CHAPTER

9

Computer Network Exploitation

INFORMATION IN THIS CHAPTER

- Intelligence and Counter-Intelligence
- Reconnaissance
- Surveillance

The term Computer Network Exploitation (CNE) is a cyber warfare term of military origin, and one that may be slightly confusing to those that are not on the inside of the environment. Although we might be tempted to think that the "exploit" in CNE refers to exploits used against systems in order to gain privileges or remote shells on them, this is not the case. In actuality, exploit in this case refers to the ability to exploit the data or information gathered on our target for our own purposes. Officially defined, CNE is "Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks" [1] Such operations are the cyber equivalent of good old-fashioned spying or espionage. CNE is the phase of cyber warfare that we are experiencing globally at this point. We commonly see cyber intelligence, reconnaissance, and surveillance (ISR) activities taking place, but we do not yet commonly see outright cyber attacks between nation-states.

Although such intelligence gathering activities are a standard part of warfare and of the normal conduct of government, in the cyber world, the mechanisms that allow such activities to be conducted can be a bit easier to carry out than they are in the physical world. When we store our darkest secrets on computer systems that are connected, however indirectly, to the global Internet, we leave a pathway open for skilled attackers to access this information.

Even when such sensitive information is not directly available, we can imply a great deal of information by examining systems and networks, even from the outside, in preparation for future attacks. Such items of intelligence, for the purposes of cyber warfare can allow us to plan attacks, perhaps down to the point of specific vulnerabilities that can be exploited on individual systems.

Cyber Warfare, *Second Edition*
http://dx.doi.org/10.1016/B978-0-12-416672-1.00009-X

Using some of the tools that we discussed in Chapter 6, we can begin to construct a very specific picture of our target environment, in preparation for Computer Network Attack (CNA), or even as a basis to plan refinements to our Computer Network Defense (CND) strategies. We will discuss CNA further in Chapter 10 and CND in more depth in Chapter 11.

INTELLIGENCE AND COUNTER-INTELLIGENCE

Identifying who exactly the enemy is for purposes of CNE can be a bit of a tricky proposition. In the virtual world, when we refer to an enemy or threat, we may actually be referring to what are really the second- or third-order effects of the actual activity of our enemy. In other words, when we see a Distributed Denial of Service (DDoS) attack coming from a group of machines in China, it is important to understand that the Chinese may not be related to the attack at all, other than in the sense of being an endpoint. To truly identify the enemy, we need to look at the targets, sources, attackers, and sponsors of the activity that we are monitoring.

Sources of Cyber Attacks

Attack sources can be a bit of a vague notion in the world of logical attacks. In this particular case, we use the term source to indicate the endpoint from which the actual attack arrived. For example, systems in China are frequently theorized to be used as a stepping stone to attack other systems. Although such a system certainly can seem to be the actual source of the attack, this may not be the case at all, due to the relative ease of compromising a system and using it as a proxy to attack another target. In fact many times both nation-states and criminals will route their attacks through countries that will not cooperate with an investigation. We can generally classify attacks as either direct attacks or proxy attacks.

Direct attacks, as they sound, are attacks conducted directly from the system that is directly controlled by the attacker, i.e., the attacker is not attached to the system remotely from another system. Although direct attacks certainly have the benefit of not spreading the route that the attacker is taking out over a series of potentially unstable connections, they do nothing to disguise the origin of the attacks.

Depending on where a direct attack is originating from, being able to trace the origin of the attack may or may not cause problems for the attacker. In many countries, a serious attack reported to an Internet Service Provider (ISP) may result in the connection that the attacker is using to be shut down. Additionally, an attacker working directly from their own system runs the risk of the target retaliating against and disabling the attacking system, or worse yet, retrieving information regarding the attacker.

Proxy attacks, those attacks that are run through one or more intervening systems, are a safer type of attack to use from the standpoint of disguising attribution. Although using a single machine as a proxy for an attack may not provide much in the way of indirection to keep the actual attacker from being discovered, this protection increases greatly with each additional step along the way. By the time an attacker has proxied through several machines, each located in a different geographical area, the attacker has created a virtual morass of networks, system, and legal structures to hide behind.

On the other side of the proxy attack situation, a consideration is also the potential set of technical issues caused by connecting through a series of systems. An attacker has not only potential technical and stability problems with the network connections and systems that they are utilizing, but with each additional layer that an attacker has in place, the attacker greatly increases the chances that the administrators or users of the system will notice the unusual activity and that the attacker will be detected.

Attackers and Sponsors of Attacks

As we discussed in Chapter 2, we will see threats from a variety of angles, and from many different types of attackers. We can generally categorize these groups into state and nonstate actors, i.e., those that do and do not have the sponsorship of, or act directly on behalf of a nation-state and those that do.

Most nation-states, and the parties that they sponsor directly, have certain sets of laws that they are generally bound to follow when conducting warfare, including warfare of a cyber variety. Although how exactly these laws apply to cyber warfare is still being sorted out, we will discuss them at some length in Chapters 12 and 13.

Additionally, we may see attack from nongovernment sponsored organizations, or nonstate actors, such as corporations, political or activist organizations, criminal groups, individuals, or any combination or variation of these. We will discuss such attackers in considerably more detail in Chapter 12.

RECONNAISSANCE

Cyber reconnaissance can be divided into three major categories, Open Source Intelligence (OSINT), passive reconnaissance, and Advanced Persistent Threat (APT). Although these three methods of reconnaissance are, for the most part, diametrically opposed, they all have their place in cyber warfare. An attacker often will want to start with the use of OSINT to gather as much information as they can without directly indicating their interest, then proceed to passive reconnaissance when they need to gather more specific information that they have not been able to gain through the passive route.

Open Source Intelligence

OSINT involves the use of methods that are designed to not alert a target to the fact that they are under observation. Many of the tools that we discussed in the reconnaissance tools section of Chapter 6 fall squarely into this category. Investigating Domain Name System (DNS) information, Google hacking, information gathered from websites, investigation of document metadata, and other similar methods can all be excellent means of executing OSINT operations, as long as they are careful to not expose their interests in the process of conducting them. In OSINT they will likely start with public information, then job-related information, then Google hacking, then DNS information, then metadata gathering, as shown

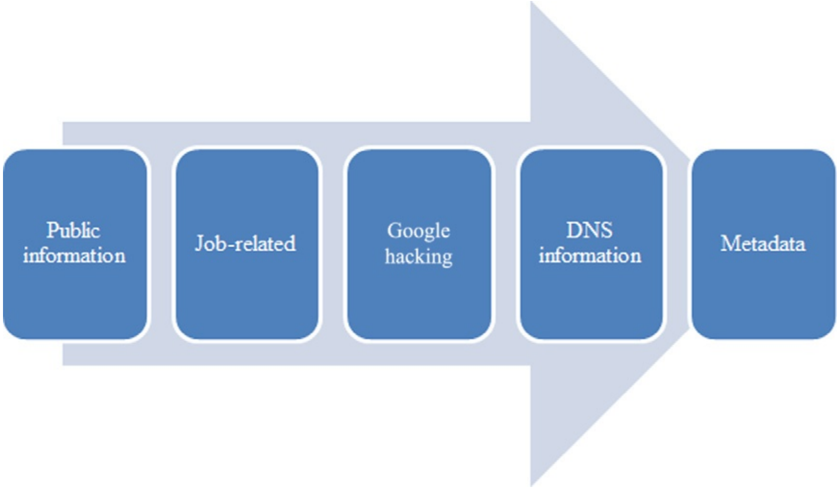

FIGURE 9.1 OSINT process.

in Figure 9.1. When conducting reconnaissance against a target the attacker will generally start with OSINT, and then move to passive.

Primarily, when taking an OSINT approach to reconnaissance, an attacker will want to use information sources that do not leak information about our interests, or at least minimize such leakage. For instance, although they may use a public web-based whois query tool to conduct research against a target, the administrators of such an application may find it interesting that the IP address block of a known government contract organization had a suddenly high level of interest in the DNS information of systems related to the Chinese government. In such cases, it is often best to use a network masking technology such as The Onion Router (Tor) and to spread such queries out over many different sources.

TIP

Tor, which can be found at www.torproject.org, is a tool that provides network anonymization by routing the traffic from a client through a variety of intermediate systems and out through one of many possible endpoints. Although Tor does indeed provide some measure of protection against a target or application being able to trace back the source of the network traffic in question, there are several attacks and configuration issues, including endpoints set up specifically to sniff traffic, that may make it possible to do exactly this.

To a certain extent, attackers can also use some network monitoring techniques for OSINT purposes. Although attackers are very limited in what they can do for sniffing on a wireless network when bound by the requirement of stealth, there are packet sniffing tools that are entirely passive in nature and are very difficult to detect without taking specific measures to do so.

NOTE

The battle between passive network sniffers and the systems that can pick them out is an ongoing one. As we note, if we put a passive sniffer on the network, it is difficult to detect, but we can do so with a properly configured Intrusion Detection System (IDS). We can also adjust our sniffers to avoid such IDSs, and tune our IDSs to ferret out such avoidance measures, and so on ad infinitum.

There are also network sniffing tools that work through induction rather than direct interface with the network that are, in theory, truly impossible to detect without physically finding the inductive tap itself [2]. Even fiber optic cables, often considered to not be passively tappable, in fact are exactly that. Low cost devices are available to read the light leakage through the jacket of a fiber cable without actually needing to cut it to insert a tap [3].

Additionally, we can eavesdrop on wireless network traffic in relative safety, as long as we are careful not to interact with the network itself. Even encrypted wireless traffic can reveal information about the devices that are connecting to it and, based off names and Media Access Control (MAC) addresses of such devices, we can often infer quite a bit of information about the environment.

A technique that we cannot discount in cyber warfare scenarios is that of passive physical observation, which is part of Human Intelligence, or HUMINT. Such techniques, as they generally require, at least at some point, the physical presence of an observer, do have the opportunity to alert the target in question that they are being watched, but when carried out carefully can be invaluable. Physical observations of traffic patterns at facilities, movement of vendors, arrival of equipment, and other similar factors can allow us to infer much about the goings on at our target location. We discussed this and some of the other intelligence gathering methods in more depth in Chapter 2.

Passive Reconnaissance

Passive reconnaissance takes more direct steps to extract information on our target environment that OSINT does, but is passive in relation to our actual target. A good example of an attack being passive relative to the specific target might be compromising a router used by the target, then disrupting or degrading other paths in order to channel packets to the compromised router where we might more easily eavesdrop on the traffic. In such a case, we have altered the environment to aid in our reconnaissance, but have not touched the target itself.

Passive reconnaissance will often involve many of the tools that we discussed in Chapter 6 that involve directly interrogating a network or system, in order to discover its particulars. Passive reconnaissance will often be, as we discussed, the next step after OSINT gathering and may be partially based on the information gathered during that activity. During passive reconnaissance, an attacker may unintentionally expose information to a target from the nodes that are active in these tasks. In this way passive reconnaissance may differ greatly in cyber warfare activity than in penetration testing.

In penetration testing, presuming that we are performing it in the recommended and legal fashion, we have permission to attack the target environment, and any attempt to gain information from our attacking systems is likely to be short lived and shallow, at best. We will also

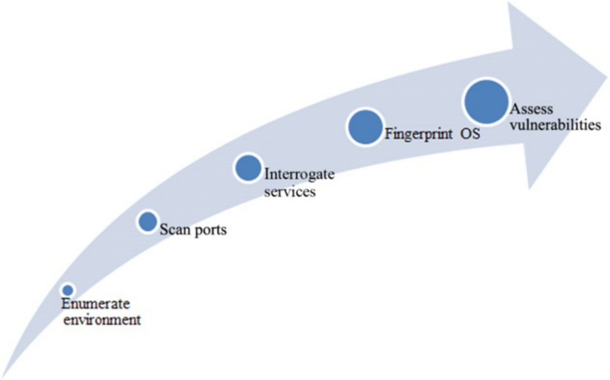

FIGURE 9.2 Passive reconnaissance process.

be unlikely to see any attempt at counter-attack or retaliation in such a scenario. In a true cyber warfare or cyber conflict, these are situations that we are likely to run into, and should take into account when planning. We can mitigate the likelihood of being noticed in our activities and, to a certain extent, retaliatory efforts by ensuring that our reconnaissance tasks are carried out from a variety of different sources, preferably from separated network blocks, at the very least, if not from geographically disparate locations. We can also mask such activities by performing them in a fashion that spreads them out over a much longer period of time that what we would normally examine when attempting to detect such attacks.

In the tools that we are likely to see used in passive reconnaissance, we will find various scanning tools, such as network sniffers for both wired and wireless networks, port scanners, vulnerability analysis tools, operating system fingerprinting tools, banner grabbing tools, and other similar utilities. We will be looking to enumerate the infrastructure devices, networks, and systems in place in the environment; assess the ports open and services operating on those ports; fingerprint operating systems; and assess vulnerabilities, as shown in Figure 9.2. This process is certainly not set in stone and is intended as a general guideline. There will be times when a chain of interesting information will lead us to one step sooner than another and there is absolutely nothing wrong with varying the approach.

We will often find our future actions or attacks will enjoy a much greater degree of success if we take the time to carefully document the information discovered regarding the specifics of our target environment. This documentation will not only ease the planning of future attacks or more detailed reconnaissance, but will also ensure that all of those involved in the operation are working from the same set of information. It is also important to keep this documentation up to date as new information is gained, or as changes in the environment are noted.

SURVEILLANCE

The major difference between reconnaissance and surveillance is that reconnaissance tends to imply a single observation of a given environment, whereas surveillance implies an ongoing observation [4]. It is certainly true that any of the tools and methods that we have discussed for conducting reconnaissance could be used in an ongoing manner as surveillance tools, and indeed some of them are, though extended operation of such tools would result in a very high likelihood of being discovered. Some of the same general techniques are still useful, but can be adapted to more long-term eavesdropping on communications of voice and data, or emissions into the electromagnetic spectrum.

Justifications for Surveillance

Although we can certainly justify the use of reconnaissance in advance of an attack, surveillance as a long-term measure is an entirely different case. Constant surveillance of voice and data communications implies the insertion of hardware, software, or both into the target environment in order to report the desired data out to a location from where it can be retrieved. In the case of surveillance being conducted by a nation-state, most countries are subject to various laws and treaties, both international and domestic, which strictly regulate such practices. In this case, any surveillance that is conducted is considered an act of espionage, which, although frowned upon, is still practiced by modern nations around the world, even allies.

WARNING

Conducting surveillance is fairly universally regulated by one or more wiretap laws in most countries around the globe. In most cases, conducting surveillance without following very specific rules, even on privately owned systems, may very well violate such laws and result in stiff penalties. In cases where such surveillance is required, consulting legal advice beforehand is strongly advised.

There is also the consideration that the target of surveillance may be internal to our nation or organization. Such cases are certainly more common in recent years, largely as a result of several large terrorist attacks having taken place. In the face of such activities, governments can often make a case, sometimes without consulting the public in the matter, for ongoing surveillance. Such programs are often implemented in the name of combating terrorism, drug trafficking, and other similar situations. Although there are also commonly laws that regulate domestic surveillance, such laws are not always followed to the letter, and in fact, are sometimes bent in the name of the public good. We will discuss some of these issues in greater depth later in this section.

Advanced Persistent Threat

Advanced Persistent Threat (APT) actors make use of organized and long-term attacks, designed specifically to access and exfiltrate information from the target systems and imply a more active role in gathering information than any that we have discussed previously. APT operations are more direct, and may have more in common with the CNA process that we will discuss in this chapter, closely matching some of the activities, but differing somewhat in intent and motivation. In APT, the steps that we might take are attack, escalate, and exfiltrate.

Attack activities in APT are motivated by getting us onto the system in order to extract the intelligence that is our main goal. Although an outright and obvious attack is certainly not necessarily out of scope here, this may not be conducive to our intelligence gathering activities. In this case, we may want to slowly and carefully infiltrate the system in order to pass unnoticed as we attack. A good example of this might be to use a client-side attack or low-impact custom malware to enter the environment quietly.

Once we have compromised the target system in order to gain access, we may need to escalate our access level in order to gain the desired information. As we are conducting an APT operation, we will likely be concerned more with gaining just enough access to carry out our task than we will be with owning the entire system. In some cases, if our attack phase has been very successful, we may be able to directly access the system with the credentials that we need, and not need to take this additional step.

Once we are on the system and we have the appropriate level of access, we will need to exfiltrate our target information. Depending on the system and the environment in question, there are a wide variety of ways we might be able to carry this out. In many commercial environments, we will often find several commonly open channels to the outside world. It may be possible to exfiltrate our data over such a channel by doing something along the lines of moving data over port 80 along with the normally large load of web traffic. In areas with higher levels of security, we may need to be more creative in our exfiltration attempts, and perhaps use an out of band method to communicate our data to the outside world one bit at a time. In either case, it may pay to move our data quietly and slowly so we do not burn the system as a source of information if we think that we might want to return again in the future.

Voice Surveillance

On voice communication systems built on older analog technologies, conducting voice surveillance was literally a matter of wiring a device into the phone line at some point, called a wire tap. As we move forward into newer systems, such tasks become increasingly easier to carry out and easier to execute from a distance as well, but we continue to use the same term. In digital phone systems, such surveillance may be as easy as activating a feature in the systems controlling the voice traffic for a particular location, rendering a once manual task into a few clicks in an administrative tool.

In recent years, Voice over IP (VoIP) traffic has begun to make large inroads toward replacing the common telephone service as the standard for voice-based communications. For those that intend to conduct surveillance on such communications, this is actually good thing, as VoIP traffic is considerably easier to eavesdrop on from a distance, and, depending on the implementation may have considerably less inherent security.

In essence, eavesdropping on unencrypted VoIP conversations, which may include many commercial and consumer services, is just a matter of having access to the network traffic in order to apply a sniffing device. Both sides of a voice conversation can be recorded in this manner and can easily be decoded and played back using a tool such as Wireshark or Cain and Abel, both of which have a simple point-and-click interface which will play back an audio version of the conversation in a given packet capture file.

Data Surveillance

Data surveillance is a longer term, and often more pervasive, version of some of the tools and techniques that we have discussed in the reconnaissance sections of this chapter and

Chapter 6. Data surveillance is often conducted by monitoring infrastructure devices that have been permanently or semipermanently installed with the express purpose of listening to the traffic going over the network or networks in question.

In smaller scale installations, such as those that we might find in a corporation wishing to conduct such surveillance, this is often carried out through the installation of specialized surveillance devices, such as those produced by NIKSUN, at key areas in the network infrastructure. Such devices can allow traffic to be captured as it goes over the network in order to allow for later analysis of attacks, application usage, communications, and any number of network-oriented activities. Although such solutions work very well for small- to medium-scale monitoring, they do not scale well when we wish to monitor much larger sets of data, such as monitoring of traffic or traffic patterns for an entire nation. For such purposes, the organizations, generally governments, that wish to do so generally implement their own solutions or have solutions custom built for them.

Large-Scale Surveillance Programs

The U.S. government provides us with several good examples of government-scale surveillance systems. One of the earlier such attempts at enabling voice and data surveillance on a large scale was seen in Echelon. Echelon is the popular term used to refer to the network of signals intelligence collection and analysis operated by the parties to the U.S.-UK Security Agreement, namely, the United States, Canada, United Kingdom, Australia, and New Zealand. Echelon is large-scale eavesdropping on international voice traffic over satellite, phone networks, microwave links, and even data sources such as fax transmissions and email. The original intent of Echelon was to monitor the communications of the Soviet Union and the countries allied with it in the 1960s. At present, it is believed to be used for monitoring of activities more along the lines of terrorism and drug trafficking, as well as to collect general intelligence information.

The Carnivore program was implemented by the U.S. Federal Bureau of Investigation (FBI) in the late 1990s. Carnivore was a device that when attached at the ISP of the target intended to be monitored could filter out and record all traffic going to and from the target. Carnivore was not contextually aware and could only filter traffic by the sending and receiving destinations [5]. After much public controversy, the Carnivore program was abandoned in 2001, and commercial replacements were put in place [6].

Another attempt at large-scale data monitoring, once more from the FBI, was Magic Lantern, first publically disclosed in 2001 [7]. Magic Lantern worked on a somewhat different principle. The tactic for this application was to implement keystroke logging on a remote machine through the use of a Trojan horse or exploit delivered via email [8]. Once the target had successfully executed the email attachment bearing Magic Lantern, it would install and presumably begin to send logged data to a monitoring station. In 2002, the FBI confirmed the existence of Magic Lantern, but stated that it had never been deployed [9].

Einstein, as discussed in Chapter 1, is a government-oriented data surveillance program. It began in 2002 as a program to monitor the network gateways of the U.S. government for unauthorized traffic and intrusions [10]. Through several revisions it became a wider reaching program until in 2008, it became mandatory for federal agencies with the exception of the Department of Defense (DoD) and certain intelligence agencies. Although intended primarily as a measure to protect the systems of the U.S. government, Einstein also collects a nontrivial amount of data as it traverses these networks [10]. The main goal of Einstein is "to identify and characterize malicious network traffic to enhance cybersecurity analysis, situational awareness and security response" [11].

Perfect Citizen, as discussed in Chapter 1, is a National Security Agency (NSA) program, designed to detect vulnerabilities in both public and privately run critical infrastructure systems and networks [12]. Although not a mandatory program, significant incentives in the form of government contracts have been offered to those that are willing to participate. Concerns have been raised over government entry into monitoring of private companies, such as utility companies.

Uses of Surveillance Data

Aside from the direct uses of surveillance data, we can also, given a sufficient amount of data, use it as a basis for detecting patterns of behavior among those being surveilled. The U.S. government, and likely other governments as well, have been searching for exactly such patterns in voice and data communications for some time.

Since the terrorist attacks that took place on September 11, 2001, the U.S. government, more specifically the NSA, has been conducting pattern analysis on voice conversations in order to detect the patterns that might presage a terrorist attack [13]. Such technologies and the policies that govern their use are continually updating and evolving. Using these types of techniques, we can infer that certain patterns of voice traffic, for example, a call from a known terrorist friendly country to a location in the United States, then sequential calls from the number in the United States to six other numbers, may very well be an indicator of unusual activity. Of course, this assumes foreknowledge of which phone numbers to watch for such patterns occurring, or an extremely powerful computing capability, likely beyond what currently exists.

SUMMARY

In this chapter, we discussed the basics of CNE. As we covered, CNE is a military term that does not use the term exploit in the way that it is typically used in the information security community, but instead uses it in the sense of exploiting data that we have gained through reconnaissance or surveillance to our own good.

We covered identifying our targets, in the sense of both gleaning information from targets of attacks, and in the sense of identifying targets to be surveilled. We discussed potential sources for attacks, and how the endpoint of the attack may only be distantly related to the identity and location of the actual attacker. We also provided historical examples of surveillance programs.

We talked about reconnaissance and how it might be used to conduct planning operations for future attacks, including CNA and CND. We covered the three major divisions of reconnaissance, OSINT, passive, and APT and the differences between them.

Lastly, we went over surveillance. We talked about the difference between reconnaissance and surveillance, this largely being a matter of scale in both the sense of time and implementation. We talked about the justifications for conducting surveillance, as well as some of the particulars of voice and data surveillance. We also covered large-scale implementations of surveillance and went over some of the programs that have been used over the years by the U.S. government. We also discussed some of the uses of data collected through surveillance methods.

References

[1] Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, http://ra.defense.gov/documents/rtm/jp1_02.pdf; 2011 [accessed 05.05.13].

[2] Leong P. Ethernet 10/100/1000 copper taps, passive or active? lovemytool.com, http://www.lovemytool.com/blog/2007/10/copper-tap.html; 2007 [accessed 03.04.13].

[3] Olzak T. Protect your network against fiber hacks. IT security, http://www.techrepublic.com/blog/security/protect-your-network-against-fiber-hacks/222; 2007 [accessed 03.04.13].

[4] U.S. Marine Corps. Imagery intelligence. s.l.: U.S. Marine Corps; 2002. MCWP 2-15.4.

[5] Tschabitscher H. How carnivore email surveillance worked. About.com, http://email.about.com/od/staysecureandprivate/a/carnivore.htm; 2010 [accessed 03.04.13].

[6] Associated Press. FBI Ditches carnivore surveillance system. FoxNews.com, http://www.foxnews.com/story/0,2933,144809,00.html; 2005 [accessed 03.04.13].

[7] Bradner S. The FBI as an ethical hacker? NetworkWorld, http://www.networkworld.com/columnists/2009/042309bradner.html; 2009 [accessed 03.04.13].

[8] Sposato I. The FBI's magic lantern. WorldNetDaily, http://www.wnd.com/2001/11/11812/; 2001 [accessed 03.03.13].

[9] Hentoff N. The FBI's magic lantern. The Village Voice, http://www.villagevoice.com/2002-05-28/news/the-fbi-s-magic-lantern/; 2002 [accessed 03.03.13].

[10] Department of Homeland Security. Department of homeland security united states computer emergency readiness team. Privacy impact assessment EINSTEIN program. s.l.: Department of Homeland Security Department of Homeland Security United States Computer Emergency Readiness Team, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_eisntein.pdf; 2004 [accessed 03.04.13].

[11] US-CERT (United States Computer Emergency Readiness Team). Privacy Impact Assessment for the Initiative Three Exercise. s.l.: Department of Homeland Security; 2010.

[12] Gorman S. U.S. plans cyber shield for utilities, companies. The Wall Street J, http://online.wsj.com/article/SB10001424052748704545004575352983850463108.html [accessed 03.04.13].

[13] Singel R. Top secret: we're wiretapping you. Wired.com, http://www.wired.com/science/discoveries/news/2007/03/72811?currentPage=all; 2007 [accessed 03.04.13].