Journal of Strategic Security

Volume 6
Number 5 *Volume 6, No. 3, Fall 2013 Supplement: Ninth Annual IAFIE Conference: Expanding the Frontiers of Intelligence Education*

Article 3

Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism

Gary Adkins
The University of Texas at El Paso

pp. 1-9

Recommended Citation
Adkins, Gary. "Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism." *Journal of Strategic Security* 6, no. 3 Suppl. (2013): 1-9.

Red Teaming the Red Team: Utilizing Cyber Espionage to Combat Terrorism

Gary Adkins

Introduction

The world has effectively exited the Industrial Age and is firmly planted in the Information Age. Global communication at the speed of light has become a great asset to both businesses and private citizens. However, there is a dark side to the age we live in as it allows terrorist groups to communicate, plan, fund, recruit, and spread their message to the world. Given the relative anonymity the Internet provides, many law enforcement and security agencies investigations are hindered in not only locating would be terrorists but also in disrupting their operations. Furthermore, law enforcement tracking capabilities are limited as the Internet's loosely-knit group of computers and routers that are spread globally with servers hosting files, forums, and chat rooms are usually located in various countries' jurisdictions. Meanwhile a website can easily be backed up and moved to another server in another country beginning the process over again. Legal obstacles also make it very difficult to seize files or listen in on communications. What if a diverse group of hackers were allowed to do what hackers do best and infiltrate not only the servers themselves but use them to spider into the terrorist's computers and even cell phones? What information might be uncovered?

Take a moment and think of the trove of information that resides on your laptop and cell phone. A quick list might include banking information, tax forms, family pictures, self-portraits, a picture of your new car. Banking information might be in the form of cookies stored on your computer when you visit the website. Tax forms, while not advisable, do reside on many hard drives. Pictures might seem benign but besides the fact that they can be used to identify someone modern cameras and cell phones contain metadata in their files such as a Global Positioning Satellites (GPS) location of any given picture taken. This sort of data was brought to the public's attention in 2010 when Adam Savage, from Myth Buster, took a picture of his Toyota Land Cruiser with his iPhone in front of his house and posted it on Twitter stating it was time to go to work.[1] The GPS tagging feature was enabled and not only gave away exactly where his house was but what kind of car he drove and when he leaves for work. In 2003 due to a bug in Photo Shop, TechTV's Cat Schwartz inadvertently exposed herself to the world when she posted a cropped photo of herself on her blog which contained Exchangeable Image File (EXIF) data which held the nude photo.[2] Metadata is not only contained in picture files but also files such as Word documents which tend to save changes made to the file using the quick save feature. These examples are of normal people living normal lives but what kind of data might be residing in a terrorist's computer?

[1] Kate Murphy, "Web Photos That Reveal Secrets, Like Where You Live," New York Times, August 11, 2010, available at: *http://www.nytimes.com/2010/08/12/technology/personaltech/12basics.html?_r=0.*
[2] Sue Chastain, "TechTV's Cat Shwartz Exposed: Is Photoshop To Blame?," About.com Guide, July 26, 2003, available at: *http://graphicssoft.about.com/b/2003/07/26/techtvs-cat-schwartz-exposed-is-photoshop-to-blame.htm..*

Terrorist's Use of Technology

Terrorism has entered the phase called New Terrorism which is mostly decentralized and non-state sponsored. Most of the major terrorist threats can be grouped in what is called the Religious Wave of terrorism, which started in the 1990's, it is based on religious ideals to justify terrorist activities.[3] Given the global and decentralized nature of terrorist groups they have begun leveraging technology such as the Internet, cell phones, and software for various activities.[4] There are many websites dedicated to various terrorist groups.[5] The Institute for Security Technology Studies has identified five ways terrorists use the web: propaganda, recruitment and training, fundraising, communication, and targeting.[6]

Propaganda

The Internet has dramatically changed how terrorist groups can spread their propaganda to the world. Previously, terrorist groups would have to rely on news outlets reporting their message to the world after a terrorist act in which the news outlet could report as much or as little of it as they wanted interjecting their own views and skewing the message.[7] Now terrorist groups can easily post the message in its entirety on their own website and include any rebuttal to opposing views which not only allows them to post their message in its entirety but also allows for two way dialog increasing the effectiveness of the message.[8] Terrorist groups can easily portray themselves as victims seeking a peaceful resolution who were forced into acts of violence as a last resort.[9] Besides normal messages of propaganda al-Qaeda offers a library services which holds over 3,000 books and monographs from "respected jihadi thinkers" which can be easily downloaded to cell phones.[10] Websites also host videos of successful attacks against American targets in places like Iraq creating jihadi heroes such as the "'Bagdad Sniper' and the 'Sniper of Fallujah'."[11]

Recruitment

Recruitment used to be accomplished through interpersonal relationships but with the Internet the terrorists groups are no longer bound by geography and can not only reach but recruit

[3] Richards, Julian, *The Art and Science of Intelligence Analysis* (New York: Oxford University Press Inc., 2010): 57.
[4] Gabriel Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," Haifa University, 2011, available at: *http://95.211.138.23/wp-content/uploads/2012/08/2012-Terrorists-using-online-social-nerworking.pdf*, 11.
[5] Maura Conway, "Reality bytes: Cyberterrorism and terrorist 'use' of the Internet," First Monday 7:11 (Nov 2002): 4.
[6] Hsinchun Chen, "Uncovering the Dark Web: A Case Study of Jihad on the Web," Journal of the American Society for Information Science and Technology 59:8 (June 2008): 1348.
[7] Carsten Bockstette, "Jihadist Terrorist Use of Strategic Communication Management Techniques," European Center for Security Studies 20 (Dec 2008): 12-13.
[8] Michele Zanini and Sean Edwards, "The Networking of Terror in the Information Age," John Arguilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), 41-42; Evan Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," Testimony before the House Committee on Homeland Security, Dec 6, 2011, 7.
[9] Freiburger, Tina and Jeffrey Crane, "A Systematic Examination of Terrorist Use of the Internet," International Journal of Cyber Criminology 2:1 (Jan 2008): 314.
[10] Jarret Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 30 Fletcher F. World Affairs 149. (2006): 153.
[11] Ibid, 155.

https://scholarcommons.usf.edu/jss/vol6/iss5/3
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.1

individuals from anywhere in the world.[12] Websites can easily be customized to reach out and recruit specific audiences.[13] Second generation immigrants whom are unfamiliar of their families' country of origin and do not quite fit in with others in their current country may turn to the Internet in search of a community to belong to people with similar problems, a susceptible target for terrorist recruiters.[14] Terrorist organizations even start planting the seeds of their ideology in the minds of children with video games, available for download on the Internet, centered on defending the world against infidel invaders of various sorts and creating a "global Islamic caliphate."[15] Terrorist supporters create "educational" cartoons such as al-Qaeda in the Arabian Peninsula (AQAP) to capture the minds of children and young people to follow in the steps of jihadi fighters.[16]

Training

Training new recruits no longer requires entering a Middle Eastern country and attending a terrorist boot camp. By leveraging technology terrorist groups are able to train recruits much like many distance learning classes offered by universities and professional training companies.[17] Many websites offer information and videos on physical training, bomb making, and kidnapping.[18] Examples are *The Terrorist Handbook* which teaches bomb making techniques or *The Mujahadeen Poisons Handbook* which teaches how to create homemade poisons and poisonous gases.[19] Message boards and chat rooms also provide a way for would be terrorists to receive instructions on bomb making by simply posting their question and receiving instructions from an expert.[20]

Fundraising

Terrorist groups raise funds in many different ways on the Internet. One way is they directly ask for funds to be donated for their jihad, this is the method favored by the Sunni extremist group Hizb al-Tahrir which has a plethora of websites with banking account information to send donations.[21] Other groups such as al-Qaeda and Hamas use charities and Non-Governmental Organizations (NGOs) such as the Global Relief Foundation and the Holy Land Foundation for Relief and Development to funnel money to them.[22] They will also sometimes sell goods through

[12] Bockstette, "Jihadist Terrorist Use of Strategic Communication Management Techniques," 14.
[13] Zanini, "The Networking of Terror in the Information Age," 43.
[14] Freiburger,"A Systematic Examination of Terrorist Use of the Internet," 313.
[15] Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 156-157.
[16] SITE, "Jihadist Announces Forthcoming AQAP Cartoon," available at: *http://news.siteintelgroup.com/free-featured-articles/904-jihadist-announces-forthcoming-aqap-cartoon*.
[17] Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 153-154.
[18] Freiburger,"A Systematic Examination of Terrorist Use of the Internet," 315; Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," 8.
[19] Gabriel Weimann, "www.terror.net How Modern Terrorism Uses the Internet," United States Institute of Peace, Special Report 116 (March 2004): 9.
[20] Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 2-3; Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 9.
[21] Ibid, 7; Chen, "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1348; Dorothy Denning, "Terror's Web: How the Internet Is Transforming Terrorism," Yvonne Jewkes and Majid Yar, *Handbook on Internet Crime* (New York, NY: Willan Publishing, 2010), 19.
[22] Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 8; Michael Whine, "Cyberspace – A New Medium for Communication, Command, and Control by Extremists," Studies in Conflict & Terrorism 22 (1999): 238.

their websites to raise funds.[23] Other means include illegal activities such as credit card fraud and identity theft.[24]

Communication

Much like the rest of the world terrorists use technology such as the Internet, email, and encryption software to instantly and securely communicate around the global.[25] Web forums such as ones used by al-Ansar, an al-Qaeda affiliate group, are used as a "matchmaking service" to coordinate new militants for the front lines in Iraq.[26] Twitter, and to some extent Facebook, are used to plan and coordinate activities and ideas.[27] Paltalk, a voice and video chat room software that can be loaded on computers and cell phones, has been used for recruitment and planning.[28] Email and email groups, such as Yahoo! eGroups, are also extensively used.[29] Encryption software can, and has, been employed by terrorists to secure many of these communications. For email, web boards, and social networking sites terrorist have used PGP (Pretty Good Privacy) or their own variants such as al-Qaeda's Mujahideen Secrets to encrypt messages.[30] To encrypt voice communications PGPfone is described as being able to create "virtual STU-III devices."[31]

Targeting

The Internet can also provide a wealth of information for planning attacks on targets.[32] Secretary of Defense Donald Rumsfeld described an al-Qaeda training manual as stating "Using public sources openly and without illegal means, it is possible to gather at least 80 percent of all information required about the enemy."[33] The aftermath of the 2008 attacks in Mumbai showed how the Lashkar-e-Taibas used GPS and Google Maps to coordinate their beach landing, by passing security forces and gaining access to India.[34] Information on public buildings or nuclear

[23] Qin, Jialun, and Yilu Zhou, "A multi-region empirical study on the internet presence of global extremist organizations," Information Systems Frontiers 13:1 (Mar 2011): 2.
[24] Chen, "Uncovering the Dark Web: A Case Study of Jihad on the Web," 1348; Dorothy Denning, "Terror's Web: How the Internet Is Transforming Terrorism," 19; Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," 117.
[25] Denning, "Terror's Web: How the Internet Is Transforming Terrorism," 1.
[26] Ibid, 14.
[27] Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 3-6; Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," 5, 10.
[28] Brachman, "High-Tech Terror: Al-Qaeda's Use of New Technology," 156; Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 3-4; Qin, "A multi-region empirical study on the internet presence of global extremist organizations," 1.
[29] Weimann, "Al Qaeda Has Sent You A Friend Request: Terrorists Using Online Social Networking," 4; Kohlmann, "The Antisocial Network: Countering the Use of Online Social Networking Technologies by Foreign Terrorist Organizations," 7; Lachow, Irving and Courtney Richardson, "Terrorist Use of the Internet: The Real Story," Joint Force Quarterly 45:2 (2007): 100-102; , "High-Tech Terror: Al-Qaeda's Use of New Technology," 150-152, 156; Denning, "Terror's Web: How the Internet Is Transforming Terrorism," 8, 20.
[30] Ibid, 21; "The Networking of Terror in the Information Age," 37.
[31] Lachow, "Terrorist Use of the Internet: The Real Story," 9
[32] Timothy Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," Parameters 33:1 (Spring 2003): 112.
[33] Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 7.
[34] Bockstette, "Jihadist Terrorist Use of Strategic Communication Management Techniques," 15.

https://scholarcommons.usf.edu/jss/vol6/iss5/3
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.1

power plants can easily be found with a click of a button.[35] Web searches for news articles can easily show weak links in the Transportation Security Administration's (TSA) airport security net.[36]

Cyber Espionage in the Wild

There are many cases of cyber espionage that will never be known, after all the whole point of espionage is to never be detected. Fortunately there have been a few cases of cyber espionage that have not only been discovered but also reported and in some cases analyzed. A few of the well-known ones are: GhostNet, Titan Rain, Operation Aurora, and Red October. These examples are by no means an exhaustive list but are some of the major cases that have been reported widely in the media.

GhostNet

Between June 2008 and March 2009 the Information Warfare Monitor conducted an extensive investigation into the GhostNet infections.[37] GhostNet targeted the Tibetan community and was most likely perpetrated by China, direct attribution of attacks in cyber space is extremely hard to obtain.[38] Given the target and that 70 percent of the control servers had Internet Protocol (IP) addresses that were assigned to China it is a safe bet that China was behind it.[39] Second the operators responsible for GhostNet seemed to all be emanating out of Hainan Island in China.[40] Another reason this attack can be attributed to China is during the investigation a young woman, and member of Drewla which is a Tibetan outreach program, was arrested on the Nepalese-Tibetan border when returning to her family in Tibet; She was interrogated for two months by Chinese intelligence who produced complete transcripts of her Internet chats over the years when she denied being politically active.[41]

GhostNet utilized the Ghost Remote Access Tool (RAT) Trojan enabling the attackers to control the computer in real time, searching for and downloading files, logging keystrokes, and silently enabling attached devices such as microphones and web cameras.[42] The first known infection of GhostNet was found to be on May 22, 2007.[43] As of the investigation GhostNet had infected 1,295 computers spread out over 103 countries; 30 percent of these infections were considered high value targets in many different country's ministry of foreign affairs, news agencies, banks, unclassified computer systems in North Atlantic Treaty Organization (NATO) headquarters, and in the Office of His Holiness the Dahlia Lama (OHHDL).[44] The main attack vector of choice was social engineering by using a spoofed email from an address like "campaigns@freetibet.org"

---

[35] Weimann, "www.terror.net How Modern Terrorism Uses the Internet," 7.
[36] Thomas, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'," 114.
[37] Deibert, Ron, and Rafal Rohozinski, "Tracking GhostNet: Investigating a Cyber Espionage Network," Information Warfare Monitor (March 2009): 14.
[38] Ibid 52.
[39] Ibid 22.
[40] Bryan Krekel, "Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation," The US-China Economic and Security Review Commission (Oct 2009), available at: *http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA509000*: 74.
[41] Deibert "Tracking GhostNet: Investigating a Cyber Espionage Network," 28.
[42] Ibid 5.
[43] Ibid 44.
[44] Ibid 5.

with a believable body and attached word document titled "Translation of the Freedom Movement ID Book for Tibetans in Exile" which once opened it would infect the computer with the Ghost RAT Trojan; in many of the cases the attachment was a legitimate document stolen from previous infections.[45] The study showed that only eleven of the thirty-four antivirus tools at Virus Total, a website you can upload suspicious files to and uses multiple antivirus tools to scan it, were able to detect the malicious code embedded in the attachments giving the attackers a high probability of not being noticed.[46] The attack seemed to be after strategic intelligence regarding the Tibetan movement gathering intelligence from both activists and in the OHHDL which held schedules for meetings with world leaders and time-sensitive communications.[47]

Titan Rain

Titan Rain was the name given to a series of cyber-attacks that concentrated on breaking into various U.S. government and contractor computer networks.[48] It appears these attacks started as defacement attacks in early 2001 with the Code Red and Lion Worm.[49] These early attacks were very noisy, and easily detectable, posing more of an annoyance than a real threat.[50] Where things got interesting was in 2003 when Shawn Carpenter, a network security analyst at Sandia National Laboratory (SNL), investigated a series of intrusions at Lockheed Martin and noticed a few months later that very similar attacks started happening at SNL.[51] While working in Counterintelligence (CI) for the Federal Bureau of Investigations (FBI), Carpenter was able to trace the attackers back to the Guangdong province in China before being told to stop his investigation.[52] The attackers were very hard to trace since they hid stolen data on the hard drive of the target before bouncing the data to various servers and before bringing them back to mainland China.[53] These attacks continued through 2006 compromising systems of the U.S. Army Information Engineering Command, Defense Information Systems Agency, U.S. Army Space and Strategic Command, Army Aviation and Missile Command, Department of Energy, Homeland Security, State Department, and Naval War College.[54] In 2006, Major General William Lord acknowledged that China had downloaded between ten and twenty terabytes of data from the Department of Defense (DoD) non-classified Internet Protocol Router Network (NIPRNet) which holds sensitive but non-classified data.[55]

Operation Aurora

Unfortunately not much has been written in the academic circles about Operation Aurora, most of the available sources are from media reports, but it is an important case none the less. Google first discovered the Operation Aurora malware in December 2009 announcing its discovery in

[45] Ibid 18.
[46] Ibid.
[47] Ibid 22.
[48] Ibid 11.
[49] Aaron Shelmire, "The Chinese Cyber Attacks formerly known as Titan Rain," *Information Warfare* 95 (2008): 2.
[50] Ibid.
[51] Nathan Thornburgh, "The Invasion of the Chinese Cyberspies," *Time Magazine* (Aug 29, 2005), available at: *http://www.time.com/time/magazine/article/0,9171,1098961,00.html.*
[52] Ibid.
[53] Shelmire, "The Chinese Cyber Attacks formerly known as Titan Rain," 3.
[54] Ibid 3-4.
[55] Ibid 4.

https://scholarcommons.usf.edu/jss/vol6/iss5/3
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.1

January 2010.[56] Adobe announced a few days later that it had also discovered the malware.[57] Security researches from iDefense announced they had discovered that thirty-three additional companies were also hit.[58] The attack used a zero-day exploit in Adobe's Acrobat reader to infect their targets.[59] An investigation by HBGary discovered that the malware had been in development since 2006.[60] So far there have been no reports as to when the malware was first used. The malware used several levels of obfuscation including encryption, up to three times, to hide itself from normal detection.[61] The main purpose of the attacks seemed to be to steal intellectual property from the various companies.[62] Google announced that during their investigation they found that dozens of Chinese human rights activists' accounts from users based in China, the U.S., and Europe were routinely breached; however, these may or may not be part of the Aurora attacks.[63]

Red October

In October of 2012 Kaspersky Lab's Global Research & Analysis Team discovered Red October, a sophisticated cyber espionage campaign originating out of Eastern Europe.[64] The earliest known attacks started in May 2007 but there are indications that they may have started earlier.[65] The main targets were various diplomatic, scientific research, and government agencies spanning over forty-two countries and more than 300 unique systems.[66] The attack was deployed in two major stages consisting of the initial infection and then deploying additional modules to gather intelligence.[67] A unique aspect of the Red October attacks is that it didn't just target normal computers but also smart phones and networking hardware such as Cisco switches and routers.[68] Kaspersky Labs have not finished their investigation into Red October so there is no information about specific data that was targeted, yet.

Utilizing Cyber Espionage

As illustrated above, terrorists have a very big presence in cyberspace which is a big enough attack surface to exploit. Cyber espionage campaigns such as Red October, Operation Aurora, Titan Rain, and in particular GhostNet show us that cyber espionage is not just theoretical but

[56] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired Magazine, January 14, 2010, available at: *http://www.wired.com/threatlevel/2010/01/operation-aurora/.*
[57] Ibid.
[58] Kim Zetter, "Google Hackers Targeted Source Code of More Than 30 Companies," Wired Magazine, January 13, 2010, available at: *http://www.wired.com/threatlevel/2010/01/google-hack-attack/.*
[59] Ibid.
[60] HBGary White Paper, "Operation Aurora," HBGary Threat Report, February 10, 2010, available at: *http://hbgary.com/attachments/WhitePaper%20HBGary%20Threat%20Report,%20Operation%20Aurora.pdf.*
[61] Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show."
[62] Steve Ragan, "Was Operation Aurora really just a conventional attack?" *The Tech Herald*, January 27, 2010, available at: *http://www.thetechherald.com/articles/Was-Operation-Aurora-really-just-a-conventional-attack/9124/.*
[63] Graham Cluley, "Google, China, Censorship and Hacking," Naked Security, January 14, 2010, available at: *http://nakedsecurity.sophos.com/2010/01/14/google-china-censorship-hacking/.*
[64] Kaspersky Labs, "'Red October' Diplomatic Cyber Attacks Investigation," *Secure List*, January 14, 2013, available at: *http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation.*
[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Ibid.

practical. To create a viable cyber espionage campaign to combat terrorism a number of things will have to happen. A team of hacking specialists will need to be assembled; equipment will need to be ordered to support the team; and an attack plan to include attack philosophy will need to be created.

The Team

High on the list of team members is the penetration specialist, known in the industry as penetration testers. Penetration testers are usually hired by companies to hack into their network to discover holes in their security; as a part of the team they would scan sites for vulnerabilities and implement the attacks. Social engineers would also be a key part of the team; they deal with hacking the human brain. Social engineers not only conduct spear phishing campaigns but specialize in getting sensitive information from people without their knowledge. Reverse engineering specialists would be used to reverse current malware to use in future attacks but also to find security holes that can be leveraged in any software that the targets might be using. Intrusion detection specialists would be used to make sure any malware and backdoors will go undetected, both in the attack phase and during the time target is compromised. Finally, language specialist will be needed because sooner or later the terrorist's native language will need to be used.

The Equipment

To support the team a number different equipment will need to be purchased. First the team will need desktops to complete work ranging from launching attacks to translating communications. Servers will need to be built for password file breaking; this ranges from brute force attacks to hosting rainbow tables which are precompiled password hashes that speed up the process of password recovery. The bulk of the cost for the equipment will come from the penetration lab. The importance of the penetration lab is to test out attacks before putting them in practice to make sure they not only work but do not just crash the target's computer thus tipping your hand. The penetration lab will need to consist of various desktops, laptops, servers, cell phones, and tablets. The lab will also be utilized by the intrusion detection specialist to make sure that attacks are not picked up by virus scanners and intrusion detection/prevention systems.

Attack Philosophy

Terrorists are unlikely to have access to network security analysts, such as Shawn Carpenter, to discover new infections and track down their source. The team will have to worry about off the shelf software and honeypots. Avoidance of detection by off the shelf software will be handled by the intrusion detection specialist. The main route of discovery will be honeypots which are computers connected to the Internet without any firewall protection that mimics various security vulnerabilities then allows itself to become infected and captures the attack's binary in a sandbox to be reversed engineered. Honeypots are how antivirus companies are able to create signatures for most malware to update their virus definitions allowing consumers of their products to scan for infections. If a virus scanner does not have a signature for an exploit it is essentially invisible to it which is why honeypots would be dangerous to team. To combat this, spreading of the attacks via automation should be kept to a minimum so that only the primary targets, and not just targets of opportunity, are attacked.

https://scholarcommons.usf.edu/jss/vol6/iss5/3
DOI: http://dx.doi.org/10.5038/1944-0472.6.3S.1

It will be important to not only keep detection unlikely during the initial attack but also make sure that detection is unlikely in the future and if they are detected that attribution as to who attacked them is made impossible. To make attribution as difficult as it can be the attackers connection should be bounced through random proxy servers to connect to a Command and Control server (C&C). The C&C will be used for downloading files and instructions after the initial infection. Similarly to a C&C attacks should be conducted outside servers or previously infected computers. To ensure that detection of any compromised computers is kept to a minimum once the intrusion detection specialist finds that an infection is discoverable the C&C server should give commands to all infected hosts to download new, and undetectable modules, then erase the compromised modules.

While the terrorist organization's web presence is the primary target the individual terrorist's desktop, laptop, cell phone, or tablet is the end game. Valuable intelligence can and should be gathered from the message boards, chat rooms, and various sites but will pale in comparison to the intelligence that can be gathered from the terrorist's personal devices. Desktops and laptops can have access to the user's emails, photos, and contact information stored in databases. If a key logger is installed, interception of encrypted communications can be achieved before the encryption takes place. Connected devices, such as microphones and web cameras, can also be activated without the user being aware. The terrorist might also attempt to hide their location by using proxy servers when visiting websites but if the computer is infected their rough location can be derived by getting their IP address given to them by their Internet service provider (ISP). Cell phones and tablets would also be a great asset to exploit because they generally hold contact information, email access, photos, and text messages. Many of the devices also have GPS chips which can be used to not only locate the terrorists but also track their movements within a few feet of accuracy. Most tables and some newer cell phones also come equipped with forward and rear facing cameras which can always be exploited.

Conclusion

Terrorist have an exploitable attack surface thanks to their web presence. Cyber espionage has a relatively low entry cost and is very low risk. The chances of being detected are very small and if they are somehow detected attribution is almost impossible. The point of attribution is illustrated very well in the above examples of cyber espionage; sure many of the attacks are thought to be of Chinese origin but direct proof is still lacking. Cyber espionage will not only be able to deliver high intelligence gains but also be able to get around the issue of transnational cooperation that plagues law enforcement.