Understanding the Methods behind Cyber Terrorism

C

Maurice Dawson
University of Missouri-St. Louis, USA

Marwan Omar
Nawroz University, Iraq

Jonathan Abramson
Colorado Technical University, USA

INTRODUCTION

Cyber terrorism is on the rise and is constantly affecting millions every day. These malicious attacks can affect one single person to government entities. These attacks can be done with a few lines of code or large complex programs that have the ability to target specific hardware. The authors investigate the attacks on individuals, corporations, and government infrastructures throughout the world. Provided will be specific examples of what a cyber terrorist attack is and why this method of attack is the preferred method of engagement today. The authors will also identify software applications which track system weaknesses and vulnerabilities. As the United States (U.S.) government has stated an act of cyber terrorism is an act of war it is imperative that we explore this new method of terrorism and how it can be mitigated to an acceptable risk.

BACKGROUND

Cyber security has become a matter of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the 1990s users have exploited vulnerabilities to gain access to networks for malicious purposes. In recent years the number of attacks on U.S. networks has continued to grow at an exponential rate. This includes malicious embedded code, exploitation of backdoors, and more. These attacks can be initiated from anywhere in the world from behind a computer with a masked Internet Protocol (IP) address. This type of warfare, cyber warfare, changes the landscape of war itself (Beidleman, 2009). This type of warfare removes the need to have a physically capable military and requires the demand for a force that has a strong technical capacity e.g. computer science skills. The U.S. and other countries have come to understand that this is an issue and has developed policies to handle this in an effort to mitigate the threats.

In Estonia and Georgia there were direct attacks on government cyber infrastructure (Beildleman, 2009). The attacks in Estonia rendered the government's infrastructure useless. The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the development of cyber defense organizations within Europe.

Laws and Policies to Combat Terrorism

The events of 9/11 not only changed policies with the United States (U.S.) but also policies with other countries in how they treat and combat terrorism. The United Nations (U.N.) altered Article 51 of the U.N. charter. This article allows members of the U.N. to take necessary measures to protect themselves against an armed attack to ensure international peace and security.

Israel is a country with some of the most stringent policies towards national and international security. This country requires all citizens to serve in the military to include multiple checkpoints throughout the country. This country has utilized stringent checks in the airport long before 9/11 however now they have additional measures to ensure security as they are surrounded by countries that have tried to invade before. Israel has

DOI: 10.4018/978-1-4666-5888-2.ch147

also deployed more Unmanned Air Vehicles (UAVs), and Unmanned Ground Vehicles (UGVs) to patrol the border in the event something occurs.

The United Kingdom (U.K.) has the Prevention of Terrorism Act 2005 and the Counter-Terrorism Act 2008 which was issued by Parliament. The first act was created to detain individuals who were suspected in acts of terrorism. This act was intended to replace the Anti-terrorism, Crime and Security Act 2001 as it was deemed unlawful. These acts seem to mirror the same ones created in the U.S. to monitor potential terrorists and terrorists. The U.K. also shared their information with the U.S. for coordinating individual that may be of risk.

In the U.S. the methods for national security were enhanced to ensure no threats occur on U.S. soil. These changes include enhanced security in all ports of entry. The signing of the Homeland Security Act of 2002 (HS Act) (Public Law 107-296) created an organization that received funding and lots of resources for monitoring the security posture of this country. Additional changes include enhanced monitoring of citizens and residents within the country to prevent terrorist activities by the mention of key words e.g. bomb, explosive, or Al Qaeda.

The USA PATRIOT was signed into law by President George W. Bush in 2001 after September 11, 2001 (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This act was created in response to the event of 9/11 which provided government agencies increased abilities. These increased abilities provided the government rights to search various communications such as email, telephone records, medical records, and more of those who were thoughts of terrorist acts (Bullock, Haddow, Coppola, & Yeletaysi, 2009). This allowed law enforcement to have the upper hand in being proactive to stopping potential acts against U.S. soil. In 2011 President Obama signed an extension on the USA PATRIOT Act. This act has received criticism from the public due to the potential to be misused or abused by those in power. This act has allowed government agencies to impede on constitutional rights.

The Protecting Cyberspace as a National Asset Act of 2010 was an act that also amends Title II of the Homeland Security Act of 2002. This act enhanced the security and resiliency of the cyber and communication infrastructure within the U.S. This act is important as the President declared that any cyber aggressions would be considered an act of war. This is also important as Estonia's entire digital infrastructure was taken down by hackers who supported the former Soviet rule. This type of attack could be damaging to the infrastructure in the U.S. causing loss of power for days or more which could result in death. In an area such as the Huntsville Metro we could have multiple nuclear facility melt downs, loss of ISR capabilities, and communication to the war fighter that we are supporting.

Additional changes from this act include the ability to carry out a research and development program to improve cyber security infrastructure. At the moment all government organizations must comply with the Federal Information Security Management Act (FISMA) of 2002. This act has shown many holes within the U.S. cyber security infrastructure to include those organizations that are leads. This act provides DHS the ability to carry out the duties described in the Protecting Cyberspace as a National Asset Act of 2010.

The most significant policy created to ensure that technically competent individuals are working on national infrastructure is the Information Assurance Workforce Improvement Program, Department of Defense (DoD) 8570.01-Mandate (M) (Directive, 2005). This mandate provides guidance for the identification and categorization of Information Assurance (IA) positions and associated certifications (Directive, 2010). However this mandate only provides the baseline certifications required to perform specialized IA functions. The certification categories are broken down in the following; Information Assurance Technical (IAT), Information Assurance Manager (IAM), Information Assurance System Architect and Engineer (IASAE), and Computer Network Defense (CND). Figure 1 displays all the specific certifications that can be used as of the updates to the DoD8570.01-M.

Stuxnet Worm

During the fall of 2010 many headlines declared that Stuxnet was the game changes in terms of cyber warfare (Denning, 2012). This malicious worm was complex and designed to target only a specific system. This worm had the ability to detect location, system type, and more. And this worm only attacked the system if it met specific parameters that were designed in the code. Stuxnet tampered directly with software in a programmable logic controller (PLC) that controlled the centrifuges at Natanz. This tampering ultimately caused a disruption in the Iranian nuclear program.