US-Russia Cyber Conflict: A Time for War

By Lauren B

Table Of Contents:

Abstract

Russia has committed acts of cyber warfare against the United States and its allies. By the Webster Dictionary and the NATO Cooperative Cyber Defense Center of Excellence commonly accepted definitions of cyber warfare, the hack of the Democratic National Committee and various other government-related persons and institutions is an act of cyber warfare committed by the Russian government. Russia has committed acts of cyber warfare against United States allies as well against the United States itself. Five case study countries are used to look at the scope of Russian cyber warfare operations: Estonia, Georgia, Ukraine, France, and the United States. Additionally, there are five areas of United States escalation and response: 1) Show of Force, 2) Diplomatic Action, 3) U.S Aid Increase, 4) International Condemnation and Sanctions, and 5) Covert Offensive, that are explored and recommended in turn. Lastly, the practice of Quiet Defense is explained as a defensive and deterrent response to any future Russian or aggressive state acts of cyber warfare and is ultimately recommended by the broader cybersecurity community.

Introduction:

The traditional form of warfare has always been boots-on-the-ground military action with specific rules and regulations deciding how to function on the battlefield to prevent unnecessary losses or violations of human rights. The technological age has changed and shaped the way modern warfare is conducted. In this modern age, computers and technology control many different aspects of the warfare command and control system from drones to communication devices to the engines of a naval ship. The usage of technology has led to new and unique forms of warfare known as cyber and information warfare.

Cyber warfare is a newly emerging threat that has been hard to define or develop responses to in the past[1]. Information warfare, however, is nothing new. What is new, is the use of information warfare tactics to conduct aspects of an cyber warfare campaign. In fact, cyber attacks and cyber warfare campaigns have been linked to continued information warfare campaigns and a new form of hybridization - combining the two types of warfare into one[2]. This combination of cyber warfare with aspects of information warfare is called cyber warfare simply because it meets all the qualifications and the current definitions of cyber warfare, the aspects of information warfare are added on to become a single warfare campaign. Cyber warfare is a unique and emerging field of study that countries such as Russia, North Korea, and China have taken advantage of.

---

[1] Clay Wilson, "Information Operations and Cyberwar: Capabilities and Related Policy Issues," CRS Report for Congress, September 14, 2006, , accessed April 26, 2017, https://fas.org/irp/crs/RL31787.pdf.

[2] ""Information Warfare: Cyber Warfare is the future warfare"," Global Information Assurance Certification Paper, 2004, , accessed April 26, 2017, https://www.giac.org/paper/gsec/3873/information-warfare-cyber-warfare-future-warfare/106165.

Defining Cyber Warfare:

Before a cyber attack can be defined as an act of cyber warfare, the definition of the term "cyber warfare" must first be defined and understood. Defining the term "cyber warfare" is important. The first reason for why a definition is important is that the definition of terms is important when deciding whether or not a cyber attack falls into the definition of an act of "cyber warfare". The second reason behind having a clear understanding of the definition of cyber warfare is that the definition itself is important to understanding what the potential responses could be once a cyber attack is determined to have been an act of cyber warfare.

The first definition of cyber warfare is the recognized dictionary definition. This definition, from the Oxford Dictionary, defines cyber warfare as "the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes"[3]. The Oxford Dictionary makes an important distinction in this definition and includes "disrupt the activities" as one of the quantifiers for a cyber attack to be an act of cyber warfare. This definition is one of the two used in this paper to determine what an act of cyber warfare is.

The second definition of cyber warfare is defined by the North Atlantic Treaty Organization's Cooperative Cyber Defense Center of Excellence (NATO CCDCOE). This organization was developed and implemented in Estonia after the first reported instance of cyber warfare in 2007. Since 2008, NATO CCDCOE has been considered one of the foremost sources

[3] "Cyberwarfare," , accessed April 20, 2017, https://en.oxforddictionaries.com/definition/cyberwarfare.

of information regarding cyber warfare and cyber defense[4]. Because the definition of cyber warfare and cyber war may vary between countries, this paper focuses on the two accepted definitions of cyber war and cyber warfare by the United States and Russia.

Cyber war is defined and accepted by both Russia and the United States as: “an escalated state of cyber conflict between or among states in which cyber attacks are carried out by state actors against cyber infrastructure as part of a military campaign. Cyber wars can be declared (formally declared by an authority of one of the parties) or de facto ones (with the absence of a declaration)[5].” There is a distinction between this definition, and the definition of cyber warfare, also defined and accepted by both the United States and Russia here as: “cyber attacks that are authorized by state actors against cyber infrastructure in conjunction with government campaign[6] .” These NATO CCDCOE definitions, along with the definition as defined by Oxford dictionary are the main criteria for determining if a cyber attack is an act of cyber warfare.

One last statement should be taken into consideration when considering what is an act of cyber warfare. This statement, given by the United States Pentagon, argues that any cyber attack originating from a computer outside of the United States can be considered an act of war from the host country[7]. This does not mean that the Pentagon will consider any and all cyber attacks

---

[4] "History," CCDCOE, June 05, 2014, , accessed April 20, 2017, https://ccdcoe.org/history.html.

[5] James B Godwin, III et al., "Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity," February 2014, , accessed April 22, 2017, https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf.

[6] "Cyber Definitions," CCDCOE, April 28, 2015, , accessed April 22, 2017, https://ccdcoe.org/cyber-definitions.html.

[7] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," The Wall Street Journal, May 31, 2011, , accessed April 21, 2017, https://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

on the United States, of which there were 77,000 in 2015, acts of cyber warfare[8]. It is important to know this statement because it speaks to the importance of cyber attacks and understanding acts of cyber warfare.

Russia and International Acts of Cyber Warfare:

The first recorded instance of Russian cyber warfare tactics was seen in 2007, when Russia attacked Estonia's cyber infrastructure and crippled the country for days with a massive Denial of Service Attack[9,10]. This act of cyber warfare against Estonia was thought to have been a response to the removal of a soviet-era statue in the capital city of Tallinn. The Bronze Soldier's removal was predicated by night of riots, and the day after the statues removal, the massive DDOS attack began against the different internet systems of Estonia[11,12].

---

[8] Reuters, "The U.S. government was hit by 77,000 cyber attacks in 2015, a 10% increase from 2014," Newsweek, May 30, 2016, , accessed April 22, 2017, http://www.newsweek.com/government-cyber-attacks-increase-2015-439206.

[9] Richard A. Clarke, *Cyber War* (HarperCollins, 2011).

[10] DAVID BATASHVILI, "Russia's cyber war: past, present, and future," EUobserver, February 15, 2017, , accessed April 26, 2017, https://euobserver.com/opinion/136909.

[11] Steven Lee Myers, "Estonia removes Soviet-era war memorial after a night of violence," The New York Times, April 27, 2007, , accessed April 22, 2017, http://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html.

[12] Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," The Guardian, May 16, 2007, , accessed April 23, 2017, https://www.theguardian.com/world/2007/may/17/topstories3.russia.

Russian-tied agents attacked “the essential electronic infrastructure of the Republic of Estonia" and “threatened the national security of [Estonia].[13]” This attack crippled the entire infrastructure of the Republic of Estonia, one of the most wired, and digitally active, countries in the entire world, for several weeks[14]. Estonia faced several weeks of constant economic disruption, and prompted calls from NATO and other organizations to cease the hostilities and to look into the attacks themselves[15].

Under both the NATO CCDCOE and Oxford Dictionary definitions, this cyber attack was an act of cyber warfare. In response to the cyber warfare operation, Estonia has developed multiple cyber security agencies to respond to future Russian cyber warfare operation attempts and, with the headquarters of the NATO CCDCOE in the capital city of Tallinn, is well prepared to combat further cyber warfare attempts[16]. Estonia has also released yearly reports, starting from 1998, to the public to maintain a degree of openness about the state of Estonian security operations over the years[17]. This has given the public a better understanding of how Estonia combats security issues - including cyber threats to its infrastructure.

---

[13] Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired, August 21, 2007, , accessed April 23, 2017, https://www.wired.com/2007/08/ff-estonia/.

[14] "A cyber-riot," The Economist, May 12, 2007, , accessed April 26, 2017, http://www.economist.com/node/9163598.

[15] Jason Richards, "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security," Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security | International Affairs Review, , accessed April 26, 2017, http://www.iar-gwu.org/node/65.

[16] "The Russian Cyber Threat: Views from Estonia," The Russian Cyber Threat: Views from Estonia | CEPA, , accessed April 26, 2017, http://cepa.org/The-Russian-Cyber-Threat-Views-from-Estonia.

[17] "Annual reviews," Kaitsepolitseiamet, , accessed April 26, 2017, https://www.kapo.ee/en/content/annual-reviews.html.

A second recorded act of cyber warfare occurred during the Russo-Georgian War of 2008 [18, 19]. During this time, Russian military coordinated their military attacks with Denial of Service Attacks against the country of Georgia to create both a military and cyber advantage within the country[20]. This was the first recorded time Russia used cyber warfare as part of the countries hybrid warfare campaign. This cyber warfare campaign occurred while Russian tanks and military troops entered into Georgian territory, and marked the first time cyber warfare was used as part of a military campaign and denoted a shift in the way warfare campaigns may be conducted in the future[21].

Some of the most well studied acts of cyber warfare committed by, and tied to, the Russian government have occurred since the 2014 annexation of Crimea from Ukraine. NATO CCDCOE published a book in 2015, *Cyber War in Perspective: Russian Aggression against Ukraine,* detailing Russian cyber warfare operations during the Annexation from 2014[22]. During the beginning stages of the conflict, it is believed that Russian intelligence agents used a botnet tied to a cyber-criminal group called The Business Club to steal Ukrainian military documents

---

[18] "2008 Georgia Russia Conflict Fast Facts," CNN, March 26, 2017, , accessed April 26, 2017, http://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/.

[19] David Hollis, "Cyberwar Case Study: Georgia 2008," Small Wars Journal, January 6, 2011, , accessed April 26, 2017, http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

[20] Graham Cluley, "Conflict between Russia and Georgia turns to cyber warfare," Naked Security, October 31, 2012, , accessed April 26, 2017, https://nakedsecurity.sophos.com/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/.

[21] Dean Takahashi, "Russia allegedly launches cyberattack on Georgia," VentureBeat, August 11, 2008, , accessed April 26, 2017, https://venturebeat.com/2008/08/11/russia-allegedly-launches-cyberattack-on-georgia/.

[22] Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO CCDCOE, 2015), PDF.

detailing potential responses to any Russian attempt at annexation of the Crimean Peninsula[23]. This itself is not an act of cyber warfare, but is a component of the military campaign run by Russia while it annexed the peninsula.

In December of 2015, and again in 2016, the power grid in Ukraine was shut down by Russian hackers in what is considered to be a textbook definition of an act of cyber warfare[24,25]. In the last few months of 2016 alone, Ukraine was hit by 6,500 cyber attacks linked to Russian agents that impacted its financial and defense ministries[26]. During this time, computer security company Crowdstrike released a report detailing the ways in which the Russian military used Android malware in order to track Ukrainian field artillery units[27].

Ukraine is a special case of cyber warfare operations, as the conflict between Russia and Ukraine is still ongoing, with new revelations about the conflict appearing every day. Multiple reports have been made detailing the cyber warfare operations going on in the region and the different attacks that have been used to compromise and halt state activities at the behest of the Russian government. As NPR reported, the Russian government is using cyber warfare

---

[23] Garrett M. Graff, "Inside the Hunt for Russia's Most Notorious Hacker," Wired, March 31, 2017, , accessed April 23, 2017, https://www.wired.com/2017/03/russian-hacker-spy-botnet/.

[24] Holly Williams, "Russian hacks into Ukraine power grids a sign of things to come for U.S.?," CBS News, December 21, 2016, , accessed April 24, 2017, http://www.cbsnews.com/news/russian-hacks-into-ukraine-power-grids-may-be-a-sign-of-things-to-come/.

[25] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, March 03, 2016, , accessed April 23, 2017, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[26] Natalia Zinets, "Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'" Reuters, December 29, 2016, , accessed April 26, 2017, http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC.

[27] "Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units," CrowdStrike, March 22, 2017, , accessed April 26, 2017, https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

operations to "aid violence and on-the-ground combat" in the region[28]. Another report, detailed by the LookingGlass Cyber Threat Intelligence Group, discovered that the Russian cyber warfare campaign had begun in 2013 and was still ongoing[29]. Ukraine has called for support from the United States, NATO, and other Western countries to help combat the cyber warfare and military operations of Russia, and have been supplied some aid to the region in response[30,31,32]. Current U.S Secretary of State Rex Tillerson called for a more "muscular response" from his administration and criticized the previous Obama Administration for a lack of an adequate response to the conflict[33].

The last case study for international Russian cyber warfare operations is a current situation occurring during the French Elections of 2017[34]. After the 2016 U.S Electoral System

---

[28] Aarti Shahani, "Report: To Aid Combat, Russia Wages Cyberwar Against Ukraine," NPR, April 28, 2015, , accessed April 26, 2017, http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine.

[29] Jason Lewis, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare," LookingGlass Cyber Solutions Inc., October 04, 2016, , accessed April 26, 2017, https://www.lookingglasscyber.com/blog/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/.

[30] The Foreign Policy Initiative, "FPI Fact Sheet: Timeline of Russian Aggression in Ukraine and the Western Response," RSS, September 18, 2014, , accessed April 26, 2017, http://www.foreignpolicyi.org/content/fpi-fact-sheet-timeline-russian-aggression-ukraine-and-western-response.

[31] Steven Pifer, "Ukraine, Russia and the U.S. Policy Response | Brookings Institution," Brookings, March 03, 2017, , accessed April 26, 2017, https://www.brookings.edu/testimonies/ukraine-russia-and-the-u-s-policy-response/.

[32] Michael B. Kelley, "BREMMER: The US Must Come To Terms With Russia Controlling Crimea," Business Insider, March 06, 2014, , accessed April 26, 2017, http://www.businessinsider.com/us-response-to-crimea-crisis-2014-3.

[33] Guy Taylor, "Rex Tillerson takes tough line on Russian hacking in tense hearing," The Washington Times, January 11, 2017, , accessed April 26, 2017, http://www.washingtontimes.com/news/2017/jan/11/rex-tillerson-us-response-russia-crimea-seizure-wa/.

[34] Andrew Higgins, "It's France's Turn to Worry About Election Meddling by Russia," The New York Times, April 17, 2017, , accessed April 26, 2017, https://www.nytimes.com/2017/04/17/world/europe/french-election-russia.html?smid=tw-nytimesworld&smtyp=cur&_r=0.

cyber warfare operation by Russia, France began preparing its own cyber defenses out of fear that Russia could attempt to hack its own election, taking place in April and May of 2017[35]. In the end of April, new reports surfaced that Presidential Candidate Emmanuel Macron was the target of similar cyber and information warfare operations as seen in the U.S Electoral System Hack[36].

Has Russia committed an act of Cyber Warfare against the U.S?

By the definition of Cyber Warfare defined earlier in this paper, Russia has committed an act of cyber warfare against the United States. The United States Electoral System Hack first occurred in mid 2015, when Russia KGB/FSB operatives hacked into the Democratic National Committee's (DNC) database as well as "additional hacking of think tanks, strategy centres, sympathetic voter roll databases, individuals at the centre core, and peripheral people that had useful information or access" about the United States Election[37].

In 2016, almost a year after the original intrusion into the systems, cyber security company Crowdstrike found and purged the hackers from the DNC servers, but by then the

---

[35] Geert De Clercq, "French military to boost defenses against cyber attacks: minister," Reuters, January 07, 2017, , accessed April 26, 2017, http://www.reuters.com/article/us-france-cyber-idUSKBN14R0OD?il=0.

[36] LORENZO FRANCESCHI-BICCHIERAI, "Russian Hackers 'Fancy Bear' Targeted French Presidential Candidate Macron," Motherboard, May 24, 2017, , accessed April 26, 2017, https://motherboard.vice.com/en_us/article/russian-hackers-fancy-bear-targeted-french-presidential-candidate-macron?utm_source=mbtwitter.

[37] The Grugq, "American Snoper," Medium, March 24, 2017, , accessed April 23, 2017, https://medium.com/@thegrugq/american-snoper-6d28e833b377.

damage had already been done and a few days later, targeted documents were released in order to attempt to influence the election result[38,39]. These documents were released through several media sites, and included the 200+ page document the DNC used as their anti-Trump dossier during the election process[40]. The release off the anti-Trump dossier, as an analyst pointed out, showed that the Russian hackers who had released the data actually supported the candidacy of then presidential candidate Trump instead of presidential candidate Clinton[41].

The hackers used a technique known as "Mail Spool Drops" to create and develop datasets that were then released via specific "cut outs and attribution fronts" such as WikiLeaks and the Guccifer 2.0 twitter account that claimed attribution[42]. This information release - the second stage in the cyber warfare campaign operations - proved to ultimately be devastating to the Democratic party and to "Americans' trust in their democracy[43]." The actual hack and compromise of the data tied to the democratic election process comprised of the first half of the cyber warfare operation - comprising and disrupting the operations of the election process on the

---

[38] "Bears in the Midst: Intrusion into the Democratic National Committee »," CrowdStrike, August 22, 2016, , accessed April 26, 2017, https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

[39] The Grugq, "The Russian Way of Cyberwar – the grugq – Medium," Medium, January 10, 2017, , accessed April 26, 2017, https://medium.com/@thegrugq/the-russian-way-of-cyberwar-edb9d52b4876.

[40] Sam Biddle and Gabrielle Bluestone, "This Looks Like the DNC's Hacked Trump Oppo File," Gawker, , accessed April 26, 2017, http://gawker.com/this-looks-like-the-dncs-hacked-trump-oppo-file-1782040426.

[41] Pwn All The Things, "Now THIS is a really interesting development in #DncHack: @Gawker has & is publishing the DNC's Trump oppo research https://t.co/4mFJ5ZgZfz," Twitter, June 15, 2016, , accessed April 26, 2017, https://twitter.com/pwnallthethings/status/743179750064037888.

[42] The Grugq, "Security, Cyber, and Elections (part 1) ," Medium, November 08, 2016, , accessed April 26, 2017, https://medium.com/@thegrugq/security-cyber-and-elections-part-1-cd04de8ed125.

[43] Hayes Brown, "How Russia Hacked Obama's Legacy," BuzzFeed, April 13, 2017, , accessed April 26, 2017, https://www.buzzfeed.com/hayesbrown/how-russia-hacked-obamas-legacy?utm_term=.tcqQ7agwp#.cu1eogxM9.

behalf of a state agency (Russia) - and the subsequent information release and push of information composed the second half of the operation.

The second stage of the cyber warfare campaign, the information release, was the most visible part of the entire cyber warfare campaign. This part involved the usage of paid internet trolls to push fake news and propaganda supporting presidential candidate Trump, while at the same time continually releasing information stolen from the election hack in order to maintain negative rhetoric around candidate Clinton[44,45].

The overall United States Electoral Hacking and subsequent information release as part of the cyber warfare campaign followed the basic structure of a cyber warfare operation, as laid out by prominent security researcher The Grugq: "1) Collection: standard computer network operations cyber collection, 2) Dissemination: analysis by the foreign intelligence service; curation into datasets; distribution to the target audience, 3) Consumption: assessment, evaluation and judgement by the target audience; essentially processing and digesting the datasets[46]." The Russian cyber warfare operation is one of the most prominent and textbook examples of an act of cyber warfare against another state and something should be done in response.[47]

---

[44] Natasha Bertrand, "It looks like Russia hired internet trolls to pose as pro-Trump Americans," Business Insider, July 27, 2016, , accessed April 26, 2017, http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7.

[45] Adrian Chen, "The Agency," The New York Times, June 02, 2015, , accessed April 26, 2017, https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

[46] The Grugq, "Security, Cyber, and Elections (part 2)," Medium, November 11, 2016, , accessed April 26, 2017, https://medium.com/@thegrugq/security-cyber-and-elections-part-2-ee6954bb587f.

[47] "Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution," Intelligence Community Assessment, January 6, 2017, , accessed April 26, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

How can the U.S Respond to Russian Acts of Cyber Warfare?

Responding to an act of cyber warfare is hard to consider - especially when the rules of this type of warfare are still being written[48]. In fact, there no broad international law or custom yet that revolves around the rules of conducting cyber warfare except for a black letter law book put out this year by the NATO Cooperative Cyber Defense Center Of Excellence (CCDCOE) called the Tallinn Manual 2.0. This book outlines some of the ways in which a nation state can respond to an act of cyber warfare[49].

Some may say that because the rules of cyber warfare are still being written, that responding to a Russian act of cyber warfare is not worth it and that this is not an area the United States should become involved in or worry about escalating and indeed the one issue with these potential responses is that they all assume that both sides of the playing field have relatively equal cyber deterrence and attack capabilities[50]. This is not the case with the United States. The United States is uniquely positioned in such a way to be one of the biggest world powers, yet one of the world's weakest links in cyberspace today[51]. However, this means that in order for the

---

[48] Morgan Chalfant, "Legislators grapple with cyber war rules," TheHill, March 01, 2017, , accessed April 26, 2017, http://origin-nyi.thehill.com/business-a-lobbying/321682-legislators-grapple-with-cyber-war-rules.

[49] Michael N. Schmitt, *Tallinn manual 2.0 on the international law applicable to cyber operations* (Cambridge, United Kingdom: Cambridge University Press, 2017).

[50] Citation - find the correct website here

[51] Bret Brasso, "Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories « Executive Perspective," FireEye, April 29, 2016, , accessed April 26, 2017, https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html.

United States to be able to respond to any acts of cyber warfare, an escalation to a new area of warfare that the United States is dominant in is the only way to feasibly respond and respond the United States should.

The five core ways that the United States can respond to an act of cyber warfare are: 1) Show of Force 2) Diplomacy 3) U.S Aid Increase 4) International Sanctions and Condemnation 5) Covert Offense. There is one last area of response that is not quite a response at all and should be done in conjunction of one of the other core responses: Quiet Defense. The message behind any action and potential response by the United States has to be understood as a response to Russian acts of cyber warfare. Any troop movement, international condemnation, or any response to these acts of cyber warfare must be known as a response to these specific acts. Ambiguity in the response of the United States as to the reasons behind any response area chosen will only lead to more confusion and even a dismissal of the response.

Show of Force

The first core area of response - show of force - involves movement and repositioning of U.S military forces to areas surrounding the Russian Federation. Specifically, this involves an increase of NATO and U.S forces to the surrounding Baltic States as a show of force. Currently, NATO has steadily increased support to the baltic region as a part of the Readiness Action Plan developed in 2014[52]. However, NATO can only increase strategic military support so much because of the 1997 NATO-Russia Founding Act agreement that dictated the terms for military

[52] NATO Review, "Securing the Nordic-Baltic region," NATO Review, , accessed April 26, 2017, http://www.nato.int/docu/Review/2016/Also-in-2016/security-baltic-defense-nato/EN/index.htm.

presence on both sides of the Russo-Baltic States borders (one before). The United States itself has increased its own military effort in the Baltic states as a deterrent show of force[53]. The previous Obama administration added additional military capability to the Baltic states in an effort to provide some form of deterrence to Russia meddling in the region[54]. New military show of force increases that are placed in additional regions surrounding the Russian government should project the specific message of deterrence and credibility to the Russian Federation regarding their act of cyber warfare against the United States.

Diplomatic Action

The second core area of response is Diplomatic action. This response area is mainly focused on communicating with other Russian officials through diplomatic and unofficial channels to express United States anger over the act of cyber warfare and to threaten further retaliation. This step was taken by President Obama at the end of his administration's term in October[55]. Obama took this diplomatic core area of response during his last few months as president and while he ejected 35 Russian intelligence agents and created new economic sanctions against Russian individuals for "cyber operations aimed at the U.S. election[56]." This

---

[53] Eric Schmitt, "U.S. Lending Support to Baltic States Fearing Russia," The New York Times, January 01, 2017, , accessed April 26, 2017, https://www.nytimes.com/2017/01/01/us/politics/us-baltic-russia.html.

[54] Andrius Sytas, "Baltic states seek more NATO help ahead of Russian exercise," Reuters, February 09, 2017, , accessed April 26, 2017, http://www.reuters.com/article/us-baltic-nato-russia-idUSKBN15O2HZ.

[55] David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," The New York Times, December 29, 2016, , accessed April 26, 2017, https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

[56] Elias GrollRobbie Gramer, "Obama Finally Hits Back at Russia for Election Hack With Sanctions, Expulsions," Foreign Policy, December 29, 2016, , accessed April 26, 2017, http://foreignpolicy.com/2016/12/29/obama-finally-hits-back-at-russia-for-election-hack-with-sanctions-expulsions/.

had little effect - especially because the response on the Obama administration's part came months after all evidence had been collected and it became apparent that Russia had committed an act of cyber warfare. As one former Russian advisor put it: “We all expected a more targeted response [57].” The Obama administration demonstrated the exact wrong way to conduct a diplomatic response to an act of cyber warfare. The proper diplomatic response involves swift action and credible threats to the aggressive government that sends a strong message, establishes future precedent, is a credible act of deterrence towards the aggressive government, and is not seen as a weak response on both sides of the political aisle[58].

U.S Aid Increase

The third core area of response is United State’s Aid Increase. This area primarily focuses on asymmetrically sending both a strong diplomatic message and a show of force to the Russian government by providing aid to border governments. This can be in several forms. One form of aid is that of military aid, a direct show of force seen in the baltics and NATO[59]. As talked about in the first core section of response, military aid can be used as a direct response. Military aid can provide a concrete show of force against the Russian government and

---

[57] Oliver Carroll, "Putin's Masterstroke of Nonretaliation," Foreign Policy, December 30, 2016, , accessed April 26, 2017, http://foreignpolicy.com/2016/12/30/putins-masterstroke-of-nonretaliation-obama-sanctions-expulsions-trump/.

[58] Jon Street, "Obama’s ‘inadequate’ and ‘weak’ response to alleged Russian hacking draws criticism from all sides," TheBlaze, December 30, 2016, , accessed April 26, 2017, http://www.theblaze.com/news/2016/12/30/obamas-inadequate-and-weak-response-to-alleged-russian-hacking-draws-criticism-from-all-sides/.

[59] NATO Review, "Securing the Nordic-Baltic region," NATO Review, , accessed April 26, 2017, http://www.nato.int/docu/Review/2016/Also-in-2016/security-baltic-defense-nato/EN/index.htm.

additionally solidify our commitment to our allies in NATO and Baltic States while sending a message to the Russian government that this is in direct response to the acts of cyber warfare committed.

A second form is democratic aid - or aid given to governments to promote democratic goals and movements of the countries as seen in Kyrgyzstan, Kazakhstan, and Ukraine. This aid is typically used to promote democratic values such as forms of government, and free and fair elections. During the Obama administration, aid was provided to multiple countries, including Georgia, Kazakhstan, and Belarus[60].

A third form of Aid Increase is propaganda aid, or increases in propaganda messaging across borders. This type of propaganda aid was commonly seen in the Cold War[61]. Propaganda can be used in multiple areas to attempt to weaken Russian government control and influence over the former soviet states. One of the most common forms of propaganda today is use of social media and “troll armies” to push propaganda rhetoric and fake news as propaganda for different regimes[62]. The United States government can use this type of propaganda and other types of aid to push new messages against the Russian government as a response to their acts of cyber warfare.

---

[60] U.S. Department of State, , accessed April 26, 2017, https://2009-2017.state.gov/p/eur/ace/factsheets/index.htm.

[61] "The Role of the Media During the Cold War," E-International Relations, , accessed April 26, 2017, http://www.e-ir.info/2013/10/26/the-role-of-the-media-during-the-cold-war/.

[62] Leo Benedictus, "Invasion of the troll armies: 'Social media where the war goes on'" The Guardian, November 06, 2016, , accessed April 26, 2017, https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian.

International Condemnation and Sanctions

International Condemnation and Sanctions is the fourth area of response to Russian acts of cyber warfare. Acting unilaterally, the United States can only inflict so much damage to the Russian government as punishment, as seen in the response mentioned in area two of responses. Additionally, the United States has specific cyber sanctions that guide how sanctions for cyber attacks are to be carried out[63]. There have been 450 sanctions placed on the Ukraine/Russia region by the United States since 1994[64]. These sanctions have not been very effective in the past and limit the impact of response.

On the other hand, the international community combined can implement a greater response impact towards the Russian government and convey a stronger message of deterrence. International sanctions and condemnation can take multiple forms including economic sanctions, UN General Assembly condemnation, mass diplomatic responses, messages of condemnation from multiple United States allies, and a general consensus of anger and retaliation towards the Russian government.

International sanctions were first proposed and implemented when Russia annexed Crimea in 2014. The European Union, United States, and other counties proposed and implemented economic and diplomatic sanctions against the Russian government for the annexation[65,66]. These sanctions have had minimal - if any - effect on the Russian government's

---

[63] U.S. Department of State, , accessed April 26, 2017, https://www.state.gov/e/eb/tfs/spi/cyber/index.htm.

[64] "Enigma Labs | Sanctions Tracker," Enigma, , accessed April 26, 2017, https://labs.enigma.com/sanctions-tracker/.

[65] U.S. Department of State, , accessed April 26, 2017, https://www.state.gov/e/eb/tfs/spi/ukrainerussia/.

actions towards Ukraine and Crimea but the economic effects on the Russian economy have sent a more credible threat to Russia as an international community than with unilateral United States sanctions on their own[67]. Russia has still continued its military effort and support of rebels in Ukraine despite these sanctions, but the message has been clear and the threat credible that these sanctions can place some effect on Russian economic function.

International condemnation and sanctions can work in time to punish Russia continually for both the annexation of Ukraine, and, with additional sanctions added, acts of cyber warfare committed against the United States and other countries[68,69]. Additionally, the European Union has increased and extended sanctions against Russia for a longer period of time, in part, some experts say, to push the current Trump administration to continue this response as well[70].

Covert Offensive

---

[66] "Official Journal of the European Union L271," European Union, September 12, 2014, , accessed April 26, 2017, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2014:271:FULL&from=EN.

[67] Tim Daiss, "Prolonged Sanctions Rip Into Russian Economy, Causing Angst For Putin," Forbes, August 27, 2016, , accessed April 26, 2017, https://www.forbes.com/sites/timdaiss/2016/08/19/prolonged-sanctions-rip-into-russia-causing-angst-for-putin/#1e2d802539e5.

[68] Outside Publications, "Are the Russia Sanctions Working?," Foreign Policy Research Institute, , accessed April 26, 2017, http://www.fpri.org/article/2016/08/russia-sanctions-working/.

[69] Iana Dreyer and Nicu Popescu, "Do sanctions against Russia work?," December 2014, , accessed April 26, 2017, http://www.iss.europa.eu/uploads/media/Brief_35_Russia_sanctions.pdf.

[70] Gabriela Baczynska, "EU agrees to extend Russia sanctions until mid-2017 in a signal to Trump," Reuters, December 15, 2016, , accessed April 26, 2017, http://www.reuters.com/article/us-ukraine-crisis-eu-sanctions-idUSKBN144289.

The fifth area of response is covert offensive. This area is mostly known as the so called "hack back" approach to an act of cyber warfare[71]. Currently, the UK and China have some form of policy dictating covert offensive measures against any acts of cyber warfare committed against their governments[72]. In the United States, recent rule changes have been put into place to allow expanded powers for the FBI to hack back against adversaries and expand warrant powers for U.S judges[73].

Covert offensive is meant to be covert, so finding confirmed examples of this "hacking back" response are difficult. However, there are reports that the National Security Agency has attempted this covert offensive approach before, and that they are currently using it against the Russian government[74]. Additionally, there have been recent rumours that the United States has been using this "hack back" approach against North Korea as both retaliation for previous acts of cyber warfare and as a preventative measure against further DPRK nuclear proliferation abilities [75]. In 2014, the State Department released its own framework for cyber stability, and it provides an overview of threats, potential international cyber cooperation and deterrence methods for

---

[71] Craig Timberg, Ellen Nakashima, and Danielle Douglas-Gabriel, "Cyberattacks trigger talk of 'hacking back'" The Washington Post, October 09, 2014, , accessed April 26, 2017, https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html?utm_term=.8e25f528e62d.

[72] "Hacking Back: Exploring a new option of cyber defense," InfoSec Resources, November 07, 2016, , accessed April 26, 2017, http://resources.infosecinstitute.com/hacking-back-exploring-a-new-option-of-cyber-defense/.

[73] Dustin Volz, "U.S. high court approves rule change to expand FBI hacking power," Reuters, April 29, 2016, , accessed April 26, 2017, http://www.reuters.com/article/us-usa-cyber-warrants-highcourt-idUSKCN0XP2XU.

[74] Lee Ferran, "The NSA Is Likely 'Hacking Back' Russia's Cyber Squads," ABC News, , accessed April 26, 2017, http://abcnews.go.com/International/nsa-hacking-back-russias-cyber-squads/story?id=41010651.

[75] Alex Lockie, "North Korea's embarrassing missile failure may have been due to US cyber sabotage," Business Insider, April 17, 2017, , accessed April 26, 2017, http://www.businessinsider.com/us-hack-north-korea-missile-system-2017-4.

cyberspace[76]. This framework provides some areas of escalation and tactics that could be used as part of a quiet offensive.

Covert offensive is the area of response most equivalent in escalation to Russian acts of cyber warfare. This response can be taken as a direct message of deterrence to the Russian government as well as threat of escalation. Potential ways for this covert offensive response include exposing the code used by the Russian government in a leak so that they cannot use the code again and exposing financial information of Russian officials as quiet offensive response tactics[77].

There is a need for caution with the response area however, because U.S cyber capabilities are not prepared to handle an increase in escalation in the cyber warfare domain[78]. Caution needs to be used here because cyber warfare and the cyber domain itself are not areas that the United States holds any sort of dominance in. This area of response should be seen as a last resort so to speak in order to make sure all other options have been exhausted first and the practice of quiet defense has been implemented.

Quiet Defense

There is one last area of response that should not be considered an area of response at all, but rather a "best practices" policy area that is important to prevent any additional acts of cyber

---

[76] International Security Advisory Board, "Report on A Framework for International Cyber Stability," U.S State Department, July 2, 2014, , accessed April 26, 2017, https://www.state.gov/documents/organization/229235.pdf.

[77] James Stavridis, "How to Win the Cyberwar Against Russia," Foreign Policy, October 12, 2016, , accessed April 26, 2017, http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

[78] Paul D. Shinkman, "America Is Losing the Cyber War," U.S. News & World Report, September 29, 2016, , accessed April 26, 2017, https://www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries.

warfare from Russia or any other aggressive state or state-sponsored actors. Quiet defense, securing the defense of the cyber infrastructure, is an important practice for a number of reasons. The first being that it is not ideal to be vulnerable to any future cyber warfare attacks as one of the most powerful nations in the world with access to a massive nuclear arsenal and online infrastructure[79]. A second reason is that any escalation to the cyberspace domain as outlined in the fifth potential area of response above leaves huge potential for the United States to lose any cyber war because of our cyber vulnerabilities[80].

Cyber security "best practices" have been released by the Obama administration for private corporations that can also be implemented at the government level[81]. Another commissioned report by the Obama administration by the Commission on Enhancing National Cybersecurity also released a series of cyber security best practices and ICS-CERT has released its own publications[82,83]. Additionally, multiple cyber security corporations and consultations

[79] "U.S. Nuclear Weapons Capability," 2017 Index of U.S. Military Strength, , accessed April 26, 2017, http://index.heritage.org/military/2017/assessments/us-military-power/u-s-nuclear-weapons-capability/.

[80] Lisa Ferdinando, "Dempsey: Cyber Vulnerabilities Threaten National Security," U.S. DEPARTMENT OF DEFENSE, January 21, 2015, , accessed April 26, 2017, https://www.defense.gov/News/Article/Article/603952/.

[81] "MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES," Obama White House, October 30, 2015, , accessed April 22, 2017, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

[82] "Statement by the President on the Report of the Commission on Enhancing National Cybersecurity," National Archives and Records Administration, , accessed April 26, 2017, https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity.

[83] "Recommended Practices," Recommended Practices | ICS-CERT, , accessed April 26, 2017, https://ics-cert.us-cert.gov/Recommended-Practices.

publish reports every few months detailing best practices that could be easily implemented by the United States government[84].

With the growing threat that acts of cyber warfare have become towards the integrity and infrastructure of the United States government, it is important that the United States implement these cybersecurity best practices on critical systems and potential foreign adversary targets. Quiet defense needs to be implemented before any escalation into the domain of cyberspace and it should be implemented as a defensive strategy to prevent any additional breaches of integrity and acts of cyber warfare from damaging the United States.

Final Thoughts and Conclusion:

Acts of cyber warfare have been defined by internationally recognized parties. By these recognized definitions, Russia has committed acts of cyber warfare against the United States, Estonia, Georgia, Ukraine, and France. Russia used cyber attacks to "disrupt the activities of a state or organization", specifically, the infrastructures of the governments of the United States, Estonia, Georgia,Ukraine, and France. These specific attacks were authorized by Russian agents and were part of a government campaign in each of these countries or regions. These acts of cyber warfare should not go without an adequate response from the United States. Ultimately, Russia should be punished for the acts of cyber warfare it has committed against the United

[84] "Reading Room," SANS Institute: Reading Room - Best Practices, , accessed April 26, 2017, https://www.sans.org/reading-room/whitepapers/bestprac.

States and its allies. Russia cannot be allowed to use cyber warfare tactics to bully and influence other countries.

The five potential areas of response for the United States to act are, 1) Show of Force, 2) Diplomacy, 3) U.S Aid Increase, 4) International Sanctions and Condemnation, and 5) Covert Offense. Each of these response areas presents it's own, unique, set of potential United States government responses to acts of cyber warfare by the Russian government. They each also present opportunities for caution and careful preparation of responses rather than swift action by the United States government. One final area of response, not necessarily to be considered a response at all, is Quiet Defense. This area of response - shoring up the cyber defenses of all United States infrastructure - is crucial. Defending our cyber systems is important to prevent any further acts of cyber warfare to de even more damaging to the United States than they already are. Implementing tools such as HTTPS and SSL across government-linked websites and following the cyber security rules of best practice are cost effective and easy to implement to provide basic protection against lower level cyber attacks. Cyberspace is a new and unfolding territory of warfare. Russia may have thrown the first stone in this arena, but that does not mean that the United States and our allies cannot respond and prepare for the future of cyber warfare.

Bibliography

U.S. Department of State. Accessed April 26, 2017. https://2009-2017.state.gov/p/eur/ace/factsheets/index.htm.

U.S. Department of State. Accessed April 26, 2017. https://www.state.gov/e/eb/tfs/spi/cyber/index.htm.

U.S. Department of State. Accessed April 26, 2017. https://www.state.gov/e/eb/tfs/spi/ukrainerussia/.

"2008 Georgia Russia Conflict Fast Facts." CNN. March 26, 2017. Accessed April 26, 2017. http://www.cnn.com/2014/03/13/world/europe/2008-georgia-russia-conflict/.

"2016 Presidential Campaign Hacking Fast Facts." CNN. March 20, 2017. Accessed April 26, 2017. http://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/.

"A cyber-riot." The Economist. May 12, 2007. Accessed April 26, 2017. http://www.economist.com/node/9163598.

"Annual reviews." Kaitsepolitseiamet. Accessed April 26, 2017. https://www.kapo.ee/en/content/annual-reviews.html.

Adler, Stephen, and Sujata Rao. "Ukrainian president calls for global response to Russian threat." Reuters. January 18, 2017. Accessed April 26, 2017. http://www.reuters.com/article/us-davos-meeting-poroshenko-idUSKBN1522X8.

"August 2008 Russian-Georgian War: Timeline." Institute for War and Peace Reporting. Accessed April 26, 2017. https://iwpr.net/global-voices/august-2008-russian-georgian-war-timeline.

"Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution." Intelligence Community Assessment. January 6, 2017. Accessed April 26, 2017.

https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf.

Baczynska, Gabriela. "EU agrees to extend Russia sanctions until mid-2017 in a signal to Trump." Reuters. December 15, 2016. Accessed April 26, 2017. http://www.reuters.com/article/us-ukraine-crisis-eu-sanctions-idUSKBN144289.

"Bears in the Midst: Intrusion into the Democratic National Committee »." CrowdStrike. August 22, 2016. Accessed April 26, 2017. https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/.

BATASHVILI, DAVID. "Russia's cyber war: past, present, and future." EUobserver. February 15, 2017. Accessed April 26, 2017. https://euobserver.com/opinion/136909.

Benedictus, Leo. "Invasion of the troll armies: 'Social media where the war goes on'" The Guardian. November 06, 2016. Accessed April 26, 2017. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian.

Bertrand, Natasha. "It looks like Russia hired internet trolls to pose as pro-Trump Americans." Business Insider. July 27, 2016. Accessed April 26, 2017. http://www.businessinsider.com/russia-internet-trolls-and-donald-trump-2016-7.

Bertrand, Natasha. "A timeline of events that unfolded during the election appears to support the FBI's investigation into Trump and Russia." Business Insider. March 26, 2017. Accessed April 26, 2017. http://www.businessinsider.com/updated-trump-russia-election-timeline-fbi-2017-3.

Bluestone, Sam Biddle and Gabrielle. "This Looks Like the DNC's Hacked Trump Oppo File." Gawker. Accessed April 26, 2017. http://gawker.com/this-looks-like-the-dncs-hacked-trump-oppo-file-1782040426.

Brasso, Bret. "Cyber Attacks Against Critical Infrastructure Are No Longer Just Theories « Executive Perspective." FireEye. April 29, 2016. Accessed April 26, 2017. https://www.fireeye.com/blog/executive-perspective/2016/04/cyber_attacks_agains.html.

Brown, Hayes. "How Russia Hacked Obama's Legacy." BuzzFeed. April 13, 2017. Accessed April 26, 2017. https://www.buzzfeed.com/hayesbrown/how-russia-hacked-obamas-legacy?utm_term=.tcqQ7agwp#.cu1eogxM9.

Carroll, Oliver. "Putin's Masterstroke of Nonretaliation." Foreign Policy. December 30, 2016. Accessed April 26, 2017.

http://foreignpolicy.com/2016/12/30/putins-masterstroke-of-nonretaliation-obama-sanctions-expulsions-trump/.

Chalfant, Morgan. "Legislators grapple with cyber war rules." TheHill. March 01, 2017. Accessed April 26, 2017. http://origin-nyi.thehill.com/business-a-lobbying/321682-legislators-grapple-with-cyber-war-rules.

Chen, Adrian. "The Agency." The New York Times. June 02, 2015. Accessed April 26, 2017. https://www.nytimes.com/2015/06/07/magazine/the-agency.html.

Clarke, Richard A. *Cyber War*. HarperCollins, 2011.

Cluley, Graham . "Conflict between Russia and Georgia turns to cyber warfare." Naked Security. October 31, 2012. Accessed April 26, 2017. https://nakedsecurity.sophos.com/2008/08/12/conflict-between-russia-and-georgia-turns-to-cyber-warfare/.

"Cyber Definitions." CCDCOE. April 28, 2015. Accessed April 22, 2017. https://ccdcoe.org/cyber-definitions.html.

"Cyberwarfare." Accessed April 20, 2017. https://en.oxforddictionaries.com/definition/cyberwarfare.

Daiss, Tim. "Prolonged Sanctions Rip Into Russian Economy, Causing Angst For Putin." Forbes. August 27, 2016. Accessed April 26, 2017. https://www.forbes.com/sites/timdaiss/2016/08/19/prolonged-sanctions-rip-into-russia-causing-angst-for-putin/#1e2d802539e5.

"Danger Close: Fancy Bear Tracking of Ukrainian Field Artillery Units." CrowdStrike. March 22, 2017. Accessed April 26, 2017. https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/.

Davis, Joshua. "Hackers Take Down the Most Wired Country in Europe." Wired. August 21, 2007. Accessed April 23, 2017. https://www.wired.com/2007/08/ff-estonia/.

De Clercq, Geert. "French military to boost defenses against cyber attacks: minister." Reuters. January 07, 2017. Accessed April 26, 2017. http://www.reuters.com/article/us-france-cyber-idUSKBN14R0OD?il=0.

Dreyer, Iana, and Nicu Popescu. "Do sanctions against Russia work?" December 2014. Accessed April 26, 2017. http://www.iss.europa.eu/uploads/media/Brief_35_Russia_sanctions.pdf .

"Enigma Labs | Sanctions Tracker." Enigma. Accessed April 26, 2017. https://labs.enigma.com/sanctions-tracker/.

Ferdinando, Lisa. "Dempsey: Cyber Vulnerabilities Threaten National Security." U.S. DEPARTMENT OF DEFENSE. January 21, 2015. Accessed April 26, 2017. https://www.defense.gov/News/Article/Article/603952/.

Ferran, Lee. "The NSA Is Likely 'Hacking Back' Russia's Cyber Squads." ABC News. Accessed April 26, 2017. http://abcnews.go.com/International/nsa-hacking-back-russias-cyber-squads/story?id=41010651.

FRANCESCHI-BICCHIERAI, LORENZO. "Russian Hackers 'Fancy Bear' Targeted French Presidential Candidate Macron." Motherboard. May 24, 2017. Accessed April 26, 2017. https://motherboard.vice.com/en_us/article/russian-hackers-fancy-bear-targeted-french-presidential-candidate-macron?utm_source=mbtwitter.

Geers, Kenneth, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, Estonia: NATO CCDCOE, 2015. PDF.

Godwin, James B , III, Andrey Kulpin, Karl Frederick Rauscher, and Valery Yaschenko. "Critical Terminology Foundations 2: Russia-U.S. Bilateral on Cybersecurity." February 2014. Accessed April 22, 2017. https://dl.dropboxusercontent.com/u/164629289/terminology2.pdf.

Gorman, Siobhan, and Julian E. Barnes. "Cyber Combat: Act of War." The Wall Street Journal. May 31, 2011. Accessed April 21, 2017. https://www.wsj.com/articles/SB10001424052702304563104576355623135782718.

Graff, Garrett M. "Inside the Hunt for Russia's Most Notorious Hacker." Wired. March 31, 2017. Accessed April 23, 2017. https://www.wired.com/2017/03/russian-hacker-spy-botnet/.

Gramer, Elias GrollRobbie. "Obama Finally Hits Back at Russia for Election Hack With Sanctions, Expulsions." Foreign Policy. December 29, 2016. Accessed April 26, 2017. http://foreignpolicy.com/2016/12/29/obama-finally-hits-back-at-russia-for-election-hack-with-sanctions-expulsions/.

Grugq, The. "Security, Cyber, and Elections (part 1) ." Medium. November 08, 2016. Accessed April 26, 2017. https://medium.com/@thegrugq/security-cyber-and-elections-part-1-cd04de8ed125.

Grugq, The. "Security, Cyber, and Elections (part 2)." Medium. November 11, 2016. Accessed April 26, 2017. https://medium.com/@thegrugq/security-cyber-and-elections-part-2-ee6954bb587f.

Grugq, The. "American Snoper." Medium. March 24, 2017. Accessed April 23, 2017. https://medium.com/@thegrugq/american-snoper-6d28e833b377.

Grugq, The. "The Russian Way of Cyberwar – the grugq – Medium." Medium. January 10, 2017. Accessed April 26, 2017. https://medium.com/@thegrugq/the-russian-way-of-cyberwar-edb9d52b4876.

Grugq, The. "HOWTO: Fight Cyberwars and Lose – the grugq – Medium." Medium. April 01, 2017. Accessed April 26, 2017. https://medium.com/@thegrugq/howto-fight-cyberwars-and-lose-6d5cc58a392e.

"Hacking Back: Exploring a new option of cyber defense." InfoSec Resources. November 07, 2016. Accessed April 26, 2017. http://resources.infosecinstitute.com/hacking-back-exploring-a-new-option-of-cyber-defense/.

Higgins, Andrew. "It's France's Turn to Worry About Election Meddling by Russia." The New York Times. April 17, 2017. Accessed April 26, 2017.

https://www.nytimes.com/2017/04/17/world/europe/french-election-russia.html?smid=tw-nytimesworld&smtyp=cur&_r=0.

"History." CCDCOE. June 05, 2014. Accessed April 20, 2017. https://ccdcoe.org/history.html.

Hollis, David. "Cyberwar Case Study: Georgia 2008." Small Wars Journal. January 6, 2011. Accessed April 26, 2017. http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

Initiative, The Foreign Policy. "FPI Fact Sheet: Timeline of Russian Aggression in Ukraine and the Western Response." RSS. September 18, 2014. Accessed April 26, 2017. http://www.foreignpolicyi.org/content/fpi-fact-sheet-timeline-russian-aggression-ukraine-and-western-response.

Kelley, Michael B. "BREMMER: The US Must Come To Terms With Russia Controlling Crimea." Business Insider. March 06, 2014. Accessed April 26, 2017. http://www.businessinsider.com/us-response-to-crimea-crisis-2014-3.

Lewis, Jason. "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare." LookingGlass Cyber Solutions Inc. October 04, 2016. Accessed April 26, 2017.

https://www.lookingglasscyber.com/blog/operation-armageddon-cyber-espionage-as-a-strategic-component-of-russian-modern-warfare/.

Lipton, Eric, David E. Sanger, and Scott Shane. "The Perfect Weapon: How Russian Cyberpower Invaded the U.S." The New York Times. December 13, 2016. Accessed April 26, 2017. https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html.

Lockie, Alex. "North Korea's embarrassing missile failure may have been due to US cyber sabotage." Business Insider. April 17, 2017. Accessed April 26, 2017. http://www.businessinsider.com/us-hack-north-korea-missile-system-2017-4.

"MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES." Obama White House. October 30, 2015. Accessed April 22, 2017. https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf.

Myers, Steven Lee. "Estonia removes Soviet-era war memorial after a night of violence." The New York Times. April 27, 2007. Accessed April 22, 2017. http://www.nytimes.com/2007/04/27/world/europe/27iht-estonia.4.5477141.html.

Nakashima, Ellen. "National intelligence director: Hackers have targeted 2016 presidential campaigns." The Washington Post. May 18, 2016. Accessed April 26, 2017. https://www.washingtonpost.com/world/national-security/national-intelligence-director-hackers-have-tried-to-spy-on-2016-presidential-campaigns/2016/05/18/2b1745c0-1d0d-11e6-b6e0-c53b7ef63b45_story.html?utm_term=.cfde1aecf20f.

"Official Journal of the European Union L271." European Union. September 12, 2014. Accessed April 26, 2017. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2014:271:FULL&from=EN.

Orenstein, Mitchell A. "Russia's October Surprise." Foreign Affairs. December 01, 2016. Accessed April 26, 2017. https://www.foreignaffairs.com/articles/russian-federation/2016-10-20/russias-october-surprise.

Parker, Emily. "Hack Job: How America Invented Cyberwar." Foreign Affairs. April 20, 2017. Accessed April 26, 2017. https://www.foreignaffairs.com/reviews/review-essay/2017-04-17/hack-job.

Pifer, Steven. "Ukraine, Russia and the U.S. Policy Response | Brookings Institution." Brookings. March 03, 2017. Accessed April 26, 2017. https://www.brookings.edu/testimonies/ukraine-russia-and-the-u-s-policy-response/.

Publications, Outside. "Are the Russia Sanctions Working?" Foreign Policy Research Institute. Accessed April 26, 2017. http://www.fpri.org/article/2016/08/russia-sanctions-working/.

"Reading Room." SANS Institute: Reading Room - Best Practices. Accessed April 26, 2017. https://www.sans.org/reading-room/whitepapers/bestprac.

"Recommended Practices." Recommended Practices | ICS-CERT. Accessed April 26, 2017. https://ics-cert.us-cert.gov/Recommended-Practices.

International Security Advisory Board. "Report on A Framework for International Cyber Stability." U.S State Department. July 2, 2014. Accessed April 26, 2017. https://www.state.gov/documents/organization/229235.pdf .

Review, NATO. "Securing the Nordic-Baltic region." NATO Review. Accessed April 26, 2017. http://www.nato.int/docu/Review/2016/Also-in-2016/security-baltic-defense-nato/EN/index.htm.

Richards, Jason. "Denial-of-Service: The Estonian Cyberwar and Its Implications for U.S. National Security." Denial-of-Service: The Estonian Cyberwar and Its Implications for

U.S. National Security | International Affairs Review. Accessed April 26, 2017. http://www.iar-gwu.org/node/65.

"Russia-Linked Hackers Targeted Macron Campaign, Cyber-Researchers Say." RadioFreeEurope/RadioLiberty. April 25, 2017. Accessed April 26, 2017. http://www.rferl.org/a/french-presidential-front-runner-macron-reportedly-targeted-russia-linked-hackers/28450238.html.

Sanger, David E. "Obama Strikes Back at Russia for Election Hacking." The New York Times. December 29, 2016. Accessed April 26, 2017. https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html.

Schmitt, Eric. "U.S. Lending Support to Baltic States Fearing Russia." The New York Times. January 01, 2017. Accessed April 26, 2017. https://www.nytimes.com/2017/01/01/us/politics/us-baltic-russia.html.

Schmitt, Michael N. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge, United Kingdom: Cambridge University Press, 2017.

Shahani, Aarti. "Report: To Aid Combat, Russia Wages Cyberwar Against Ukraine." NPR. April 28, 2015. Accessed April 26, 2017.

http://www.npr.org/sections/alltechconsidered/2015/04/28/402678116/report-to-aid-combat-russia-wages-cyberwar-against-ukraine.

Shinkman, Paul D. "America Is Losing the Cyber War." U.S. News & World Report. September 29, 2016. Accessed April 26, 2017. https://www.usnews.com/news/articles/2016-09-29/cyber-wars-how-the-us-stacks-up-against-its-digital-adversaries.

"Statement by the President on the Report of the Commission on Enhancing National Cybersecurity." National Archives and Records Administration. Accessed April 26, 2017. https://obamawhitehouse.archives.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity.

Stavridis, James. "How to Win the Cyberwar Against Russia." Foreign Policy. October 12, 2016. Accessed April 26, 2017. http://foreignpolicy.com/2016/10/12/how-to-win-the-cyber-war-against-russia/.

Street, Jon. "Obama's 'inadequate' and 'weak' response to alleged Russian hacking draws criticism from all sides." TheBlaze. December 30, 2016. Accessed April 26, 2017. http://www.theblaze.com/news/2016/12/30/obamas-inadequate-and-weak-response-to-alleged-russian-hacking-draws-criticism-from-all-sides/.

Sytas, Andrius. "Baltic states seek more NATO help ahead of Russian exercise." Reuters. February 09, 2017. Accessed April 26, 2017. http://www.reuters.com/article/us-baltic-nato-russia-idUSKBN15O2HZ.

Takahashi, Dean. "Russia allegedly launches cyberattack on Georgia." VentureBeat. August 11, 2008. Accessed April 26, 2017. https://venturebeat.com/2008/08/11/russia-allegedly-launches-cyberattack-on-georgia/.

"The Role of the Media During the Cold War." E-International Relations. Accessed April 26, 2017. http://www.e-ir.info/2013/10/26/the-role-of-the-media-during-the-cold-war/.

Taylor, Guy. "Rex Tillerson takes tough line on Russian hacking in tense hearing." The Washington Times. January 11, 2017. Accessed April 26, 2017. http://www.washingtontimes.com/news/2017/jan/11/rex-tillerson-us-response-russia-crimea-seizure-wa/.

"The Russian Cyber Threat: Views from Estonia." The Russian Cyber Threat: Views from Estonia | CEPA. Accessed April 26, 2017. http://cepa.org/The-Russian-Cyber-Threat-Views-from-Estonia.

Reuters. "The U.S. government was hit by 77,000 cyber attacks in 2015, a 10% increase from 2014." Newsweek. May 30, 2016. Accessed April 22, 2017. http://www.newsweek.com/government-cyber-attacks-increase-2015-439206.

Things, Pwn All The. "Now THIS is a really interesting development in #DncHack: @Gawker has & is publishing the DNC's Trump oppo research https://t.co/4mFJ5ZgZfz." Twitter. June 15, 2016. Accessed April 26, 2017. https://twitter.com/pwnallthethings/status/743179750064037888.

Twitter Thread from known security researcher and analyst @PwnAllTheThings

Timberg, Craig, Ellen Nakashima, and Danielle Douglas-Gabriel. "Cyberattacks trigger talk of 'hacking back'" The Washington Post. October 09, 2014. Accessed April 26, 2017. https://www.washingtonpost.com/business/technology/cyberattacks-trigger-talk-of-hacking-back/2014/10/09/6f0b7a24-4f02-11e4-8c24-487e92bc997b_story.html?utm_term=.8e25f528e62d.

Traynor, Ian. "Russia accused of unleashing cyberwar to disable Estonia." The Guardian. May 16, 2007. Accessed April 23, 2017. https://www.theguardian.com/world/2007/may/17/topstories3.russia.

"U.S. Nuclear Weapons Capability." 2017 Index of U.S. Military Strength. Accessed April 26, 2017.

http://index.heritage.org/military/2017/assessments/us-military-power/u-s-nuclear-weapons-capability/.

Volz, Dustin. "U.S. high court approves rule change to expand FBI hacking power." Reuters. April 29, 2016. Accessed April 26, 2017. http://www.reuters.com/article/us-usa-cyber-warrants-highcourt-idUSKCN0XP2XU.

Williams, Holly. "Russian hacks into Ukraine power grids a sign of things to come for U.S.?" CBS News. December 21, 2016. Accessed April 24, 2017. http://www.cbsnews.com/news/russian-hacks-into-ukraine-power-grids-may-be-a-sign-of-things-to-come/.

Wilson, Clay. "Information Operations and Cyberwar: Capabilities and Related Policy Issues." CRS Report for Congress. September 14, 2006. Accessed April 26, 2017. https://fas.org/irp/crs/RL31787.pdf.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired. March 03, 2016. Accessed April 23, 2017. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zinets, Natalia. "Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'" Reuters. December 29, 2016. Accessed April 26, 2017. http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC.