Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

FROM PITCHFORKS TO LAPTOPS: VOLUNTEERS IN CYBER CONFLICTS

Rain OTTIS

CCD COE, Tallinn, Estonia

Abstract: The capability and mandate for organized violence in the international setting has normally been the domain of nation-states. Cyberspace, however, provides an international arena where almost anyone has the power to attack any target at will. While most of these attacks have little effect, there is often little disincentive to using them, as attribution of cyber attacks and effective punishment of attackers is still the exception, instead of the norm. Thus, 21st century farmers with pitchforks or cyber militia become more than a local force and, if organized well enough, can mount an offensive cyber campaign that affects a nation-state on the other side of the planet.

In order to test this claim, I will consider the potential threat from the Internet users who are untrained in hacking techniques and who have very limited resources. In general, there are two types of activities that are open to such persons: supporting the cyber campaign by providing resources, cover and training (among other things) and launching cyber attacks as part of the cyber campaign. It is important to note that an untrained individual is probably more useful when providing support to skilled attackers, instead of actually participating in the cyber attacks.

Based on the overview of the simple options that are available for a novice cyber attacker, I will draw some conclusions on the actual threat posed by a (ad-hoc) cyber militia of amateurs.

Keywords: patriotic hacking, hacktivism, cyber militia, cyber attack, cyber conflict

Disclaimer: This paper is a product of the author. It does not represent the opinions or official policies of the CCD COE or NATO and is designed to provide an independent position.

INTRODUCTION

The emergence of the Internet has transformed the way ordinary citizens can take part in global politics. On the one hand, information from political conflicts can be relayed in near real time to people who are interested in the conflict. On the other hand, people can take part in shaping the conflict from their homes, regardless of the distances involved, because cyberspace has become a new medium for political activism. This may manifest as an information dissemination campaign in support of or against some political entity. However, it can also take the form of a politically motivated cyber attack campaign by patriotic hackers or hacktivists.

Recent international conflicts have often been accompanied by virtual side-conflicts that mirror the underlying political situation. While such events took place as early as the 1990s, they have become more common and widespread over the last decade (Denning, 2010). Usually these virtual campaigns cannot be directly attributed to any state, although it is often clear which state(s) the attackers support. Instead, there seems to be a trend of (anonymous) private citizens forming into on-line militia groups to perform cyber attacks against political opponents (Carr, 2009; Nazario, 2009).

It is important to note that even if there are no official ties between a government and an on-line cyber militia, the government may still use the militia as an instrument of state power. This approach would provide deniability and allow the state to distance itself from the attacks (Ottis, 2009).

Carr (2009) has identified that many active participants of cyber campaigns display very little training and experience. In other words, around a core group of experienced hackers there are a large number of untrained attackers. This is similar to some medieval campaigns, where a group of well-trained and equipped knights were supported by untrained and poorly equipped peasants. Arguably, this has led to the phrase “farmers with pitchforks”, which describes an amateur force. Let us extend this phrase to the twenty-first century, by providing the notional farmers with another easily accessible and necessary tool – the laptop.

In order to increase the understanding of the threat posed by a group of these low-level militiamen, I will first define them by minimum required skills and resources. I will list several options that are available to such individuals both for participating in the cyber attack campaign, as well as supporting it, assuming that they have access to a communications channel where more experienced persons can provide them with tools and advice. Finally, I will draw some conclusions about the threat posed by these so-called “farmers with laptops”.

1. “FARMERS WITH LAPTOPS”

Obviously, the low-end membership of an on-line cyber militia does not need to consist of farmers. The real issue is that they are neither trained for “cyber combat”, nor is hacking a serious hobby for them. They are merely drawn to a political conflict and are motivated and willing to contribute their effort and resources to make a difference via cyberspace. Let us first define the skills and resources that such attackers can be realistically assumed to have.

1.1 HACKER ZERO – SKILLS

The people in question are assumed to have no special training or experience with cyber attacks, but they should be familiar with basic computer use. Therefore, it should be fairly safe to assume that they at least know how to use:

- *A web browser*. Specifically, they need to be able to navigate to websites (if they have the link or know the address), run simple queries on search engines, post content in forums, as well as download files from a website (link) to their computer.
- *An e-mail client or a web interface for e-mail.* Simple operations like writing and sending an e-mail with attached files to a given e-mail address.
- *Basic features of the operating system on the computer that they will use (most likely a version of Microsoft Windows).* Basic features include opening/executing and copying files, as well as installing software with default settings (“Next – Next – Next”) and copying/pasting information between different applications (from web browser to command prompt).

1.2 HACKER ZERO – RESOURCES

It should be safe to assume that the attackers have access to at least:

- *A personal computer*. For example a laptop with the operating system mentioned above and a web browser.
- *Internet access.* This access does not need to be fast, nor constantly available. For example, access to public WiFi could be enough.

Since the militia is expected to consist of volunteers, not direct representatives of a government or commercial entity, we cannot assume “corporate sponsorship”, although it is likely that some members have control over commercial or government-owned systems. For the purposes of this work, however, a basic computer with an Internet connection is sufficient.

2. BASIC OFFENSIVE ACTIONS

Since *cyber attack* was not listed in the skill set, they must first find some information. A simple web search query will provide plenty of potential attack methods. More than likely, a search result will also point to specialized forums that discuss cyber attack techniques. If the person is a member in a group that considers a cyber campaign, then it is enough if only one of them finds the information – he can then share it with the rest. A more likely scenario is that someone in the group has a deeper understanding of conducting cyber attacks (including choice of correct targets and tools) and can provide the necessary information (or links to it) himself.

At this stage, the militia members have used the skills and resources at their disposal to gain access (either searching the web or communicating online via e-mail or web forum, etc.) to simple cyber attack instructions and tools. Let us analyze some potential options available for them, bearing in mind that this is not the complete list of possible options, but merely a sample of approaches.

2.1 MANUAL (DISTRIBUTED) DENIAL OF SERVICE

A Denial of Service (DoS) attack abuses some vulnerability in the target or supporting infrastructure to make it unavailable for normal use. Usually this is achieved by exhausting the resources of the target or by disabling the target by exploiting a logic flaw in the system. Assuming that the instructions and tools are shared in the interested community, we get many people from different locations performing the DoS. In effect, the cyber militia becomes a human botnet that is launching a distributed denial of service (DDoS) attack. Let us consider some very basic ways to attempt a denial of service attack.

A simple way to generate extra network traffic for a website is to continuously refresh the website in the browser (for example, by holding down the F5 key while at the website). Another way to accomplish this is to continuously click through links in the website (opening them in tabs) without actually taking the time to look at it. These are not designed as attack features, but they can be used to attack the server nevertheless. They tie down the resources of the target (processing power, bandwidth, memory) by over-using legitimate services. In order to be effective, however, many attackers must coordinate their actions for the duration of the attack.

Yet another way is to send email (with attachments, or with very long text, or with malware). A single person will most likely not be able to have a serious effect on an e-mail server. However, thousands of people doing it at the same time may actually have a significant effect. Especially considering that they are sending e-mail from many different addresses (source blocking will not work in the beginning) and with very different content (automated content scans will be of limited use).

One can also misuse the ping command, which is a basic tool for network administrators. There have been examples of attack instructions that basically tell the user to open the command prompt and paste a pre-written ping command (with longer packet length and specified number of attempts) in it (Ottis, 2008). Once the user hits enter, his computer starts sending out a steady stream of packets (ICMP ECHO) to the target system in order to exhaust its resources. Again, this approach requires a large number of people.

These are just a few of the simpler methods to attack the target system. While any one of them is too weak to achieve much alone, they could become a serious availability problem, if coordinated and performed by a large group.

2.2 DoS SCRIPTS AND ATTACK KITS

While manual DoS attacks can be easy to do, they require time and effort, especially if one wants to maintain pressure on the target. However, this problem is easily mitigated by automation. In the same websites and forums, where manual attack instructions are available, people can usually find automated attack tools (Carr, 2009; Ottis, 2008).

Simple script files can be downloaded and executed on the attacker's computer. For example, the script can automate the pinging process explained above. The attacker only needs to start the script once and the computer will continue to attack the target on its own.

Furthermore, specialized attack tools can be disseminated via website or forum. For example, there are programs that can be used for generating various types of network traffic (including http traffic). All one needs to do is to download it, start the program, insert the target address and start the attack. Often there are also easy ways to customize the attack (traffic type, packet size and frequency, etc.) by ticking the necessary boxes and inserting the necessary values.

This type of attack is much more powerful than the manual attack, as it can result in much more "attack traffic" per attacker and it can last longer. It is also important to note that the attackers do not have to write any code, nor do they have to understand how the data packets are created, routed and processed. All they need to do is to download a program and use it.

2.3 WEB DEFACEMENT

Web defacement refers to an attack where the perpetrator gains unauthorized access to the web server and changes the content of the website. While this requires knowledge and experience beyond our defined set of attackers, there are still ways for an untrained person to perform a web defacement attack.

Some web server vulnerabilities allow the attacker to make the web server execute (exploit code) files that are located on a third party server (so-called cross site scripting). For example, this could be done by adding a customized text string (provided by someone else) to the target web address in the web browser's address bar. Note that this type of attack is highly reliant on specific vulnerabilities in the code or configuration of the target server. It only works if the system is unpatched or if there is no patch available or if the system is configured so it allows the exploit to run. Therefore, it is highly unlikely that this type of attack works on a specific target server. However, the attacker may try this approach on a large number of servers and may have success on some of the servers.

Once again, it is possible to automate this process. A program may cycle through a set of differently "customized" web addresses on a range of target websites. The web site can be defaced, if even one automatically detected vulnerability is present at the target. In the end, the attacker only needs to download and start a program, add the payload (for example, a text that will be displayed on the defaced site) and potential target addresses and start the attack. Note, again, that this attack is best suited for sweeping a broad set of targets, but is probably not effective against a small target set.

There are many other ways to deface a website. However, the chance of success for an untrained attacker is quite low, so web defacement most likely remains a tool for specialized attackers. For example, the web portal Zone-H.org maintains a list of reported web defacement attacks that are likely performed by specialized attackers.

2.4 MALWARE ATTACK

Introducing malware to the target system is another method that is available for an untrained attacker. While they are not able to write the malware themselves, they can download it from the web and then deliver it to the target.

The simplest way would be to just e-mail the malware to the users of the target system. However, this may not be effective, as the malware can be identified and neutralized (deleted, quarantined, etc.) by anti-virus software before it reaches the victim. Furthermore, the malware may not work in the system, because it targets a vulnerability that is not present. For example, the target could be running a different operating system or a different mail client (or whatever application's vulnerability is targeted).

Another simple way would be to send the victim an e-mail enticing him to download the malware (masquerading as something else) or to visit a web site that automatically attempts to infect the victim's system (a so called drive-by download).

Yet another way is to deliver it to the target system manually. If the attacker has access to the system, he may copy or download the malware directly to the system (insider attack). However, a safer way to do it would be to "lose" a data carrier (USB memory stick, CD, etc.) where the victim may find it or to mail it to the victim as something else (with a plausible explanation, using social engineering techniques, to dispel any doubt on behalf of the victim). This way, the victim will circumvent the boundary protection mechanisms of the system and introduce the vulnerability at his workstation.

The malware itself could be configured to achieve many objectives, ranging from covert information collection to systematically corrupting all data in the system. During a crisis situation, this approach could have serious consequences for the organization that owns the system.

2.5 INTELLIGENCE GATHERING

All the examples in this section provide potential intelligence value. DoS and DDoS can be used to test the bandwidth or some other capacity of the target system. Defacement and malware attacks allow the attacker to collect information about the system itself, the data in it and its users.

3. SUPPORT ACTIONS

In addition to carrying out cyber attacks, there are many ways to support a cyber attack campaign. While these support actions may not create any direct damage or consequences, they can have a strong influence on the effectiveness and scale of the cyber campaign in question. It should be noted that these support actions can be performed with the basic skills and resources defined above.

3.1 PROPAGANDA AND RECRUITMENT

Most contemporary conflicts are fought in the minds of the participants and the spectators. In order to win, it is not necessary to kill every soldier in the opposing army or to raze the cities of the enemy. Instead, the participants compete to be *perceived* as the winning side. This is especially true in cyber conflicts, where permanent damage (physical damage, physical injury or death) is difficult to achieve. At the same time, the relative anonymity in the Internet causes attribution problems, which in turn make effective deterrence and retaliation nearly impossible. Therefore, in cyber conflicts it is very important to maintain the upper hand in the battle for the minds.

Creating a propaganda message requires no computer skills, while spreading it can be easily accomplished by e-mail, forum posts, etc. Therefore, a person can participate in an information operation or psychological operation (see Joint Publication 3-13) that supports the cyber campaign by affecting the morale of the participants (and spectators) and recruiting new members for the campaign.

3.2 SUPPLY

If one is not willing to participate in cyber attacks, one may still be interested in supplying the attackers. This may range from financial donations to corporate resource sharing.

Conceptually, one can find many ways to donate funds to a cyber militia. For example, a personal transaction (cash, wire transfer, check, etc.) is easy to accomplish, but it may leave a trail for the investigators and compromise the anonymity of the person. However, there are also alternative options, like donating stolen credit card information or channeling funds through on-line games and artificial worlds in cyberspace. It is also possible to offer personal resources, such as infecting one's computer with malware in order to add it to a botnet controlled by the militia.

Corporations and educational facilities tend to have much greater bandwidth and processing power than the average home user. Therefore, providing access (either physical access on site, or login credentials for remote access) to corporate resources can be very beneficial for the cyber militia.

3.3 TRAINING

A very useful way to contribute to a cyber militia is to provide training. This could range from posting simple attack instructions, such as the ping sequence described above, to a complicated real-time walkthrough of compromising a target system.

However, we have assumed the people in question to have no offensive skills, so the training aspect would be limited to finding instructions on the web and posting them on the shared forum. This does illustrate, however, that the presence of even one expert can significantly affect the qualitative danger posed by the group.

3.4 RECONNAISSANCE & TARGETING

An important part in any offensive plan is to determine the right set of targets. This also holds true in cyberspace. It is very easy to cause collateral damage to systems that merely have a similar address or are located in the same IP address range with the intended target.

For example, let us assume that a conflict has erupted in a country that the attacker has little experience with. How does one determine which systems to attack if one does not understand the language used in the target country? Targeting everything within the country domain will spread the attack too thinly and may affect neutral and friendly systems in the area.

However, if there is someone in the group who knows the country in question, or at least can understand the language, he can help by pointing out which addresses should be targeted.

In addition, the group members can use dedicated tools to gather information about the configuration and vulnerabilities of the target system. It is important to note that these tools are not necessarily created for cyber attacks and may or may not be legal. Instead, they are often designed and used by security professionals who look for weaknesses in the system. For example, the attacker may use a vulnerability or port scanner software in order to identify potential avenues of attack for the group.

While scanning is not an attack, strictly speaking, it can be considered malicious, because the average Internet user should have no legitimate reason to do it. However, the information gained from the scan can then be forwarded to the more experienced attackers. This distracts the defenders, who will be aware of the scanner.

3.5 OBSERVATION AND FEEDBACK

Aside from providing targeting information, a “local” can also serve as an observer in the conflict and provide valuable feedback to the group. For example, if the group has organized a large-scale DDoS attack against a web server, it would be useful to verify that the system is inaccessible in the country or region of interest. The defenders could just drop all traffic coming from outside the region and continue to serve the local clients, so only a “local” can easily verify whether or not the system is actually down.

Another observation function is to relay the effect on population to the attacking group. What are the locals talking about? Do they know who is responsible for the attack? Are they even aware of the attack? Has the local law enforcement or government made any statements in regard to the attacks? What effects does the attack have?

Having personal knowledge about the situation “in the field” can be very valuable for the people who are planning the cyber campaign. It can prevent “friendly fire” incidents, shift targets if the attack is unsuccessful, etc.

3.6 FOG OF WAR

Having the correct and up-to-date picture of the situation is important to all sides in any conflict. One way to exploit this is to inject confusing information to distract the attention and resources of the defenders.

For example, if the defenders rely on human reports (for lack of an automated reporting tool) for detecting successful attacks, then one could just generate false reports. The defenders will then have to waste precious time and resources to verify the information. Furthermore, if the “reporting” is public, then the “attack” will live on as a rumor even after proven false. One could also report fake events that are difficult to verify, such as counterattacks from the defenders (“they defaced several sites in country X as retaliation!”), temporary failure of critical services (“the 911 system was down for 20 minutes!”), some other group taking responsibility for the attacks, etc. This will reduce the situational awareness of the defenders.

In addition, one could provoke people to join the conflict on either side, as well as recruit support from third parties. Another option is to abuse the legal framework of the defenders to overload them with legitimate, but pointless, information queries (for example, requesting information that the target is required to provide, such as official contact information). In the end, there are many ways to make the fog of war thicker for the defenders, thus reducing their ability to effectively deal with the situation. As the examples demonstrate, these options do not require in-depth technical skills and can be easily performed by the cyber auxiliaries.

4. CONCLUSIONS

While the analysis has focused on the options available for untrained individuals, the examples from recent cyber conflicts clearly demonstrate that they do not work alone, but rather support the efforts of more skilled attackers. As a result, untrained individuals have successfully participated in cyber attacks that affect entire states, while there has been little or no direct attribution to any state or individual (Carr, 2009; Nazario, 2009).

There is no question that an unskilled attacker can find instructions on the web, but they are not likely to mount a successful attack against a well-defended system. The cyber attack categories reviewed here – DoS, DDoS, web defacement and malware attacks – are all accessible to persons with no prior experience. However, in most cases these attacks would not be severe enough to pose a serious threat in the international setting, because the untrained attackers can only use the most primitive attack forms.

In order to really be effective as a cyber militia, at least some of the members must have a deeper understanding of cyber attacks. While the "farmers with laptops" can carry out simple commands or run custom scripts and programs, someone still needs to provide them with the right tools, the correct instructions and point them against a reasonable target. This implies that defenders should focus their investigation and potential counter-actions against the cadre of instructors.

It is also clear that people, who are untrained in cyber attacks, can provide support to the experts, who can then focus on the cyber attacks. The main benefit of the support actions may be to create confusion for the defenders, because it is often useful to strike from chaos (fog of war) and keep the opposition guessing on your identity, aims and capabilities.

Of the examples provided, the most dangerous attack option is probably to implant malware into the target system in a time of crisis. The most influential support option, on the other hand, is to provide training and tools for the group. However, a person who wants to participate is not limited to just one option. Instead, active members of a (ad hoc) cyber militia can be expected to contribute in multiple ways, including both attack and support options.

5. SUMMARY

The (ad hoc) volunteer cyber militia groups have played a visible role in many recent international conflicts by waging a parallel campaign in cyberspace. While there seems to be evidence that most of the people engaged in this activity are untrained in the art of cyber war, they can still pose a threat if they are organized and “armed” by a more experienced *cadre*. Specifically, someone needs to provide them with attack instructions and software tools.

I have described some relatively simple ways to participate in cyber attacks, as well as to support others in doing so. Based on the described options, I have drawn conclusions on the danger posed by untrained cyber attackers.

REFERENCES

- Carr, J., 2009. *Inside Cyber Warfare*. Sebastopol, CA: O'Reilly Media.
- *Joint Publication 3-13.*, 2006. *Information Operations.* Chairman of the Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf. [Accessed 25.02.2010]
- Nazario, J., 2009. Politically Motivated Denial of Service Attacks. In: Czosseck, C. & Geers, K. (eds.), *The Virtual Battlefield: Perspectives on Cyber Warfare,* Amsterdam: IOS Press, pp 163-181.
- Ottis, R., 2008. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. *Proceedings of the 7th European Conference on Information Warfare and Security,* Plymouth. Reading: Academic Publishing Limited, pp 163-168.
- Ottis, R., 2009. Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability. *Proceedings of the 8th European Conference on Information Warfare and Security,* Lisbon. Reading: Academic Publishing Limited, pp 177-182.