NATO Science for Peace and Security Series
D: Information and Communication Security - Vol. 42

Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses

Edited by
Mehmet Nesip Ogun (Ed.)

IOS
Press

NATO
OTAN

This publication is supported by:

The NATO Science for Peace and Security Programme

Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses

Edited by

Mehmet Nesip Ogun
NATO COE-DAT, Turkey

IOS Press

Amsterdam • Berlin • Tokyo • Washington, DC
Published in cooperation with NATO Emerging Security Challenges Division

Proceedings of the NATO Advanced Training Course (ATC) on Terrorist Use of the Internet
Ohrid, former Yugoslav Republic of Macedonia
8-12 December 2014

ISBN 978-1-61499-527-2 (print)
ISBN 978-1-61499-528-9 (online)
Library of Congress Control Number: 2015950601

Publisher
IOS Press BV
Nieuwe Hemweg 6B
1013 BG Amsterdam
Netherlands
fax: +31 20 687 0019
e-mail: order@iospress.nl

Distributor in the USA and Canada
IOS Press, Inc.
4502 Rachael Manor Drive
Fairfax, VA 22032
USA
fax: +1 703 323 3668
e-mail: iosbooks@iospress.com

PRINTED IN THE NETHERLANDS

Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses
M.N. Ogun (Ed.)
IOS Press, 2015

Foreword

Mehmet Nesip Ogun[a,1]
[a]*Associate Professor, NATO Centre of Excellence Defence Against Terrorism*

The South East European (SEE) region is comprised of NATO member countries (Slovenia, Croatia, Albania and Bulgaria) as well as Partnership for Peace (PfP) countries (Bosnia and Herzegovina, FYROM[2], Montenegro and Serbia). Opportunities and challenges related to cyber are prevalent in SEE.

Unlike the rest of the world, however, this region faces unique circumstances:

1. The dominance of the illicit goods market / transit in the SEE impacts NATO countries, PfP, Mediterranean Dialogue nations as well as key regions to the Alliance elsewhere in the world;

2. Terrorist groups increasingly interface with criminality in SEE to support their efforts;

3. Terrorism has been an enduring problem in SEE;

4. SEE and in particular FYROM, has made it a priority to increase their IT sector to achieve development goals; and

5. Political instability in the region may be mitigated by training and cooperation on cross-border issues such as terrorists' use of cyber and technology which benefits the Alliance.

As in the rest of the world, Information, Communications and Technology (ICT) plays a crucial role in the South Eastern Europe (SEE) region. The pursuit of modernization, the quest for Euro-Atlantic integration, and the undeniable necessity of foreign direct investment urged SEE countries to invest in the development of cyber. Furthermore, this domain has become the dominant place for social, economic and political interactions in the SEE region. However, this ICT-based dynamism has brought both positive and negative effects.

The increasingly growing dependence on cyber and technology in SEE has not been matched by a parallel focus on security. Recent practices show that the cyber domain

---

[1] Associate Professor Mehmet Nesip Ogun, PhD is currently working as Lessons Learned Specialist at NATO COE-DAT, nesip75@yahoo.com

[2] Turkey recognises the Republic of Macedonia with its constitutional name

has turned into both a battle-space for modern terrorists' ideological and informational warfare and a medium for global radicalization. Terrorist organizations and violent radical religious insurgents are using the internet and modern ICT as a tool for radicalization and recruitment, a method of propaganda, a means of communication, a mechanism for attacking other entities and a suitable ground for training.

The dynamics of the changing security environment around the globe in general and in the region of SEE in particular over the past decades have produced new adversaries to SEE stability. This has the potential to directly and indirectly affect NATO countries' interests, security and stability. On several occasions NATO has strongly emphasized that threats from cyber and technology against NATO countries and Partners are real (NATO Parliamentary Assembly in 173 DSCFC 09 E BIS - NATO and cyber defence, NATO's New Strategic Concept - 2010; the 2012 Chicago declaration, etc.). It is critical to note that SEE nations Slovenia, Croatia, Albania and Bulgaria are NATO members while Bosnia - Herzegovina, FYROM, Montenegro and Serbia are Partnership for Peace (PfP). Hence addressing the issue of terrorists' use of a cyber and technology in the current security environment remains as important as ever.

These actors are a hybrid mix of terrorists, criminals, insurgents and religious extremists, as well as other non-state entities who challenge SEE stability and security. The 2011 attack on the U.S. Embassy in Bosnia and Herzegovina, the 2012 attack and murder of five civilians in FYROM, and the 2012 attack on the Israeli tourists in Bulgaria, along with the numerous reports of thwarted attacks or arrests (e.g., Bosnia and Herzegovina, Serbia, Croatia, Kosovo, etc.) all confirm that this threat is genuine. Furthermore, recent trends in active support of radical Islamic groups in Syrian resistance and growing numbers of internet-based recruitments for these supporters along with the alleged online radicalization connected to the region prior to attacks around globe, raise serious concerns over the terrorist use of cyber and technology in SEE. If this development is not addressed seriously, then the growing trend of radicalization, recruitment and attack through cyber and technology holds the potential to render SEE's efforts to create a cyber-platform for increased development into one that becomes a breeding ground for training and launching pad for cyber-attacks on SEE, the Alliance, her partners and others.

As new developments occur every day in technology, terrorists are easily adjusting themselves to this change. In this new age of terrorism, terrorism is transnational, institutionalized, technologically advanced, and global. In this respect, today's terrorist organizations are using cyberspace for different purposes. The Internet has become the new and main source of communication in terms of disseminating propaganda for terrorist activities.

In modern terrorism, almost all terrorist organizations are benefitting from the Internet to commit their activities such as message delivering to the masses in the frame of propaganda activities, facilitate communication, and recruit new members to their organizations, raising funds, or to train the new hired members. Multimedia sources are so vulnerable for terrorist exploitation. The Internet offers terrorists so many advantages such as: easy access; no regulation, censorship, or other forms of government control; so many audiences; anonymity of communication; fast flow of information; interactivity; inexpensive development and maintenance of a Web presence; a multimedia environment (the ability to combine text, graphics, audio, and video and to allow users to download films, songs books, posters, etc.).

The area of concern, as a consequence of Internet exploitation, has been extended not only in the domestic realm, but also additionally to transnational and international arenas. The secrecy of conducting aforementioned activities can easily be resumed by means of covered or coded methods on the Internet. Thus, a comprehensive research of Cyberspace terrorist activities ought to be analyzed.

Governments usually take legal measures to prevent the unlawful usage of the Internet by applying to the national courts. However, flexible opportunities to run a Web site by changing servers, tags, proxies, and so forth do not deter or deny terrorist organizations to exploit the Internet. Thus national and international authorities, responsible for security, can also exploit and analyze the design and the context of the pro-terrorist organizations' Web sites to exhibit the context of the activities of the terrorist organizations.

A full cooperation and coordination of efforts are required to prevent the Internet usage of terrorist organizations. In this context, both state and non-state level cooperation must be institutionalized to create a check mechanism. Ever since terrorism and other types of transnational criminal activities have become the main topic in the international arena, the term "cooperation" has become a focal point for every government.

It is widely accepted that terrorism is a real and constant threat and no part of the world can be considered immune from it. However, by following a pro-active nature and keeping up with this evolving threat, we will become successful in overcoming it in very near future.

Contents

Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Responses
M.N. Ogun (Ed.)
IOS Press, 2015

doi: 10.3233/ 978-1-61499-528-9-1

The Use of Internet Technology by Cyber Terrorists & Cyber Criminals: The 2014 Report

Alan BRILL[a,1]
[a] *Kroll Cyber Security & Investigations, Secaucus, NJ, USA*

Abstract. This chapter examines The Use of Internet Technology by Cyber Terrorists & Cyber Criminals: The 2014 Report. 2014 has been an interesting one in the area of the use of cyberspace by cyber-criminals and cyber-terrorists. it is clear that cyber security has become a matter of vital importance to all organizations, whether in the public or private sectors. It is a matter that should be considered at the highest level in the organization.

Keywords. Cyberterrorism, cybersecurity, cyber defense, criminal law.

1. Introduction

2014 has been an interesting one in the area of the use of cyberspace by cyber-criminals and cyber-terrorists.

In the month of December, the United States suffered what appears to be the first large-scale cyber-terrorist attack. The motion picture production company Sony Pictures Entertainment suffered a severe data breach, reportedly in reaction to the planned Christmas-day release of a new motion picture called "The Interview." This motion picture – a comedy – involved a situation in which an inept TV interviewer and his producer are invited to interview the head of the North Korean government, and are tasked by the CIA with assassinating him.

The incident involved the release of both intellectual property – copies of five motion pictures – four of which had not yet been released to theaters – and sensitive

[1] Corresponding Author, Senior Managing Director, Kroll Cyber Security & Investigations, Secaucus, NJ, USA, E-mail: abrill@kroll.com

information including emails and documents (which are still being released at the time of writing.)

However, in addition to the theft of data, the perpetrators made terroristic threats of violence (referencing the September 11, 2001 attacks and warning people to protect themselves by staying away from venues showing "The Interview."

As a result of these threats, a number of theatre chains stated that they would not play "The Interview" on their screens, and Sony Pictures Entertainment decided to cancel the release of the film, saying in a press statement that "We are deeply saddened at this brazen effort to suppress the distribution of a movie, and in the process, do damage to our company, our employees and the American public." The potential effect of this action to motivate hactivists and terrorists to make threats relating to books, movies, writers or television shows they object to will remain to be seen, but it certainly represented a first for US consumers to have a product pulled from circulation because cyber-terrorists (specifically, a group that has no association with physical violence) threaten some form of action if their censorship orders are ignored. Sony received a great deal of negative publicity because of their decision, even to the extent of the President of the United States declaring the decision to cancel the release "a mistake." Just before Christmas, Sony reversed its decision, but given the decisions of major theater chains to show the movie, they arranged for it to open, as originally scheduled, on December 25, at several hundred independent theaters, where most of the showings quickly sold out, with some theatergoers quoted as saying that going to see the film was a matter of freedom of speech. But within 24 hours, the gaming networks of Sony's PlayStation product and Microsoft's X-Box product were attacked with a denial-of-service methodology and rendered unreachable. As of the time of this writing, it is not known whether this action is linked to Sony's release of "The Interviiew" against the wishes of the original hackers, and the government of the Democratic People's Republic of Korea.

Looking at the past year as a whole, US Navy Admiral Mike Rogers, current head of the National Security Agency, said in recent testimony before a congressional committee, that he expects a major cyber attack on the United States in the next decade. "It's only a matter of the 'when,' not the 'if.' That we are going to see something

dramatic." Admiral Rogers said in his testimony that adversaries can infiltrate the network fo industrial-control systems, the electronic brains behind infrastructural elements like the electrical grid, nuclear power plants, air traffic control systems and subway systems. "There shouldn't be any doubt in our minds that there are nation-states and groups out there that have the capability to do that."

In looking back at the attacks that were either made public or that we worked on in 2014 there is no question that cyber attacks continue to occur at a high volume. While we see some attacks that are very high-tech in their nature (sometimes involving previously unknown security flaws called "zero days") many of the attacks involve low-tech means like phishing that exploit human weaknesses, and are often very successful. The perpetrators show increasing sophistication in getting information from weakest-link sources. They may go through a contractor or vendor to gain access to an otherwise well-protected network. They may do research to enable them to create highly targeted spear-phishing messages to induce an employee or vendor to click on a link or open an attached (infected) file.

In our work, we have come to understand that many successful attacks were ultimately predictable.

In terms of why cyber-criminals and cyber-terrorists attack various targets, there are a number of reasons:

- Financial motivation seems to be the leading motive. With nearly a billion records stolen, there continues to be an active market for stolen credit card and identity data.
- Espionage. Whether done by governments or private-sector companies or hackers, we are seeing a continuing stream of cases in which corporate plans, formulae, business processes and financial information is targeted. Reputedly, some of this is done by or on behalf of national intelligence services, but others are commercial espionage and stll others schemes by employees who are either selling information or who leave with company secrets/data to form a competitive enterprise.

- Hactivism – This is the use of cyber methodologies to carry forward political or social causes. This is a difficult area to judge as it can be a convenient cover for theft, misappropriation of intellectual property or cyber-terrorism.
- Offensive Cyber Warfare or Cyber Terrorism. It is unquestioned that an increasing number of nations have developed both defensive and offensive cyber-warfare capabilities. Indeed, the United States has indicted five officers in the Peoples Liberation Army of the Peoples Republic of China for cyber espionage activities. It is also believed that the Stuxnet malware that resulted in the destruction of uranium enrichment gas centrifuges in Iran was the result of a cyber-operation. Similarly, the destruction of data on approximately 30,000 computers used for administrative operations at the Saudi Aramco oil company is believed to be the result of a state-sponsored cyber attack. As of the time this is written, there is also speculation as to whether the attack on Sony Pictures Entertainment was the work of North Korea or agents working for the North Korean government.

2. Top Threats

According to multiple sources, the major current threats (and these dangers exist whether they are fielded by cyber-terrorists, state-sponsored actors, or cyber criminals) are:

- The use of stolen/compromised credentials – In many cases we find that the bad guys gain or have access to authorized accounts, often privileged accounts. This is a combination of problems including the use of default accounts/passwords, shared accounts, not minimizing account privileges, weak passwords and others.
- Malware which causes data exfiltration – There are thousands of types of malware that seeks sensitive data and sends it to the perpetrators. The malware involved in the attacks on retail point-of-sale systems (which has been ongoing since at least 2008) which is sometimes called "memory scraper" malware is an example.
- Phishing and Social Engineering – These techniques continue to be highly effective. People click on links that they shouldn't and provide information on

phone calls and emails that they shouldn't. One effective variant of these techniques is "spear phishing" in which the perpetrators conduct research to make their messages very specific to a particular organization or specifically targeted individual to induce them to provide information. In one of our cases, when the management of a company was at an off-site conference, a spear phishing attack targeted a mid-level accountant who believed he was in email communication with his CEO, who instructed him to wire funds relating to a secret acquisition to a bank account in Asia. Many millions of dollars were lost in this well-planned and crafted scheme.

- Unencrypted or Unnecessary Sensitive Data – The old rule that bad guys can't steal something you don't have is true. We see sensitive data stolen that companies had no need to have kept. In other cases, sensitive data that should be stored in an encrypted form ends up being stored unencrypted.
- Back Doors – Hackers often attempt to install malware on networks that provide a back door through which they can gain long-term access. It is alleged that some computers and smart phones have back doors built into them, and that these can be misused.
- Physical Breaches – It's easy to forget that poor physical security can lead to cyber-breaches. Having physical access to machines can allow physical devices like key-loggers to be installed, or network devices to be installed. There are commercially available devices built to look like power strips that can facilitate the theft of data from wired and wireless networks. Some time ago, we had a case involving a start-up company in Silicon Valley that failed to pay attention to physical security. Their offices were broken into over a weekend, and their servers and backup tapes were stolen.
- Knowing Misuse – employers, contractors, vendors and others with authorized access can deliberately misuse their privileges for a wide variety of reasons. Sometimes it is done to specifically harm the victim company. Sometimes it is a means of making money by selling data. Sometimes it is done with the belief that the person is helping the company – for example by moving sensitive data to personal cloud storage in the belief that it would help them to better perform their job.

- Failing to Monitor Systems – It is impossible to completely prevent intrusions into a network. It has become necessary to monitor network activity to identify intrusions and provide information to identify, localize and defeat these incidents. Without monitoring, intrusions can go on for weeks, months or even years without being detected.
- Failure to Share Information – One of the problems in many industries is a lack of facilities for sharing of information about breaches, effective preventive measures and means of detection when breaches occur. It will take a combination of governmental and private sector efforts to facilitate security information sharing.
- Failure to know your own network. Do you have an accurate picture of everything attached to your network? Would you know if an unauthorized device was added? If a problem was traced to a device could you find it? Failure to understand a network's topology and configuration of protective devices can lead to issues in preventing and detecting incidents. For example, a firewall that has a well thought-out rule set for data from an address using the IPv4 format may have no protection designed for addresses using the newer IPv6 format.

3. Everyone's An Expert – Or Think They Are

The advent of tablets, smartphones, applications ("apps") and "cloud" storage and similar technologies has led to individual workers feeling empowered to change the way that they would to use what they believe are more effective. Unfortunately, in some cases, the actions they take can damage security and provide the ability for cyber-criminals, cyber terroriists or hactivists to gain access to data they should not have. A speaker at the 2014 CITE coference in San Francisco said that with the new technologies available to them, there is a tendency to characterize the corporate IT organization as "The Department of NO" and look to bypass it. "Legions of app-happy, cloud comfortable employees are not going to stop finding and downloading productivity tools that help them to do their jobs faster and better, bypassing the IIT department along the way." Unfortunately, there may be legal , compliance, contractual and other issues that limit how data can be acquired, stored, shared and used, and these

locally developed methodologies may ignore these, placing the organization in jeopardy. One example given at the CITE conference by vendor Spiceworks was their finding that 50% of corporate system users made some use of unapproved file sharing tools like Dropbox, OneDrive, iCloud or similar online storage systems.

The problem was summarized in a presentation by another vendor, Pertino. They said that security and compliance policies in place today are from a time when the assumption was that most assets were behind a corporate firewall and was being accessed through a personal computer. But now, people with their personally owned tablets and smartphones are accessing assets online in the cloud, and it's a huge disconnect. Clearly, this disconnect between security and compliance and what is actually found in practice is helpful to both cyber terrorists and cyber criminals.

4. Issues to Consider

While cyber security, cyber crime and cyber terrorism continually evolve, here are some of the issues that organizations worldwide in both the public and private sectors should consider:

- People tend to over-share on social networks. They provide information that enables others to gain access to their accounts. For example, information that people put on social networks is often the same information that is used as answers to "secret questions" used to re-set passwords. Reportedly, this was how a hacker gained access to the email account of former Alaska governor Sarah Palin when she was a candidate for Vice President of the United States.
- The integration of communication systems has made international telephone calling available at little or no cost. As a result, there has been a growth of something referred to as Voice Response Phishing, or "Vishing." For example, you receive a text message informing you that your bank debit card has been deactivated for security purposes. It provides a phone number to re-activate it. When you call the number, a voice guides you through the process of entering your card number and passcode, and then tells you that your card has been re-activated. In carryiong out these schemes, hackers use servers that they control (through having hacked them,) take advantage of free email to SMS services and low-cost Voice Over Internet Protocol phone lines. The

value of vishing to a cyber criminal or cyber terrorist looking for an easy way to collect money was estimated by vendor PhishLab based on each server getting data on 250 cards per day. The data entered on the phone call is transferred to the magnetic strip of a card, which is used with the password to withdraw money from an ATM. Assuming even a moderate daily limit of US$ 300 per card, the daily take can be $75,000 or more. The data is also used to make online purchases. In looking at this scheme, it might be argued that you can't generate a fake debit card with only a card number and password, because there are certain codes (CVV1/CVC) that are not known to the user and therefore couldn't be obtained through vishing. However, PhishLabs found that some banks do not actually verify debit card transactions using the CVV1 or CVC codes, making it possible to generate a usable card, even without knowledge of those codes. Governments should urge banks to actually use those codes to verify transactions.

- One of the issues that repeatedly arises in cases we investigate is the failure to understand your own network, and what's connected to it. Not knowing what's connected makes it easier for perpetrators to carry out their attacks in an environment and not be interdicted. For example, in one case, a wireless access point was attached to a bank's network and was not detected, and was used to compromise highly sensitive information relating to a potential sale of the bank. During an investigation of another matter, our wireless testing identified an access point not on the network diagram – in fact the device was a brand not in use at the bank. It's vital to know everything attached to your network and to be able to identify when something is connected that is not authorized.
- Similarly, knowing *who* is connected is vital, but so is regulating what each user can access on the network. In the major intrusion involving the U.S. retailer Target, the intruder was found to have accessed Target's network by first gaining access to the credentials of an employee of a company that provided service to heating and air conditioning systems at various Target facilities. It should be clear that access provided to an air conditioning and heating vendor should not allow anyone from that vendor to get to the retailer's point-of-sale system. There is no valid reason that they would need

such access. But at Target, by using an access credential associated with the vendor, the hackers navigated around Target's network, and were not only able to get to the point-of-sale system, they were able to install and control malware that was able to intercept credit card data before it could be encrypted, and store it in a location that the hackers could access to get it out of Target's network. Each user should have access to any resources they need, but should be prevented by system access rules from even seeing portions of the network they don't need.

- Another major issue that became very public in 2014 concerns the use of what is called "open source" software, and mistaken perception of the security of such code. While there were several incidents, the one that garnered the most publicity was a problem that came to be known as "Heartbleed." This was the name given to a mistake that was discovered in a widely-used open-source security package called "OpenSSL." This code was incorporated into literally millions of systems running various versions of the LINUX operating system. It could also affect Android phones. The problem occurred when the programmer wanted to allow OpenSSL to interact with the LINUX "Heartbeat" command, which allows you to keep a connection open over time. Unfortunately, in adding the four lines (out of more than 5,000 lines in OpenSSL) to the program, he made a mistake. The error, which was in the code base for more than year, allowed a hacker to repeatedly ask OpenSSL for 64,000 byte blocks of memory, which could contain passwords, account information, or even network encryption keys. Exploiting this error did not raise any alarms or leave a trace or record. As a result, it is impossible to definitively know how frequently it was exploited to steal data. Ultimately, the small group that was responsible for maintaining OpenSSL admitted that no one had checked the new code before it was placed into operation. This came as something of a shock to many in the computer community. There was a general assumption that open source software was tested and reviewed, and could thus be trusted. A repair was implemented, and required the addition of only one line of new code. Major corporations are now working together to provide a mechanism for funding reviews of open-source code on a regular