Cyber Militias

We need to define the threat

by Capt Troy Edward Mitchell

Cyber militias are exploiting networks and computers by disrupting services that the world takes for granted. As the militias continue to unite under common ideologies, they execute an increasing number of successful attacks upon the worldwide infrastructure. Each attack has the ability to affect the economic, physical, and geographical domains by ceasing or degrading functions from the virtual world. In the virtual world, physical distance is not an obstacle to conducting such attacks. As opposed to conventional warfare, cyber militias do not have to receive support from a specific state since anyone can conduct attacks in the borderless Internet.

Members of cyber militias unite under a common leader who guides the militia's objectives by providing resources to the group and a specific target list to assist in focusing the efforts. To conduct these attacks, the militia must attempt to hide any evidence of its capabilities while conducting computer network reconnaissance in the form of sniffing and probing, leading to exploitation operations.[1] These operations assist in enabling the group to identify where the weaknesses are within its victim's virtual domain. The classic example of this is UNIX (Uniplexed Information and Computing System) root exploitation. When a militia performs the root exploit, members of the group are attempting to assume the identity (and therefore authority, access, or ability) of the root administrator of a UNIX system. By conducting a root exploit, the militia is actively involved in changing the target system's configuration or software.[2]

Anyone with the correct tool has the ability to log onto a network and control the domain. Internet hacker tools like NetBus, Nmap, and Brian have become vehicles of political and social warfare.

>Capt Mitchell is currently the Assistant Intelligence Officer, 26th MEU. He teaches cyber warfare and counterterrorism for Henley-Putnam University. This was his submission for the LtCol Earl "Pete" Ellis Essay Contest.

Although the global domain is a virtual territory where citizens can relate to content through national affiliation, it is a borderless target for cyber militias.[3] In this sense, countries like China, Iran, or North Korea are not a large, conventional military threat to the United States. What *is* a current and continuous threat that has the ability to affect worldwide each individual in his home is a motivated cyber militia that intends to terrorize a state or local population. When combined with the conventional and cyber threats, countries like China and Russia could become an enormous threat.

This article seeks to address three categories of cyber militias that can affect our military domains and operations. Many of the militias have hybrid attributes that originated as other identities, but the premise of the categorization stems from the group's ability to sustain for a long period of time the organization or support and the group's ideology. The three categories of cyber militias are clan, cell, and state sponsored.

Clan Militias

The clan is based on the online gamers categorization where players unite to play games like World of Warcraft and Battlefield Heroes. When a user signs into an online session, he joins a clan with which to play within the gaming community. The clan is an ad hoc cyber militia that is organized around a central communications platform where the members share information and tools necessary to carry out cyber attacks against their chosen adversary for a limited duration of time.[4] Typically, after an attack or series of attacks, the clan has a tendency to disband.

The clan unites likeminded people who are willing and able to use cyber attacks in order to achieve a political or social goal.[5] A clan serves as a command and control platform where skillful active members can post motivational materials, attack instructions, attack tools, and so on. A key attribute for the clan to be a successful organization is its ability to recruit members and to clearly articulate the virtual agenda for the militia. Another important concern for the clan is its ability to ensure that the militia is accessible and easy to find. Through creative marketing, gaming, and social networking sites, clans can successfully corral individuals who share similar ideologies.[6]

Once connected, the clan has the opportunity to quickly mobilize in response to an event that is important to the members. With the wave of technologically connected individuals, the group can be united to similar members of Facebook in the form of "liking" organizations, which in turn will add the user to their information distribution lists that will publish the class's agenda. While there can be a core group of people that remain actively involved over extended periods of time, the membership can be expected to surge in size when the underlying issue becomes sensitive, or if the clan needs a certain resource to conduct an attack.[7]

Following an escalation in an underlying issue, the clan quickly forms via a rallying cry on the global domain. Within hours or even minutes, volunteers gather around a communications platform, share attack instructions, pick designated targets, and start performing cyber attacks. Once the repercussions that motivated the clan to unite for a specific action have occurred, the group has a tendency to disband, except for the clan's key members who organize the group's agenda. The membership of the clan forms a loose network centered on the communications platform, where few, if any, people know each other in real life.

Cell Militias

The cell model refers to hacker cells that engage in politically motivated hacking over a long period by consuming smaller clans as a means of support. This type of militia includes hackers, crackers, and script kiddies from the above category. One of the primary examples of a hacker cell is the Anonymous militia. Unlike the clan militia, cell militia members are likely to know each other in real life while remaining anonymous to the outside observer. Since their activities are almost certainly illegal, trust is a key attribute amongst the cell's members. Due to the members having to trust and know one another, the militia's higher headquarters size is limited and requires an extensive vetting procedure for any new recruits who are promoted from a lower clan. As the membership is experienced in cyber attack techniques, the cell militia can be proficient at attacking against unhardened targets.

> ***The command and control structure of the cell can vary from a clear, self-determined hierarchy to a flat organization where members coordinate their actions, but do not give or receive orders.***

Prior hacking experience also provides a potential weakness. If a member consistently utilizes the same affiliation or hacker alias, it is highly plausible that law enforcement knows the identity of the hacker. While there may not be enough evidence, damage, or a legal base for law enforcement action in response to their criminal attacks, the politically motivated attacks may provide a different set of rules for local law enforcement. Similar to entities previously mentioned, the hacking cells are similar to a mafia-style organization that will get rid of anyone who is selfish or counter to the organization's principles. In this case, those hackers who consistently brag in public forums or conduct their own attacks are exposed and ousted by the cell.

The command and control structure of the cell can vary from a clear, self-determined hierarchy to a flat organization where members coordinate their actions, but do not give or receive orders. In theory, several cells can coordinate their actions in a joint campaign, forming a confederation of hacker cells under a common ideology, similar to al-Qaeda.[8] Cells employ such common means or techniques to enable their agenda. The cells execute their plans through their tools and resources while recruiting clans that have a required capability. Most of the clans that are recent to the global domain are attracted to supporting the attacks of a higher, respective entity. Some of the cells that exist are Anonymous and the People's Liberation Front, or those that collectively executed attacks through the Israel-Palestine conflict.[9]

State-Sponsored Militias

"State-sponsored militia" refers to a traditional hierarchical model that can be found within government-sponsored volunteer organizations, as well as in cohesive, self-organized, nonstate actors. For example, the People's Liberation Army of China includes militia-type units in their information warfare battalions and leadership positions. The hierarchy militia model forms two generic submodels: anonymous and identified membership.[10] In some cases, nation states will use their universities or cells to act as their research and development or computer network exploitation elements to assist them anonymously.

In 2003 the People's Liberation Army included a hacker who attempted to map Florida Power and Light's computer infrastructure. In the implementation of his tool, the hacker *executed* the tool instead of simply performing noninvasive "discovery" activities by conducting reconnaissance on the network. When the hactivist executed his tool, he affected 3 million customers in southern Florida. In this instance, officials believe that the intrusion may have precipitated the largest blackout in North American history. A 9,300–square mile area including Michigan, Ohio, New York, and parts of Canada lost power, with an estimated 50 million people affected.[11]

The state-sponsored militia model is similar in concept to military units, where a unit commander exercises power over a limited number of subunits. The number of command levels depends on the overall size of the organization, and each subunit can specialize in some specific task or responsibility as delegated. This hierarchy militia model is the most likely option for a state-sponsored entity since it presents a more formalized capability and understandable structure. The control ability is vitally significant since the actions of a state-sponsored militia are, by definition, attributable to the state.[12]

On the other hand, some states have utilized cells to conduct their attacks. By using this method, the state can claim nonattribution of those entities that conducted the attack. Without attribution, there will be no real retribution for the cyber attack; therefore, if the state does not know for certain who attacked it, it cannot officially respond. On the other hand, if governments like the United States develop technology that attributes cyber attacks to cyber criminals, soon other governments will do the same. A potential outcome—if promoted by a country—is that the respective country will suppress free speech and abridge other civil rights.[13]

The obvious strength of a state-sponsored militia is the potential for efficient command and control and the availability of resources. A state-sponsored militia may exist for a long time even without ongoing conflict. During peacetime, the militia's capabilities can be improved with research and development, recruiting, and training. This degree of formalized preparation with no immediate action in sight is something that can set the state-sponsored militia apart from the clan and cell militias. If the militia is state sponsored, then it can enjoy state funding and infrastructure, as well as cooperation from other state entities such as the law enforcement or intelligence communities.[14]

On the other hand, a potential issue with the state-sponsored militia model is its ability to conduct scalable operations. Since this approach requires some sort of vetting or background checks before admitting a new member, it may be highly time consuming, thereby slowing the growth of the organization. At the same time, it may depend upon the nation-state's strategy and execution. Additionally, any activities attributed to the state-sponsored militia are attributed to the state. This puts heavy restrictions on the use of cyber militias during peacetime, as the legal framework surrounding state use of cyber attacks is currently unclear.[15]

A Warfare Transformation

The history of the attack on Georgian web sites via Russian advocates shows the world that a purely defensive posture can pose a significant risk. During the brute-force attacks, Georgia was at the mercy of hacktivists, with the government not being able to defend its networks in a timely manner to ensure its services; therefore, their government did not have the ability to communicate and function within the desired capacity. As the hacktivists operated within the syntactic level, they were able to take advantage of a vulnerability identified through computer network reconnaissance and surveillance to allow the hackers to exploit the operating system and gain access to the system to provide the malicious codes.[16]

Will we be prepared to counter cyber attacks? **(Photo by PFC Sarah Anderson.)**

Project Grey Goose estimates that Russia utilized, probably as a covert program, a mix between private and military hackers to enable the initial shaping actions to occur, which enabled the Russian military to maneuver into position to conduct its kinetic offensive operations. Through the private and military hacker organizations, the hierarchy command structure provided the necessary resources, tools, targeting matrices, and reconnaissance of mapping the networks. With the hierarchy conducting the trace routes, port scanning, enumeration, and exploitation, it allowed the incompetent hackers the ability to download a user-friendly tool identified within the forums and the attacks.[17] What remains interesting regarding the offensive cyber operation is the hacktivists' network's ability to display tactical patience, as they waited for specific direction from the informal chain of command.

Within this capacity, cyber warriors drew together to unleash vicious attacks against Georgia's networks, thereby paralyzing its ability to communicate in the brink of a stewing conflict. Cyber attacks, network security, and information pose complex concerns for a state's national security and public policy. The world's dependence upon computer operations will become the Achilles heel of great nations. A rival nation or group could exploit these vulnerabilities as a means to penetrate a poorly secured computer network thereby disrupting or even shutting down critical functions (i.e., geopolitical, supervisory control and data acquisition—transportation, power, water, etc.) and leaving command and control remaining. By shutting down critical functions, the nation creates a new set of problems for national security. For most of the critical infrastructure, multiple sustained attacks are not a feasible scenario for hackers or nation states, as was the case with the country of Georgia. In this case study, Russia showed the world a capability that was not fathomed, a capability that is somewhat compatible with the Cold War mentality, as governments do not want to identify their potential offensive weapons resources.

From a military vantage point, cyber operations have several appealing characteristics. First, the warning time for an attack and the timeframe for a defensive response is quite limited. Since cyber attacks travel at the speed of light and require little physical preparation, the attack could happen as quickly as a key stroke. Second is the lack of attribution. Cyber operations can assume a layered and varied route to their targets. By passing through so many Internet protocol addresses, only the last computer through which the route traveled may be identified. Without truly knowing who attacked the state, the victim state cannot accurately counterattack. Third, cyber operations can confuse other states, which can lead to frustration. One of the great scares within the cyber realm is hackers' ability to affect power grids, financial systems, and other critical infrastructure. By attacking these systems, the system could be rendered inoperable or create the same amount of destruction that would result from a kinetic attack by military forces. On the other hand, a nation may not have the ability to mount a cyber counterattack. Possibly more detrimental than a kinetic counterattack would be when nation states were to retaliate through cyber operations. If this occurs, other nations may see the cyber attack as unjustified and escalatory because no one has outlined through policies what an act of cyber war is.[18]

With the Pacific theater forming to be the next great battlefield with the technology potential of North Korea, China, and others, the United States is under the impression that a conflict with China is near. As such, China assumes that the U.S. military would begin early preparations with a deployment or buildup phase in the event of a conflict. With this impression, China has forecasted conducting offensive cyber operations on U.S. logistics functions during the proposed buildup phase as a means to delay or disrupt U.S. forces moving into their region. In this case, China has established four key elements. The first element lies in its defense, as China must protect its own assets first as a means to preserve its capability to move to an offensive mindset. Second, China also believes that if it is to pursue cyber attacks, it must initiate the strike in the initial phases of the conflict before its adversaries have the opportunity to defend themselves. Third is the power to influence warfare through information operations. In this capacity, cyber operations can be used to manipulate the adversary's perception of the crisis by planting inaccurate or incorrect information. The fourth element is the United States' dependency on technology. China believes that the United States is dependent on information technology, which can lead to its ability to exploit this suspected weakness.[19]

Conclusion

To decisively win in cyberspace we need to take our adversaries' abilities away. Cyber attacks, regardless of what country or entity benefits from them, could be initiated from anywhere in the world. This calls for new alliances and NATO partnerships when it comes to developing and establishing our presence within the global domain. To do so, we must be able to respond to any cyber threat within seconds and minutes. Currently there is no existing policy that outlines what an act of cyberspace warfare actually is, a position that needs to be rectified.

Notes

1. A sniffer is a keystroke logger that the hacker can plant on a system to snare passwords, credit card numbers, or other valuable information transmitted across the network. Once the sniffer retrieves one or more passwords, the hacker can use those them to hijack a legitimate user's account. If the sniffer happens to capture the password of a system administrator, the hacker can use the system administrator's account to gain root access (Wang, W., Steal This Computer, Book 3, N. Startch Press, San Francisco, CA, 2003).

2. Parks, R.A., "Principles of Cyber-Warfare," workshop on information assurance and security, West Point, NY, 5 June 2001, pp. 122–25.

3. Saad, S.B., "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield," Saint Joseph University, Beirut, Lebanon, 2007.

4. Ottis, R., "Theoretical Offensive Cyber Militia Models," Cooperative Cyber Defence Centre of Excellence, United Kingdom, 2011.

5. Ibid.

6. Ibid.

7. Ibid.

8. Ibid.

9. The People's Liberation Front conducted denial of service attacks against government web sites in Tunisia, Iran, Egypt, and Bahrain.

10. Ottis.

11. Harris, S., "China's Cyber-Militia: Chinese Hackers Pose a Clear and Present Danger to U.S. Government and Private-Sector Computer Networks and May be Responsible for Two Major U.S. Power Blackouts," *National Journal*, Washington, DC, 2008.

12. Ottis.

13. Bucci, S., "Should We Seek Cyber Attribution?" 2010, accessed at securitydebrief.com on 6 August 2011.

14. Ottis.

15. Ibid.

16. Cyberspace consist of three levels: physical, syntactic (above the physical), and the semantic layer on top. The syntactic level contains the instructions that designers and users provide the system, as well as the protocols that enable machines to communicate with one another. This is the level where hackers operate. See M. Libicki, *Cyberdeterrance and Cyberwar*, RAND Corporation, Arlington, VA, 2009.

17. Goodin, D., "Georgian cyber-attacks launched by Russian crime gangs," London, 2008, accessed at www.theregister.co.uk on 5 May 2011.

18. U.S.-China Economic and Security Review Commission, *Report to Congress of the U.S.-China Economic and Security Review Commission*, Government Printing Office, Washington, DC, 2008.

19. *China's Proliferation Practices, and the Development of its Cyber and Space Warfare Capabilities*, testimony of Dr. J. Mulvenon at a hearing before the U.S.-China Economic and Security Review Commission, Washington, DC, 2008.