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 crit-

ical 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