223.

[Jones et al. 2006] Jones, A. K., Fedorov, I., Branscomb, L. M., Medvedev, N. V., Shiyan, Y. K., Wells III, L., Wolin, M., Sharber, A. C.: "Report of U.S.-Russian working group on cyber terrorism issues, countering urban terrorism in Russia and the United States"; Proceedings of a workshop, 9-13, retrieved September 12, (2008), from `http://www.nap.edu/catalog/11698.html`.

[Levesque 2006] Levesque, M.: "Hacktivism: The how and why of activism for the digital age"; The International Handbook of Virtual Learning Environments, (2006), 1203-1214.

[Matusitz 2006] Matusitz, J. A.: "Cyberterrorism: A postmodern view of networks of terror and how computer security experts and law enforcement officials fight them"; Ph.D. Dissertation, University of Oklahoma, U.S.A.

[Miller 2005] Miller, A.: "Trends in process control systems security"; IEEE Security & Privacy, September/October, (2005), 57-60.

[Oppliger et al. 2005] Oppliger, R., Gajek, S.: "Effective protection against phishing and web spoofing"; IFIP International Federation for Information Processing, LNCS 3677, (2005), 32-41.

[Qin et al. 2007] Qin, J., Zhou, Y., Reid, E., Lai, G., Chen, H.: "Analyzing terror campaigns on the internet"; Technical sophistication, content richness, and web interactivity. International Journal of Human-Computer Studies, 65, (2007), 71-84.

[Stohl 2006] Stohl, M.: "Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games?"; Crime Law Social Change, 46, (2006), 223-238.

[Tang and McMillin 2008] Tang, H., McMillin, B.: "Security of information flow in the electronic power grid"; IFIP International Federation for Information Processing, 253, critical infrastructure protection, (2008), 43-56.

[Weimann 2004] Weimann, G.: "How modern terrorism use the Internet"; Special Report, US Institute of Peace, retrieved October 14, (2008), from `http://www.usip.org/pubs/specialreports/sr116.pdf`.

[Weimann 2005] Weimann, G.: "Cyber terrorism: The sum of all fears?"; Studies in Conflict and Terrorism, 28, (2005), 129-149.

[Zhou et al. 2005] Zhou, Y., Reid, E., Qin, J., Chen, H., Lai, G.: "US domestic extremist groups on the web: Link and content analysis"; IEEE Intelligent Systems (Special Issue on Homeland Security) 20, 5, (2005), 44-51.