CHAPTER

12

Non-State Actors in Computer Network Operations

INFORMATION IN THIS CHAPTER

- Individual Actors
- Corporations
- Cyber Terrorism
- Organized Cyber Crime
- Autonomous Actors

We have spent a great deal of time discussing the activities of nation-states in cyber warfare. Nation-states have the advantage in warfare, cyber or otherwise, of being on the formally accepted legal and ethical side of things, as we will discuss in Chapters 13 and 14. They also have the potential advantages of having greater access to resources and materials. They do, however, have the considerable disadvantage of being bound by the rules and morals that are imposed on such entities and are to a great extent restricted in their actions.

Non-state actors, logically, are those that take actions of a cyber nature, but are not directly part of a nation-state. States may certainly directly or indirectly employ or support such agents, particularly when they wish their activities to be clandestine. Non-state actors may include, to name just a few, script kiddies, scammers, hacktivists, blackhat hackers, criminal organizations, or any of a number of other individuals or groups. We will talk about these actors more in this chapter.

Also under consideration when we look at non-state actors are the activities of terrorist groups. While such organizations once depended solely on physical activities, largely revolving around the use of explosives to destroy people and resources, they too have been able to make use of the tools of modern technology. Terrorists can now make use of systems and networks to not only plan and coordinate their attacks, but potentially to carry out the attacks themselves.

Many non-state actors rightly fit into the same category as any other cyber criminal. One possible exception in this group is the corporation. Although we would like to think that most

http://dx.doi.org/10.1016/B978-0-12-416672-1.00012-X

corporations generally follow the rules and regulations that bind such entities, we can see many illustrative examples in the media of this not being the case, the Enron scandal presenting an excellent example.[a] Corporations are, in many cases, entities with access to a great deal of resources and should certainly not be discounted as a factor in a cyber conflict.

Another category with the potential to carry out cyber operations to great effect are criminal organizations. Such groups not only have a great deal of resources with which to back cyber attacks on a large scale, but also have the organizational elements needed to manage them on such a scale as well. Criminal organizations can operate in a similar organizational manner to corporations, although they do not have the same compunctions to follow the rules, nor the same penalties for not doing so, and are often not bound by physical or national borders.

INDIVIDUAL ACTORS

In cyber warfare, many of the actions that we presently see taking place on a daily basis are presumed to not be the actions of nation-states, due to their potential conflict with the laws of war, as we will discuss further in Chapter 14. We see an innumerable host of small attacks: port scans, SQL injection attacks, cross-site scripting, and click fraud, as we discussed in Chapter 6, just to name a few. These activities are mainly the work of individuals and small groups who are acting to gain notoriety, steal Personally Identifiable Information (PII) to be used in identity theft, and even doing so just for the illicit thrill.

Such attackers range greatly in skill level, from the lowliest script kiddie who can only run automated tools, although often to great success, to the most highly skilled hacker, who can penetrate a system with disturbing ease and leave no trace for the owners of the system to detect. As with many professions, there are a great number of those operating at the lowest levels of skill, and only a rarefied few at the opposite end of the skill spectrum. As with ordinary criminals, those that are caught and prosecuted by law enforcement are often those that lack the skill to properly hide the traces of their activities, thus allowing them to be discovered.

As we covered briefly in the threatscape section of Chapter 2, the general list of non-state attackers can include actors such as script kiddies, malware authors, scammers, blackhats, hacktivists, and patriotic hackers. This is by no means an exhaustive list, but it does cover the main groups of such attackers. These groups are not mutually exclusive, and a given attacker may indeed fit in more than one group. Additionally, the terms used to describe such individuals or groups are rather arbitrary and tend to vary wildly from one source to another. A mapping of the terms used in this chapter to some of the alternative terms that may be used is presented in Table 12.1.

Script Kiddies

Script kiddies are often the least skilled, but most common, of the non-state attackers. The term script kiddie, often used in a derogatory sense, is used to describe someone of no

[a] http://www.time.com/time/2002/enron/

TABLE 12.1 Mapping of Terms for Non-State Actors

Terms Used in This Chapter	Alternative Terms
Script kiddies	Newb, hacker, cyber gang, criminal
Malware authors	Criminal, coder
Scammers	Criminal, phisher, identity thief
Blackhats	Hacker, hacker group, greyhat, cracker
Hacktivists	Environmental hacker, activist group
Patriot hackers	Political hacker, religious hacker, hacktivist

particular skill at attacking systems. Script kiddies generally use scripts and tools that have been written by others in order to conduct their attacks, but have no great skill or ability beyond the use of such tools. Even so, such attackers are often successful owing largely to the poor state of security in the systems being attacked and the very large number of Internet-facing systems that are available to be attacked. The large number of easy to use system penetration tools that are available also contributes to the sheer number of attacks that come from this set of attackers.

Malware Authors

Malware authors can be, but are not always, a very specialized type of attacker and may be independent or work for an organization. For those that actually write original items of malware, some certain amount of skill at programming and knowledge of the target operating systems is required. Such talented developers of malware are capable of developing the malware that botnets utilize, complex tools such as rootkits, and other similarly crafted tools.

The other source of malware, and the source of much of the malware that is loose in the wild, is in variations that are created from already existing sources. When we examine any item of common malware, we will likely find variants of it ranging into the dozens, if not far more. Often, the reason for so many variations of a particular item of malware existing is the use of malware creation kits. Such software packages allow malware to be created by choosing from a set of options allowing the user to vary delivery methods, payload, means of propagation, and other similar factors; the one from column A, one from column B, one from column C approach. Those that create malware using such tools are often grouped into the same category as script kiddies, as creating malware by such means requires no particular skill at programming. Again, as with the tools used by script kiddies, this renders them no less effective.

Scammers

Scammers are often considered to be the lowest of the low when it comes to attackers. They use many of the same techniques con artists have used for decades. The scammers that are

caught and discussed publically often do not have the technical skill with attack tools of even the worst of script kiddies, as they prefer other methods of gaining their target information. Such scammers instead use tools that are of a social engineering nature, such as phishing or pharming attacks, in order to trick their victims into willingly parting with the information that they wish to obtain.

NOTE

Scammers, like other criminals in general, are often largely represented in the public eye by the least skilled members of their profession. When law enforcement parades such people in front of the media after their arrests, it is easy for us to think that they are representative of the level of skill present among the entire group of people. It is good to bear in mind that the highly skilled scammer will be considerably more careful and subtle, and we may not even realize that anything has happened until after they are long gone.

The goal of scammers is to separate their unwitting victims, often those that are not technically savvy, from their PII, including names, addresses, social security numbers, financial data, and other such information. Given this information scammers will seek to drain the victim's bank accounts and run their credit cards up to the limit, often moving such funds out of the country where they cannot be recovered easily.

The motivations of scammers are almost universally financial in nature. Scammers exist to, in one fashion or another, separate their victims from whatever items of value that they might have. This might mean actual currency, information, physical objects, or any number of other means of storing value.

Blackhats

Blackhat hackers, often known simply by the term blackhats (think cowboy movies), are the bad guys of the hacker world. Such hackers often have no particular care for the rule of law, the systems that they disrupt, or what ill effects that they cause. Blackhats are distinguished from whitehats, the good guys, who are often found working to foil the efforts of the blackhats, and grayhats, who ride the line between the two, often crossing from one side to the other.

Identifying an attacker as a blackhat often implies that they possess a certain level of skill at attacking and exploiting systems and networks, at least in excess of the average script kiddie. Blackhats may attack a system or network with a variety of motivations in mind. They may be doing so just for the thrill of exploiting a system, may be after specific information on the system, may be using the system as a "pivot" to attack other systems on the same network, or any of a number of other reasons.

Hacktivists

Hacktivists are, in essence, hackers that use their skills to support a particular point of view. One relatively well-known work on the subject, *Hacktivism and the Future of Political*

Participation, defines hactivism as "the nonviolent use of illegal or legally ambiguous digital tools in pursuit of political ends" [1]. The tools of the hacktivist can include website defacement, mass emailing, Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, Domain Name Service (DNS) hijacking, or any of a number of other methods.

In February of 2010, a group known as Anonymous, well known for similar attacks, launched a DDoS attack against the website of an Australian senator, as well as the Australian Parliament House. Anonymous claimed to have launched the attack due to the attempts of the Australian government to introduce a mandatory Internet filtering service for the entire country [2].

The motivation of the hacktivist is almost entirely politically or religiously oriented in some fashion, and focused on influencing opinions on the particular issue in question. Causes that are supported by hacktivists can be nearly endless, but may include such topics as free speech, civil rights, religious rights, and so on. Nearly any issue that we can find supported or attacked by activist groups, protesters, and the like will have some element of hacktivist support, even if it is not an overt one.

Patriotic Hackers

Patriotic hackers may actually be reasonably argued to be a subset of hacktivists but are generally tied to national conflicts and can even join into cyber wars as independent players. They use many of the same tools and methods: Web site defacement, DDoS, attacks, and so on but generally act in support of a particular country, or an effort on the part of a country, although not in any officially sponsored sense.

There have also been occasions where such patriot hackers have been rumored to have actually been in the employ of a state and have been paid to carry out their activities. One such occasion in December of 2009 involved the theft and public posting of thousands of emails from the University of East Anglia Climatic research unit. It is believed that the patriot hackers involved in the incident were acting on behalf of Russia in order to discredit the need for reduction in carbon emissions to help fight global warming [3].

Patriot hackers will likely have many of the same motivations as hacktivists, although with a much more nationalistic focus. The activities of patriot hackers may additionally be of a somewhat more sharp and directed nature than those of a hacktivist.

CORPORATIONS

Large corporations can be possessors of great power and resources, often rivaling those of small countries. Corporations in the technical industry are often well organized, staffed with highly trained employees, and have access to the latest technologies and equipment, including those with which cyber warfare can be carried out.

Outside of organizations that are taking part in regular criminal activities, which we would define as organized criminal organizations and will discuss later in this chapter in the section on organized cyber crime, many corporations do not engage in overt cyber warfare activity. In general, we are more likely to find, with some exceptions, activities along the lines of

espionage and intelligence gathering, which we discussed in Chapter 9. There is a long tradition of organized commercial and industrial espionage in business and politics, dating back to at least the height of the ninja of Japan in the fourteenth century [4].

Motivation for Corporations to Act in Cyber Warfare

The activities of corporations acting in cyber conflicts can be broken down into two primary areas: legal actions and illegal actions. Corporations carrying out acts in support of cyber war in a legal fashion will typically be doing so in the employ of a nation-state. In the United States, we can see many examples of corporations performing such roles on behalf of the U.S. government. Large defense contractors such as Northrop Grumman, General Dynamics, Lockheed Martin, TASC, and Raytheon provide expertise and resources to the government, enabling it to carry out the required cyber activities [5]. Another set of companies that support these efforts are think tanks and Federally Funded Research and Development Centers (FFRDCs). In such situations, the cyber warfare activities of these corporations are allowed and legally blessed, and the corporations are well paid for their efforts.

On the other side of corporate activities, we could potentially find similar actions taking place without the legal authorization of the powers that be. In such cases, we might see any number of activities taking place to benefit the corporation. Depending on the country in which the corporation is operating, it may have great flexibility in the cyber operations that it is legally allowed to carry out. As we will discuss in Chapter 13 when we talk about legal issues, the laws regarding cyber warfare, hacking, espionage, and similar activities can vary greatly from one country to another. By strategically placing equipment, resources, and subsidiaries of the corporation in various countries, it may be possible for the corporation to take certain activities with relative impunity, as long as it is careful in matters of scale during such activities. Certain outright attacks might be sufficient to draw international attention and cause difficulty for the host country, which would likely not be desirable for the corporation.

CYBER TERRORISM

Cyber terrorists are a rather emotionally charged category of attacker, subject to much debate and discussion. Cyber terrorism has been defined as “a criminal act perpetrated by the use of computers and telecommunications capabilities, resulting in violence, destruction and/or disruption of services to create fear by causing confusion and uncertainty within a given population, with the goal of influencing a government or population to conform to a particular political, social, or ideological agenda” [6]. Ultimately cyber terrorism can surely be seen as being related to both hacktivists and patriotic hackers, differing largely in both the scale and the intensity of their actions.

Cyber terrorists, as with conventional terrorists, are likely to choose targets that are highly disruptive and publicly obvious. One of the commonly supposed targets for cyber terrorism is the many large-scale electrical grids that provide power in various countries. The 2003 blackout that we discussed in Chapter 7 was, at first, investigated for signs of terrorist activity due to the nature of the attack [7].

Reasons for Cyber Terrorist Attacks

The motivation of cyber terrorists, as with any other branch of terrorism, is ultimately to influence the victim or victims of the attack into a particular line of activity or thinking. Cyber terrorists are also much more likely to resort to attacks that cause large-scale damage or destruction than hacktivists or patriot hackers.

Supervisory Control and Data Acquisition (SCADA) systems are often considered to be a prime target for cyber terrorist attacks. As we discussed in Chapter 7, such systems are responsible for control and monitoring of many processes that make life in an industrialized world possible, such as the distribution of power, flow of oil, communications, and many others.

TIP

As we discussed in Chapter 6, there are tools on the market that allow SCADA systems to be tested from a security perspective to help mitigate such threats. Nessus, for instance, has a whole section in its professional feed dedicated to finding vulnerabilities in SCADA systems. Use the tools that are out there, security through obscurity is not good enough!

Due to the nature of such systems, it would be possible to cause great physical disruption or damage by manipulating the devices such SCADA systems control in order to cause them to fail or behave erratically. Given that the nature of terror attacks is to evoke feelings of unrest, anxiety, and others of a similar nature in the target populace, highly visible and highly effective targets such as these present a great source of opportunity to terrorists.

What will Happen When we see a Cyber Terrorist Attack?

As we have not seen, at the time of this writing, what would be considered a terrorist attack of a cyber nature, it is difficult to say exactly what will happen when one does occur, but we can speculate. If we look at the activities surrounding the 9/11 attack in the United States, we can see a quick series of activities that took place. We saw great changes in the intelligence apparatus of the government, some good, some bad, but all designed to collect and share information in manner that would obviate the stovepiping of intelligence that allowed the attack to go unmitigated. New laws and new powers were enacted to allow more and greater amounts of information to be collected to feed the intelligence agencies as well. In general, a great deal more monitoring was put in place in an attempt to halt future attacks of a similar nature.

We also saw a great deal of military build-up, some directly within the branches of the U.S. military, but a great deal within defense contractors as well. Much of this was in support of the conventional war that was swiftly taken to the area of the world that was deemed responsible for the attacks. Whether this was reasonable or effective is a matter of much debate and largely inconsequential to this discussion.

Within the borders of the United States, we saw greatly tightened security for a period of time, with armed soldiers standing in airports and places of public interest. Directly after the event, such controls were very tight for a period of time, but relaxed considerably as more

time passed without another large attack getting through. Generally, we saw a huge spike in security for a period of a year or two, then things relaxed but we can definitely still see some of the changes resulting from the attacks that were made permanent.

Given that response to a cyber terrorist attack is likely to be led by the same military thinking and leadership that responded to the last attack, it is fair to assume that the response will be of a similar nature. The 9/11 attack was a new attack, in both the sense of scale and technique, that the United States had not faced before and did not have hard experience in dealing with. Some mistakes were surely made in the process, but the end result was an overall heightened security posture in order to prevent a repeat of this type of attack and retaliatory action against those that we thought supported it.

In the cyber world, at present, our defenses are in a poor state to withstand such an attack. The virtual world has no borders to speak of, and, even if it did, the attack could very well come from within them, and we have no good way to prevent such a thing from happening. In the physical world, we can attempt to detect and prevent the entry of materials that might be used to cause mass casualties, but we have a considerably more difficult task in preventing the entry of or use of weapons of cyber terrorism. At present, our systems and defenses for dealing with such an attack are reactive only.

In the event of a large cyber terrorist attack, we would likely begin to see the development of borders and security in a virtual sense. This would be a difficult task indeed, due to the myriad of communications methods that can be used to move data in and out of a given country, and we would likely never be able to police them all, but it is something that could eventually be made to work, although with a great deal of pain being involved in the process. To say that the technical challenges involved in such an undertaking would be great and would be a massive understatement, but we would likely see an attempt made in such a direction.

A possible alternative would be to create a secure network for the specific use of critical infrastructure systems. Such a network could be considerably more restrictive than anything that needed to carry public traffic, as it would serve a more specialized set of needs. Although such a network, in and of itself, would not be technically challenging to create, standardizing the environments that might connect to it certainly would be. In addition, as with 9/11, we would likely see military action of a conventional warfare nature taken to the attacker if we could apply some sort of attribution to the source of the attack. While such attribution is very difficult to prove from a technical standpoint, when faced with a cyber terrorist attack that caused a great deal of physical damage, we would likely be able to track it back, to a certain extent, through the intelligence channels, presuming that it did come from a terrorist organization. Due to the nature of such organizations, such an attack is unlikely to be carried out without an increase in chatter, a term often used to describe the volume of communications among suspected or known terrorist organizations [8].

ORGANIZED CYBER CRIME

Although many of the different types of attackers that we have discussed in this chapter can clearly be considered cyber criminals, those that participate in organized crime can be considered to be in a different category entirely. Organized crime has existed since time immemorial, but cyber crime is a much more recent invention, and one that has been taken

up wholeheartedly by such organizations. Those involved in the efforts of organized crime make use of malware, DDoS attacks, identity theft, phishing, outright cyber warfare, and any number of other tactics that might be the means to the particular end they wish to accomplish.

When looking to obtain identities for fraudulent use, financial or otherwise (but largely financial), organized cyber criminals have begun to target the organizations where large amounts of such data are warehoused, often credit card processing centers and other financial institutions. In some cases, the same criminal organizations have been implicated in breaches spanning multiple companies. Such efforts prove to be extremely lucrative, with one Ukrainian criminal organization that had been taken down shown to have made $900 million in a single month [9].

Motivations for Criminal Organizations

The motivations of those in organized crime are twofold: money and power. Given the tools, cyber and otherwise, that are at their disposal, and the resources that they can bring to bear against an enemy, such organizations are truly to be reckoned with. Of all of the non-state actors that we have discussed in this chapter, organized criminals have the most potential to be on an even footing with a nation-state in the areas of resources and effectiveness.

Cyber criminals, in the course of their activities, often develop real world skills in penetrating the defenses of their targets. Some of these attackers, whose activities have later been uncovered, have been found to have been operating inside the networks and systems of their targets for extended periods of time without discovery. Evidence has also been shown regarding cooperation between cyber criminal organizations and coordination in selecting targets so as not to interfere with the activities of other such groups [9].

AUTONOMOUS ACTORS

Another type of actor that we are just beginning to see on any large scale is the autonomous actor. We presently see such actors almost entirely in the form of malware. When malware is released into the wild, or is disconnected from its command and control structure, certain forms of it will continue to carry out their functions independent of any outside control. This has been the case in a primitive sense since the very first pieces of malware were seen outside of controlled environments.

In cyber warfare, the speed of actions, whether offensive or defensive in nature, is limited only by the speed of the networks and systems on which they take place, and primarily by the speed of the networks. As both of these factors are, in most cases, no longer particularly limiting, this means that engagements in cyber warfare can take place at speeds far in excess of the capabilities of humans to keep pace, as long as said humans do not interject themselves in the process and slow it down with human speed monitoring, approvals, and other activities. We are already at a place where the defenses of our systems and networks, through the use of tools such as firewalls and Intrusion Prevention Systems (IPSs), are allowed to act in a largely autonomous fashion, with human oversight in the areas of monitoring and, in some cases, configuration.

Exploratory Systems

As we discussed in Chapter 9, the first step in the attack process is to gather intelligence on the systems against which we intend to pursue further action. We need to map out border devices and networks, fingerprint systems, and gather as much information on our targets as we can. At present, there are tools that serve such exploratory functions, such as the famous tool Nmap, although they generally do so with very heavy interaction with the user of the tool, and are not very adaptive to the information that is gathered as they move along through the mapping process.

A good example of a tool designed with an exploratory purpose in mind, implemented as an item of malware, is the infamous Morris worm. The Morris worm, one of the first worms ever created, was written in 1988 by a Cornell University student named Robert Morris. Morris created the worm as a tool to gauge the size of the Internet. He took steps to disguise its point of origin, and used flaws in sendmail, finger, and rsh, as well as a process to break weak passwords, in order to propagate it from one machine to another [10]. Ultimately, due to a flaw in the worm's design, the result of its propagation was actually a DoS attack against the infected machines. The Morris worm ended up infecting an estimated 6000 systems, about 10% of the systems on the Internet at that time [11].

The potential for autonomous exploration systems is great, from the standpoint of automating a somewhat laborious task, particularly for large networks, and freeing up resources for activities that require more direct human interaction. Of course, depending on how such tools were implemented, they also have the potential to go disastrously wrong, as did the Morris worm. Particularly during the intelligence gathering phase of a cyber warfare attack, accidentally launching a DoS attack on our target would certainly ruin an element of stealth or surprise that we hoped to gain by quietly mapping out the systems and networks of our opponents.

Attack Systems

At present there are a wide variety of attack tools that are available to those wishing to conduct cyber attacks, ranging widely in toolsets and utility. Some such tools, such as the Metasploit Framework, provide an excellent library of attacks, but only a certain level of automation, and surely not autonomy. Other tools (such as those that we discussed in Chapter 6) combine multiple different applications into tool chains in order to add some level of automation to the process. Although such tools are not usually autonomous we can presently see autonomous or semiautonomous examples of attacks tools that are already functioning.

Much of the malware that exists in the wild can be considered autonomous to a certain degree. Such tools are constructed with a certain goal in mind, whether this is simple replication, information retrieval, or any of a number of other goals, and let loose into the world. We have seen numerous examples of malware over the years that have been, at least briefly, successful enough to infect millions of machines in the process of carrying out their programming.

In addition to simple items of malware, we can also look at greater structures that are built using malware, called botnets. Botnets are networks of systems running malware that have been recruited without the authorization of the system owners and connected to command

and control networks that allow the systems to then be remotely operated en masse. Such botnets can consist of millions of machines, and can be used to conduct DDoS attacks, crack encryption, or almost any task that can benefit from the application of distributed computing. Botnets are generally under the direct control of their operators, but they are also certainly capable of carrying out their tasks without such interaction, presuming that they have been assigned some task to carry out. The malware that recruits new nodes into botnets will generally continue to spread and grow the network in size, even if no commands are being given to the machines.

In 2008 and 2009, the Conficker worm was a regular news item in security and malware circles. The worm, in a variety of revisions, ultimately infected machines in the millions, with estimates generally ranging between 5 and 10 million devices. Regardless of the variety of interesting attack, propagation, and defense measures that were used by the worm, one item of interest for many researchers was that the worm was also recruiting devices into a botnet. As we mentioned earlier, such botnets are generally in the control of an operator or set of operators, who use them for various tasks. In the case of the Conficker botnet, no such operator appeared to be guiding its actions. The botnet continued, through the propagation of the worm, to recruit new devices until it grew to be one of the largest botnets that had ever been recorded at the time. One of the later and more prevalent variants of the Conficker network, Conficker E, quietly self-destructed in May of 2009, taking the control connections to a large number of botnet nodes with it. While a number of theories abound as to the reason behind the apparent inactivity of this botnet and its later self-destruction, one possibility is that it was created as a proof of concept for a cyber weapon, and had simply served its purpose and was then deactivated. Other variants of Conficker still continue working as of this writing.

WARNING

Experimenting with automated attack or counterattack tools is likely to be a fairly dicey proposition, potentially leading to a trip to prison, even when we have the best intention. In many countries, such tools operating outside of a very controlled environment will likely violate a variety of laws. Additionally, autonomous tools, no matter how well crafted, will likely not be possessed of any great deal of judgment in whom exactly they choose to fire upon. Yes, these are cool ideas, but they have great potential to burn the wielder.

Autonomous attack systems have great potential to change the face of cyber warfare, as long as we are not terribly picky about the results. Such tools would, in theory, be an offshoot of malware, and would exist with the express purpose of attacking a particular target or targets. Although we can go to great lengths to ensure that we control and limit the attacks of such tools, this is an area in which there are many examples of bugs in existing malware. In addition, the botnets that are active in the world today do not demonstrate aggressive behaviors, instead waiting for the command of the botnet operators. If such tools were created for the express purpose of attack, there is no reason that they could not be made to be sneakier, carry out their own attacks, and generally operate without human guidance. We could potentially, after the release of such an autonomous tool, find ourselves on the receiving end of its attacks, unable to call it off.

Defensive Systems

As we mentioned earlier in this section, we are already at a place where we have defensive systems that verge on autonomy. When we look at the standard Intrusion Detection System (IDS) and IPS in combination, what we essentially have is a system that will, based on its configuration settings, take automatic action to protect the application, system, or network that it is charged with monitoring. Such measures can be at a gross level, for instance dropping all traffic from a target or network that appears to be launching an attack; they can be very granular, in the case of dropping only specific packets that are part of a carefully crafted attack, or at any level of specificity in between. Systems such as these that can react without the express permission of an administrator are necessary in order to be able to handle cyber-related issues in a sufficiently short period of time.

As a variation on the traditional IDS/IPS usage, we could also consider a slight variation on the idea and include some facility for counterattack. We might call such a system, to slightly overload a term, an Intrusion Response System (IRS). An IRS (yes, we could aim the IRS on someone) might go slightly further than the traditionally defensive measures taken by an IPS, and actually launch an attack in return, perhaps using a somewhat "safe" attack such as a DDoS from a botnet built for the purpose. Such a solution is absolutely rife with problems, to include collateral damage and attribution, but might very well be implemented by a non-state actor that felt less restricted legally. We can certainly envision a scenario where multiple IRSs attacking each other created a chain reaction, resulting in a DDoS of truly monumental proportions.

Issues such as these could potentially create the need for new and, as of yet unimagined, defensive scenarios in order to maintain functionality in such a chaotic environment. As cyber warfare and its associated logical weapons begin to reach maturity, we may see the landscape of the Internet change dramatically in order to cope with such situations.

SUMMARY

In this chapter, we discussed the various non-state actors that might take part in cyber warfare. We covered a variety of actors that might take part in such activity on an individual scale or in smaller groups, such as script kiddies, malware authors, scammers, blackhats, hacktivists, and patriot hackers.

We covered the place of corporations in cyber warfare. Corporations not in the employ of nation-states may be involved in cyber warfare from a largely espionage-oriented standpoint. Other corporations may take place in cyber warfare to a more full degree, as they are providing such services to a nation-state and actually supplying the technical expertise for the state to carry out such operations.

We talked about the place of cyber terrorists in cyber warfare activities. The motivation behind cyber terrorism, as with other varieties of terrorism is to strike fear into targets and to influence the thoughts and actions of victims. The likely targets for such activities are those that are very publicly visible, or those that are capable of causing large-scale physical disruption, such as SCADA systems.

Organized cyber criminal groups are another major consideration in cyber warfare. Such organizations can be very powerful and well coordinated, and they often have access to

highly skilled individuals and copious technology resources. Organized crime groups are largely motivated by gain of money and power, the increase of both are easily enhanced through the use of cyber techniques.

Lastly, we covered the participation of autonomous actors in cyber activities. We commonly see the use of such tools, at present, implemented in malware and defensive tools. We are likely to see the use of such tools become more commonly used in cyber warfare, as the speeds at which such activities take place preclude the use of waiting for human authorization at every step. Additionally, we discussed the potential use of autonomous attack tools and some of the dangers inherent in using them.

References

[1] Samuel A. Hacktivism and the future of political participation, http://www.alexandrasamuel.com/dissertation/pdfs/index.html; 2006 [accessed 26.04.13].
[2] Staff W. Australian Government websites blitzed by DDoS attack. SC Magazine Australia/NZ, http://www.securecomputing.net.au/News/166860, australian-government-websites-blitzed-by-ddos-attack.aspx; 2010 [accessed 26.04.13].
[3] Telegraph.co.uk. Climategate: was Russian secret service behind email hacking plot? Telegraph.co.uk, http://www.telegraph.co.uk/earth/copenhagen-climate-change-confe/6746370/Climategate-was-Russian-secret-service-behind-email-hacking-plot.html; 2009 [accessed 26.04.13].
[4] Crowdy T. The enemy within: a history of espionage. s.l. Osprey Publishing; 2006, 978-1841769332.
[5] Drew C, Markoff J. Contractors Vie for Plum work, hacking for U.S. The New York Times 2009; http://www.nytimes.com/2009/05/31/us/31cyber.html [accessed 26.04.13].
[6] Hendershot H. CyberCrime 2003 – terrorists' activity in cyberspace, http://www.slideworld.com/slideshows.aspx/Cyberterrorism-ppt-713859; 2003 [accessed 26.04.13].
[7] Red Star Cafe. The Northeast blackout of 2003. Red star cafe. March 29, 2008, http://redstarcafe.wordpress.com/2008/03/29/the-northeast-blackout-of-2003/; 2010 [accessed 26.04.13].
[8] Barbara S, et al. Plots, evidence and chatter put U.S. on alert. CNN.com, http://archives.cnn.com/2002/WORLD/meast/10/10/terror.roundup/; 2002 [accessed 16.04.13].
[9] Flack E. Experts: cyber crime now a billion dollar business. Wave3, http://www.wave3.com/story/13184652/cyber-crime-a-billion-dollar-business-say-computer-experts; 2010 [accessed 26.04.13].
[10] Lowell B. A report on the internet worm, http://www.ee.ryerson.ca/elf/hack/iworm.html; 1998 [accessed 26.04.13].
[11] Graham P. Breaking news: the suit is back! The submarine, http://www.paulgraham.com/submarine.html#f4n; 2005 [accessed 26.04.13].