Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability

Rain Ottis
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
rain.ottis@ccdcoe.org

Abstract: Recent events in Estonia and Georgia have elevated the threat of cyber attacks to the international consciousness. While this has added visibility to the topic, it has not brought more clarity to the discussion. Terms like cyber warfare and cyber terrorism are widely used, but their definitions are rarely agreed upon. As a result, there is lot of skepticism about the true nature of cyber threats and whether governments are engaging in such attacks in cyberspace.

It should be safe to assume that all governments are developing and using defensive cyber capabilities to some degree. Defending computer systems is considered a right and typically legal frameworks support such activity. As soon as one goes on the cyber offensive, however, they are off the map. There is little consensus, let alone legal guidance, regarding the use of cyber attacks to further a political or military goal. Very few nations have announced an offensive capability in cyber space, but it is reasonable to assume that more are covertly creating such a capability.

In this paper the term offensive cyber capability is used instead of the better known computer network attack (CNA). Offensive cyber capability differs from CNA by including actors from outside the direct control of the government, such as freelance hackers, criminals and flash mobs as possible extensions to a nation-state's offensive capability.

This paper offers a theoretical model composed of three approaches that a nation-state might use when creating an offensive cyber capability. First, the traditional use of 'own forces' is analyzed. The second way is to cultivate a volunteer force that can be guided to attack designated targets with little or no attribution to the government. The last approach is to outsource the problem to digital mercenaries. Each option has unique benefits and drawbacks, while some aspects remain universal across the board. In reality, the most effective approach is most likely a combination of all three.

Keywords: offensive cyber capability, cyber attack, computer network attack, People's War

1. Introduction

Attacks in cyberspace have been a part of many international conflicts over the last ten years (Geers 2008). Arguably the most influential of these attacks occurred in Estonia in 2007 and in Georgia in 2008. It is notable, however, that in both cases the attackers remained largely anonymous and no direct state sponsorship has been proven in either cyber campaign. Instead, it looks like the attacks were planned and launched by concerned individuals who merely were expressing their political views via computer hacking. While this approach may be true on the surface, it fails to explain the lack of international law enforcement cooperation and open propaganda support for the attackers by the Russian authorities (Ottis 2008, Carr 2008).

This paper proposes a theoretical model that consists of three general ways to create a nation-state level capability to inflict damage on another nation-state or even non-state actors via cyber attack. The first option is the 'do-it-yourself' approach, or using the nation-state's own forces. The second is to cultivate a volunteer force that can be guided to attack designated targets with little or no attribution to the government. The last approach is to outsource (parts of) the problem to other governments, commercial entities or the criminal underworld in a mercenary model. As shown in Figure 1, combinations of two or three approaches can also be used, if there a need for it exists. The benefits, drawbacks and ways to recognize each approach are qualitatively analyzed in the following chapters.

According to Joint Publication 3-13 (Information Operations), computer network operations (CNO) represent one of the five core capabilities of information operations (IO). CNO, in turn, consists of three elements: computer network attack (CNA – offensive), computer network defense (CND – defensive) and computer network exploitation (CNE – intelligence). In this paper the term *offensive cyber capability* is used instead of the better known CNA, which refers to "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves" (JP 3-13 2006). The difference between CNA and offensive cyber capability is not in the action, but with the actor. While not explicitly stated as such, the implied actor of a government-backed computer network attack in the context of information operations seems to be an organic part of the government (for example, a military unit). Offensive cyber capability, however, includes actors outside the direct control of the government. For example, freelance hackers, criminals and flash mobs can be used to attack a target by proxy, thus extending the offensive cyber capabilities of a nation-state.

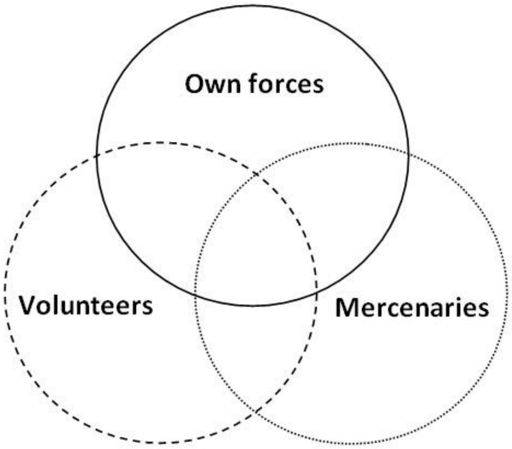

Figure 1. Three approaches for setting up an offensive cyber capability

2. The "own forces" approach

Historically, if a new capability is required by a state, it is often done with redistributing existing resources in the state apparatus or by creating a new body to take on the task. It is a natural approach for a government and it ensures that the activities are under the government's control. Need to put an American into orbit? No problem, let there be NASA. Need to project your military power in cyberspace? No problem, let there be a Cyber Command to plan, prepare, execute and exploit cyber attacks as part of everyday military activity.

The Cyber Command mentioned above is just an abstract example – a cyber force could take many forms from straightforward regular military units to shadowy intelligence agencies to scientific red teams. The common factors they all share are professional membership and a clear and unambiguous link to the state. The state link enables cooperation and coordination with national military/intelligence/law enforcement, although this is very likely seldom achieved in full. However, even partial coordination with physical operators will surely multiply the effect of a cyber attack and *vice versa*. For example, an air strike against an enemy radar system would be much more effective if cyber attacks could disable the missile batteries guarding the site.

Setting up another unit or agency for this purpose should be a routine process and most likely easily accommodated by the legal framework of the state. The main question may be the policy issue of creating an *offensively* oriented organization but there are solutions for that as well. The simplest option could be to create this organization in secret and add it to the intelligence structure.

A different aspect of maintaining a low profile is the fact that some of the cyber attacks can fall outside the current box of legal tools and toys. Arguably this question may not emerge in a straightforward military conflict where tanks, helicopters and ships are used to deliver more tangible damage every day. A cyber attack could be categorized as just another activity to gain a military advantage over the enemy. The problem is that much of the military infrastructure is linked to, if not based upon, civilian infrastructure. Therefore, a cyber attack against a military target may cause considerable collateral damage. To make matters even worse, civilian systems (banks, internet service providers, phone companies etc.) may become primary targets in a conflict as they will hamper the economy of the target nation (war of attrition) or disrupt the target nation's ability to communicate with the outside world (communications jamming or information blockade). Therefore, the layer of secrecy may be required in order to protect the cyber warriors from potential legal consequences.

States tend to be fairly secretive about the specifics of their defense budget. As a result, a significant amount of resources can be channeled to build up an offensive cyber capability to the required level without much fuss in the public eye. Therefore, the absence of a published doctrine does not always mean a lack of capability or intent. If it is in the state's interest to keep the creation of an offensive cyber unit a secret, they are well within their rights to do so.

One of the main benefits of having a state-run organization is direct access to the state's resources and the ability to coordinate actions within a unified framework. Access to state funds, personnel and training resources can provide a strong, disciplined, well-equipped and trained force that is on call at a moment's notice. Thus the key strengths of this approach are reliability, predictability and control.

However, this approach does have its weaknesses. Of the three options considered here, it is likely the most expensive one to implement. Having a pool of trained experts on call takes a lot of resources, considering that they may never see any action. This problem is similar to the one haunting nuclear forces.

The second problem relates to attack attribution. In a pure military style cyber attack against a specific target, it is very difficult to deny state involvement, even if the trail goes cold in a third party country. The methodical approach that a government run operation would likely take could also indicate who the attacker is. Furthermore, creating a cyber storm to provide the necessary background noise would most likely affect some collateral targets. This would invoke a host of potentially troublesome legal issues. For example, consider having to explain to the international community why it was necessary to attack a multi-national bank in order to apply political or military pressure on an adversary government. In fact, it is possible that similar line of reasoning has deterred at least one potential state level cyber attack against a civilian target in the past. During the Kosovo campaign the US forces supposedly considered hacking Milosevic's foreign bank accounts but were not given a green light to execute (Yurcik 2001).

In order to identify a cyber attack sponsored by a nation-state, an observer should be looking for the following signs:

- the state in question may have an official policy and designated organization(s) for carrying out offensive cyber operations;
- a state's traditional military operations could 'coincide' with cyber attacks;
- the political enemies of the state (internal and/or external) may be targeted by cyber attacks that do not display typical criminal motivation (money), especially when politically-favored organizations suffer few or no attacks;
- law enforcement does not make any effort or progress in catching attackers suspected of living within their borders.

3. Volunteer force approach

The wide-scale adoption of information technology has undoubtedly transformed both government and civil society over the past two decades. One aspect of this transformation is that people now have unprecedented access to information and global communications. The Internet is an ideal tool for sharing ideas, finding contacts, and creating new business opportunities. In that sense, the Internet has empowered people. On the other hand, it also means that people are now empowered to carry out new types of attacks against other residents of the information society.

While the original, stereotypical hacker may have been a lonely specialist looking for an intellectual challenge, many cyber attacks today are carried out by criminals or political activists. When criminals conduct cyber attacks for financial gain, political activists participate in such campaigns to support a particular ideology. It is this politically active and potentially dangerous segment that can be harnessed as a volunteer cyber militia. As recent political cyber campaigns in Estonia, Georgia, and Israel show, individuals can and will take part in cyber attacks against state targets. The question is whether this force can be mobilized in a timely and controlled manner.

It is important to note, however, that most volunteer cyber militias have a spontaneous start, likely based on an underlying grass roots movement or community. It is not known, how many and if some of these have been set up by deliberate government action. Nevertheless, it is possible for a government to 'hijack' a cyber militia by either infiltrating its ranks or applying pressure on the membership.

Managing a volunteer cyber force could be achieved in many ways. For example, by persuading existing 'hacker' organizations to work for the state or by setting up a new organization to run a proxy campaign for the government. Alternatively, the state may indirectly *guide* the citizens or supporters to take part in cyber attacks individually, without actually relying on any real, underlying organization.

Such a loose network of attackers could be very difficult to defend against, because the different skill sets, locations, time zones and resources of the attackers could make the attack large in volume as well as highly heterogeneous in nature. There would be no 'silver bullet' defense that could effectively cut off all the attackers, aside from cutting the target's connection to the outside world altogether. Volunteers representing large nations (and their diaspora) or global political movements are well placed to carry out around-the-clock attacks for extended periods of time. Further, if some attackers are identified, their arrest will have little direct impact on the rest of the attackers. The only noteworthy effect would likely be psychological, but this could either discourage other attackers or it could recruit more fighters to the cause.

An added bonus for using a volunteer force is that the state could deny any links to cyber attacks, as they would seem to come from individuals with no direct link to the state. This is true only if the state can manage the volunteers in an indirect manner. One way is to infiltrate the volunteer community with provocateur and motivator agents who use propaganda and other psychological operations techniques to manipulate the volunteers. This would not be very difficult, because the volunteer community typically communicates and 'meets' via online forums, discussion groups, etc. Authentication, if attempted or desired, is very difficult to enforce and can be circumvented with 'sleeper' agents.

This type of indirect control brings out one of the chief weaknesses of this approach: unpredictability. It is impossible to accurately predict what the reaction of the community will be to orders from the state. How fast will they mobilize? What skills and resources will they contribute? Will they attack collateral targets and needlessly expand the conflict? When will they finish - too soon or too late? These questions remain unanswered and they illustrate the potential dangers that are inherent in this approach. Therefore, planning a "People's War" campaign (Wu 2004) would have to incorporate a wide margin for error. As a precursor to a conventional military attack or as a digital harassment campaign, this may not matter, as the main goal of the cyber attack could be simply to confuse the target.

An interesting aspect of the volunteer force approach is that offensive campaigns would have to be relatively frequent and regular. In essence, one would have to make sure that the 'reserve' is trained and ready to fight. The only way to do this is to make sure they have a 'training exercise' every now and then, because otherwise they may find something better to do. This concept of *training the reserve* has several negative side effects: increase in related cyber crime, tense relations with political opponents (national or international) and the potential for the force to be overextended. If the attack campaigns occur too frequently or are used against strong opponents, then the motivation level of the volunteers will likely drop and they may find an alternative pastime.

On a positive note, compared to the other options presented here, a volunteer force is likely the cheapest version in terms of direct costs. The time, resources and training of the volunteers will be covered by the volunteers themselves. The only real direct costs to the state are to hire some agents to spur and direct the volunteers. The indirect costs from rising cyber crime levels and lost productivity, however, may significantly decrease the economic effectiveness of this option.

It is important to note that by using an indirectly-controlled volunteer approach, the state would have to cultivate a society where cyber attacks are an acceptable course of action. Political attacks like this can't be prosecuted by law enforcement, as this would discourage people from volunteering. On the other hand, accepting cyber attacks as a valid political tool may provoke an undesired cyber campaign against the sponsoring government in the future.

To identify the managed volunteer approach, an observer should be looking for the following signs:

- the state publicly glorifies people who have participated in cyber attacks against the state's 'enemies';
- the political enemies of the state (internal and/or external) are often targeted by cyber attacks that do not display typical criminal motivation (money), while politically-favored organizations suffer few or no attacks;
- law enforcement does not make any effort or progress in catching the attackers.

4. Mercenary approach

While outsourcing may be a widely accepted business practice, it is rarely an acceptable solution for an organization's core business functions. The same holds true for national security and military power. Transporting fuel to the operations area may be left to civilian freight companies, whereas engaging with the enemy should be done by one's regular armed forces. As such, the possibility of outsourcing the *offensive cyber capability* of a state may not come naturally for a government. However, this does not mean that it can't be done.

Employing mercenaries is possible, but often not a scalable solution. Conducting raids and providing personal security is one thing, but the cost of running a mercenary *army* to fight an all-out war would probably be too high for most, if not all, states. However, two aspects make this option different in a cyber conflict. First, a cyber attack need not be very wide spread in order to seriously hurt the target. Second, cyber attacks are asymmetric in nature, where the number of attackers can be less important than in the physical world. Skill, time and knowledge of the target infrastructure can more than make up for any deficiencies in numbers. Therefore, outsourcing the cyber attack to a group of digital mercenaries is a viable option from a financial perspective. Indeed, it is probably much cheaper than to organize, train and maintain a conventional unit that is only rarely needed.

Practical examples of outsourcing cyber attacks include renting a botnet for denial of service attacks, contracting hackers to take down a specific website, or asking an ally to help out. As the last example indicates, not all the options here need to be illegal.

Outsourcing the capability is very useful if the intent is to conduct a non-attributable campaign. If the state does not have an official policy, organizational structure or the know-how to conduct an offensive cyber campaign, then it is very hard to prove that the state is behind the attacks that were launched by well-known criminal organizations.

Obviously the outsourcing option also has drawbacks. The biggest is most likely reliability, as it is very difficult to guarantee that the service is available when needed and meets the required level of quality. Another worry is a loss in international prestige if the link ever comes out. Another logical threat is that the outsourcing party may at some point change sides or go rogue and start to blackmail the government.

If criminals are used then a very important secondary effect could come back to haunt the state. In order to maintain a working relationship with them, the state must in effect allow them to pursue their criminal activities. It is very unlikely that a criminal organization will provide a service to the government if its members are being hunted down and prosecuted for everyday crime. Therefore, the crime level, especially cyber crime, will likely increase in the country that has chosen the outsourcing option. However, this kind or approach requires a moral ambiguity from the government to begin with and it follows that the government may not consider these effects a problem.

Obviously, it is possible to contract these services from a criminal organization in a different country as well, but then the state has much less control over the attacks and fewer levers to manipulate the criminals.

To discover a possible use of the mercenary outsourcing option, an observer should look for the following signs:

- cyber criminals get very light sentences or are released early for unclear reasons;
- the political enemies of the state (internal and/or external) are often targeted by cyber attacks that do not display typical criminal motivation (money), while politically-favored organizations suffer few or no attacks;
- law enforcement does not make any effort or progress in catching attackers suspected of residing within their borders.

5. Comparison of the approaches

When comparing these three approaches to managing cyber attacks, it is clear that in reality a combination of two or three approaches might be used. For example, volunteer campaigns can raise funds to buy botnet time from the criminals.

The most important reason to adopt the ‘own forces’ approach is to have direct control over the attacking force. While outsourcing to mercenaries may provide some quality-of-service guarantees, it will never be on par with the control over integrated military units. Volunteers may or may not be interested in the current conflict and they may also get out of control, expanding the conflict and potentially provoking a third party to enter on behalf of the adversary.

In terms of direct costs for setting up an offensive cyber capability for a state, the volunteer option is probably the cheapest, while the ‘own forces’ approach is the most expensive. The volunteer and mercenary options do incur a sizeable secondary cost in terms of higher crime levels and lost productivity. Therefore one shouldn’t make decisions based on the up-front costs alone.

Depending on the goals and the moral stance of the state, it may be necessary to keep offensive cyber activities secret, no matter what approach is chosen. This is especially important if the state needs plausible deniability to distance itself from the attacks. The proper attribution of cyber attacks will always be a difficult task, but building in an extra layer of secrecy – as well as ensuring a lack of law enforcement cooperation – will make it a futile task.

6. Limitations and future work

This paper does not consider sub-state level actors acting on their own agenda. Nevertheless, the three approaches described here should be applicable to commercial entities, organizations and even private persons. The main interest, however, remains on the capabilities of nation-states, as they have the most resources and the strongest influence in the international political arena.

The approaches presented here provide just one way of analyzing this subject area. They are by no means meant to exclude any other frameworks or models and should be considered an effort to bring greater understanding to the still developing concept of cyber warfare.

Of the three approaches presented above, the volunteer option remains the most intriguing for further study. Every year brings more examples of this approach to light; whether they are spontaneous in nature or driven by covert government action is unknown. As such, there are many data points from which to build a theoretical framework for this approach. More specifically, the methods for organizing such a force and developing a method for estimating or measuring the potential effectiveness of a volunteer campaign will remain in focus for the coming year.

7. Conclusion

Understanding the nature of cyber warfare is a difficult task, but one that must be attempted nonetheless. While warfare has been typically a prerogative of a state, the various forms it can take often include non-state actors. Volunteer guerilla fighters and hired mercenaries have often turned the tide of battle, if not the war. Therefore, it is logical to assume that digital versions of non-state fighters will also have an important role to play in nation-state level cyber conflicts. Moreover, it may be in the interests of some states to harness this force and to integrate it into the state's overall offensive capabilities.

The three approaches described in this paper form a theoretical model of the options available to a nation-state. Often, due to limited resources, it may be more useful for a state to cultivate a volunteer cyber militia instead of building a fully professional force. And volunteers, especially if they are free of restrictions (legal concerns, doctrinal constraints etc.), can be resourceful and flexible, thus achieving success where a conventional force may fail.

References

Carr, J. et al. (2008) *Russia/Georgia Cyber War – Findings and Analysis*. [Online] Project Grey Goose. Available at: http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report. [Last accessed 04 February 2009]

Geers, K. (2008) "Cyberspace and the Changing Nature of Warfare." In *NATO RTO Symposium on Information Assurance for Emerging and Future Military Systems*, Ljubljana.

Joint Publication 3-13. Information Operations. (2006) Chairman of the Joint Chiefs of Staff. Available at: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf. [Last accessed: 05 February 2009]

Ottis, R. (2008) "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective." In *Proceedings of the 7th European Conference on Information Warfare and Security.* Reading: Academic Publishing Limited, pp 163-168.

Wu, C. (2004) "An Overview of the Research and Development of Information Warfare in China." In Edward Halpin et al (eds.) (2006) *Cyberwar, Netwar and the Revolution in Military Affairs*. Palgrave MacMillan, Hampshire, pp 173-195.

Yurcik, W. and Doss, D. (2001) "Internet Attacks: A Policy Framework for Rules of Engagement." [Online] In *The 29th Research Conference on Communication, Information and Internet Policy*, Alexandria. Available at: http://arxiv.org/ftp/cs/papers/0109/0109078.pdf. [Last accessed: 03 February 2009]