A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
Chapter 1
A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism

Maurice Dawson
University of Missouri – St. Louis, USA

ABSTRACT
Cyber security is becoming the cornerstone of national security policies in many countries around the world as it is an interest to many stakeholders, including utilities, regulators, energy markets, government entities, and even those that wish to exploit the cyber infrastructure. Cyber warfare is quickly becoming the method of warfare and the tool of military strategists. Additionally, it is has become a tool for governments to aid or exploit for their own personal benefits. For cyber terrorists there has been an overwhelmingly abundance of new tools and technologies available that have allowed criminal acts to occur virtually anywhere in the world. This chapter discusses emerging laws, policies, processes, and tools that are changing the landscape of cyber security. This chapter provides an overview of the research to follow which will provide an in-depth review of mobile security, mobile networks, insider threats, and various special topics in cyber security.

INTRODUCTION
Cyber security has become an important subject of national, international, economic, and societal importance that affects multiple nations (Walker, 2012). Since the early 90s users have exploited vulnerabilities to gain unauthorized access to networks for malicious purposes. In recent years the number of attacks on United States (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 (Dawson, Omar, & Abramson, 2015).

DOI: 10.4018/978-1-4666-8345-7.ch001
In Estonia and Georgia there were direct attacks on government cyber infrastructure (Beildleman, 2009). The attacks in Estonia rendered the government’s digital infrastructure useless (Dawson, Omar, & Abramson, 2015). The government and other associated entities heavily relied upon this e-government infrastructure. These attacks help lead to the rapid development of cyber defense organizations throughout Europe which has raised the profile of cyber attacks to include awareness to the potential severity of attacks (Dawson, Omar, & Abramson, 2015).

MOBILE NETWORKS

Mobile networks are found in large cities in America to villages in West Africa. Thus the importance of security in mobile networking is essential to maintaining security and privacy for everyday citizens. Mobile devices have become the preferred device for web browsing, emailing, using social media and making purchases (Wright et al, 2012). Many individuals rely on their mobile devices for texting, checking email, making online purchases, and even remote controlling their home alarm system. Thus attackers have developed malware to specifically target these platforms. Understanding the Human Computer Interaction (HCI) and behavioral issues with mobile devices is a start in understanding human pitfalls in security.

DIGITAL CURRENCY

Digital currency has become a new commerce that is growly quickly and gaining the attention of large financial institutions. This crypto currency has been termed “memory” in monetary economics literature (Luther & Olson, 2013). Bitcoin is a peer to peer electronic cash system in which no one controls and there are not an associated printed currency (Nakamoto, 2008). Bitcoin allows for anonymity to occur in this peer to peer electronic currency systems (Reid & Harrigan, 2013). Some argue that the main benefits are lost if a trusted third party is necessary to prevent the action of double spending (Nakamoto, 2008). The technical infrastructure of this decentralized digital currency relies on several cryptographic technologies.

Luther and Olson state that the principle finding of the money and memory literature is that both devices are capable of facilitating exchange (Luther & Olson, 2013). What is missing from the literature is data concerning the use of Bitcoin for illicit activities. However some researchers attempt to assess potential damages and threats to national security, banking industry, child pornography, drug trade, financial fraud, and more. In relation to cyber warfare Bitcoin could pose as an enabler for plausible deniability of foreign governments and institutions for involvement in cyber attacks (Hilse, 2013). Further cyber criminals could store stolen digital funds on any device that can be used as storage (Hilse, 2013). This could pose a threat as laundered, stolen, or self generated funds can be taken anywhere on a storage device such as a micro Secure Digital (SD) that can hold up to 64 Giga Bytes (GB). This could pose an issue in terms of search and seizure of assets as many police forces have inadequate training and personnel to pull off such measures of cyber forensics on a large scale.

In recent year researchers tackle what they have coined the dark side of cyber finance (Bronk, Monk, & Villasenor, 2012). The key theme to take away is that government and industry will need to be able to react quickly and adapt as the criminals and terrorists to meet the threat (Bronk, Monk, & Villase-
A Brief Review of New Threats and Countermeasures in Digital Crime and Cyber Terrorism

nor, 2012). In a world where monetary funds are difficult to track down through foreign bank accounts, digital currency has added yet another layer of difficulty that allows illicit funds to hide in plain sight. Therefore, the only limitations placed on criminals are their imagination and skill of individuals who come up with new innovative ways to use technology.

**CYBER ESPIONAGE AND SECRECY**

Cyber espionage or cyber spying is yet another method of cyber warfare. This method allows for the ability to obtain secrets without the permission of the data owner. The rise in cyber espionage is yet another reason governments must improve cyber security infrastructure. Nakashima details that the U.S. was the target of a massive cyber espionage campaign (Nakashima, 2013). During the Obama Administration, the U.S. expanded its cyber reach and infrastructure. However, this expanded reach has received negative reviews due to WikiLeaks and Edward Snowden.

**WikiLeaks and FinSpy**

WikiLeaks is an international, online, non-profit, journalistic organization that has published classified and sensitive information. This organization claimed to have a database of more than 1 million documents archived from 2006-2010. The servers that were pointing to the website were being shut down one by one (Benkler, 2011). The site contains a section labeled SpyFiles. This section on the site contains SpyFiles with 2 releases in 2011, 1 in 2013, and a release September 2014. The recent release provides insight on FinFisher, which is a German company that produces and sells exploitation tools that can extract data from multiple Operating Systems (OSs) such as OS X, Windows, Linux, Android, iOS, Blackberry, Symbian, and Windows Mobile devices. FinSpy appears to be a malicious Trojan designed to intercept and record a variety of information from an infected computer and applications. This software application has been found in Ethiopia aimed at political dissidents (Hankey & Clunaigh, 2013). Even more alarming is that this malicious application has been found within the hands of 25 governments that have questionable records on human rights (Pelroth, 2013). The application has been used to spy on their own citizens. Even Egyptian government members had been given a proposal by the Gamma Group to purchase this Trojan. More troubling is how this application is running on multiple servers with little oversight.

**Edward Snowden**

Edward Snowden’s actions will have people regarding him as a patriot or traitor (Goldfarb et al., 2015). Snowden’s leak displayed just how big the reach was of the Intelligence Community (IC) into the American public. Snowden’s use of a Linux distribution, Tails, that was originally developed as a research project by the U.S. Navy Research Laboratory (NRL) displays the ability to evade detection.

**Cyber Weapons: Stuxnet Worm and Flame Malware**

During the fall of 2010 many headlines declared that Stuxnet was the game-changer 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.

Flame was yet another highly sophisticated malicious program being used as a cyber weapon in various countries. This program was discovered by Kaspersky and it was the largest weapon to date uncovered of its type. Flame was designed to carry out espionage by stealing information about systems, stored files, contact data, and audio conversations (Munro, 2012). Flame conducted as series of attacks against Iran’s oil industry. Attacking a nation’s critical infrastructure and resources are military strategic tactics that have known been successfully conducted via thousands of line of code.

**OPEN SOURCE INTELLIGENCE (OSINT) AND OPEN SOURCE SOFTWARE (OSS)**

Open Source Intelligence (OSINT), which is one of several sub-intelligence collection disciplines, is intelligence collected from publicly available sources. Publicly available sources can be but are not limited to newspapers, magazines, industry newsletters, online forums, social media, and web queries. OSINT is the opposite of what is known to many as covert intelligence or intelligence gathered through classified means. However OSINT does not mean the information in the publicly available domain does not have a classified value. It only means that we all have access to it but the associated labels of combined information still remains secret or tied to another unknown data classification per the associated agency.

Open Source Software (OSS) can be defined as software that is made available in source code form. This is important as this source code may fall under the General Public License (GPL) which is a widely used free software license that is managed under the GNU Not Linux (GNU) Project (Dawson et al, 2014). There are currently thousands of active projects on sites such as SourceForge that provide access to innovative tools that make OSINT techniques relatively painless. Chinese and Australian researchers have reviewed the many OSS applications available for data mining and published an extensive review discussing findings (Chen, et al, 2007). These researchers note issues such as usability, maintainability, and stability as an issue (Chen et al, 2007). However OSS applications such as the R programming language, also identified as GNU S, has become one of the most powerful tools among statisticians in industry and academia. Table 1 below provides a review of power software applications that can be used in a variation of cyber related activities.

**LAWS AND POLICIES TO COMBAT TERRORISM**

The events of 9/11 not only changed policies with the 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. However this article raises important issues under international law regarding the use of force (Murphy, 2002). 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 07-296) 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 keywords e.g. bomb, terrorism, 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 the 2011 year, 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 11 of the Homeland Security Act of 2002. This act enhanced 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.
REFERENCES


Luther, W. J., & Olson, J. (2013). *Bitcoin is Memory*. Available at SSRN 2275730.


**KEY TERMS AND DEFINITIONS**

**Authentication**: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual’s authorization to receive specific categories of information (Harris, 2002).

**Availability**: Timely, reliable access to data and information services for authorized users (Harris, 2002).

**Bitcoin**: Bitcoin is a peer to peer electronic cash system that no one controls and there are not printed currency (Nakamoto, 2008).

**Confidentiality**: Assurance that information is not disclosed to unauthorized individuals, processes, or devices (Harris, 2002).

**Cyber Terrorism**: Attacks with the use of the Internet for terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses, worms, Trojans, and zombies (Janczewski & Colarik, 2008).

**Integrity**: Quality of an IS reflecting the logical correctness and reliability of the OS; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information (Harris, 2002).

**Non-Repudiation**: Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the data (Harris, 2002).

**Open Source Intelligence**: Intelligence collected from publicly available sources.