U.S. WARFARE WITHIN THE FIFTH DOMAIN: DETERRING RUSSIAN CYBER AGGRESSION

Dominick Namias, Jacob Chace

Helms School of Government

Liberty University

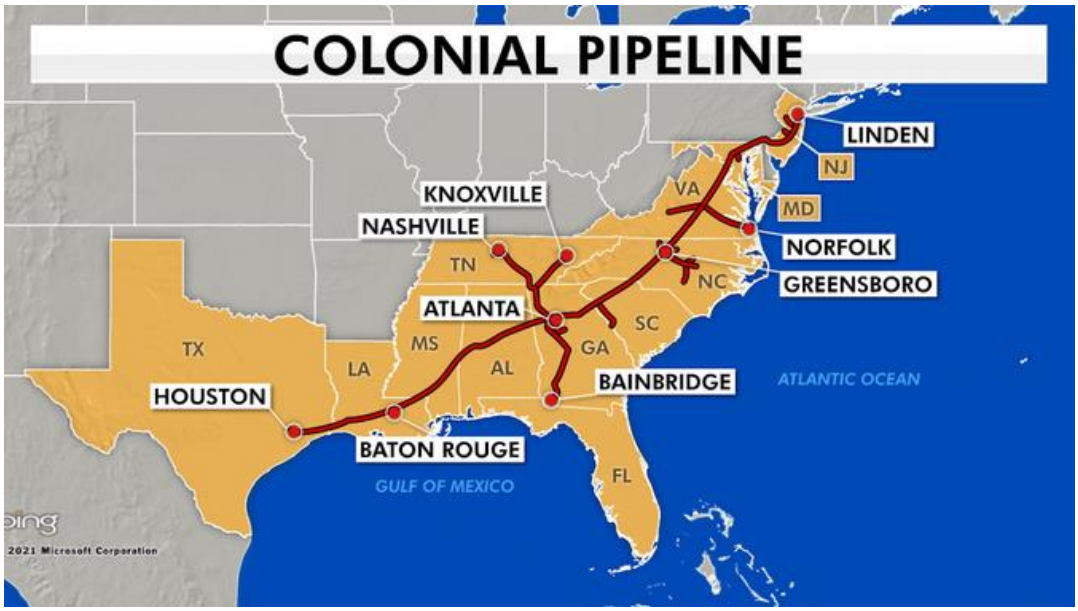
Abstract

Foreign policy is a crucial factor in ensuring the safety and prosperity of any nation. In some cases, this may include projecting strength and taking decisive action towards other countries. Entities within the Russian Federation have engaged the United States and other democracies such as Ukraine and Estonia in multiple offensive cyber-attacks, each increasing in scope and destruction. These cyber-attacks have caused a significant amount of damage to each countries' economy, industry, and infrastructure. The United States should take a strong, more proactive approach towards cybersecurity through persistent engagement and further collaboration with the private sector. In addition to addressing the issue unilaterally, the United States should work with NATO counterparts to identify, intercept, and expose the actors committing cyber-attacks. Moreover, the U.S. should promote its allies to take conjoint actions against Russian cyber-attacks. U.S. allies could voluntarily support each other's responses to significant malicious cyber incidents through intelligence sharing, public statements of support for actions taken following an attack, and participation in the charge taken against the perpetrator state/entity. The United States should also place economic sanctions on the aggressors within Russia that conduct cyber-warfare with the United States and/or its allies. These sanctions should only follow thorough intelligence leading to accurate identification of the perpetrators. These actions will project strength, promote security, and bolster relationships between the U.S. and other free nations.

Introduction

Ensuring a safe and secure United States requires projecting strength and taking decisive action. Recently, cyber-attacks from entities within the Russian Federation have targeted the economy, industry, and infrastructure of the United States, Ukraine, and Estonia. The cumulative effects of these cyber-attacks have caused a significant amount of damage and there seems to be no end to these transgressions. The United States needs to take a strong, proactive approach towards cybersecurity through persistent engagement and further collaboration with the private sector. In addition, the United States should work with NATO counterparts to identify, intercept, and expose the actors committing cyber-attacks, and promote all U.S. allies to take conjoint actions against Russian cyber-attacks. Furthermore, the United States should place economic sanctions on the entities within the Russian Federation when they conduct cyber-warfare with the United States and/or its allies. These actions will project strength, promote security, and bolster relationships between the U.S. and other free nations.

Entities within the Russian Federation have engaged the United States in two recent cyber-attacks which caused considerable damage. These were ransomware attacks targeting Colonial Pipeline and all JBS's U.S. meatpacking facilities. The Colonial Pipeline ransomware attack took place on May 7th, 2021. This 5,500-mile pipeline supplies 45% of fuel consumed on the East Coast of the United States and runs from Houston, Texas to Linden, New Jersey.



[1]

[1] Jonathan Garber, "Colonial Pipeline's Shipping System Hit with Brief Outage," FOXBusiness (2021), https://www.foxbusiness.com/markets/colonial-pipeline-communications-system-down-report.

Moreover, this pipeline transports around 2.5 million barrels of gasoline, diesel, jet fuel, and other products in a day.[2] The results of this attack led to gas shortages throughout several states. Colonial Pipeline was forced to pay a $5 million ransom to the hacker group within Russia to allow gas to flow again.[3]

A few weeks after the Russian ransomware attack on the Colonial Pipeline, JBS USA meatpacking facilities were forcefully shut down throughout the United States on June 2nd, 2021. The majority of these facilities were shut down for at least a day according to JBS USA. Additionally, the attack affected servers supporting its IT (Information Technology) systems not only in North America but also Australia.[4] This ransomware attack caused meat shortages throughout the U.S. and raised prices for consumers. JBS USA released a media statement on June 9th, 2021, confirming that it paid $11 million in ransom to a hacker group within Russia to allow the facilities to become operational again.[5]

Entities within the Russian Federation have additionally engaged Ukraine in multiple cyber-attacks. Two recent cyber-attacks on Ukraine have been the NotPetya cyber-attack and the Ukrainian Government website shutdowns. The NotPetya cyber-attack took place on June 27th, 2017, affecting many businesses throughout Ukraine. Eventually, this attack spread to other companies within Germany, Russia, France, the United Kingdom, Norway, Denmark, and the United States. When this cyber-attack first appeared, it was thought to be a ransomware attack. The victims were notified that their files would be locked until ransom money was paid to the assailants. However, this cyber-attack infected an accounting software known as MeDoc which existed on multiple platforms used by organizations that do business in Ukraine.[6] The infected software disrupted, damaged, and gained unauthorized access to various company servers. This

[2] Marlene Lenthang & Josh Margolin, "Ransomware cyberattacks shuts down major US pipeline, company says," ABC News (2021), https://abcnews.go.com/US/cyberattack-shuts-us-pipeline-supplies-45-fuel-east/story?id=77573904.

[3] Christiana Wilkie, "Colonial Pipeline paid $5million ransom one day after cyberattack, CEO tells Senate," CNBC (2021), https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

[4] Rob McLean, Alexis Benveniste, and Allie Malloy, "Major Meat Producer JBS USA Hit by Cyberattack, Likely from Russia," CNN (2021), https://www.cnn.com/2021/06/01/tech/jbs-usa-cyberattack-meat-producer/index.html.

[5] "JBS USA Cyberattack Media Statement - June 9 — JBS Foods," JBS Foods (2022), https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9.

[6] Counter Threat Unit Research Team, "NotPetya Campaign: What We Know About the Latest Global Ransomware Attack," 2022 Secureworks Inc, (2017), https://www.secureworks.com/blog/notpetya-campaign-what-we-know-about-the-latest-global-ransomware-attack.

software caused $10 billion in losses around the world.[7] The CIA (Central Intelligence Agency) [8] and United Kingdom NCSC (National Cybersecurity Centre) have found with certainty that the mock ransomware virus dubbed NotPetya was created by the military spy agency of the Russian Chief Intelligence Directorate (GRU).[9] According to the U.S. Department of Justice, six Russian GRU officers were charged in connection with the Notpetya cyberattacks with worldwide deployment of destructive malware and other disruptive actions in cyberspace.[10] The official charges are as follows:

> On Oct. 15, 2020, a federal grand jury in Pittsburgh returned an indictment charging six computer hackers, all of whom were residents and nationals of the Russian Federation (Russia) and officers in Unit 74455 of the Russian Main Intelligence Directorate (GRU), a military intelligence agency of the General Staff of the Armed Forces…[t]hese GRU hackers and their co-conspirators engaged in computer intrusions and attacks intended to support Russian government efforts to undermine, retaliate against, or otherwise destabilize: (1) Ukraine; (2) Georgia; (3) elections in France…"[11]

The Ukrainian Government website shutdowns took place on January 14th, 2022. The Ukrainian Government's agency Center for Strategic Communications and Information Security issued a statement directly blaming Russia for the hack considering increased tensions between Ukraine and Russia. The hackers left text in Ukrainian, Polish, and Russian on some of the websites stating, "Ukrainians! All your personal data was uploaded to the internet. All data on the computer is being destroyed. All information about you became public. Be afraid and expect

[7] Michael Schmitt, "Russian Cyber Operations and Ukraine: The Legal Framework.", Lieber Institute West Point, (2022), https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/.

[8] Nakashima Ellen, "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," The Washington Post (2018), https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

[9] "Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack," n.d., https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

[10] "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," The United States Department of Justice, October 19, 2020, https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[11] Ibid.

the worst."[12] However, the attack was merely simple defacements, Ukraine suggests.[13] Moreover, this attack was solely to provoke and intimidate Ukrainians.

Though Estonia has not been a recent victim of Russian cyber-attacks, it is relevant to mention that Russian cyber-attacks were highly effective in hampering Estonia's cyber-sphere. These attacks were successful in crippling dozens of Estonian government, corporate, and bank websites. The attacks commenced in April and May of 2007. Some of these sites were taken down while others were just disrupted. This assault lasted a relentless 22 days.[14]

Working with the Private Sector

Entities within Russia, sometimes in collaboration with state actors, have been notorious for the onslaught on nation cyber-spheres in recent years. It is imperative that the United States come up with new and improved ways in deterring these attacks on itself and its allies. Hence, taking a stronger, more proactive approach towards cybersecurity through persistent engagement and further collaboration with the private sector. This is imperative to avert Russian cyber aggression.

The United States has already been using federal agencies like the Federal Bureau of Investigation (FBI) to work with cybersecurity organizations in the U.S. private sector for some time now. On October 28th, 2021, the Director of the FBI, Christopher Wray explained that the FBI has a dedicated Office of Private Sector, private sector coordinators in every field office across the country, and teams in operational divisions like Counterintelligence and Cyber coming up with ways to protect the American people in working with the private sector on threats they encounter.[15] He identifies that we need the insight, knowledge, and experience that cybersecurity experts possess. He explains that sharing information is in the best interest of the American people and lays out tactics such as combining intelligence that has been collected. This would bolster the overall security posture of U.S. entities before breaches occur. In addition, sharing indicators with one another, the United States can build a productive cycle that strengthens the country.[16] This further emphasizes the idea that the U.S. private sector is extremely innovative and that solely relying on the U.S. Government for progression is inefficient.

---

[12] Michael Schmitt, "Russian Cyber Operations and Ukraine: The Legal Framework," Lieber Institute West Point, (2022), https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/.

[13] Ibid.

[14] Ivana Kottasová, "How Russian Threats Turned This Country into the Go-to Expert on Cyber Defense," CNN, https://www.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html.

[15] "Working with Our Private Sector Partners to Combat the Cyber Threat," n.d. Federal Bureau of Investigation, https://www.fbi.gov/news/speeches/working-with-our-private-sector-partners-to-combat-the-cyber-threat-wray-ecny-102821.

[16] Ibid.

The U.S. has recently prioritized further collaboration with the private cybersecurity sector and has recruited more companies working in this field. Government contract mainstays such as Lockheed Martin and Raytheon continue to play an integral role. As of 2021, this exclusive list has expanded to include tech giants such as Alphabet Inc., Apple, and Microsoft.[17] These companies, while powerful and moderately knowledgeable regarding cybersecurity, can pose a threat to national security. The United States should be conscientious when integrating product-based companies into its strategy of deterring cyber aggression. These companies, while based in the United States, do not have any obligation to the United States Government or to protect its citizens or interests. They are also well implemented in countries such as Russia and China as product suppliers with an economic incentive to continue service in those countries. According to Statista, in Q2 of 2021, 67% of Apple's revenue was generated outside of the United States.[18] Provided that the U.S. Government remains the highest bidder for these tech giants, the security risks will remain manageable, but this is not a compromise the United States should make.

Apple, Microsoft, and Alphabet are primarily focused on the individual consumer and implement cybersecurity in personal products. These tech commodities are created to be accessible and convenient for the consumer. While security is a high priority for each of these companies, this is not their primary concern or area of expertise. Security risks have also been noted by cybersecurity professionals in many products provided by these three companies. The United States should invest in smaller, more experienced cybersecurity companies in the private sector that are based solely in America. This will counteract conflicting interests and ensure a further level of loyalty to the U.S. Government. Russian cyber aggression will be best deterred through this course of action.

NATO has been generally successful in implementing the private sector of their various nations into the cyber defense field and serves as an example of the private cybersecurity industry aiding the public sector. Through NCI Agency, the information technology, communications and cyber defense arm of NATO, billions of dollars have been invested in private companies from NATO countries to train and equip professionals in the public field to defend against attacks.[19] This is an example of successful strategy that has also been used by the U.S. Department of Defense. These investments show a common strategy among NATO member states which has been extremely successful. Through sharing strategies and information, the U.S. and NATO can learn from one another the best means to deter cyber aggression.

An additional course of action our federal government can take to strengthen the nation's security would be to invest tax paying dollars into private sector companies who are willing to accept government contracts to educate K-12 students on the fundamental cybersecurity

---

[17] Rakesh Sharma, "US Government Enlists Tech Firms' Help on Cybersecurity," Investopedia (2021), https://www.investopedia.com/us-government-enlists-tech-firms-help-on-cybersecurity-5196484.

[18] Feb 2, "Non-U.S. Share of Apple's Revenue 2006-2021," Statista, February 2, 2022, https://www.statista.com/statistics/263435/non-us-share-of-apples-revenue/.

[19] "Private Sector Plays Bigger Role in NATO Cyber Strategy," National Defense Magazine (2022), https://www.nationaldefensemagazine.org/articles/2017/2/8/private-sector-plays-bigger-role-in-nato-cyber-strategy.

vocabulary, history, tactics, and operations. Following the Russian cyber-attacks in April and May of 2007, NATO ally Estonia took a like-minded approach. The response to this 2007 attack was the creation of a program aimed to educate Estonia's young population, from kindergarten to 12th grade, on digital skills and staying safe online. This initiative successfully created a young generation of competent Estonians on cybersecurity, bolstering the countries national security.[20] The implementation of a program like this would better prepare the United States in fighting the war of the fifth domain. This program would also encourage high school students to take up careers in the cybersphere industry producing a massive amount of American cybersphere professionals. This would equip the United States with the right assets to deal with the ever-growing cyber threat.

An example that backs this proposal is how the United States reacted to the launch of Sputnik. The U.S. had fallen behind the Soviet Union in the science and tech realm. In response, the United States passed the National Defense Education Act in 1958 which provided large amounts of financial funding to education at all levels of the public and private sector.[21] After this program was initiated the United States tech advancement significantly increased. Some thought this was an invasion of the federal government in schooling at all levels.[22] However, it was necessary in competing with Soviet Russia's goal of achieving superiority in spaceflight capabilities in the 20th century which could have been detrimental to U.S. national security. The United States needs to implement a program to enhance education in the cybersecurity sphere to ensure we do not have another Sputnik incident which could turn into something more dire, such as large-scale cyberattack grid shutdowns.

Working with NATO Counterparts

NATO was founded in 1949 with the full intention to "safeguard the freedom, common heritage and civilization of their peoples, founded on the principles of democracy, individual liberty and the rule of law...to promote stability and well-being in the North Atlantic area."[23] The 12 founding countries have since grown to 30 nations all with the same goal of furthering security and prosperity in the North Atlantic region. According to NATO, the alliance was formed to meet three objectives: "[to deter] Soviet expansionism, [forbid] the revival of nationalist militarism in Europe through a strong North American presence on the continent and

[20] "Exclusive: How Estonia Is Training Young People to Spot Fake News," GovInsider (2019), https://govinsider.asia/connected-gov/mart-laidmets-kristel-rillo-estonian-ministry-of-education-and-research-fake-news-digital-competence/.

[21] "National Defense Education Act | US House of Representatives: History, Art & Archives," @USHouseHistory (2020), https://history.house.gov/HouseRecord/Detail/15032436195.

[22] Thomas C. Hunt "National Defense Education Act | United States [1958]." In Encyclopædia Britannica (2018), https://www.britannica.com/topic/National-Defense-Education-Act.

[23] NATO, "The North Atlantic Treaty," NATO, (1949), https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

[encourage] European political integration."[24] The expansion of NATO has driven the alliance closer to its main aggressor, Russia, with the addition of four former Warsaw Pact members (Czech Republic, Hungary, Poland and Romania) and three former-Soviet states (Estonia, Latvia and Lithuania). This has broadened NATO's responsibilities and increased the threat from Russian interference in NATO activities.

NATO has focused heavily on cybersecurity since 2014 and as recently as January 2022 re-emphasized their commitment to security in the fifth domain:

> To keep pace with the rapidly changing threat landscape and maintain robust cyber defenses, NATO adopted an enhanced policy and action plan, which were endorsed by Allies at the Wales Summit in September 2014. An updated action plan was endorsed by Allies in February 2017. The 2014 policy established that cyber defense is part of the Alliance's core task of collective defense, confirmed that international law applies in cyberspace, set out the further development of NATO's and Allies' capabilities, and intensified NATO's cooperation with industry.[25]

NATO has recently alluded to a policy of physical military action against any cyberattacks on member states:

> Appearing at the Atlantic Council's headquarters in Washington ahead of NATO's summit in Brussels, Stoltenberg said NATO did not distinguish between cyber intrusions and other forms of attacks. He noted that cyber aggression could trigger a military response through "other means." "In a way, it doesn't matter whether it's a kinetic attack or a cyberattack, we will assess as allies whether it meets the thresholds for triggering Article 5. It sends a message that we regard cyberattacks as seriously as any other attack."[26]

This has yet to be implemented based solely on an aggression against a member state, but the 2021–2022 Russo-Ukrainian crisis can be traced back to Russian cyberaggression against the Ukrainian central government. The response by the United States and NATO allies is the correct approach to a cyberattack from within the Russian Federation. According to intel from the Ukrainian Government, hackers from within the Russian Federation shut down major government websites on January 14, 2022, "The websites of the country's cabinet, seven ministries, the treasury, the National Emergency Service, and the state services website, where

---

[24] NATO, "A Short History of NATO," NATO, https://www.nato.int/cps/en/natohq/declassified_139339.htm.

[25] NATO, "Cyber Defence," NATO, (2022), https://www.nato.int/cps/en/natohq/topics_78170.htm.

[26] Alicia Hope, "NATO Warns That Cyber Attacks on Member States Could Trigger a Coordinated Military Response," CPO Magazine, June 26, 2021, https://www.cpomagazine.com/cyber-security/nato-warns-that-cyber-attacks-on-member-states-could-trigger-a-coordinated-military-response/.

Ukrainians' electronic passports and vaccination certificates are stored, were temporarily unavailable on Friday as a result of the hack."[27]

Russia coincided this aggressive action by building a significant military force on Ukraine's eastern border, furthering the idea of simultaneous kinetic and cyber aggression. NATO and the U.S. responded accordingly by deploying troops to eastern Europe to defend the NATO alliance and Ukraine from invasion: "Denmark, Spain, France and the Netherlands were all planning or considering sending troops, planes or ships to eastern Europe, NATO said. Ukraine shares borders with four NATO countries: Poland, Slovakia, Hungary and Romania."[28]

The 2021-2022 Russo-Ukrainian crisis is revealing of Russia's ultimate strategy in two ways. Firstly, it is now clear that a cyberattack will more than likely precede a kinetic attack, especially when there is little resistance to that aggression. Secondly, there will be more aggressive action coming out of the Russian Federation and NATO and the U.S. are not properly prepared on the cyber-defense front. The evidence for the latter point has been addressed earlier with the examples of successful cyberattacks against the United States such as the Colonial Pipeline and JBS infrastructure attacks as well as the Notpetya attack.

NATO has been primarily concerned with building up cybersecurity in member states. The next step, led by the United States, is to go on the offensive and accurately identify the sources of these cyber aggressions. On several occasions, Russia has been able to hide behind the idea that the cyber-attackers are not state-affiliated and fiend responsibility of aggressions from within the Federation:

> Three successive U.S. administrations have failed to develop any form of doctrine to adequately address increasingly problematic cyberattacks from unattributable sources that plague U.S. businesses and can even endanger lives. Instead, the private sector has been left to deal with ever more destructive and dangerous ransomware attacks unassisted, and Russia continues to do nothing about cyberattacks originating from Russian territory.[29]

This is an epidemic that can be cured by shifting from a conservative policy regarding the cyberworld and towards a more proactive position. If the United States were able to identify actors with precision, further measures could be taken to prevent attacks on the U.S. infrastructure and on the private sector. In addition, being able to identify these actors would allow the United States and its allies to expose the perpetrators worldwide through media with solid evidence, damaging the perpetrator state's reputation with the international community. Once the United States can present solid evidence against cyber criminals, the United States and

---

[27] Al Jazeera, "'Be Afraid': Cyberattack in Ukraine Targets Government Websites," Ukraine-Russia Crisis News (2022), https://www.aljazeera.com/news/2022/1/14/be-afraid-cyberattack-in-ukraine-targets-government-websites.

[28] Sabine Siebold, Dmitry Antonov, "NATO Sends Reinforcements and U.S. Puts Troops on Alert as Ukraine Tensions Rise," Reuters (2022), https://www.reuters.com/world/europe/nato-sends-ships-jets-eastern-europe-ukraine-crisis-2022-01-24/.

[29] Michael John Williams, "Make Russia Take Responsibility for Its Cybercriminals," Foreign Policy (2021), https://foreignpolicy.com/2021/11/09/cyberattacks-russia-responsibility-ransomware/.

NATO allies can voluntarily take conjoint actions against the perpetrator state/entity. This can be done through intelligence sharing, public statements of support for actions taken following an attack, and participation in the charges taken against the perpetrator state/entity. This strategy is reliant upon the ability of the United States and its allies to accurately identify perpetrators with a proactive joint campaign.

Economic Sanctions on the Aggressors within the Russian Federation

Although some of the aforementioned cyberattacks have not been officially linked to the Russian Government, they are originating within the Russian Federation. There has been significant intelligence procured by the United States and its allies suggesting, and in some cases proving, that there is a clear connection between the Russian Government, and these cyberattacks.[30] The United States should adopt a proactive approach to identifying connections between the individuals threatening U.S. cybersecurity and the Russian Government if those connections do indeed exist. Understanding the ultimate goals of these cyberattacks is important and should inform the response of the U.S. Government. It is increasingly crucial that the U.S. holds those who are truly behind these aggressions accountable, be that the Russian Government or unaffiliated sources. This begins with a focus on precise identification and definitive retaliatory actions such as sanctions against the perpetrating entities.

One of the many tools in the U.S. arsenal of diplomacy is economic sanctions levied against nations, companies, or individuals. Within the realm of cybersecurity, economic sanctions on the Russian oil and natural gas trade would be an effective deterrent against further cyberaggression. The U.S. has ample experience with sanctions against Russia to varying success. The sanctions in response to cyber threats must be swift and sweeping to be of maximum value to the United States. Depending on the level of devastation following an attack from Russia, the U.S. should incrementally increase sanctions on the financial sector of the Russian Government.

This course of action coincides with the ability of the U.S. and its NATO allies to identify the individual perpetrators of cyberaggression. These aggressors may then be personally punished through addition to the SDN List (Specially Designated Nationals and Blocked Persons List) in the United States. This will serve multiple purposes and cause financial harm to the individuals responsible for attacks against the U.S. and its allies. According to OFAC (Office of Foreign Assets Control) attorneys, "...as a result of their...designation they find that their assets in the United States have been blocked, their bank accounts have been closed, and their credit cards have been cancelled. I've seen people lose their jobs in major multinational companies, lose their pensions, and lose access to other important property as a result of being placed on the SDN list."[31]

It is important to note that every preceding strategy must also be explored and applied. Economic sanctions cannot be the exclusive means of deterring cyberattacks from within the

[30] "Ukraine Cyber-Attack: Russia to Blame for Hack, Says Kyiv," BBC News (BBC, January 14, 2022), https://www.bbc.com/news/world-europe-59992531.

[31] "OFAC Attorney Explains the SDN List: OFAC Sanctions Attorney," OFAC Lawyer (2017), https://ofaclawyer.net/specially-designated-national/sdn-list/.

Russian Federation. U.S. sanctions have a mixed record at best when attempting to force a change in behavior. This is largely due to the application of economic sanctions being the main, and sometimes only, strategy used by the U.S. These sanctions must coincide with a diverse group of other methods when dealing with a threat of such magnitude.

Conclusion

In conclusion, ensuring a safe and secure United States requires projecting strength and taking decisive action to deter the cybersecurity threats that have come out of the Russian Federation in recent years. It is imperative that the United States takes a stronger, more proactive approach towards the fifth domain through persistent engagement and further collaboration with the private sector. In addition, the United States should work with NATO counterparts to identify, intercept, and expose the actors committing cyber-attacks, and promote all U.S. allies to take conjoint actions against Russian cyber-attacks. Moreover, the United States should place economic sanctions on the individuals responsible for the cyberattacks originating within the Russian Federation depending on the level of devastation. These actions will project strength, promote security, and bolster relationships between the U.S. and other free nations.

Bibliography

Al Jazeera. "'Be Afraid': Cyberattack in Ukraine Targets Government Websites." Ukraine-Russia crisis News | Al Jazeera. Al Jazeera, January 24, 2022. https://www.aljazeera.com/news/2022/1/14/be-afraid-cyberattack-in-ukraine-targets-government-websites.

CNN, Ivana Kottasová. n.d. "How Russian Threats Turned This Country into the Go-to Expert on Cyber Defense." CNN. https://www.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html.

Counter Threat Unit Research Team. "Notpetya Campaign: What We Know about the Latest Global Ransomware Attack." Secureworks. Secureworks, June 28, 2017. https://www.secureworks.com/blog/notpetya-campaign-what-we-know-about-the-latest-global-ransomware-attack.

"Exclusive: How Estonia Is Training Young People to Spot Fake News." 2019. GovInsider. July 5, 2019. https://govinsider.asia/connected-gov/mart-laidmets-kristel-rillo-estonian-ministry-of-education-and-research-fake-news-digital-competence/.

Garber, Jonathan. 2021. "Colonial Pipeline's Shipping System Hit with Brief Outage." FOXBusiness. May 18, 2021. https://www.foxbusiness.com/markets/colonial-pipeline-communications-system-down-report.

Hunt, Thomas C. 2018. "National Defense Education Act | United States [1958]." In Encyclopædia Britannica. https://www.britannica.com/topic/National-Defense-Education-Act.

"JBS USA Cyberattack Media Statement - June 9 — JBS Foods." n.d. Jbsfoodsgroup.com. https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-june-9.

Lenthang, Marlene, and Josh Margolin. "Ransomware Cyberattacks Shuts down Major US Pipeline, Company Says." ABC News. ABC News Network. Accessed February 7, 2022. https://abcnews.go.com/US/cyberattack-shuts-us-pipeline-supplies-45-fuel-east/story?id=77573904.

McLean, Rob, Benveniste, Alexis, Malloy, Allie. "Major Meat Producer JBS USA Hit by Cyberattack, Likely from Russia." CNN. https://www.cnn.com/2021/06/01/tech/jbs-usa-cyberattack-meat-producer/index.html.

Nakashima, Ellen. 2018. "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes." The Washington Post, January 12, 2018. https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

"National Defense Education Act | US House of Representatives: History, Art & Archives." 2020. @USHouseHistory. 2020. https://history.house.gov/HouseRecord/Detail/15032436195.

Nato. "A Short History of NATO." NATO. Accessed February 7, 2022. https://www.nato.int/cps/en/natohq/declassified_139339.htm.

Nato. "Cyber Defence." NATO, February 4, 2022. https://www.nato.int/cps/en/natohq/topics_78170.htm.

Nato. "The North Atlantic Treaty." NATO, April 1, 2009. https://www.nato.int/cps/en/natolive/official_texts_17120.htm.

"NATO Warns That Cyber Attacks on Member States Could Trigger a Coordinated Military Response." CPO Magazine, June 26, 2021. https://www.cpomagazine.com/cyber-security/nato-warns-that-cyber-attacks-on-member-states-could-trigger-a-coordinated-military-response/.

News, A. B. C. (n.d.). Ransomware cyberattack shuts down major US pipeline, company says. ABC News. https://abcnews.go.com/US/cyberattack-shuts-us-pipeline-supplies-45-fuel-east/story?id=77573904

"OFAC Attorney Explains the SDN List: OFAC Sanctions Attorney." OFAC Lawyer, January 31, 2017. https://ofaclawyer.net/specially-designated-national/sdn-list/.

Person, and Sabine Siebold Dmitry Antonov. "NATO Sends Reinforcements and U.S. Puts Troops on Alert as Ukraine Tensions Rise." Reuters. Thomson Reuters, January 25, 2022. https://www.reuters.com/world/europe/nato-sends-ships-jets-eastern-europe-ukraine-crisis-2022-01-24/.

"Private Sector Plays Bigger Role in NATO Cyber Strategy." National Defense Magazine. Accessed February 7, 2022. https://www.nationaldefensemagazine.org/articles/2017/2/8/private-sector-plays-bigger-role-in-nato-cyber-strategy.

"Russian Military 'Almost Certainly' Responsible for Destructive 2017 Cyber Attack." n.d. Www.ncsc.gov.uk. https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack.

Schmitt, Michael N. 2022. "Russian Cyber Operations and Ukraine: The Legal Framework." Lieber Institute West Point. January 16, 2022. https://lieber.westpoint.edu/russian-cyber-operations-ukraine-legal-framework/.

Sharma, Rakesh. "US Government Enlists Tech Firms' Help on Cybersecurity." Investopedia. Investopedia, August 9, 2021. https://www.investopedia.com/us-government-enlists-tech-firms-help-on-cybersecurity-5196484.

"Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace." The United States Department of Justice, October 19, 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

Statista Research Department. "Non-U.S. Share of Apple's Revenue 2006-2021." Statista, February 2, 2022. https://www.statista.com/statistics/263435/non-us-share-of-apples-revenue/.

"Ukraine Cyber-Attack: Russia to Blame for Hack, Says Kyiv." BBC News. BBC, January 14, 2022. https://www.bbc.com/news/world-europe-59992531.

"What Is Notpetya Ransomware? – Computer Forensics World." n.d. Www.computerforensicsworld.com. Accessed January 29, 2022. https://www.computerforensicsworld.com/what-is-notpetya-ransomware/.

Wilkie, Christina. 2021. "Colonial Pipeline Paid $5 Million Ransom One Day after Cyberattack, CEO Tells Senate." CNBC. June 8, 2021. https://www.cnbc.com/2021/06/08/colonial-pipeline-ceo-testifies-on-first-hours-of-ransomware-attack.html.

Williams, Michael John. "Make Russia Take Responsibility for Its Cybercriminals." Foreign Policy, November 9, 2021. https://foreignpolicy.com/2021/11/09/cyberattacks-russia-responsibility-ransomware/.

"Working with Our Private Sector Partners to Combat the Cyber Threat." n.d. Federal Bureau of Investigation. https://www.fbi.gov/news/speeches/working-with-our-private-sector-partners-to-combat-the-cyber-threat-wray-ecny-102821.