Russia's approach to cyber warfare

Policy Briefing on the Imminent Russian Cybersecurity Threat: The Need For Action Against Russian Cybercrimes

In recent years, Russia has found a reliance on using cyberwar and crimes as a tactic to achieve their strategic goals both in their near-abroad and against Western countries. TheUnited Statesmust be prepared to retaliate against any cyber attack directed at our nation by assessing options to limit and counter the Russians without leading to an overescalation and possible war.

Background:

The frequency with which we hear about Russian hackershackinginto a country's important information and systems has become more and more regular, and as a result of this it is important to trace back the history of Russian cyber warfare.

The first instance of a large scale Russian cyber attack happened in Estonia in 2007. At the time, tensions were high between Russia and the former Soviet State, and the Kremlin authorized a campaign which targeted Estonian governmental agencies and businesses through use of massive DDoS (distributed denial of service) attacks that shut down countless websites essential to the functioning of these agencies and businesses (Batashvili).

In 2008, Russia coordinated an even larger cyber attack during the Russo-Georgian War.

On August 7, a cyber attack was conducted from Russia against Georgian government and media websites, while at the same time Russian troops were crossing the Georgian border. According to the Report of the Independent International Fact-Finding Mission on the Conflict in Georgia, the attack lead to several Georgian servers and high amounts Internet traffic being taken control of and placed under external control (Batashvili). The offensive persisted through the conflict lasting until ceasefire was announced on August 12. Furthermore, the Kremlin had tested their abilities in the lead up to the invasion, shutting down the official website of the president of Georgia for an entire day on July 10. The Russian cyber attacks affected practically all Georgian government websites, crippling the state’s ability to respond to the conflict. Additionally, attacks targeted Georgian media, business, and other political organizations in order to control them from turning the conflict away from Russia’s favor by making it difficult for information of what was happening inside of the conflict zone to spread out to the rest of the world. According to a report by the US Cyber Consequences Unit, “ the primary objective of the cyber campaign was to support the Russian invasion of Georgia, and the cyber attacks fit neatly into the invasion plan”. The attacks achieved their intent, since they “ significantly impeded the ability of the Georgian government to deal with the Russian invasion by interfering with communications between the government and the public, stopping many payments and financial transactions, and causing confusion about what was happening” (US Cyber Crimes Unit).

Recent cyber attacks against Ukraine are a worrying signal of a continued use of this strategy. Ukrainian president Petro Poroshenko said that during in the final two months of 2016, Ukrainian state institutions had 6, 500 instances of hacking, most directed towards the ministries of defence and finance, in addition to Kiev’s power grid and the treasury. According to the

Poroshenko, the operation came at the hand of the Russian security services, following the same playbook as they had in Georgia (Batashvili).

Russian cyber operations are not use solely in tandem with military offensives however, with many also being employed in the wars on information, especially against Western nations. The 2016 American presidential election, while highly publicized is not the only instance in which there is evidence of Russian interference with the 2017 French and German elections also being targeted. Numerous French officials and agencies, including the Defense Minister and DGSE have raised concern over the issue of Russian interference in the nation’s election, citing concern that fake news and cyber attacks were being directed to now President Macron and his party as they were not the candidates the Kremlin believed would be most beneficial to the Russian state interests.

German intelligence agencies have also brought up similar concerns about Russian cyber activities being directed against Germany and its election, with Chancellor Angela Merkel, herself seeing attacks as threatening the foundation of German democracy and the effective functioning of the German state (Delker).

Russian Objectives:

As practiced today, Russian use of cyberwarfare has three common and consistent objectives:

- Capturing Territory Without Resorting to Overt orConventional Military Force

This was the strategic goal we sawRussia trying to achieve in 2014, when they successfully annexed Crimea. Theannexation of Crimea relied on a group of Russian Special Forces operativesknown as the “ little green men”, who took their directives from a newly createdRussian special operations command. The deployment of these highly trainedoperatives, in coordination with a massive information warfare campaign, aswell as the involvement of local Russianloyalist proxies created the opportunity for Russia to takeover without needingto shed blood as they had forced momentum to shift in their favor allowing forCrimeans in Ukraine to vote for secession from Ukraine (Chivis). In 2008, Russia used similar tactics in its invasion of Georgia, during which theysimilarly coordinated cyber attacks against essential government computingservices while simultaneously operating special operation forces incoordination with Russian loyalists from the Georgian State. A major impact ofthese tactics has led to a weakened ability to integrate these countries withWestern thought.

In 2013, Russian Chief of the General Staff, General Valery Gerasimov showed Russia’s current views on such hybrid cyber warfare tactics, stating that in modern conflicts non-military means are put to use more than 4 times as often than are conventional military operations (Gerasimov). This suggests in the future such cyber attacks will be likely, and even at this point many are not being properly identified. In its use of cyberspace, Russia has shown it can find success in achieving territorial expansion goals in a manner that is nonviolent and seemingly peaceful, however there is always the underlying threat of actual military force being used unsparingly.

- Creating a Pretext for Overt, Conventional Military Action

In a similar manner to capturingterritory through covert, non-militarial expansion, Russia is also capable ofusing cyber warfare in order to create a conflict which gives them solidreasoning to use military force in foreign nations (Chivis). For instance, theRussian annexation of Crimea has lead to a reasonable concern that the Kremlincould engage in a hybrid strategy to manufacture a conflict worthy of militaryaction elsewhere, possibly the Baltic states. As it did in Crimea, Russia couldtry to create tension in a country like Estonia by conducting a campaign whichfoments discord between the minority Russian population and the Estonians. Increating these sentiments which portray the government of Estonia as oppressivetowards the minority Russians, the Kremlin can justify a Russian militaryintervention their behalf of the Russian minority, as Russian sentiment stillsees these people as their own. Conducting an operation of this sort requiresthe accompaniment of simultaneous cyber operations directed at inflamingattitudes and creating difficulties in executing both national and NATOresponses. It would almost certainly be accompanied by efforts to influencebroader European and world opinion in ways that favored Russia’s interventionthrough use of propaganda and opinion shifting which portrays Russia as actingon behalf of a repressed population that seeks its aid. On the ground, it wouldinvolve the use of Russian secret agents and proxies, both to act asaid/support for local populations creating tensions, and to coordinate withmilitary forces awaiting instruction and guidance.

- Using Hybrid Measures to Influencethe Politics and Policies of Countries in the West and Elsewhere

This last objective is the mostpressing for the United States and Western countries out of the near vicinityof Russia. In this objective, the Kremlin seeks to use cyber operations in lieuof military action or war to create tension and distress in Westerngovernments. The goal of this strategy is to influence and create favorablepolitical outcomes in targeted countries to serve Russia’s national interests(Chivis). The countries where these types of operations are most likely to findsuccess are those with high levels of corruption and weak legal systems. However, more stable countries such as the United States and the United Kingdomare similarly susceptible to such operations. Examples of ways the Kremlin canengage in cyber operations to influence an outside nation’s political systeminclude the use of fake “ troll” accounts used on social media to spreadpropaganda and create divides amongst the citizens of that nation. Also thehacking of servers of government officials can provide them with material whichthey can use to either influence that official through blackmail, or which canbe leaked to induce further tension. In creating these narratives, Russia hasthe ability to influence democracy by planting false information andmanufacturing biases against those that act against the interests of theKremlin.

American Stakes:

The continued use of cyber attacks by the Russian government brings up very realistic threats both domestically and internationally for the United States.

Internationally as Russia continues with their their goals of territorial expansion, the United States is faced with the concern of a wider influence of Russian thought and expansion of pro-Russian policies in areas where the

United States has worked to promote democracy and peace. The desire of Russia to reassemble the Soviet Union remains very real, and as seen in Estonia, Georgia, and Crimea cyber attacks can play a key role in these territorial gains. By allowing continued expansion of the Russian state, the United States risks losing the strategic relationships they have developed with these countries as well as the progress they made towards finding them more independence from Russia as democracy began to take its roots in these nations. Furthermore, these attacks can be used by Russia in places like Syria as a way to promote the Assad regime which works in coordination with Russia in achieving other strategic goals, such as the development of an oil pipeline through Syria.

Domestically, Russian cyber attacks can destabilize the US government by creating rifts and tensions amongst the American populace through the spread of false information and fake news. As seen by the hacks against the DNC as well as the use of trolls during the 2016 Presidential Election, Russia’s use of cyber attacks can undermine American democracy by allowing for a foreign nation to alter the minds of our citizens, feeding them lies and inflammatory material to create disarray in our democracy. This is especially hurtful as Russia can cite American disorder as a reason to not take our example and implement democracy in the American fashion to foreign nations. Attacks by Russia can also cripple the government’s ability to function towards the service of its citizens.

Government Organization for a Cyber Attack

The 2016Presidential Policy Directive (PPD) 41 – United States Cyber IncidentCoordination – defines a significant cyber attack as “ likely to result indemonstrable harm to national security interests, foreign relations, thedomestic and global economy, public confidence, civil liberties, or publichealth and the safety of the American people.” (PPD 41). Cyber attacks byRussia against domestic communication or critical IT infrastructure fall underthis classification.

Should such anattack actually occur, the National Cyber Response Group would lead thedefensive response as an arm of the National Security Council (PPD 41). TheSecretary of Defense, in tandem with the directors of our Intelligence agencieswould be responsible for managing incoming threats, and coordinating anystrategy or movement that would require active military response. In the eventthat the telecommunications systems of the National Security and EmergencyPreparedness sector fail, the National Coordinating Center for Communicationswould be tasked with re-establishing communications. Furthermore, PPD 41stipulates that if an operation with clear attribution is found to haveoccured, the Cyber Response Group shall assemble a team of qualified andskilled cyber personnel to respond to the cyber incident. This response teamshall have experience together in the form of practice sessions and war games.

U. S. Strategic Responses

After addressingthe immediate effects of a Russian cyber attack, it’s imperative the UnitedStates consider its options of strategic and tactical responses. One option forthe United States is response through non-military means such as indictment, diplomacy, or sanctions (Bate). A lower-level military and intelligencestrategy that could possibly be employed by the United States is the use ofcounter-surveillance intelligence operations, non-attributable cyber orconventional attacks, or attributable cyber or conventional attacks (Herb). These operations would target Russian military, civilian, or criticalinfrastructure systems.

Since NATOclassifies cyberspace as the fifth operational domain, it is likely that if theUnited States identified a significant cyber incident against its citizens asoriginating from Russia, their response would come in the form of aggressivecyber tactics. The possibility of conventional military expeditions may beexplored, however the risk of further escalation makes it more likely that theUnited States respond only through cyber operations.

Low-Level Attributable Cyber Intrusion

One possibleresponse the United States could utilize in retaliation to Russian cyberattacks is low-level cyber intrusion, distributed across a array of cyberincidents that could not be collectively categorized as a major attack. Thisintrusion would appear as a result of what is called " loud cyber weapons", which are tools that can be traced back to the U. S military (Herb). The USmilitary would send these weapons, embedded with encrypted codes, into Russiannetworks. The United States would then publicly provide the encryption key toend the intrusions caused by these weapons as a way to claim responsibility forthe attack. The purpose of taking credit for the attacks is a key paradigmshift in U. S military strategy, now emphasizing attribution as a key aspect ofa successful operation, and public knowledge as vital for deterrence. TheUnited States also has the option of conducting more basic cyber attacksagainst Russia's network, including by not limited to: alteration of governmentwebsites, disruptions of Internet service, interferences and disablements ofcommunications, or the spreading of propaganda (Department of Defense Law ofWar Manual). In the aftermath of the hack of the DNC, senior officials weighed optionsfor counter attacks on the Russian Federal Security Service (FSB) and the MainIntelligence Agency (GRU), including the use of the NSA’s TreasureMap tool, which tracks all global connections to the Internet, and can be utilized toinstall malware in targeted Russian computer systems with the purpose ofintelligence gathering and future cyber-assaults (Bamford).

Medium-Level Cyber Attack -No Immediate Casualties

The United States also has to ability toemploy the use of “ logic bombs” in cyber operations targeting both military andnon-military targets in Russia. “ Logic bomb” are codes developed with thepurpose of overloading a computer’s system rendering them incapable to operateby presenting them with an endless amount of logic questions to answer. Sendingthese “ logic bombs” into computer systems critical to Russia’s infrastructurewill lead to the United States causing dramatic economic and operationaldamages to the Russian government and its people (Sternstein). The UnitedStates has invested a large sum of money into the development of these “ logicbombs”, with initial investment coming back in 2014 when U. S. Cyber Commandoffered a $460 million contract to develop a “ computer code capable of killingadversaries.”(Storm).

High-Level Cyber Attack – Possible Casualties

The United Statescould use logic bombs or other cyber intrusion methods to attack Russiancritical infrastructure in a more serious fashion, leading to a largerpotential for loss of human life or safety. These attacks include targetingsystems such as those of a dam above a populated level where a hackingcould lead to floodgates being opened onto Russian citizens, or disabling airtraffic control services leading to air safety where planes pose a threat toeach other and the land beneath them. These options, particularly if they areeasily traceable, have the potential to escalate quickly into furtherintensified conflict.

Military-Level Cyber Attack – Escalatory

The United States also has the ability touse similar cyber operations to directly attack Russian military targets, withpossible targets including the shut off of power at a nuclear facility or anairfield, which will lead to the cause of serious casualties. These attackswill most definitely lead to a triggering of a notable escalatory threshold ofresponse by the Russians. It is significant that many Russian industrialnetworks run computer systems operating Windows XP, and in some cases evenolder systems, while maintaining connections to the Internet. Not only are thesedated systems particularly vulnerable to attack, as evidenced by the UnitedStates already demonstrating its ability to break into these systems. InNovember 2016, the United States reportedly penetrated Russian militarysystems, leaving behind malware to be activated in retaliation in the case ofRussian interference of U. S. elections (Dilanian et. al). This demonstratedboth confidence in the success of the malware implant, and politicalwillingness to trigger a consequential conflict given Russia attacks the UnitedStates in a serious manner (Bernish).

Strategic Considerations for U. S. Decisions

In response to aRussian cyber attack, the United State’s strategic responses should be a resultof its classification of the attack as being non-significant,

significant, oran act of war. State Department Cyber Coordinator Chris Painter said the UnitedStates would respond to incidents on a case-by-case basis in testimony beforethe House Subcommittee on Information Technology and National Security in November2016, saying that retaliation " could be through cyber means. It could bethrough diplomacy. It could be through indictments and law enforcementactions."(Pellerin).

Some of theseresponses require action while others do not; the path taken must be dependenton actual and anticipated effects of a cyber attack, including damage, injury, and death. Painter testified that, " cyber activities may in certaincircumstances constitute an armed attack that triggers our inherent right toself-defense as recognized by Article 51 of the U. N. Charter"(Hearing on " Digital Acts of War: Evolving the Cybersecurity Conversation"). The United States could also identify acyberattack as being an infringement upon its territorial integrity andpolitical independence, per Article 2(4) of the Charter. However, recentpolitical happenings indicate that the United States would be hesitant ininvoking Article 51, regardless of whether a Russian cyber attack lead tonominal death, injury, or damage. Instead, the United States could limit itsdeclarations and address the attack as a " significant cyber incident," invokingthe full support of the U. S. military while avoiding over-escalation. Furthermore, even though NATO justifies military response in the realm ofcyberspace, the lack of precedent means that the United States actually hasmore options in responding to Russia if it were to employ use of cyber means, that may or may not lead to conventional consequences. The United States wouldneed to decide between conducting a covert or overt counter-cyber attack. Thetactical considerations noted above show that hidden, non-attributable cyberattacks do not fall within the Department of Defense’s deterrence strategy, andwould not be treated as a suitable strategy. In the aftermath of the 2014 SonyPictures hacking by the North Korean government, the United States didn’trespond with a public cyber operation, and it was “ unclear how the UnitedStates may have retaliated against the North in secret, if it even didso.”(Sanger). The lack of a publicly noticed retaliation as well mild economicsanctions now seems ineffective as punishment. A situation could come up thatwould give the United States the opportunity to execute an immediatelyobservable cyber attack or a preparatory attack (logic bomb), with the targetbeing either a Russian military or civilian infrastructure. Similar to Russia, the United States should also avoid directly targeting a military structure inorder to avoid escalation to full-scale war. As a result of this, the UnitedStates should choose to deploy a cyber weapon against critical Russianinfrastructure, leading to conventional consequences being faced by Russia. Even the use a medium-level choice in terms of retaliation, would requireglobal ramifications to be taken into account.

Even still, it ismy recommendation to engage in a retaliatory strategy, which employs the use ofboth a combination of an observable cyber attack through use of “ loud cyberweapons” and “ logic bombs” against significant parts of the Russianinfrastructure. The United States cannot allow Russia to attack them and takeglobal credit for the attack without retaliating in some way to show dominanceover Russia. “ Loud cyber weapons” are particularly suitable for retaliationthat the public is aware of and will show the world that the United States isnot only willing to retaliate, but is better skilled in cyber war and confidentenough in its abilities to retaliate swiftly. “ Logic bombs” targeted againstnon-military sites that still hold significant value to Russian infrastructurewill be the second leg of the suggested attack. The crippling of essentialinfrastructure will both warn the Russians that an attack on us will be metwith an attack that hurts their citizens and keep them from being able toretaliate back since they will not have the resources to come back at theUnited States.

Works Cited

Batashvili, David. “ Russia’s Cyber War: Past, Present, and Future.” EUobserver, 15 Feb. 2017, euobserver. com/opinion/136909.

Delker, Janosch. “ Germany Fears Russia Stole Information to Disrupt Election.” POLITICO, POLITICO, 28 Jan. 2018, www. politico. eu/article/hacked-information-bomb-under-germanys-election/.

The Military Doctrine of the Russian Federation, approved byRussian Federation presidential
edict on February 5, 2010 (translated). Accessed
athttp://carnegieendowment. org/files/
2010russia_military_doctrine. pdf.

Understanding Russian “ Hybrid Warfare” and What Can Be Done About It (2017) (testimony of Christopher S. Chivvis). Print.

US CyberConsequences Unit. (2009) ‘ Overview by the US-CCU of the cyber campaign againstGeorgia in August of 2008’

Valery Gerasimov, “ The Value of Science is in the Foresight: New Challenges Demand Rethinking theForms and Methods of Carrying out Combat Operations,” Voyenno-PromyshlennyyKurier, February 26, 2013.