CYBERCRIME, CYBERESPIONAGE, AND CYBERSABOTAGE: UNDERSTANDING EMERGING THREATS

NADAV MORAG, PHD
UNIVERSITY DEAN,
COLLEGE OF SECURITY STUDIES

Colorado Technical University

In February of this year, Homeland Security Secretary Jeh Johnson noted that cybersecurity is one of the most important missions of the Department of Homeland Security*. Indeed, as the country and the global community become more dependent on computers and computer networks, America's adversaries, whether nation-states, criminals, or terrorists, will increasingly seek to exploit vulnerabilities in US computer networks in order to undermine America's economy and national security. In this context, there are three categories of threats that will be of increasing concern: cyberespionage, cybercrime, and cybersabotage. Let us look at each of them separately.

*www.dhs.gov/news/2014/02/12/remarks-secretary-homeland-security-jeh-johnson-white-house-cybersecurity-framework

CYBERESPIONAGE

Cyberespionage represents the strategy of breaking into computer systems and networks in order to extract sensitive governmental or corporate information. As with other forms of espionage, the goal is to better understand rival countries' capabilities and intentions or, in the case of industrial espionage, to gain access to proprietary corporate information to understand a rival company's business strategy or to steal its intellectual property.

Foreign attempts to penetrate US government and corporate websites and computer networks occur on a regular basis. One example of this was a Russian attempt in November 2008 to access the Department of Defense's classified computer network (SIPRNET – Secure Internet Protocol Router Network), which is not accessible from the Internet or other computer networks, via leaving infected thumb drives outside Department of Defense facilities. In at least one case, a DoD employee took one of the thumb drives and used it to access the Department's non-classified network (NIPRNET), thus opening that network to Russian penetration.

Many governments understand that modern dependence on computer networks make attacking those networks a priority not only to obtain information about an adversary's capabilities and intentions, but also to disrupt an adversary's ability to function during a conflict. The essence of warfare, after all, is to disrupt and ultimately end an enemy's capacity to fight, and this requires, in the past as well as the present, disrupting the enemy's command and control as well as the enemy's economic capacity to continue to wage war. During the Second World War, for example, the United States engaged in strategic bombing campaigns against Germany and Japan with the intent of destroying factories, road and rail networks, and other centers of economic activity, in order to destroy those countries' ability to wage war.

One of the differences between that type of strategic warfare and the kind that exists today is that this sort of disruption, via disrupting computers and computer networks, can occur under the surface, even when two countries are not actually in an overt state of warfare. Moreover, this type of activity can be waged not only by governments, but also by private citizen hackers working on their own or at the behest of the government – similar to the way in which citizens become guerrilla fighters (known as "partisans," in World War II). In a report leaked in back in 1996, it was clear that the Chinese were already thinking about this sort of cyber-guerrilla warfare at that time and viewed information warfare as something that the public could also engage in.

The Chinese have been particularly active in state-based hacking and, in fact, in May of this year, the FBI took the unprecedented step of identifying and indicting five Chinese military officers for hacking activities[1]. All in all, according to a study commissioned by the telecommunications company Verizon, nearly half of cyberespionage attacks were traced back to east Asia with the majority coming from China and Korea. The report also suggested that some 85 percent of hackers were government-backed[2].

While many foreign governments routinely attack US government and corporate computer systems in order to find vulnerabilities and exfiltrate data, overt conflicts could lead to a shift from this sort of activity to attacks against computer networks in order to cause them to fail, thus disrupting America's ability to maintain economic activity and the functioning of government. The Chinese are well-known for not wanting to invest in huge amounts of expensive military hardware (such as numbers of carrier groups to challenges the US Navy's supremacy in the Pacific) but rather to focus on cheaper ways of denying the US the ability to effectively confront China militarily, particularly near its waters and borders (this is known as Area Denial[3]). One of the ways of doing this is through massive cyber attacks. Consequently, those responsible for cyber defense in the government and corporate world will need to be aware of certain regional flashpoints that could result in a Chinese decision to "up the ante" in terms of cyber attacks, particularly with the objective of disruption. These include tensions around disputes over seabed and land ownership in the South China Sea, any attempt by Taiwan to declare independence or otherwise

[1] www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s

[2] www.cnbc.com/id/101605470#

[3] www.heritage.org/research/reports/2014/07/the-us-needs-an-integrated-approach-to-counter-chinas-anti-accessarea-denial-strategy

move significantly away from its claim to be a part of China, tensions with Japan over the ownership of islands in the Pacific, and tensions on the Korean Peninsula that could convince China to intervene on the side of North Korea.While China is certainly a concern, Russia is also very active as a cyber threat and changes in balance of power in the Ukraine, including a strong NATO response in the event that the Russians decide to grab even larger swaths of the country, could unleash a massive Russian cyber attack on the United States. In 2007, cyber attacks (possibly at least partially on the part of private Russian citizens) against Estonia lead to the temporary shut-down of Estonia's Internet-based governmental functions, as well as disruptions in economic activity[4].

North Korea also represents a threat. It has reportedly trained thousands of students to act as cyberwarriors and North Korea has been implicated in distributed denial of service attacks against South Korea in 2009, 2011, and 2013[5].

Finally, Iran represents a threat of significant proportions. In 2013, Iranian government hackers reportedly infiltrated Navy and Marine Corps computer networks and have been blamed for attacking Saudi Arabia's national energy company and the supplier of about ten percent of the world's oil, Saudi Aramco, erasing data from some 30,000 computers[6]. A scenario in which the US, or Israel, attack one or more of the facilities implicated in Iran's nuclear weapons program, could result in a massive cyber attack campaign against both countries' governments and corporate sectors.

[4] www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/#.VDr7wPldV8E
[5] www.foxnews.com/tech/2014/02/14/cyberwar-experts-question-north-korea-cyber-capabilities/
[6] www.complex.foreignpolicy.com/posts/2014/02/18/forget_china_iran_s_hackers_are_america_s_newest_cyber_threat

CYBERCRIME

Cybercrime is, of course, also an area of growing concern. Criminal hackers, that is, those motivated primarily by economic gain through illegal penetration of computer networks, no longer generally fit the stereotype of the twenty-something computer science graduate living in his parent's basement. Most significant cybercrime today is carried out by organized criminal enterprises. According to a report by cybersecurity company McAfee, cybercrime is thought to cost the global economy some $445 billion annually of which the US share is a loss of approximately $100 billion per year, which could translate into as many as 200,000 people losing their jobs due to cybercrime[7]. Cybercrime appears to be partially supplanting traditional forms of crime. For example, according to FBI data, bank robberies have been decreasing since 2008 while cybercrime has been increasing during the same period of time. This should not be surprising as cybercrime is considerably safer than bank robbery and the perpetrator has a far greater chance of avoiding arrest and prosecution. Cybercrime falls into a variety of categories including several types of fraud, sale in contraband and counterfeit items, and scams.

Cybercrime is attractive, in part, because it is often hard to investigate and prosecute. Cybercriminals exploit jurisdictional boundaries - a cybercriminal may be based in one country, use a server in another country, and defraud victims in yet another country, meaning that the suspect, the evidence, and the victim, may all fall under different national jurisdictions, legal systems, and enforcement and investigative agencies. This makes for tremendous challenges in coordinating a multi-national law enforcement response and dealing with very different legal frameworks and restrictions. Effective cybercriminals also enjoy a high degree of anonymity, manipulating the Internet and other computer networks to hide their identity and location thus making it difficult to identify and convict criminals. According to the FBI's 2010 Internet Crime Report, 303,809 complaints of criminal activity resulted in only 1,420 criminal cases being prepared and these resulted in only six convictions (one criminal in prison for every 50,635 victims). Given this reality, cybercrime, more often than not, does pay[8].

Additional problems that further stymie law enforcement attempts to investigate and prosecute cybercriminals include the underreporting of cyber crimes (many companies fear the negative publicity that could be generated by reporting breaches), the absence of law enforcement expertise in cybercrime investigation, and, in some cases, inadequate laws, both domestically and internationally, for coping with cybercrime.

[7] www.csis.org/files/attachments/140609_McAfee_PDF.pdf
[8] www.infoworld.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html

CYBERSABOTAGE

While the term "cyberterrorism" has been used somewhat frequently, it is, in my view, difficult to argue that there have been any cases, thus far, of terrorists killing people (or effectively threatening to do so) via computer networks. However, terrorists, nation-states, and criminals can decide to try and disrupt and destroy computer networks via cybersabotage. Consequently, I would argue that "cyber sabotage" is a more effective way to think about the issue.

This is not to suggest that people cannot be killed due to impacting computer networks. In 2009, due to human error, 75 people lost their lives at the Shushenskaya Dam in Siberia, because a computer operator hit the wrong keys thus turning on an unused turbine leading to a buildup of pressure that caused the floor to cave in and flooding to commence. While this was not a case of sabotage, conscious efforts to cause disruptions in critical infrastructure facilities or other locations could result in the kind of damage that could threaten workers, not to mention cause millions of dollars in damage and disrupt the operations of power plants, dams, etc.

In the recent past, we have seen attacks by hackers designed to disrupt websites and economic activity on the part of groups or individuals trying to achieve a political agenda - such groups and individuals are known as Hacktivists. The pro-regime Syrian Electronic Army, has been implicated in the defacement of government and press websites, including that of Forbes magazine[9]. Also, the hacktivist collective known as Anonymous has been involved in online attacks against government and organizations such as the Church of Scientology. Anonymous is a particularly interesting organization. It is what is known as a flat organization, lacking any clear hierarchy, and it is made up of individuals or cells that sometimes work as part of Anonymous, when they identify with its goals, and sometimes do not. Anonymous's attacks occur when an issue raised motivates hacktivists to swarm (create informal partnerships in order to take down websites or engage in other means of sabotage).

The Internet in general, and social media websites in particular, are often used by terrorists to propagandize, radicalize and recruit, fundraise, share information, and provide training and skills. The rise in the use of Improvised Explosive Devices (IEDs) in a number of different theaters of counterterrorism activity (including Iraq, Syria, Lebanon, Gaza, Chechnya, and Afghanistan) has been attributed, at least in part, to the sharing of information on IEDs, their construction, and their use, via the Internet. Some of the approximately one hundred Americans (and thousands of Europeans) recruited to fight in Syria for the Islamic State or the Syrian Al-Qaeda affiliate, Jabhat al-Nusra, are thought to have been radicalized on the Internet[10].

[9] www.forbes.com/sites/andygreenberg/2014/02/20/how-the-syrian-electronic-army-hacked-us-a-detailed-timeline/

[10] www.bbc.com/news/world-us-canada-28958980

RISKS AND VULNERABILITIES

Given the aforementioned threats, those charged with protecting computer systems are faced with a daunting challenge. Ultimately, the goals of computer security can be summed up with the acronym CIA – Confidentiality, Integrity, and Availability. Cyber Defenders need to try and ensure the highest degree of confidentiality (to keep data private), integrity (to try and ensure systems have not been altered by unauthorized persons), and availability (to try and ensure that systems are accessible to users). One hundred percent success is unlikely, given the quantity and scope of cyber attacks, and consequently governments and the private sector must decide what constitutes risk, where they should put their defensive resources, and how much disruption they can tolerate.

Computer systems are vulnerable to six types of risk: 1) risks due to Information Technology (hardware, software, people, processes), 2) risks due to interconnection with outside parties and providers (banks, other companies, etc.), 3) risks due to outside suppliers (cloud providers, subcontractors, etc.), 4) risks due to disruptions in IT equipment and logistics, 5) disruptive new technologies (such as the emerging Internet of Things, and 6) threats to upstream infrastructure (power supply, water supply, etc.)[11].

As the world moves towards embedding computer systems into various types of hardware (aka the Internet of Things) the vulnerabilities will increase exponentially. For example, the embedding of sensors in clothing may allow tracking of individuals, the use of wireless pacemakers may allow the disruption of a patient's cardiac rhythms, and the increasing use of augmented and virtual reality may allow cyber attackers to cause psychological harm.

Other evolving threat areas include disrupting the growing cloud infrastructure, physical attacks against server farms and internet exchanges, the use of data mining for criminal intelligence, the creation of false augmented realities for fraud and social engineering, hijacking unmanned vehicles (drones, self-driving cars, etc.), and even avatar hijacking.

Critical infrastructures are particularly vital in terms of thinking about cyberattacks because disrupting these infrastructures will have far-reaching economic and social effects. The Department of Homeland Security has identified 16 critical infrastructure sectors including the energy and power sector, the water sector, the information and telecommunications sector, transportation, banking and finance, and others.[12] Not all the sectors are created equally because a disruption in first tier infrastructures, such as the energy and power sector, will disrupt second tier infrastructures (such as transportation or banking and finance), and disruptions in these will in turn disrupt third tier infrastructures (such as the agriculture and food sector or the emergency services sector).

Consequently, creating greater equities in the more critical assets, in terms of defense against cyber attacks, makes more sense. Network Analysis can be a useful tool for determining where significant vulnerabilities lie and where assets should be placed. In any system, there will be critical nodes (networks, hardware, software, etc.) on which multiple systems depend and other assets may be less critical because they are not vital nodes. In principle then, one should allocate 80 percent of the resources on 20 percent of the assets, after having identified the critical nodes in the system that are vital for the continued functioning of the enterprise.[13]

[11] Atlantic Council and Zurich Insurance Company, Beyond Data Breaches: Executive Summary (Washington, D.C. and Zurich: 2014), p. 2.
[12] www.dhs.gov/critical-infrastructure-sectors
[13] See Ted G. Lewis, Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation (Hoboken, NJ: Wiley and Sons, 2006

PREPARING FOR THREATS

In addition to understanding the nature of the threats and conducting analyses of system weaknesses, Red Teaming can also be a useful technique for uncovering vulnerabilities and determining how to address them. Effective Red Teaming requires trying to understand reality from an adversary's perspective…in other words, trying to think like the enemy. This technique is regularly used by government agencies and can be very helpful for the private sector. Cyber Red Teams can be used to continually try to breach a company's computer systems in order to identify vulnerabilities and help design strategies to overcome these…including vulnerabilities having to do with human nature.

While computer hardware, software, and communications systems all have vulnerabilities that can be exploited by skilled and determined cyber spies, criminals, and hacktivists, one of the greatest vulnerabilities in any computer network are the humans who have access to the system. Humans, of course, can be manipulated and, indeed, are manipulated by spies, criminals, and hackers. It is imperative therefore that personnel who have access to critical cyber systems be trained in how to recognize and avoid being manipulated.

Elicitation is a well-known technique for extracting information that can be effectively used by people who pose a cyber threat. An individual trying to elicit information from an employee with access to computer networks will try to exploit natural tendencies in most people to be polite and helpful, to appear well-informed, to feel appreciated, to show off, to gossip, to correct errors made by others, to believe others are honest, and to be truthful. Spies, criminals, and hacktivists can exploit these tendencies through using elicitation techniques such as:

1 **ASSUMED KNOWLEDGE:** Pretend to have knowledge or associations in common with a person. "According to the computer network guys I used to work with…"

2 **BRACKETING:** Provide a high and low estimate in order to entice a more specific number. "I assume rates will have to go up soon. I'd guess between five and 15 dollars." Response: "Probably around seven dollars."

3 **CAN YOU TOP THIS?** Tell an extreme story in hopes the person will want to top it. "I heard Company M is developing an amazing new product that is capable of …"

4 **CONFIDENTIAL BAIT:** Pretend to divulge confidential information in hopes of receiving confidential information in return. "Just between you and me…" "Off the record…"

5 **CRITICISM:** Criticize an individual or organization in which the person has an interest in hopes the person will disclose information during a defense. "How did your company get that contract? Everybody knows Company B has better engineers for that type of work."

6 **DELIBERATE FALSE STATEMENTS / DENIAL OF THE OBVIOUS:** Say something wrong in the hopes that the person will correct your statement with true information. "Everybody knows that process won't work—it's just a DARPA dream project that will never get off the ground."

7 **FEIGNED IGNORANCE:** Pretend to be ignorant of a topic in order to exploit the person's tendency to educate. "I'm new to this field and could use all the help I can get." "How does this thing work?"

PREPARING FOR THREATS (CONTINUED)

8 **FLATTERY:** Use praise to coax a person into providing information. “I bet you were the key person in designing this new product.”

9 **GOOD LISTENER:** Exploit the instinct to complain or brag, by listening patiently and validating the person’s feelings (whether positive or negative). If a person feels they have someone to confide in, he/she may share more information.

10 **THE LEADING QUESTION:** Ask a question to which the answer is “yes” or “no,” but which contains at least one presumption. “Did you work with integrated systems testing before you left that company?” (As opposed to: “What were your responsibilities at your prior job?”)

11 **MACRO TO MICRO:** Start a conversation on the macro level, and then gradually guide the person toward the topic of actual interest. Start talking about the economy, then government spending, then potential defense budget cuts, then “what will happen to your X program if there are budget cuts?” A good elicitor will then reverse the process taking the conversation back to macro topics.

12 **MUTUAL INTEREST:** Suggest you are similar to a person based on shared interests, hobbies, or experiences, as a way to obtain information or build a rapport before soliciting information. “Your brother served in the Iraq war? So did mine. Which unit was your brother with?”

13 **OBLIQUE REFERENCE:** Discuss one topic that may provide insight into a different topic. A question about the catering of a work party may actually be an attempt to understand the type of access outside vendors have to the facility.

14 **OPPOSITION/FEIGNED INCREDULITY:** Indicate disbelief or opposition in order to prompt a person to offer information in defense of their position. “There’s no way you could design and produce this that fast!” “That’s good in theory, but…”

15 **PROVOCATIVE STATEMENT:** Entice the person to direct a question toward you, in order to set up the rest of the conversation. “I could kick myself for not taking that job offer.” Response: “Why didn’t you?” Since the other person is asking the question, it makes your part in the subsequent conversation more innocuous.

16 **QUESTIONNAIRES AND SURVEYS:** State a benign purpose for the survey. Surround a few questions you want answered with other logical questions. Or use a survey merely to get people to agree to talk with you.

17 **QUOTE REPORTED FACTS:** Reference real or false information so the person believes that bit of information is in the public domain. “Will you comment on reports that your company is laying off employees?” “Did you read how analysts predict…”[14]

[14] For more information, see the FBI webpage on elicitation techniques: http://www.fbi.gov/about-us/investigate/counterintelligence/elicitation-techniques

PREPARING FOR THREATS (CONTINUED)

While employees with access to secure networks are all vulnerable, to one degree or another, to manipulation, Insider Threats often represent the most insidious and potentially impactful human threats. Employees can constitute Insider Threats if they decide to actively work with foreign intelligence agencies, cybercriminal organizations, or hacktivists, to leak data or sabotage systems, or both. Witness the tremendous damage done to the United States intelligence community and the broader US government due to the willful leaking of sensitive information by Bradley Manning and Edward Snowden. Snowden, in particular, as a contractor for the National Security Agency, used his role as an IT specialist to fraudulently obtain passwords of co-workers at the NSA and then hack into systems to download thousands of classified documents on US intelligence-gathering operations, thus causing incalculable harm to America's national security efforts.

Individuals that constitute an Insider Threat can be motivated by money, ideology, a sense of disgruntlement, a vulnerability to blackmail, or personal problems of various kinds. Given the potentially catastrophic damage that a person who is an Insider Threat can cause, it makes sense for government agencies and companies to monitor employees, particularly those with access to vital computer networks, in order to spot unauthorized behavior and other anomalies. These kinds of behaviors could include poor security of passwords and documents, querying of matters outside the employee's "need to know," working odd hours without authorization, unnecessarily copying materials, sending emails to unauthorized persons from a work computer, fear of being investigated, excessive personal contacts with competitors, career disappointments, or life crises.

Agencies and companies can also sometimes inadvertently magnify the potential damage that can be caused by Insider Threats through not controlling access to protected materials and systems, not adequately protecting proprietary information, having undefined computer security policies, creating a perception of lax security, and the absence of training on security protocols.

CONCLUSION

Ultimately, the nature of cyber threats, whether in the form of cyberespionage, cybercrime, or cybersabotage, is such that government agencies and companies must realize that they can never achieve 100 percent success and security. The key then, is understanding the threats (and when they might peak), understanding risks and vulnerabilities, knowing how to prepare and what to look for in terms of network-based, as well as human factors that can impact the vulnerability and security of the nation's computer networks.

CTU cannot guarantee employment or salary. 4435 North Chestnut Street. Colorado Springs, CO 80907. 852-0806281 0806296 10/14