Sun Tzu was a Hacker: An Examination of the Tactics and Operations from a Real World Cyber Attack

Billy K. RIOS[a]
[a] *GreyLogic., LLC*

Abstract. This text will cover the operational and tactical techniques used in a "real world" cyber-attack and includes an analysis of the planning, command, control, execution, and outcome of these cyber-attacks. The text focuses on the cyber-attacks against the nation state of Georgia in 2008, as the author was in a unique position to observe the communications, execution, and responses from both attacking and defending entities. The various aspects of the attacks will be described and linked back to traditional concepts of Maneuver Warfare as described in Marine Corps Doctrinal Publication 1 (MCDP-1).

Keywords. cyber warfare, cyber attack, offensive cyber capability, defensive cyber capability, Georgia, maneuver warfare

Introduction

"*Doctrine must evolve based on growing experience, advancements in theory, and the changing face of war itself.*"

General C.C Krulak, *MCDP-1*

The computer system sitting on your desk brings a new dimension to modern warfare. Just as the machinegun and airpower changed the face of warfare, so does offensive cyber capabilities. The ubiquity of computer systems in our military, government, and civilian infrastructure have solidified the importance of offensive cyber capabilities to the point where packets will be the "bullets" that will be fired in future conflicts. Software loaded on computer systems will be considered the "terrain" on which cyber warfare is waged. The use of packets as weapons presents a novel approach to warfare and will inevitably cause changes in military doctrine within our lifetime; however the employment of cyber capabilities continues to abide by many of the traditional concepts and principles of warfare. Associating the concepts of cyber war in the terms of conventional warfare and known doctrine can make analysis less daunting and provides a new perspective when measuring the impact and deciding how best to employ cyber capabilities. In this text, the author will examine the execution of a cyber-attack and correlate the principles of the attack to traditional concepts studied in maneuver warfare. The specific scenarios examined in this study involve the cyber-attacks conducted against the country of Georgia in 2008. Although the author uses a

specific cyber-attack to illustrate his points, the author hopes that the concepts presented in this text can be universally applied to any cyber-attack.

1. Maneuver Warfare

The principles of maneuver warfare will be referred to extensively in this text. While a complete description of all the concepts associated with maneuver warfare are beyond the scope of this text, the author begins by providing a fundamental description of maneuver warfare and its foundations. According to the Marine Corps Doctrinal Publication 1 (MCDP-1), maneuver warfare is described as a:

"war fighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope"

The focus on disrupting enemy cohesiveness makes maneuver warfare unique from other military doctrine. In maneuver warfare, entire enemy units and strongholds are bypassed in order to reach a "decisive opportunity" to exploit a "critical vulnerability" in the enemy's position [1]. Exploitation of critical vulnerabilities provides a pathway to attacking the enemy's "center of gravity" [1]. It is important to understand that despite its name, maneuver warfare is not limited to the maneuvering of units or spatial operations. Temporal actions such as psychological and technological disruption are also key elements of maneuver warfare. In maneuver warfare, well timed combat power brought to bear on strategic points on the battlefield, preemptive strikes geared towards the elimination of the enemy's decision making ability, surgical strikes on communication systems, elimination of the enemy's logistical chains, and suppression of enemy combat power are all more highly valued over high body counts or gained geography [1].

While the physical destruction of enemy forces and equipment is not the primary focus of maneuver warfare, physical destruction and firepower do play a central role at decisive points in battle, especially when destruction of enemy forces results in the degradation of the enemy's overall cohesion. Advanced weapon systems and technical superiority such as superior weaponry, stealth technology, and highly trained special operations forces (SOF) can increase the aggressor's opportunities to deliver decisive firepower on the right targets at the right moments, disrupting the enemy's normal operating rhythm and decision making ability. For example, in the lead up to Operation Desert Storm in 1991, SOF and air power disabled and destroyed a significant portion of the Iraqi command and control systems, disrupting Iraqi command and control at the highest levels [2]. While the success of the air power and SOF units would not have "won the war" in isolation, they disrupted the enemy's cohesion and decision making, allowing for more effective follow on operations which would ultimately win the war. It is this "disruptive capability" that is the quality that makes offensive cyber capabilities so attractive. The ability to disrupt the enemy's tempo, rhythm, and decision making from afar, in a lighting fast manner, while exposing very little, is extremely appealing to many commanders.

Although offensive cyber capabilities offer a novel approach to disrupting the enemy's normal rhythm and decision making, the prudent commander understands that much like air power, naval power, intelligence, and other individual military

capabilities, offensive cyber capabilities cannot "win a war" by itself [3]. Instead, these offensive cyber capabilities must be used as a component in the overall combined arms effort focused on disrupting the enemy's cohesion and exploiting critical vulnerabilities. Once the enemy's battle rhythm and decision making is disrupted, the disruption must be exploited via follow on actions. Disruption creates opportunities that should be ruthlessly exploited. This exploitation often leads to additional opportunities, which eventually leads to a decisive opportunity to launch a decisive attack against the enemy [1].

The author will present specific scenarios where offensive cyber-attacks were used in a manner that was consistent to the principles of maneuver warfare. The author chooses to focus on the 2008 cyber-attacks launched against the nation state of Georgia. These attacks are chosen due to the resources and vantage points the author held whilst the conflict progressed [4]. These resources and vantage points gave the author an insight into both sides of the conflict; however most of the examples and scenarios will focus on the aggressor and offensive actions. Before diving into the specific attacks that occurred against the Georgia infrastructure, it is important to define several terms which are used regularly in describing maneuver warfare. The author chose to focus on the following terms throughout the course of the text.

- Decentralized Command and Commanders Intent
- Combined Arms
- Initiative
- Centers of Gravity and Critical Vulnerabilities

1.1. Commanders Intent

The commander's intent provides the means for subordinates to exercise judgment and initiative. MCDP-1 states that each mission has two parts: (1) the task to be accomplished and (2) the reason or intent behind it. Commander's intent provides the reasoning and intent behind the assigned tasks and missions. Commanders intent is crucial for as the situation changes on the battlefield, the specific tasks assigned to the subordinate may become obsolete, but the intent is lives beyond the assigned tasks and continues to guide the subordinate's actions [1]. If the subordinate understands the commander's intent, they will be able to execute actions without the presence of direct orders and those actions will be in line with the commander's desires (which should ultimately advance strategic objectives).

In addition to the promotion of initiative, effective use of commander's intent allows for decentralization of command, pushing decision making to the lowest level. It is at these levels where forces are able to react and exploit opportunities in the most effective and efficient manner. Decentralized command and asynchronous execution is essential in the success of conventional operations in today's "small wars" [5] as well information based campaigns.

1.1.1. Target Lists and Commanders Intent

In August of 2008, the Grey Goose project commenced. Grey Goose was a pure open source intelligence initiative aimed at gathering and analyzing intelligence related to the Georgia cyber-attacks. During Phase I of the Grey Goose project, a number of

Russian hacker forums were mined for data detailing over 29,000 separate forum events with correlation of those events to status of Georgia cyber infrastructure [4]. One of the first items discovered on the various Russian hacker forums were target lists, providing the domain names of various Georgian servers to be attacked. A portion of the target list is shown in figure 1.

Сайт	Доступ с РФ (есть/нет)
www.parliament.ge Парламент;	-
http://occupation.tspteam.com	+
www.cec.gov.ge Избирком;	+
www.mdf.org.ge Муниципальный фонд развития;	-
www.mfa.gov.ge МИД;	+
www.corruption.ge Anti-Corruption Program;	-
http://smr.gov.ge/en/home	+
http://stoprussia.org/	+
www.insurance.caucasus.net Страхование;	-
www.mc.gov.ge Минкультуры;	-
www.nsc.gov.ge Совет безопасности;	-
www.supremecourt.ge Верховный суд;	+
www.iberiapac.ge Минтранс;	
www.court.gov.ge Department of material service;	+
www.civil.ge Ассоциации ООН в Грузии;	-
http://www.forum.ge/	+

Figure 1. Target list from Russian hacker forum

The target lists discovered on the various forums were simple and provided no specific direction or instruction as to how the various sites were to be attacked. The targets lists were simply lists of servers that should be targeted and attacked by forum members. Forum members were not assigned specific tasks, the specific techniques to be used were not defined, and the definition of a "successful attack" was broad and conceptual. Instead of publishing specific actions, the publisher of the target list allowed the forum members to decide the best course of action to carry out the attacks. Soon after the target list was posted, the forum was filled with chatter related to the most effective means of attacking the various servers. The communication was not directed to "higher" (to the forum administrator) asking for guidance, but instead focused on "lateral communication" (to other forum members), updating each forum member on newly discovered vulnerabilities and weaknesses [6]. As the lateral communications increases, each forum member cherry picks the data most appropriate to their interests and skillsets. This prejudicial filter helps maximize the impact of each individual forum member by allowing them to focus on applying their specific skillsets to attacking the servers on the target list, quickly identifying those servers that are most

vulnerable to those specific skills possessed by the individual. An individual contribution to the forum is shown in figure 2.

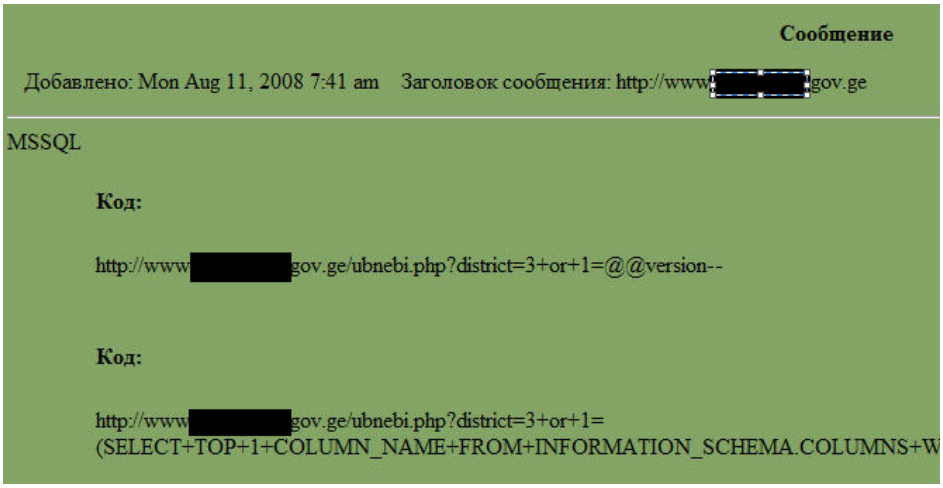

Figure 2. Various Forum Members Discussing Vulnerabilities

Despite its lack of detailed instruction, the target list established the framework for the most effective use of forum member skillsets. The target list and broad concepts of "success" are prime examples of an effective use of commander's intent [7]. As opposed to identifying individual forum members, attempting to determine their skillset, and assigning the forum members specific tasks/servers/exploits, the forum administrator establishes the overall intent of the attacks and essentially publishes the intent. The forum administrator publishes the target list (task to be accomplished) and broad guidance (the reasoning/intent behind the task). The forum administrator provides little/no guidance as to how the tasks are to be accomplished. Instead, the forum administrator relies on the forum members to develop their own methods to accomplish the tasks within the overall intent, exploiting weaknesses as they become evident, and relaying updates through lateral communications. As the situation changes (new vulnerabilities discovered, new defenses encountered, new tools released…etc.) the forum members proceed within the original intent and do not wait for further instruction. This allows maximum flexibility and effectiveness in attacking, a flexibility that simply cannot be matched in a highly centralized, top down command and control structure [1].

1.2. Combined Arms

Combined arms are utilized to maximize combat power. The term "combined arms" refers to making use of all the available resources to the best possible advantage. Combined arms are typically achieved through the complementary use of different weapon systems [1]. The weaknesses of one weapon system are supplemented by the strengths of a different weapon system. The classic example of combined arms automatic direct fire weapons (machine guns) and indirect fire weapons (grenade launchers). If the enemy infantry becomes pinned down by the automatic fire, they

become vulnerable to grenade attacks. If the enemy maneuvers to avoid the grenade attack, they expose themselves to the automatic weapons fire. The ultimate goal of combined arms it to utilize a full integration of various arms to achieve a situation so that when the enemy counteracts one arm, they are making themselves more vulnerable to another [1].

1.2.1. SQL Injection, DDOS Tools, and Combined Arms

In order to extract the maximum effect from offensive cyber strikes, the strikes must be used as part of a combined arms effort. This combined arms effort can involve the leveraging the exploitation a single cyber related vulnerability to accomplish successful exploitation of another cyber related vulnerability. The combined arms effort could also involve the exploitation of cyber related vulnerabilities in conjunction with the use of kinetic weapons or conventional forces. During the investigation of data made available to the Grey Goose project, exploitation of several SQL injection vulnerabilities against various Georgia applications were discovered [4]. SQL injection attacks in the logs of a Georgia server are shown in figure 3.

```
[Tue Jul 01 05:32:43 2008] [error] [client 91.XXX.XXX.XXX] File does not exist:
/home/virtual/XXX/public_html/small4, referer: http://www.XXX.gov.ge/full_text.php?nid=-
6038%20union%20select%201,2,3,4,5/*
[Tue Jul 01 05:33:19 2008] [error] [client 91.XXX.XXX.XXX] File does not exist:
/home/virtual/XXX/public_html/small4, referer: http://www.XXX.gov.ge/full_text.php?nid=-
6038%20union%20select%20unhex(hex(version())),2,3,4,5/*
[Tue Jul 01 05:33:35 2008] [error] [client 91.XXX.XXX.XXX] File does not exist:
```

Figure 3. Examination of log files show evidence of SQL Injection attacks

These SQL injection vulnerabilities were initiated from Russian IP addresses and log data provides many of the exact SQL injection queries that were used in the attacks. These targeted SQL injection attacks began in July of 2008, months before the high profile attacks against Georgia in August of 2008. The SQL injection attacks started with simple fingerprinting of the backend database servers being used by the vulnerable applications. An examination of the log files shows that once the fingerprinting of the backend database was complete, the Russian hackers extracted the usernames and passwords associated with the vulnerable applications. The usernames and passwords are valuable because they provide the foundation for attacks against other systems. For example, once the usernames and passwords are extracted, the hacker can test those username and password combinations against other, better protected information systems (password reuse) [8]. If any of the users of the compromised application have reused their password on other systems, the hacker can now masquerade as a legitimate user on that other system. Password reuse can also lead to the compromise of personal and business email accounts, providing a stream of intelligence that can be used in conjunction with other attacks (both cyber and conventional). If a hacker has gained access to the business and personal email systems of those employees, the hacker will be in a prime position to collect intelligence on those individuals, feeding the captured data into traditional intelligence analysis and fusion.

Figure 4. Forum Members Make DDoS Tools Available to Novice Hackers

Once the attacks against Georgia became public and conventional action was imminent, many of these SQL injection vulnerabilities were posted on various hacker forums, allowing others to take advantage of the SQL injection vulnerabilities. In addition to the SQL injection attack vectors, tools were developed and posted to enable the flooding of Georgia servers, creating a distributed denial of service attack against various parts of the Georgia infrastructure. The automated tools gave even novice hackers the ability to disrupt communications while also spreading the attacking surface. An example of the tools being distributed is shown in figure 4. Both highly skilled, targeted attacks coupled with unskilled, broad DDoS attacks were used against the Georgia infrastructure, forcing the defender to address both issues simultaneously. Once attention and resources were dedicated to defending the information systems, the Russian military began the conventional campaign [9].

The exploitation of a single application level vulnerability leads to further compromise and exploitation, long after the initial vulnerability is fixed. Pilfered information leads to more pilfered information, which in turn leads to even more information theft and swells into enormous amounts of sensitive data being stolen. This data is fed into traditional intelligence analysis efforts, helping to paint the picture of the lives of government employees involved with various projects on separate, seemingly unrelated servers [10]. As the situation changes, some vulnerabilities can be repurposed to fit new situations and scenarios. Various attacks (SQL injection, Command Injection, DDoS…etc.) are launched simultaneously, forcing the defender to addresses multiple scenarios and skillsets simultaneously. Eventually, the Russian military initiated contact though conventional means, adding yet another dimension onto the defenders dilemma [9]. This chain of events began with the targeted exploitation of a single vulnerability in a single application and grew into multiple attacks launched simultaneously, along with the beginning of a conventional campaign.

1.3. Initiative

MCDP-1 describes two states that all actions in war are based upon; “initiative” and “response”. MCDP-1 describes initiative as the ability to “dictate the terms of the conflict and force the enemy to meet us on our terms” and response as “resistance to initiative” [1]. Taking the initiative is considered the more preferable of the two states as, “it is through the initiative that we seek to impose our will on the enemy” [1]. In traditional military operations, initiative is established by forcing the enemy to assume a reactionary stance against active actions. These actions typically gain initiative though the effective use of surprise, tempo, concentration, and audacity. Offensive

cyber capabilities offer tremendous opportunities to gain the initiative [11]. The very nature of cyber-attacks brings about the elements that are commonly associated with initiative: surprise, tempo, concentration, and audacity. Initial contact can be initiated with little risk as attacks can be launched from a variety of locations, including non-state sponsored educational and commercial networks. The nature of today's networking makes uncovering undisputable links to State sponsorship an extremely difficult task [12]. These attacks have the ability to disrupt conventional systems and decisions making from long ranges, helping shape the battlefield well before any rounds are fired.

An example of how cyber-attacks can be used to help establish the initiative for conventional forces is presented in the attacks against Georgia in 2008. In July of 2008, before a single shot was fired by conventional forces, Russian based hackers had already penetrated Georgia government applications with SQL injection and other application level attacks [13]. During the pre-emptive cyber strikes, several high profile systems (such as the website of the President of Georgia) were compromised. The pre-emptive attacks undoubtedly captured the attention of the Georgia government, forcing parts of the Georgian government to utilize a "decision making cycle" in order to determine the appropriate response [14]. By initiating contact and forcing the Georgian government to enter the decision making cycle, the Russian hackers gain the initiative, forcing a reactionary stance by the Georgian government. Much like conventional attacks, a single, un-sustained attack is insufficient in maintaining the initiative, so the Russian hackers followed with sustained attacks against a wide range of government systems. Eventually, these cyber-attacks were followed by conventional ground and air attacks. Each phase of the attack is meant to keep the enemy off balance and in a reactionary state. Agility, tempo, and surprise continuously disrupt the defenders decision making, allowing the attacker to dictate the terms of engagement. As the defenders observe, orient, decide, and attempt to act upon targeted attacks, the attackers launch broad denial of service attacks against the entire infrastructure. As the defenders rush to observe, orient, decide and act to defend the wide scale cyber-attacks, the attacker changes the terms of engagement and initiates the conventional ground and air campaign. These offensive cyber-attacks were not the ultimate end state; instead they were used to augment the achievement of initiative in conventional warfare in support of the true main effort.

1.4. Centers of Gravity (CoG) and Critical Vulnerabilities

Building a combat capability is not sufficient to win a war; to win a war, the built up combat capability must be directed towards a decisive objective. Although several interpretations for Centers of Gravity (CoG) exist, MCDP-1 considers CoG as the "sources of strength for the enemy". These sources of strength need not be physical and can encompass "intangible characteristics such as resolve or morale". MCDP-1 states that centers of gravity are to be attacked (although not directly, if well-defended). While CoG focuses on the enemy's strengths, critical vulnerabilities focus on the enemy's weaknesses. While the enemy is likely to have several vulnerabilities, some of these vulnerabilities will result in greater damage than others. Some these vulnerabilities may "contribute significantly to the enemy's downfall while others may lead to only minimal gains" [1]. Those vulnerabilities which offer the greatest impact

are known as critical vulnerabilities. These are the vulnerabilities that are to be pursued by attacking forces and should be the focus of efforts.

The ubiquity and prevalence of information systems increases the overall attack surface and number of exposed vulnerabilities. Finding, classifying, and determining which of these vulnerabilities are "critical vulnerabilities" is crucial in the effective employment of offensive cyber capabilities. Once again, planners must not silo cyber capabilities, as information weapons can be used to create opportunities for maneuver against conventional critical vulnerabilities and ultimately CoG. Much effort has already been placed in determining the CoG and critical vulnerabilities in planning for conventional warfare, these CoG should be reevaluated to find avenues where offensive cyber capabilities can help maneuver against critical vulnerabilities and create opportunities for attacks against CoG. Critical infrastructure is one such conventional CoG that has already been identified where offensive cyber capabilities can bring new avenues of attack and exploitation [15]. The enemy's critical infrastructure has always been a prime target for conventional and kinetic weapons, information weapons simply bring new avenues to reaching and disrupting this critical infrastructure. As planners begin to understand the capabilities of offensive information weapons, some CoGs and critical vulnerabilities will change. Not all of these new CoGs and critical vulnerabilies will be purely military, civilian infrastructure will be affected as well. As CoG to blur from military objectives to civilian objectives, war will truly become an "extension of politics" as opposed to a struggle between two different military forces.

2. New Weapon Systems, Classic Principles

"Over time, perhaps as little as in twenty years, and as the leverage provided by technology increases, this threshold will finally reach its culmination - with the ability of one man to declare war on the world and win."

John Robb, *Brave New War*

Conventional weapons (rifles, indirect fire weapons, explosives…etc) have physical limitations. These physical limitations cannot be overcome even if the individual employing that weapon system is highly skilled or experienced with that weapon system. These physical characteristics provide the basis for the development of tactical guidance for effective employment of the weapon system. For example, the M4 carbine is designed to be employed as a short/medium range weapon in force while the M24 Sniper Weapon System is designed for precision, long range fire from trained marksmen [16]. This foundation for the employment guidance for the M4 and M24 are based on the specific characteristics and physical capabilities of the weapon system. The skillset of the individual employing the conventional weapon system may stretch the weapon systems capabilities in a small way, but the ultimate capabilities of the weapon system remained tied to the physical characteristics of the weapon.

The weapons (information weapons) used in cyber-attacks are different from conventional weapons. With conventional weapons, the physical weapon system represents the capabilities being brought to the battlefield. Information weapons enjoy a different type of relationship. With information weapons, the attacking power of the weapon system is directly correlated to the skillset of the individual using the weapon system. The capabilities of conventional weapons systems are bound to the physical

characteristics of the weapon system. Two identical rifles fired by two differently skilled operators will continue to fire with the same muzzle velocity and rate, as the physical characteristics constrain the ultimate capabilities of the weapon. Information weapons on the other hand, are bound directly to the skillset of the individual employing the information weapon [17]. Two identical laptops employed by two differently skilled operators will have completely different capabilities. As the individual's skillset increases, so does the striking power and effectiveness of the information weapons employed by that individual. Creating an offensive cyber capability is less about finding the right hardware and more about finding the right people and skillsets.

The importance of the individual brings about unique challenges for intelligence organizations when attempting to understand and estimate the enemy's offensive cyber capabilities. With conventional weapon systems, capability can be tracked via procurement, tracking of the physical location of the weapon systems, and active surveillance of the weapon system. Physical movement and logistical operations associated with the employment of conventional weapons are eagerly watched by intelligence organizations and is used in all types of intelligence analysis. Developing a nuclear capability for example, require distinctive materials, specialized knowledge, and distinctive facilities for development. Non-proliferation is tracked through safeguards which monitor materials, inspections of facilities, and surveillance. Each safeguard has a threshold that indicates when a nation state may be attempting to create a nuclear capability. Nation states developing an offensive cyber capability can do so in a much more subtle way. There are no specific thresholds, distinctive materials, or facilities that indicate an offensive capability is being developed [18]. Individuals with a solid understanding of offensive security can be trained or recruited from both academia and corporate environments putting impressive offensive cyber capabilities within reach of every nation, regardless of size or economy. These individuals are the capability. With information weapons, the capability rests with the operator of the information weapon, not the equipment itself. The commercially available laptop available at any major retail outlet can be used to conduct attacks against any nation in the world. The striking power of this attack is measured not by the hardware, but the skillset of the operator. This makes tracking via procurement and logistical operations impossible. The wide spread availability of sufficient hardware coupled with the lack of distinctive, easily tracked characteristics not only lowers the barrier for entry for establishing an offensive cyber capability, it makes determining the true source of the attacks virtually impossible. Intelligence organizations must now shift focus from identifying physical equipment and logistical actions to identifying key capabilities and specific skillsets possessed by individuals. This is an extremely difficult and daunting task, making determining the true capabilities of nation's offensive cyber capabilities difficult.

In August of 2008, the Grey Goose project kept a Russian hacker forum under surveillance watching the interaction of the various forum members. Investigators determined that the forum had over 600 registered members (users were required to register in order to read/write posts). A sample of the forums member list is shown in figure 5.

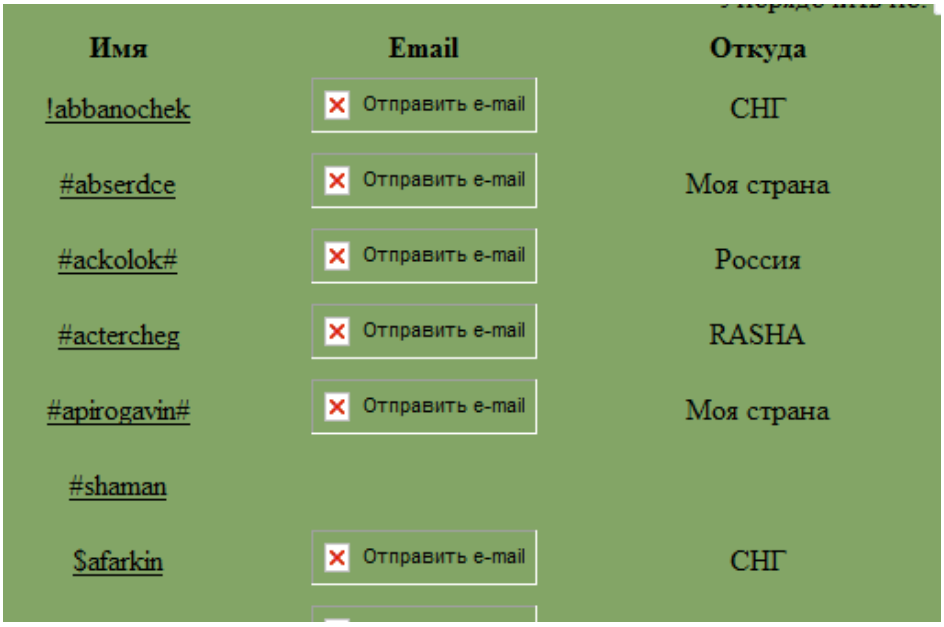

Figure 5. Member List from a Russian Hacker Forum

It was impossible to immediately determine which of the forum participants represent a legitimate offensive capability and which forum members are simply "script kiddies" (unskilled participants). Analysts for the Grey Goose Project were forced to analyze thousands of forum events, learning about the various topics being discussed by the forum members. Each forum post was analyzed for technical sophistication and technical leadership. Relationships between forum members were mapped using technically sophisticated Palantir analysis platforms [19]. Only after extensive analysis could the Grey Goose investigators determine which members represented the true offensive capability of the forum. Once these individuals were identified, surveillance focused was focused on these key individuals. Each individual was noted and ranked using forum participation as the key indicator of their technical sophistication (individual contributed vulnerabilities, contributed tools, provided advice for exploitation…etc.). This approach allowed the analysts to focus on the handful of individuals driving the offensive capabilities of the entire forum. It was these individuals that were offensive capability, not the tools, hardware, or even the forum [4].

3. Conclusions

"*Preparing to win in combat must be the highest priority in the allocation of time, dollars, and rewards, at every level and under all circumstances*"

William S. Lind, Maneuver Warfare Handbook

3.1. Employment

The focus on using cyber capabilities to "win wars" must be at the forefront when developing doctrine. It is easy to become enamored with the seemingly magical displays of exploitation and technical jargon; however planners must recognize that cyber capabilities represent one of many dimensions of warfare. Planners must not silo cyber capabilities, employing them in isolation, but must consider how best to augment conventional capabilities with cyber capabilities. Having a robust cyber capability is important, however winning the "cyber-battle" while losing the conventional war is unacceptable in any scenario. In time, information weapons will be the weapons of force, perhaps establishing themselves as the "main effort" in campaigns with conventional forces designated as "supporting efforts". Until that time, information weapons are to be employed much like other conventional weapon systems as supporting efforts, helping shape the battlefield in support of the main effort (typically conventional forces). Planners must strive to integrate cyber capabilities into conventional warfare as a supporting arm. Information weapons, much like other supporting arms, must be cognizant of the main effort and should strive to shape the battlefield in support of the main effort. Commanders must be acclimated as to how to request supporting cyber capabilities and understand what gaps offensive cyber capabilities can cover.

3.2. Command

Rigid, highly centralized command makes the development and effective employment of offensive cyber capabilities difficult. Commanders must be careful not to impose rigid requirements or artificial constraints onto cyber capabilities. Judicious use of commander's intent is essential in establishing the decentralized operational command necessary for the development and effective employment of offensive cyber capabilities. A top down, micromanaged effort will kill the speed, tempo, and most importantly the creativity required in effective cyber-attacks. Hierarchical, centralized ***administrative*** chains of command are essential for the good order and discipline in military ranks; however ***operational*** chains of command should strive to push decision making down to the lowest level, using commanders intent to guide decision making and initiative. This forces a more decentralized approach to employment of cyber capabilities, allowing for the need flexibility needed to successfully employ offensive cyber capabilities. Without this decentralized approach, employment of offensive cyber capabilities will ultimately fail.

3.3. The Individual is the Weapon System

The leverage technology brings coupled with the increasing ubiquity of information systems builds upon the power wielded by individuals with the right skillsets. As operational commands become more and more decentralized and the impact of the individual becomes more and more powerful eventually, a tipping point will be reached and the individual will represent the offensive capability. The concept of the measuring a nation state's striking power and capability through the surveillance and tracking of ground forces, air, and naval equipment will eventually succumb to the identification of highly skilled individuals that represent the offensive cyber capability. As our reliance on technology continues to evolve, the ability of the lone individual to disrupt conventional operations also increases. Eventually, the power of the lone individual will grow until a lone, highly skilled individual (or a small team of highly skilled individuals) will be able to impose their "political will" on other individuals, corporations, and even nation states.

References

[1] United States Marine Corps, *Marine Corps Doctrinal Publication 1 - Warfighting*, United States Marine Corps, Quantico, VA, 1997. http://www.dtic.mil/doctrine/jel/service_pubs/mcdp1.pdf

[2] Department of Defense, *Conduct of the Persian Gulf Conflict*, Department of Defense, Washington, DC, 1991. http://www.dod.gov/pubs/foi/reading_room/305.pdf

[3] Correlli Barnett, *Victory Through Air Attack? It's a Pie in the Sky*. TimesOnline, 2009. http://www.timesonline.co.uk/tol/comment/columnists/guest_contributors/article5469051.ece

[4] Jeffery Carr, *Grey Goose Phase I.* GreyLogic, 2008. http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report

[5] Kevin Benson, *Tactics for Small Wars.* Institute of Land Warfare, 2008. http://www.ausa.org/SiteCollectionDocuments/ILW%20Web-ExclusivePubs/Landpower%20Essays/LPE08-1.pdf

[6] Marine Corps Combat Development Command, *Offensive Fundamentals I*. Marine Corps Combat Development Command, 2009. http://www.usna.edu/USMCInfo/Documents/Pubs/b0354.pdf

[7] Lt Col. Lawrence Shattuck, *Communicating Intent and Imparting Presence*, Military Review, 2000. http://www.au.af.mil/au/awc/awcgate/milreview/shattuck.pdf

[8] Ives, Walsh, Schnieder, *The Domino Effect of Password Reuse*, Communications of the ACM, 2004. http://portal.acm.org/ft_gateway.cfm?id=975820&type=pdf&coll=GUIDE&dl=GUIDE&CFID=38680500&CFTOKEN=56506836

[9] Kenneth Corbin, *Lessons From The Russia-Georgia Cyberwar*, Institute of Communications Studies, 2009. http://ics.leeds.ac.uk/papers/vp01.cfm?outfit=gdr&folder=442&paper=750

[10] Whitaker, Evans, & Voth, *Chained Exploits: Advanced Hacking Attacks from Start to Finish*, Pearson, 2009.

[11] Office of the Secretary of Defense, *Military Power of the People's Republic of China 2006*, Office of the Secretary of Defense, 2006. http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf

[12] William Jackson, *US Already at War in Cyberspace*, Government Computer News, 2009. http://www.gcn.com/Articles/2009/04/22/RSA-cyberwar.aspx

[13] Toomas Hobermagi, *Estonia Promises Georgia Help in Fighting a Cyberwar*, BalticBusinessNews.com, 2008. http://balticbusinessnews.com/Default2.aspx?ArticleID=4743f52b-6f71-4ebd-ad1c-ca4ab13ad921

[14] Wikipedia, *OODA Loop*, Wikipedia.com, 2009. http://en.wikipedia.org/wiki/OODA_Loop

[15] Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure Protection*, Greenwood Publishing 2002.

[16] Department of Defense, *Basis of Issue Plan – M24,* Department of Defense. http://www.fas.org/man/dod-101/sys/land/docs/bnI063AA.htm

[17] Killgannon & Cohen, *Cadets Trade the Trenches for Firewalls*, Nytimes.com, 2009. http://www.nytimes.com/2009/05/11/technology/11cybergames.html?_r=2&ref=technology

[18] Wikipedia, *Nuclear Proliferation*, Wikipedia.com, 2009. http://en.wikipedia.org/wiki/Nuclear_proliferation

[19] Palantir Technologies, *Palantir Government Services*, 2009. http://www.palantirtech.com/