Strategy Research Project

RUSSIAN CYBERSPACE STRATEGY AND A PROPOSED UNITED STATES RESPONSE

BY

LIEUTENANT COLONEL RICHARD G. ZOLLER
United States Army

USAWC CLASS OF 2010

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
25-01-2010	Strategy Research Project	

4. TITLE AND SUBTITLE

Russian Cyberspace Strategy and a Proposed United States Response

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lieutenant Colonel Richard G. Zoller

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Charles Van Bebber
Department of National Security and Strategy

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Russia has made cyberspace attack a major factor in its military strategy in order to coerce "near abroad" nations to align with Russian national interests. This paper analyzes two cases of purported cyberattacks by Russia in 2007 and 2008. Although subsequent investigations were inconclusive, the cyberattacks were widely believed to be instigated by the Russian government. Based on the analysis of these two case studies, this essay recommends a foundational strategy United States strategy to counter the Russian strategy of coercing its "near abroad" nations using cyberspace.

15. SUBJECT TERMS

Computer, Georgia, Estonia, Deterrence, Networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	28	

USAWC STRATEGY RESEARCH PROJECT

RUSSIAN CYBERSPACE STRATEGY AND A PROPOSED UNITED STATES RESPONSE

by

Lieutenant Colonel Richard G. Zoller
United States Army

Colonel Charles Van Bebber
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Richard G. Zoller

TITLE: Russian Cyberspace Strategy and a Proposed United States Response

FORMAT: Strategy Research Project

DATE: 25 January 2010 WORD COUNT: 5,021 PAGES: 28

KEY TERMS: Computer, Georgia, Estonia, Deterrence, Networks

CLASSIFICATION: Unclassified

Russia has made cyberspace attack a major factor in its military strategy in order to coerce “near abroad” nations to align with Russian national interests. This paper analyzes two cases of purported cyberattacks by Russia in 2007 and 2008. Although subsequent investigations were inconclusive, the cyberattacks were widely believed to be instigated by the Russian government. Based on the analysis of these two case studies, this essay recommends a foundational strategy United States strategy to counter the Russian strategy of coercing its “near abroad” nations using cyberspace.

RUSSIAN CYBERSPACE STRATEGY AND A PROPOSED UNITED STATES RESPONSE

> The numerous cyber attacks launched in recent years against advanced information societies aimed at undermining the functioning of public and private sector information systems have placed the abuse of cyberspace high on the list of novel security threats. The acknowledgment that such attacks pose a threat to international security reached new heights in 2007 owing to the first-ever co-ordinated cyber attack against an entire country - Estonia – and also because of large-scale cyber attacks against information systems in many other countries as well.
>
> —Estonian Cyber Security Strategy[1]

As can be inferred from the statement above, cyberattacks[2] have become a part of military strategy. Countries such as China have been exploiting cyberspace for years to engage in computer espionage and have exfiltrated enormous amounts of sensitive information. Going a giant step further, Russia has made cyberspace attack a major factor in its military strategy in order to coerce "near abroad"[3] nations to align with Russian national interests. As recently as January 2009, Kyrgyzstan, one of the Russian "near abroad" nations, was the latest to suffer from cyberattacks by computers located in Russia.[4] This paper will analyze two cases of Russian cyberattacks and recommend a United States strategy to counter the Russian strategy.

Background

In order to understand and develop a United States' strategy to counter Russian cyberstrategy, some terms must be defined regarding cyberspace. Cyberspace has been defined in many different ways. For the sake of consistency, the Department of Defense (DOD) definition will be used here. According to a Deputy Secretary of Defense memorandum, cyberspace is defined as, "A global domain within the information environment consisting of the interdependent network of information

technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] Cyberspace operations were further defined by a later DOD memorandum as "The employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in and through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[6] Cyberspace operations are subdivided into two main components, Computer Network Operations (CNO) and Network Operations (NETOPS). Computer Network Operations is further subdivided into Computer Network Attack (CNA), Computer Network Exploitation (CNE) and Computer Network Defense (CND). Joint Publication 1-02 (JP 1-02) defines CNA as, "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."[7] JP 1-02 defines CNE as "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."[8] CNE is fundamentally different from CNA. Computer Network Exploitation is more comparable to spying, whereas CNA is focused on disruption or corruption of an adversary's systems or networks.[9] Computer Network Defense is defined as, "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks." [10]

Two other terms which are extremely relevant to any discussion of cyberstrategy are deterrence, in general, and cyberdeterrence, in particular. JP1-02 defines deterrence as "the prevention from action by fear of the consequences. Deterrence is a

state of mind brought about by the existence of a credible threat of unacceptable counteraction."[11] In RAND's monograph, "Cyberdeterrence and Cyberwar", the author chose to define cyberdeterrence as, "deterrence in kind to test the proposition that the United States…needs to develop a capability in cyberspace to do unto others what others may want to do unto us."[12]

The Estonia Case

In April 2007, the small Baltic state of Estonia was hit by an unprecedented cyberattack. The Estonians relocated a Russian war memorial, the Bronze Soldier, from Tallinn to a military cemetery, which outraged Estonia's Russian-speaking citizens, leading to two days of rioting.[13] Throughout April and early May 2007, Estonia was the victim of several weeks of clearly coordinated cyberattacks against its social, political and financial institutions.[14] Key Estonian web sites were flooded with Distributed Denial of Service attacks (DDOS) that effectively shut them down. Additionally, key government web pages were hacked and botnets (short for Internet Robot Networks) were used to take control of computers.[15] Estonia is a small country but it is extremely Internet dependent and conducts much of its business in cyberspace. Also, hundreds of thousands of Estonians work outside the country and use cyberspace to wire money back to their families.[16] Estonia conducts an astonishing 98 percent of its banking online and when the Distributed Denial of Service attacks disconnected its two largest banks for hours, the impact was nearly paralyzing.[17] It has been argued that the source of the attacks cannot be conclusively traced back to the Russian government or military but Estonia has insisted that the attacks represented the culmination of Russia's year long plan to attack the Estonian government for their anti-Russian policies.[18]

Because the attacks used botnets, the cyberattacks cannot be conclusively attributed to the Russian government. Botnets are used to remotely take over a computer by loading it with rogue software, usually without the knowledge of the computer owner. The computers, once hijacked using botnets, were then used to send thousands of messages per minute to Estonian servers, causing them to crash.[19] One such attack against an Estonian Internet Service Provided disrupted Estonian "government communications for at least a "short" period of time."[20] Because it is difficult to trace the origination of the botnets, it neither proves Russian guilt nor its innocence. As will be discussed later, attribution is one of most difficult aspects of cyberwar. It is possible that Russia could have used government agents to "incite patriotic Russian hackers, of which, there are plenty, as well as cybercriminals to attack Estonian targets".[21] Because the cyberattacks were well coordinated with organized violent demonstrations in Tallinn among Russians and in Moscow against the Estonian embassy, it seems evident that the computer attacks were sanctioned in Moscow "and reflected a coordinated strategy devised in advance of the removal of the Bronze Soldier from its original pedestal."[22]

Because of Estonia's dependence on cyberspace in all facets of life, they were particularly vulnerable to a cyberattack but also better prepared to respond. In the immediate aftermath of the attacks, Estonia took the matter to the North Atlantic Treaty Organization (NATO) of which it has been a member since 2004.[23] Estonian's Defense Minister Jaak Aaviksoo said, "that the cyberattacks were a threat to Estonia's national security and likened their effect to a blockade of a country's sea ports".[24] Although Estonia asked for NATO's help in responding, a senior civilian NATO official said "that

Estonia's response ...was so effective as to preclude the need for drastic NATO action" and "NATO experts summoned by Estonia during the weeks of the attacks had learned at least as much as they had contributed in terms of advice".[25] In fact because of Estonia's leadership in cyberspace, seven NATO nations signed the documents to establish a Cooperative Cyber Defence (CCD) Centre of Excellence (COE) in Tallinn, Estonia.[26]

The Georgia Case

As with Estonia, Georgia suffered a similar cyberattack during its conflict with Russia in 2008. On 8 August, just as Russian troops were moving into South Ossetia to defend the so called Russian compatriots, "a multi-faceted cyber attack began against the Georgian infrastructure and key government web sites".[27] Again, the attacks included web defacement, and distributed denial of service attacks but also included ""Web-based Psychological Operations" and a "fierce propaganda campaign".[28] In addition to hacking hundreds of Georgian government and news sites, the attackers hacked the Georgian parliament site and replaced content with images comparing Georgian President Saakashvili to Adolf Hitler. The attackers were even able to disrupt President Saakashvili's telephonic interview with CNN.[29] In their report, the United States Cyber Consequences Unit (U.S. CCU) stated that "signs of advance preparation and planning, suggests that cyber attacks against Georgia had been on the Russian agenda for some time."[30] According to the Benton Foundation, "the leading suspect behind the attacks, which disabled key government Web sites, is a cybercriminal organization known as the Russian Business Network."[31] As Marcus H. Sachs, Director of the SANS Internet Storm center states, "RBN is a virtual safe house for Russian criminals responsible for malicious code attacks, phishing attacks, child

pornography and other illicit operations."[32] Though it is not clear what precisely is the nature of the interaction between the Russian government and those who executed the attacks, it does seem that it is likely to become part of Russia's standard operating procedure henceforth to use cyberspace as part of an integrated strategy to coerce its "near abroad" nations.[33]

Again, because of the ability to remain anonymous in cyberspace it is difficult to attribute the attacks directly back to the Russian government. However, according to "Internet technical experts, it was the first time a known cyberattack had coincided with a shooting war"[34], leading to the possible conclusion that the Russian government was behind the attacks. Of course, the Georgians accused the Russians who in turn denied any responsibility.[35] A "wilderness of mirrors" which is used to describe intelligence agencies is an appropriate metaphor describing cyberwar and can be used to depict what happened in Georgia during the attack.[36]

Because Georgia doesn't rely as heavily on cyberspace, the attacks had far less immediate impact than it did in Estonia "where vital services like transportation, power and banking are tied to the Internet."[37]

Russia's Cyberspace Strategy

The two cases described above should lead one to believe that Russia has integrated cyberspace as part of an overall military strategy. Although there is an absence of any formal charges within the international community against Russia, their complicity in the cyberattacks remains uncertain. Russia first used the term cyber in April 2008 when the deputy director of the Department of Information Society Strategy, Vladimir Vasilyev, used the term several times in charts explaining President Vladimir Putin's document, "The Strategy of Information Society Development in Russia."[38] In

fact, Russia, like China prefers to use the term “informationization” and recognizes that “informationization” highly influences the means and methods of conducting war.[39]

When one analyzes the way in which the cyberattacks were orchestrated against both Estonia and Georgia, it is easy to recognize that the cyberattacks were not an end in themselves but part of an integrated strategy. As Kenneth Geers, the United States representative to the Cooperative Cyber Defense, Center of Excellence states in his article *Cyberspace and the changing nature of warfare*, “practically everything that happens in the real world is mirrored in cyberspace”[40] and that “strategists must be aware that part of every political and military conflict will take place on the internet.”[41] More than any other nation state, Russia uses the cognitive domain of cyber as much as the technical domain.[42] Where Western definitions of cyberspace focus on technical aspects of information technology, “informationization” takes on a much broader definition. “Informationization” can be broadly defined as, applying modern information technologies into all fields of both social and economic development, including intensive exploitation and a broad use of information resources.[43] What this means is that Russia uses cyberspace more to disrupt an adversary’s information than to steal or destroy it. This can be seen in both cases described above. While attackers defaced web pages and temporarily shut down cyberspace services in both Estonia and Georgia, no permanent damage was made. The attacks, especially against Georgia, demonstrate a key component of the Russian’s cyberspace strategy of coercion. As John Bumgarner, a former cyber security expert for the CIA and other U.S. intelligence agencies told reporter Steve LeVine, “they [the attackers] didn't attempt to cripple sites that could

have caused chaos or injury, such as those linked to power stations or oil-delivery facilities, but merely those that could trigger comparative “inconvenience”." [44]

As Timothy L. Thomas, a senior analyst at the Foreign Military Studies Office at Fort Leavenworth, Kansas explains in his chapter, “Nation-state Cyber Strategies from China and Russia”, the “targets of disorganization are not only weapons and decisionmakers on the field of battle but also in the mind of average citizens.”[45]

Possible Cyber Strategies

In the December 2008 report, “Securing Cyberspace for the 44th Presidency”, the Center for Strategic and International Studies commission spelled out three major findings. First, “cyberspace is now a national security problem for the United States.”[46] Second, “decisions and actions must protect privacy and civil liberties.”[47] Finally, and most importantly for the subject of this paper, “only a comprehensive national security strategy that embraces both the domestic and *international* (emphasis added) aspects of cybersecurity will make us more secure.”[48] In the 2009-2010 Chairman of the Joint Chief of Staff’s guidance, Admiral Mullen states that “we must put more resources -- intellectual, money and people – into accelerating development of our cyber capabilities and integrating them into our daily operations.”[49] In dealing with Russia in cyberspace, the United States must not only protect and defend American interests but also those of our allies, which include Russian “near abroad” nations, such as Poland, Slovakia, Romania, and the Baltic states. In the case of Estonia, international interest was high when that country asked for a reinterpretation of NATO’s Article 5, which states that “an armed attack against one (member)…shall be considered an attack against them all.”[50] Although not invoked after the attacks on Estonia, future cyberattacks could be deemed

damaging enough to U.S. and NATO security interests that it could result in invocation of Article 5.

The United States has multiple strategic options in dealing with cyberattack by Russia either directed against the United States or its allies. First, the United States can continue to rely on a reactive defensive posture using routers, firewalls, intrusion detection systems (IDS) and anti-virus programs to defend cyberspace and not engage in cyberattack or exploitation. This strategy would require the United States not only to defend its own cyberspace but assist other nations in defending theirs. The second option is to continue cyberdefense but also engage in a strategy of cyberdeterrence using both cyber exploitation and active cyberattack. A third option is a strategy to continue to conduct cyberdefense and cyber exploitation but use non-cyberattack (kinetic and non-kinetic) deterrence options. The strategy selected should be one that best postures the United States to prevent, reduce vulnerability to, and minimize damage and recovery time from, cyberattacks against its own national interests and Russian "near abroad" states.

A policy of "defense only" sends a strategic message to the Russians that a cyberattack on a particular portion of cyberspace that is a national interest to the United States is an act of war. This, in and of itself, creates disincentives for Russia to start hostile action in cyberspace, i.e., it provides deterrence. Any "defense only" posture must anticipate future attacks.[51] To rely on a "defense only" policy, the USG would have to not only protect critical cyber infrastructure but "become adept at predicting the type, time and location of the next"[52] inevitable cyberattack. To accomplish the latter, the United States and its allies would have to establish national and international watch-

and-warning networks to detect and prevent cyberattacks as they emerge. Then the United States could successfully respond to an attack and minimize damage and significantly reduce recovery time.

The option to continue cyberdefense but also engage in a policy of cyberdeterrence using both cyber exploitation and active cyberattack certainly legitimizes cyberattack and sends a strategic message to Russia and other potential adversaries that cyberattack is an acceptable act. There are two strong arguments against engaging in cyberattack. First, cyberattacks travel over civilian networks. Second, the owners/operators of those networks can, at least at some point, identify data as cyberattack traffic, as opposed to the normal traffic they usually carry. Therefore, the civilians who own and operate the constituent networks that create cyberspace can, in effect, exercise a veto over cyberspace operations.[53] The owners and operators of civilian networks could exercise their ability to prevent the attacked state from launching retaliatory cyberattacks and to stop the attacking state from launching further offensive cyberattacks. In this scenario, the cyberspace owners and operators are essentially neutral.[54] There is another, more dangerous scenario; the private owners of the network could choose to intervene. They could allow the traffic of the attacking state's cyberattacks and prevent the defending state from counterattacking. [55]

There is another strong argument against using cyberattack. True “conventional” warfare poses two adversaries head-to-head in order to achieve decisive battle, but attacks in cyberspace are essentially anonymous and at best, difficult to attribute to the attacker.[56] Cyberspace data moves across the world in milliseconds. What’s more, code

sent by an attacker can traverse numerous countries, and those countries could refuse to pass on the information they have to investigators. Attacking nation states can easily use the anonymity of cyberspace in their favor.

Many experts say that cyber is the new global commons.[57] While that may be true, one must be careful in making such close comparisons to the air, land, and sea. When thinking about cyberattack, a better comparison may be with the use of biological weapons. Although our adversaries may develop and consider using biological weapons, we would not consider responding in kind. The thought of the United States unleashing a biological weapon is unthinkable. Once released, the United States or its allies could not control for certain how the weapon would spread. This is comparable to the effect of releasing a cyberattack. Although the United States may target a particular system in cyberspace, there is no guarantee that the attack may not spread beyond the original target, possibly spreading to an ally's infrastructure, or even worse, back to the United States' infrastructure. Richard Kugler, a former Distinguished Research Professor in the Center for Technology and National Security Policy at the National Defense University argues that a United States, "cyber deterrence strategy has not been articulated and released, at least publicly."[58] This fact could easily lead one to believe that the United States does not want to have an explicit cyberdeterrence strategy due to the political and diplomatic problems of endorsing a cyberattack capability.

A strategy of continuing to conduct cyberdefense and cyber exploitation while using non-cyberattack (kinetic and non-kinetic) deterrence options sends a strategic message to Russia and other potential cyber adversaries that cyberattack is

unacceptable and is considered an act of war when directed against a U.S. national interest. Again, considering the analogy given with biological weapons given above, responding to a cyberattack with non-cyberattack response options is reasonable. If the United States can determine that Russia has committed a cyberattack against an American interest (to include our allies in the Russian "near abroad") it can consider that event as an act of war and that it would have the endorsement of the international authority to respond to the attack. The response could range from responding with sanctions to kinetic attack to ensure Russia cannot continue the attack. Stating that the United States would respond this way would also provide a deterrent to the Russians and other potential cyber adversaries. Washington could also continue to exploit cyberspace. This would allow the United States to conduct forensics of cyberattacks to determine their origins, allowing it to carry out flexible response options against the aggressive state actor.

Evaluation of a United States Cyberstrategy

While each of the three potential strategies examined above depend heavily on cyberdefense as a foundation, they differ significantly in their ability to deter Russia and other potential adversaries from attacking United States national interests in cyberspace. All differ in the ability to deter a cyberattack. Deterrence has two components, both which are intended to dissuade an attack.[59] The proposed strategy of cyberdefense only, has the component of deterrence by denial. Deterrence by denial is to deny the ability of an adversary to successfully attain their political goal of a cyberattack. Because all cyberattacks exploit vulnerabilities in cyberspace, if all vulnerabilities could be eliminated an adversary would be deterred by knowing that they could not successfully attack a state interest. The next two proposed strategies rely on

deterrence by punishment.[60] Punishment can be through a retaliatory cyberattack (as in the second proposed strategy) or retaliation through other kinetic or non-kinetic means (as proposed in the final strategy). Deterrence by denial and deterrence by punishment can work in tandem, thus each of the three strategies has cyberdefense as its foundation.

Cyberspace is complex and was built on a foundation of protocols and underlying technologies to ensure users could *share* information, not to ensure *security* for the information. Therefore, in practice all cyberspace systems are vulnerable.[61] Potentially the gravest threat in cyberspace today is the abysmal state of security of so many of the systems connected to it. Many factors contribute to the problem, including commercial off-the-shelf software, in which many of the desired features and rapid time to get on the market outweigh an underlying security design.[62] It would be naïve to believe that all cyberspace vulnerabilities could be found and eliminated. Instead of ensuring that all vulnerabilities are corrected, some argue that the ability to respond to an attack and restore operations is more important. In the 2003 *National Security Strategy to Secure Cyberspace*, the Bush administration noted that, "the first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events... and to improve the international management of and response to such attacks."[63] In the cases of attacks on Estonia and Georgia, both were able to recover from the attacks in a reasonable amount of time and without permanent damage to any infrastructure.

If cyberdefense alone is not enough to deter Russia, there are two other possible responses if a cyberattack is instigated against the United States or an ally. The United States could employ cyberattack capabilities for a retaliatory attack on the networks of

Russia or it could "maximize deterrence by applying a full set of other mechanisms – political, diplomatic, economic and military."[64] This is the significant difference between the proposed second and third strategies. Does the United States retaliate with cyberattack or with other kinetic or non-kinetic effects? According to Kugler, "these other instruments may be more potent than cyber retaliation."[65] This may be especially true with Russia, which focuses its capabilities on the cognitive domain of cyberspace. Russia has shown that it is much more willing to coerce its "near abroad" states by denying and disrupting their capabilities to operate in cyberspace rather than destruction of their information or infrastructure. As Thomas explains, the Russian effort "is aimed as much at disrupting an adversary's information as it is at obtaining information supremacy."[66]

Recommendations for a United States Cyberstrategy

The goal of any United States strategy in cyberspace designed to meet the challenges of Russia's cyberstrategy should be to influence them not to launch cyberattacks against the United States or any of its allies. While there is no substantive evidence that Russia has launched a cyberattack directly against the United States, the case studies examined above indicates that they will either directly or indirectly use cyberattack as part of their integrated strategy to coerce their "near abroad" states. As detailed in the U.S.-CCU report, "it would be very surprising if future disputes and conflicts involving Russia and its former possessions or satellites weren't accompanied by cyber campaigns."[67] The United States and international partners must develop a strategy to counter Russian political motives.

Based on the analysis above, the recommended foundational cyberspace strategy for the United States should be to continue to conduct cyberdefense and cyber

exploitation but use non-cyberattack (kinetic and non-kinetic) deterrence options. As stated earlier, by not condoning cyberattack, it sends a strategic message to Russia and other potential cyber adversaries that cyberattack is unacceptable and is considered an act of war when directed against a United States national interest. To support this foundational strategy, the United States Government should implement the following supporting strategic and operational recommendations.

First, at the strategic level, the President of the United States should have an explicit policy that the United States will not conduct cyberattacks and will use all other instruments of national power such as diplomatic, economic and even military to deter or retaliate against cyberattacks directed at America or its allies. This statement should send a message clear message to Russia and other potential cyber adversaries that the United States will not tolerate states which conduct cyberattack or knowingly and deliberately harbor cyberattackers and shield them from criminal enforcement. As Kugler states, "a good place to present it would be in the next National Security Strategy."[68]

Second, the USG should work with international partners to build alliances in cyberspace. Working through the United Nations, NATO or even bilaterally for cyber security collaboration, may convince Russia or other potential cyberattackers, "that their efforts, while tactically sound, are strategically counterproductive."[69] An example of this was seen immediately following the cyberattacks on Georgia. Initially, Georgia attempted to thwart the cyberattacks by blocking Russian Internet Protocol addresses. This response failed when the hackers circumvented the blocks by using foreign servers to stage further attacks.[70] In an unorthodox move, Georgia relocated it cyberspace

services to websites in Estonia and within the United States. By relocating services, the Georgian's could filter out the attack traffic and had greater bandwidth to handle the DDOS data.[71] Georgia literally "asymmetrically moved around the attack."[72] Efforts should be made to formalize these types of agreements with international partners so they don't have to be done while the crisis is occurring. As the United States-Cyber Consequences Unit report stated, "although the amount of talent the Georgians were able to involve informally was impressive, it is noteworthy that there was no international organization they could contact for help."[73]

Third, the United States Government needs to build a strategic partnership with private industry and academia. As recommended in *Securing Cyberspace for the 44th Presidency,* "government should rebuild the public-private partnership on cybersecurity to focus on key infrastructures and coordinated and preventative response activities." [74] This partnership should also include academia and both public and private sector individuals from partner nations. Cyberspace is a global domain which makes any vulnerability, anywhere, a vulnerability to the entire network. While the government has authorities to conduct operations in cyberspace, most of the infrastructure is owned by private companies. By bringing the best and brightest from each sector, the United States could reduce the vulnerabilities across cyberspace making it less likely that a cyberattack could be successful. In order to successfully implement this recommendation, the USG needs to grant the needed level of security clearances to individuals in both private industry and academia. Too often the private sector and academicians are not allowed to be privy to the full capabilities of certain government

agencies that work cyberspace efforts and this consequently, significantly hinders progress in cybersecurity

Finally, the United States should lead the international community in developing a cyberspace architecture that can be secured. As stated earlier, the current architecture was founded on the ability to share information, not to secure it. Although this would take many years to accomplish and would be a huge undertaking, intense efforts should begin now rather than later. This is an area where collaboration between academia, government, private sector and the international community could result in a reliable and robust cyberspace that is less susceptible to cyberattack.

At the operational level, the United States is already moving in the right direction. The establishment of United States Cyber Command (USCYBERCOM) as a sub-unified command under United States Strategic Command will at least unify efforts in the military's portion of cyberspace. Although this paper has previously recommended not conducting cyberattack, USCYBERCOM should nonetheless study and develop cyberattack capabilities. At first this may seem contradictory. Why study and develop offensive cyberattack capabilities if you explicitly state that you won't use them? First, to defeat a cyberattack, one needs to understand how the attack is occurring. Second, in order to better defend cyberspace, "the military needs to develop a robust modeling and simulation architecture for proactive cybersecurity."[75] By modeling cyberspace, trained military "cyber warriors" can simulate attacks on the network, therefore discovering vulnerabilities before an adversary can use them to attack the network. One cautionary recommendation for USCYBERCOM is that with limited resources, they should not focus on cyberattack at the expense of cyberdefense. As the RAND report

concludes, “it is thus hard to argue that the ability to wage strategic cyberwar should be a priority area for U.S. investment.”[76]

Conclusions

Whether actually proven to be complicit in the cyberattacks on Estonia and Georgia, it seems evident that Russia does indeed have a cyberstrategy. As Thomas concludes in his chapter on *Nation-state Strategies*, “developments…indicate that Russia’s cyber and information strategy deserve examination for the direction they are headed and for basic content.”[77] It would appear from the case studies examined above that the Russian strategy is to continue to intimidate and coerce its “near abroad” states through the use of cyberattack. If the United States is to continue to be the champion of spreading democracy across the globe and supporting developing democracies, it is imperative that it not ignore the cyber strategies that other nation states are using to enforce their political will on their neighbors. Estonia, Georgia and other Russian “near abroad” states look to the United States to support their democratic development. Therefore the United States should implement the recommendations outlined above to deter Russia from using cyberspace to coerce its neighboring states.

Because of the ubiquity of cyberspace, no nation will be able to act alone in dominating this new commons. The United States must work in concert with industry, academia and international partners to exploit and defend cyberspace to protect its national interest and the interest of its allies and partners. Cyberspace operations must be integrated into all future strategies – the advantage of dominating cyberspace can no longer be overlooked. While cyberspace strategies and tactics favor nations with robust information technology, the Internet is an extraordinary tool for a weaker state to attack a stronger conventional foe.[78] As President Obama stated on May 29, 2009, in his

remarks on securing our nation's cyber infrastructure, "this status quo is no longer acceptable -- not when there's so much at stake. We can and we must do better."[79]

Endnotes

[1] Cyber Security Strategy, Cyber Security Strategy Committee, Ministry of Defence, Estonia, Tallinn 2008, 3.

[2] The inconsistent usage of cyber and related cyber terminology may be due to the relative newness of cyber as a domain. Therefore, unless using a direct quote, this paper will use cyber, along with its related term as one word (no space). For example, cyberspace, cyberattack, cyberdefense, and cyberdeterrence will be used vice cyber space, cyber attack, cyber defense, and cyber deterrence.

[3] Russians use the term "near abroad" in reference to the other fourteen former Soviet republics that declared independence when the Soviet Union was dismantled in 1991. "Russia The Near Abroad", http://www.photius.com/countries/russia/government/russia_government_the_near_abroad.html (accessed January 13, 2010).

[4] *Cyber attacks disrupt Kyrgyzstan's networks*, January 30, 2009, http://www.securityfocus.com/brief/896 (accessed January 21, 2010).

[5] U.S. Deputy Secretary of Defense Gordon England, "The Definition of Cyberspace'," memorandum for Secretaries of Military Departments, Washington, DC, dated 12 May 2008.

[6] Deputy Secretary of Defense Memorandum, dated 15 Oct 2008.

[7] Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms", 12 April 2001, (As Amended Through 31 October 2009), 111.

[8] Ibid.

[9] Libicki, Martin C., "Cyberdeterrence and Cyberwar", 2009, linked from the RAND homepage at http://www.rand.org (accessed December 17, 2009).

[10] Joint Publication 1-02, 374.

[11] Ibid., 159.

[12] Libicki, Martin C., "Cyberdeterrence and Cyberwar".

[13] Ibid., 1.

[14] Steven Blank, *Web War I: Is Europe's First Information War a New Kind of War?* (Carlisle Barracks, PA: Strategic Studies Institute, September 2008), 227.

[15] Ibid., 227.

[16] Libicki, “Cyberdeterrence and Cyberwar”, 1.

[17] Kenneth Geers, “Cyberspace and the Changing Nature of Warfare”, August 27, 2008, http://www.scmagazineus.com/cyberspace-and-the-changing-nature-of-warfare/article/115929/ (accessed January 8, 2010).

[18] Blank, *Web War I*, 227.

[19] James A. Hughes, “Cyber Attacks Explained”, CSIS Commentary, Center for Strategic and International Studies, Washington, D.C., June 15, 2007, http://csis.org/files/media/csis/pubs/070615_cyber_attacks.pdf (accessed December 28, 2009).

[20] Geers, “Cyberspace and the Changing Nature of Warfare”.

[21] Blank, *Web War I*, 227.

[22] Blank, *Web War I*, 228.

[23] Ahto Lobjakas, “News Analysis: How Vulnerable Are Countries To Cyberattacks? Ask Estonia!”, April 29 2008, http://www.rferl.org/content/article/1109653.html (accessed December 28, 2009).

[24] Ibid.

[25] Ibid.

[26] NATO News, “NATO opens new centre of excellence on cyber defence”, May 14, 2008, http://www.nato.int/docu/update/2008/05-may/e0514a.html (accessed December 28, 2009).

[27] Kevin Coleman, “Cyber War 2.0 — Russia v. Georgia”, August 13, 2008, http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/ (accessed December 28, 2009).

[28] Ibid.

[29] Kesavan Unnikrishnan, “Google helps Georgia get back online after Russian cyber attack”, August 12, 2008 http://www.digitaljournal.com/article/258508 (accessed January 12, 2010).

[30] U.S. Cyber Consequences Unit. “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008”, (U.S. Cyber Consequences Unit: August 2009), 5.

[31] Benton Foundation, “Georgia States Computers Hit By Cyberattack”, August 18, 2008, http://www.benton.org/node/16036 (accessed December 28, 2009).

[32] Marcus H. Sachs, “Russian Business Network - Additional Analysis”, November 22, 2007, http://isc.sans.org/diary.html?storyid=3681 (accessed January 8, 2010).

[33] Jeremy Kirk, “Georgia cyberattacks linked to Russian organized crime”, August 17, 2009, http://www.computerworld.com/s/article/9136719/Georgia_cyberattacks_linked_to_Russian_organized_crime?source=rss_news (accessed January 8, 2010).

[34] John Markoff, “Before the Gunfire, Cyberattacks, August 12, 2008, http://www.nytimes.com/2008/08/13/technology/13cyber.html (accessed December 28, 2009).

[35] Ibid.

[36] Ibid.

[37] Ibid.

[38] Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, eds., *Cyberpower and National Security*, (Washington, D.C.: National Defense University Press, 2009), 476.

[39] Ibid., 477.

[40] Geers, “Cyberspace and the Changing Nature of Warfare”.

[41] Ibid.

[42] Kramer, *Cyberpower and National Security*, 476.

[43] “Hitachi Data Systems Partners with Lenovo Group to Address Storage Needs in China”, May 24, 2004, http://www.hds.com/corporate/press-analyst-center/press-releases/2004/gl040526a.html (accessed January 12, 2010).

[44] Steve LeVine, “Cyber-Attack Strategy: Part of Russian Attack on Georgian Pipelines, Report Finds”, August 24, 2009, http://www.energybulletin.net/node/49938 (accessed January 13, 2010).

[45] Kramer, *Cyberpower and National Security*, 486-487.

[46] Center for Strategic and International Studies, “Securing Cyberspace for the 44th Presidency” (Washington, D.C., December 2008), 1.

[47] Ibid.

[48] Ibid.

[49] Michael G. Mullen, *Chairman of the Joint Staff Guidance for 2009-2010* (Washington, DC: December 21, 2009), 4.

[50] The North Atlantic Treaty (Washington, DC, April 4, 1949), http://www.nato.int/cps/en/natolive/official_texts_17120.htm (accessed December 28, 2009).

[51] Bruce D. Caulkins, *Proactive Self-Defense in Cyberspace*, Strategy Research Project (Arlington, VA: Institute of Land Warfare, 2009), 9.

[52] Ibid.

[53] Susan Brenner, “Networks and Nationalization”, Jul 21, 2009, http://www.circleid.com/posts/networks_and_nationalization/ (accessed January 13, 2010).

[54] Ibid.

[55] Ibid.

[56] Shane Harris, “The Cyberwar Plan”, November 14, 2009, linked from *National Journal Magazine Home Page* at http://www.nationaljournal.com/njmagazine/cs_20091114_3145.php (accessed January 13, 2010).

[57] There are numerous cyberstrategists that will argue for and against cyberspace as a new common.

[58] Kramer, et al., eds., *Cyberpower and National Security*, 313.

[59] Libicki, “Cyberdeterrence and Cyberwar”, 7.

[60] Ibid.

[61] Ibid., 18.

[62] Howard F. Lipson, “Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues”, (Pittsburg, PA: Carnegie Mellon Software Engineering Institute November 2002).

[63] George W. Bush, The National Security Strategy to Secure Cyberspace, (Washington, D.C.: The White House, February 2003), x.

[64] Kramer, et al., eds., *Cyberpower and National Security*, 328.

[65] Ibid.

[66] Ibid., 486.

[67] U.S. CCU. “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008”, 8.

[68] Kramer, et al., eds., *Cyberpower and National Security*, 332.

[69] Ibid., 106.

[70] Brian Prince, “Cyber-attacks on Georgia Show Need for International Cooperation, Report States”, August 18, 2009, http://www.eweek.com/c/a/Security/Cyber-Attacks-on-Georgia-Show-Need-for-International-Cooperation-Report-States-294120/ (accessed January 12, 2010).

[71] U.S. CCU. “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008”, 7.

[72] Stephen Korns, “Botnets Outmaneuvered”, January 2009, linked from *The Armed Forces Journal Home Page* at http://www.armedforcesjournal.com/2009/01/3801084/ (accessed December 29, 2009).

[73] U.S. CCU. “Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008”, 7.

[74] Center for Strategic and International Studies, “Securing Cyberspace for the 44th Presidency”, 43.

[75] Caulkins, *Proactive Self-Defense in Cyberspace,* 11.

[76] Libicki, “Cyberdeterrence and Cyberwar”, 137.

[77] Kramer, et al., eds., *Cyberpower and National Security*, 476.

[78] Geers, “Cyberspace and the Changing Nature of Warfare”.

[79] Barack Obama, “Remarks by the President on Securing our Nation’s Infrastructure”, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed January 13, 2010).