

## Proactive Defense Tactics Against On-Line Cyber Militia

Rain Ottis

Cooperative Cyber Defence Centre of Excellence

[rain.ottis@ccdcoe.org](mailto:rain.ottis@ccdcoe.org)

There is a developing trend of “popular” cyber campaigns that mirror political, economic or military conflicts in cyberspace. The Estonian case from 2007 showed that a whole nation-state can be affected by cyber attacks, whereas the Georgian case of 2008 is an illustration of a cyber campaign that mirrors an armed conflict. In both cases at least part of the attacks were likely committed by patriotic hackers – volunteers who use cyber attacks to take part in intra- or international conflicts.

In such cyber conflicts usually only the targets are known while the aggressors remain anonymous. It is often difficult to discern where state capability ends and independent patriotic hacker groups begin. Furthermore, it is relatively easy to form a new cyber militia from people who have little prior experience with computers. I define *cyber militia* as a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal. I further define *on-line cyber militia* as a cyber militia where the members communicate primarily via Internet and, as a rule, hide their identity.

What the newly-minted cyber warriors may lack in skill and resources, they can often compensate with numbers. However, even an ad-hoc cyber militia that is not under direct state control can be a useful extension of a state’s cyber power. On the other hand, they can also become a threat to national security. Due to the global nature of the Internet, this threat is most likely coming from multiple jurisdictions, which limits the law enforcement or military options of the state. Therefore, other approaches should be considered.

In order to understand the potential threat from cyber militias, either ad-hoc or permanent, we need to explore how they are organized. I provide a theoretical overview of a specific type of on-line cyber militia and then propose tactics to neutralize it. The tactics are based on a proactive defense posture and primarily use information operation techniques to achieve the effect from within the cyber militia itself.

**Keywords:** cyber conflict, cyber militia, proactive cyber defense, information operations, hactivism

### 1. Introduction

Over the past few decades the malicious activity in cyberspace has grown to levels, where it is now considered a national security issue. This is arguably due to the fact that computers have become nearly ubiquitous in modern societies. They are easy to use and very accessible, allowing the people to regularly communicate, learn, work and have fun in cyberspace (Ottis 2010).

On the other hand, it is now also easier to use this technology for malicious purposes. There are automated cyber attack kits, vulnerability databases and instruction manuals for conducting offensive operations in cyberspace. The skill level of the attacker today does not need to be high. On the contrary, some of the more visible attacks are often perpetrated by individuals with little or no computer training (Carr 2009).

While cyber crime continues to thrive in the quest for illegitimate income via cyberspace operations, the politically motivated attacks are becoming ever more common and visible. Many international conflicts in recent years have had a mirror campaign in cyberspace. The question that often develops is whether or not the cyber campaign is sponsored by the state(s) involved in the conflict, as the attacks usually seem to be the work of patriotic hackers. (Carr 2009, Nazario 2009)

However, it is quite possible that even without a direct command link with the state, the attackers still act according to the state’s agenda. After all, the state may use this volunteer force in order to maintain deniability. The official cyber warriors (military, intelligence etc.) of the state are just one of the potential components of a national offensive cyber capability. Volunteers (patriotic hackers, hactivists) and mercenaries (criminals, commercially hired experts etc.) can augment the organic cyber capabilities of the government. (Ottis 2009)

People can also mobilize as a result of a true grass roots movement. Such independent groups could organize a cyber attack campaign as a sign of protest or to promote their views. If compared to an entity that has hidden state sponsorship, they would most likely look very similar to an outside observer. Either way, this type of on-line group can evolve into a threat beyond mere inconvenience as seen in cases like the Estonian and Georgian cyber conflicts. (Ottis 2008, Carr 2009, Nazario 2009, Denning 2010)

In order to cope with this threat, we must first understand how it works. Therefore, I will provide a theoretical overview of the organizational aspects of non-state political activist groups who use cyber attacks and then look at some tactics to counter these groups.

## **2. On-line cyber militia**

Denning (2010) describes three categories of non-state attackers (separate from the ordinary cyber criminal): patriotic hackers, electronic jihadists and hactivists. The main difference among them is the choice of targets, although Denning admits that they could all be lumped together as hactivists. For the purposes of this research, however, this distinction does not matter, as the focus is on how they are organized, not who they are fighting for or against. In particular, I am interested in finding potential weaknesses in the organization and operation of cyber militias.

Let us define *cyber militia* as a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal. Let us further define *on-line cyber militia* as a cyber militia where the members communicate primarily via Internet and, as a rule, hide their identity (for example, by using a hacker alias). Cyber militias can be ad-hoc (gathering only for a specific occasion) or permanent.

The word "volunteers" in the definition refers to people who participate in the cyber militia of their own free will. They do not get paid for their activities, nor do they have a contractual obligation to the militia. They have the right to choose their level of commitment and to leave the militia, if and when they wish. Therefore, volunteer soldiers who join a government run cyber attack unit are not considered a cyber militia.

The word "political" in the definition refers to all aims that transcend the personal interest of the volunteer. This includes religious views, nationalistic views, opinions on world social order etc.

In the context of this analysis, I am focusing on a subset of on-line cyber militias that meet the following criteria:

- The communication within the militia is centralized
- There is no direct state support or control of the militia
- The members are loosely connected in real life

The centralized communication constraint is a fairly standard arrangement for communicating, preparing, planning and coordinating a cyber attack campaign of the cyber militia. Perhaps the most used communication channels are on-line forums and instant messaging services. (Carr 2009, Denning 2010) This is also very useful for the defending side, especially for observing, infiltrating and neutralizing the cyber militia.

A cyber militia that receives direct support or instructions from the government should be considered as an organic component of the state and is therefore outside the scope of this research. However, indirect or covert state support or control (as long as it is not well known among the militia) remains still in the area of interest.

Although the leadership or core group in a militia probably is personally acquainted, as a whole the members of the on-line cyber militia are loosely connected in real life. In this case loosely connected means that most members know no or few other members and nobody knows the entire membership in person. This requires them to communicate over the Internet and coincidentally makes them more susceptible to information operations techniques. While this constraint is not true in every case, it should

be a safe assumption in large (numbering in the hundreds) militias and can also hold in smaller organizations.

From the forum posts it should be possible to identify the roles of the people in the cyber militia. Key "officer" roles include leaders, trainers, suppliers, while the rest could be categorized as soldiers, and "camp followers". The leaders provide motivation for action, coordination of effort and direction of attacks. The trainers provide instructions for reconnaissance, attack and covering tracks. Suppliers provide tools, such as scanners, attack kits and malware. Soldiers participate actively in the attacks, but can be expected to remain relatively passive on the forum, potentially reporting attack results or targeting information. Camp followers read the forum for their own interest, but do not participate in the planning or execution of attacks. Identifying the different roles in the organization offers individual targeting opportunities as well as potential avenues for infiltration.

Since the cyber militia is not necessarily a formal organization, the same person may have several roles, which can change over time. It is also important to note that an "officer" role is often not appointed by the militia, but acquired by the member by actively participating in the activities.

### **3. Neutralizing an on-line cyber militia**

Assuming that on-line cyber militias can be a considerable threat to national security, there should also be ways of neutralizing this threat. Using traditional law enforcement methods or military force is often not feasible, because personal attribution is seldom achieved and the militia members can reside in a number of different unfriendly and uncooperative jurisdictions. Therefore I will consider alternative tactics of neutralizing an on-line cyber militia. In particular, I will propose options from the strategic starting point of information operations and proactive defense.

An important caveat here is that I do not presume universal legality of any of the tactics. It would be very difficult to do, given that the legal status of the cyber militia and its actions may vary greatly, depending on the case. For example, the cyber militia may act completely within the legal framework of the host state. On the other hand, militia members could be considered illegal combatants who may be targeted for military action (Schmitt 2002). Therefore, the tactics below should be considered as theoretical options only, not as a policy manual for dealing with a cyber militia.

There are two points where the activity of an on-line cyber militia is potentially visible for observation. First, there are the logs at the targeted sites. Second, the shared communication channel (a forum, for example) where they gather, exchange opinions and plan their activities. The two places where the militia is visible are also the places where one can fight them.

Sun-Tzu said: "Thus the highest realization of warfare is to attack the enemy's plans; next is to attack their alliances; next to attack their army; and the lowest is to attack their fortified cities" (cited in Sawyer 1994). I will use this principle as a loose framework for considering tactics. The analogies do not need to be an exact fit and should be interpreted liberally. First, I will look at how to neutralize the militia's ability to plan and coordinate attacks. Second, I will look at ways of attacking the virtual alliances between the members that make up the cyber militia. Third, I will look at neutralizing the effectiveness of the militia's cyber attacks. Last, I consider a counter-attack against the actual communication service that is the heart of the militia's operations.

It is important to note that for the countermeasures to work, it is necessary to gain access to the main communication channel of the militia. This may be as simple as monitoring a public forum, but a more likely scenario would require at least some form of infiltration into the channel. The infiltration does not need to be very deep - a "soldier" level access would likely be sufficient to gather the necessary information about the militia. Infiltration is required, because any sufficiently mature cyber militia will likely try to hide or protect itself from outside entities. For example, the StopGeorgia.ru forum blocked US-based IP addresses to stop researchers from accessing the forum during ten days in August of 2008 (Carr 2009).

### 3.1 Attacking plans

One way to neutralize the militia can be called *poisoning the well* tactic. It refers to corrupting the shared communication channel with de-motivational posts, self-destructive or ineffective attack tools and methods, bad targeting data, etc. As a result, the channel loses its effectiveness as a means for coordinating the actions of the militia, the members grow frustrated with apparent lack of coherence, and the aggression gets released inside the militia in the form of angry debate. If the militia is perceived as ineffective by the members, it will eventually disband.

An alternative approach would be to hijack the militia by shifting the debate to attacking other targets. This would basically deflect the blow from the original target, making it safe.

Yet another approach is to carry out an attack in the name of the militia against a powerful third entity in order to provoke a counterstrike against the entire militia (a false flag attack). In other words, pull a strong opponent into the fight, forcing the militia into defensive positions. As a result, the militia will have to drop its plans for the original target.

### 3.2 Attacking alliances

Presumably, members of the militia want to remain *anonymous* and would leave or become inactive if there was a serious chance of being personally identified. This presents another opportunity to disband the militia from within by breaking the virtual alliances between militia members.

Without attribution there can be no personal consequences. On the other hand, if the anonymity is lost (or perceived lost by the membership), the militia will lose its trustworthiness. As a result, the militia will either disband or search for an alternative (clean) communication channel. However, since the infiltrated agents will also move over to the new channel, it would only be a temporary solution.

The question is, then, how to identify the members of the forum. In reality, it is probably not necessary to identify all or even most of the members. Most likely it is enough to break the cover of one or a few people, in order to create mistrust and fear of real life consequences in a considerable portion of the membership.

There are many ways to potentially achieve attribution of a few individuals. The simplest is to "break the cover" on infiltrated agents (can use fake identities, as they would be difficult to verify by other members) and have them "confirm" it. Another is to offer attack tools to the forum that provide the information that is necessary for personal attribution (basically a Trojan). Yet another is to correlate target log data with forum posts, and go through the legal channels. Of course, attribution may be achieved by simply arranging a meeting in real life.

Note that it may not be necessary to actually follow up the attribution with legal or military action. Just posting the personal details of some users on the forum could be enough to make a considerable portion of the members leave.

### 3.3 Attacking the army

The loose analogy to an army in this case could be the cyber attacks organized by the militia (the soldiers that have marched to the city gates). Obviously, the defensive actions at the target come from the long list of standard cyber security measures. However, these can be deployed much more effectively, if the infiltrated agent can relay the attack plans to the defenders. Knowing when, where and how the attack will come makes the work of defenders much easier and blunts the effectiveness of the attackers. This, in turn, may have a demoralizing effect on the militia.

### 3.4 Attacking fortified cities.

If we take the forum to be the fortified city that serves as a home base for the cyber militia, then obviously there are ways of attacking it. Conceptually the easiest would be to use law enforcement to have it taken down, or if that fails, launch a denial of service attack against the server that hosts the service. Alternatively, one could take over and shut down the forum with hacking techniques. The problem with

this approach is that the militia can easily regroup using a secondary meeting point (for example, a pre-determined IRC channel or a website). In addition, the counterattack will likely motivate them to continue the fight, as it is now a more personal matter. Therefore, this option, while potentially the easiest to achieve, is also least likely to generate a lasting effect.

In addition, it would be possible to post messages and materials in the channel that are against the enforced laws in the jurisdiction (vs posting attack instructions, which may be illegal but not enforced by a militia-friendly government), thus provoking a collateral response from the Internet service provider or law enforcement community.

#### **4. Limitations and future research**

All views in this work are attributed to the author and should not to be considered as the views or policy of the Cooperative Cyber Defence Centre of Excellence or the North Atlantic Treaty Organization.

The analysis of the on-line cyber militia is based on existing literature and provides only a theoretical viewpoint to the problem area. It is a generalized model, which may not apply to all cases.

The outlined tactics are a blend of information operation techniques and offer a more proactive defense posture against an on-line cyber militia. However, depending on the case, they may contain elements that can be considered against the law. Issues that may arise include perfidy, freedom of speech, computer crime, illegal surveillance and personal data protection, to name a few. Therefore, it should not be viewed as a policy manual, but a theoretical overview of alternative tactics.

One way to move this research forward is to use social network analysis on cyber militia forum logs to identify the roles and interactions of key actors in cyber militia. This could help develop a better model for a generic cyber militia and a more detailed method for targeting key members in the militia.

#### **5. Conclusion**

The rising trend of politically motivated cyber attacks by non-state actors has changed the balance of power in cyberspace. On-line cyber militia is a type of organization that allows everyone with a computer and an Internet connection to become active in the world of cyber conflict.

Since on-line cyber militias have shown the capability to become a threat to national security, it is important to study them. I have given a theoretical overview of a specific type of cyber militia, which relies on a mass of anonymous members for its "firepower". More importantly, I have provided some generic tactics for neutralizing the on-line cyber militia, under the strategic approach of information operations and proactive defense.

#### **References**

Carr, J. (2009) *Inside Cyber Warfare*, Sebastopol, CA: O'Reilly Media.

Denning, D. E. (2010) "Cyber Conflict as an Emergent Social Phenomenon", *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (Hold, T. & Schell, B. eds.), IGI Global. [to appear]

Nazario, J. (2009) "Politically Motivated Denial of Service Attacks", *The Virtual Battlefield: Perspectives on Cyber Warfare* (Czosseck, C. & Geers, K. eds.), 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.

Ottis, R. and Lorents, P. (2010) "Cyberspace: Definition and Implications." *Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, US*. [accepted for publication]

Schmitt, M. (2002) "Wired Warfare: Computer Network Attack and International Law", *International Review of the Red Cross*, Vol 84, No 846, pp 365-399.

Sawyer, R.D. (1994) *Sun-Tzu: The Art of War*, Boulder: Westview Press.