2020-5

A Twist of The Knife: A Research Design on Russian Information Warfare

Quinn Newman

A Twist of The Knife: A Research Design on Russian Information Warfare

Quintin W. Newman
Xavier University
201 South Stone Avenue
newmanq@xavier.edu

Abstract:

This paper primarily addresses the reasoning behind the 2016 cyber-attack orchestrated by the Russian Government against the United States. The primary question behind this paper is why did hackers operating on behalf of the Russian government decide to commit to an espionage-style attack to steal emails and documents during the 2016 election? This is important due to the danger that these cyber-attacks pose to the United States already tense political environment and integrity of the country's election systems as well as the democracy of other states. There is a real danger of the country's democratic functions being impeded due to the presence of foreign vested interests in the outcome of our elections. Major research has shown that there are marked deficiencies within the United States cyber defense infrastructure and a significant vested interest by the Russian government in seeing this attack carried out. This paper argues that the failure of the federal and state governments to improve and centralize their cyber security defenses is a major part of the reasoning behind why Russia conducted the attacks.

I. Intro

Cyber security has become a hot topic in international relations discourse as of late due to its increasing relevance in the field of statecraft and international espionage. It has resulted in a growing focus on how near instant communications across international borders has changed the dimensions of sovereignty and statehood. This has led to some states, like Estonia, to focus heavily on ensuring the safety and security of their citizens data due to the relatively small size of their populations (The Consequences of Cyber Attacks 2016, 176). This kind of awareness and protection has not been universal between all North Atlantic Treaty Organization members and we have seen significant attacks against many member nations.

In 2016, the United States was subject to one of the worst cyber-attacks in its history during a particularly contentious and fraught election that saw Donald Trump win the race. After the election, it emerged that the cyber-attacks had originated from agents working directly for the Russian government who had deliberately ordered the attack. This attack consisted of a breach of the Democratic Party National Committee (DNC) database and saw thousands of damaging emails released onto the website Wikileaks (Olhin 2017, 1579). This attack had a tremendous effect on the rest of the election calling into account the legitimacy of the Democratic party and giving the Republican party ammunition against the Hilary Clinton campaign. Given the already fraught relationship between the United States and Russia, which had recently come to blows over the Syria situation, why did the Russian government conduct such a massive and effective cyberattack on the Democratic party? Determining why the Russian government acted in this way is an important issue as The 2020 elections have been thrown into a state of chaos due to the current public health crisis. This attack is something that scholars have been actively studying as

the integrity of future elections in the United States depend adequate cybersecurity. In order determine the cause for the hacking of the DNC database in 2016, we must answer several questions about why the Russian government and its agents thought they could do it and what motivated this attack. This paper will seek to answer what the background to the event was, what have others said about this event, and if can compare this to another event in order to determine what was the reasoning behind the event was.

Given the evidence and the slow response of the United States to respond to the breach in the DNC database, it is likely that the Russian government chose to attack the United States in this manner because they knew that the United States's Cybersecurity infrastructure would not be able to defend against it. To prove this, we will conduct a qualitative analysis between how the UK and The United States handled cyberattacks and what were the distinguishing variables that lead to the DNC being chosen as a target.

II. Structure and definition of terms

This will be a qualitative analysis that presents a two-fold argument behind why Russia conducted the 2016 cyber attack on the United States election. This will be determined via analysis of two variables. These variables will be analyzed within the context of two comparative cases. One of these cases will be the 2016 attack on the US Democratic party database and the other will be the similar hack of the 2016 United Kingdom European referendum by suspected Russian operatives. These were chosen due to proximity in time, the similarity in kind of attack, and the involvement of operatives of the Russian Federation's government.

In order to best give background behind the content of the attack, it is important to give some background terms for clarification and identification purposes.

- Sovereignty-Concept derived from the treaty of Westphalia. It is a principle that depends on the domain and the practical needs of each state but primarily deals with the ability to retain political power and control over a set territory. The Tallinn Manual states that it applies to cyberspaces (Jensen 2017, 740).
- Cyber Espionage-Defined as any act undertaken clandestinely or under false pretenses that uses cyber capabilities to gather, or attempt to gather, information (Jensen 2017, 756).
- Cyberattacks-Online activities done by a group or individual that involve the stealing of corporate secrets, the spreading of false information, or the breach of government computers in an attempt to steal state secrets
- Database-A structured set of data held in a computer, especially one that is accessible in various ways.
- The Democratic National Committee-This is the entity that acts as the governing body for the United States Democratic Party. They coordinate strategies and supplies to support candidates throughout the country for local, state, and national office. It organizes the national Convention held every four years before the presidential election to nominate and confirm a candidate for President of the United States via delegates.
- Distributed Denial of Service (DDOS) Attack-This is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

- Wikileaks-This website was created in 2006 by Julian Assange as a non-profit organization for releasing documents obtained from anonymous sources (Zittrain and Sauter 2010).
- Internet Research Agency-A Russian company that works on behalf of Russian political and economic interests to engage in online influence and cyber warfare in favor of Russian interests.

This piece is primarily concerned with a comparative analysis of the 2016 DNC attack and the attack that took place in Britain during the Brexit referendum to make the case for the reasoning behind this attack. The paper will not discuss other foreign policy moves by the Russian Federation except as context for previous foreign policy actions similar attacks to the one that took place in 2016. It will also not cover similar attacks done by other entities except to bring them up in the context of modern states having a history of this kind of activity.

III. Views on the attack

Amongst the literature on Russian foreign affairs, there have emerged several distinct schools of thought to explain this particular event. While this attack is contemporary, the amount of research that has already been accomplished has been quite substantial. Amongst the discourse, some find an explanation of the issue via the filter of Realpolitik/realist views while others point to the lack of concrete law in international cyberspace and the ineffectiveness of the United States's response before, during, and after the attack. While there are many schools of thought, the two most relevant ones are the realist and liberal schools of thought as they provide research and scholarship that takes into account both Russian History and United States policy failures in a thorough and constitutive way.

One of the many leading schools of thought surrounding this event would have to be the school of conventional political realism. The school of realism has many offshoots but similar roots in the work of Hobbes, Morganthau, and Mearshimer. Their assumptions are the primary actors within international relations and that the international system is anarchic and unable to be ruled. The realist school therefore explains this cyber-attack as retaliation against United States actions prior to 2016 and is best introduced through the concept of "Vested Interest Theory". This theory, proposed by Johnathan J. Godinez presumes that in international relations, there are certain countries which possess a degree of political, economic, and military that they might be considered "predator-countries" which through means of espionage can conduct massive foreign electoral intervention (Godinez 2018, 1). The United States and the Russian Federation have been determined to possess this kind of power and are thus identified as "predator-countries". These kind of countries operate this way out of a belief that participating in foreign electoral intervention that will provide them with the furthering of their own interests, betterment and well being (Godinez 2018, 4). This implies the realist outlook of individual sovereign states operating in a global anarchy with very little international oversight. With this being known, what are Russia's interests? Scholars have pinned down that "for Russian foreign policy, the key goals are, first, to ensure the country's high international status and to influence global affairs; and second, to exclude external influences from what Russia defines as its privileged sphere of interest" (Libman and Obyendenkova 2018, 1045). There are numerous examples of Russia acting in this way in the recent past via means that even go past electoral interference in states like Ukraine and Georgia (Sadłocha 2019, 254). Both are states with significant Russian minorities and are in the process of being courted by the United States and the European Union

for participation in their institutions (Sadłocha 2019, 242). It also should be understood that Russia has conducted similar efforts to the US election cyber attack in the past with many attacks taking place after the 2014 Ukrainian Conflict. These attacks have often originated from the Internet Research Agency in Russia. This private organization works on behalf of the Russian government and has conducted significant influence campaigns that seek to destabilize democracies on a mass scale (Sinclair 2018, 118).They function as a mouthpiece for rhetoric on Russian strength and Western weakness while also functioning as a spearhead and tool for Russian government official in the cyber domain. This fits in well with the idea of contemporary Russian realists who espouse rhetoric that fits in well with both Godinez's assertions about "Vested Interest theory" and how a state is perceived being crucial to the prestige of said state.

Another view in this school of realist thought comes from the perspective of sovereignty and how it is used and viewed by the Russian government. It has been widely held in the international community that interference with a foreign political process may be illegal and it is primarily frowned upon when it occurs in the system of international relations. However there are issues with how the legal argument for its illegality are constructed and how each of the terms are used. Sovereignty can be defined as the political will of the people of a particular state, but "the notion of sovereign will described above does not accord with the concept of sovereignty as public international lawyers usually use the term" according to scholars of the issue (Ohlin 2017, 1595). Lawyers and jurists use the term in the context of the rights of a state to control its territory. This is where it is tricky to make the argument in the ways lawyers do about this topic because what Russia attacked was not territory or interests, but instead a technical apparatus of a political party. However, while this kind of attack does not play into

conventional ideas of what sovereignty means to the United States government and law professionals, the conducting of this attack was very much in tune with Russian behaviors towards its sovereignty. For Russia, it tends to view its own sovereignty in a proactive way and views threats from abroad as not simply territorial. They tend to view threats in the in terms of economic, cultural, and social thus enabling broad strategies for foreign policy maneuvers (Deyermond 2016, 965). To them "Russia was not causing any disturbance in the international order, but merely protecting its national interests" and thus using more of the general term for sovereignty (Sadłocha 2019, 240). All of this fits well within the school of neorealism in particular with its focus on the international relations system and how different countries have perceptions of national interests, how that is influenced by their political systems, and where a state is located geopolitically.

However, one of the big driving factors behind the realist school is an emphasis on practically and pragmatism that the modern Russian government seems to embrace. This is the school of Realpolitik, and it can be seen as the grandfather to a plurality of realist political dispositions in the world today. Realpolitik has its origins in the political career of Otto von Bismarck who helped unify Germany as a contiguous sovereign state through strategies that often allowed for violence and negative integration. Realpolitik has been a consistent feature amongst Russian leadership since the days of the Russian Tzars and it continues to be seen in the foreign policy moves that the Ministry of Foreign Affairs chooses (Sadłocha 2019, 240). This is a mindset of embracing practical yet sometimes contradictory solutions to political issues out of a need for strength and prestige. According to several scholars "the elements of the *Realpolitik* policy have become a constant element of the identity of Russian leaders and social expectations

towards the greatness of the Russian country and its prestige in the world have shaped the current identity of the Russian society" and thus enables them to act in ways that outsiders might view as aggressive (Sadłocha 2019, 256). To citizens of the United States, an attack on the US Democratic party database is criminal, but to the Russians it is a practical way to ensure their foreign policy goals are met. However, in the realist school there is another branch that some have ascribed to in order to better understand their actions.

The school of thought known as civilizational Realism argues that instead of being anathema to existing international mechanisms, the Russian Federation's government instead wishes for a higher degree of international arbitration and conflict deterrent mechanisms with the caveat that they favor Russian interests. Overall, through analysis of past interventions like in Ukraine it has been determined "that Russia is not rejecting the traditional international framework of conflict resolution. Rather, by making its counterarguments within the same framework, it is reaffirming its importance"and necessity (Petro 2018, 324). They do not reject international law and order as a concept but instead wish to combat the perceived hegemony of the United States and European Union. Their version of multipolarity relies on a great degree of negotiation which Moscow has become quite adept at in recent years (Karagorav 2012, 75). This attitude is partially a rejection of the old Soviet view of international order under communist rule and signifies more influence from the Realpolitik school than the school of radicalism in respect to Russia's foreign policy goals. This also fits well into previous conceptions of the Kremlin's approach to nationalism and national interest with many identifying the approach to be inconsistent and more pragmatic towards international law (March 2012, 417). Russian foreign

policy is not guided by one principle, but instead has many layers. With that being said, how does one actually operationalize the reasoning on display here?

The independent variables that this school of thought seems to use are United States elections on the national level and can be measured by the significance the election in question. This argument is one of the stronger arguments available because we can actively measure a correlation by looking at the presence of cyber attacks during important elections in western democracies like the United States and others. However, there are flaws in regard to how this school considers other elements such as international organizations like the UN, economic interests, and the competing ideas presented by the United States and Russia respectively

The point that the school of Liberalism in international relations theory makes about this attack points to the lack of concrete international law and retaliatory measures for cyber warfare and terrorism.This school of thought believes that the current case of Russian cyber-warfares was primarily due to the lack of coherent international laws surrounding cyber terrorism and information warfare in general.

Those who follow this school are mostly those who ascribe to the theory of neoliberal institutionalism and its notions of international relations. This discourse concerns how countries looking for mutual benefit will be willing to make transnational agreements. While there may be multinational organizations with a degree of regulation making and administrative power, there are still some cracks which have not been filled. The often cited “Talinn Manual” only sets out recommendations and guidelines for NATO, thus making it hard to pin down exactly what constitutes and attack by a foreign power (Jensen 2017, 735). This is supported by scholars like Logan Hamilton who believe that this attack is because “neither the UN charter nor customary

international law can apply to such actions or provide a remedy to impacted states" amongst other grievances with the current way the major powers deal with cyber espionage and attacks (Hamilton 2017, 183). The current paradigm essentially allows for state actors to be treated the same way as non-state actors and to get away with major violations of electoral law and privacy law in the countries that are affected by attacks. This is due to the lack of overarching and shared definitions as what qualifies as a cyber attack. Because there exists this discrepancy, when one does occur there are some who do not consider it a true crime and thus the response is limited. This is not helped by the idea that in cyber warfare, the idea of a *neutral ground* loses a lot of veracity. This is brought up by scholars like Jeffrey T.G. Kelsey whom argue that in the zone of cyber space, "Violations of the traditional principles of distinction and neutrality are more likely to occur" in an online space (Kelsey 2008, 14-27). With a lack of a shared concept of neutrality means that a belligerent state like Russia would never have to suffer any consequences for attacks against non-military or non-hostile targets because there are no agreed terms of neutrality. For this part of the school, the major issue is the lack of establishment of norms and what that does to the world.

In contrast to the more internationally based neoliberal school, there is a more defense oriented that one could identify as closer to traditional liberal assumptions about the way states act. The main ideological backbone of this school is Immanuel Kant and other enlightenment thinkers and does not assume that there are moral actors. This school firmly believes that the cyber-attack was carried out with the expectation that the United States was not prepared for an attack despite numerous attempts beforehand by other actors. Both China and North Korea have attempted to gain access into files concerning government and civilian infrastructure which

resulted in the infamous North Korean Hack of the Sony servers in 2014 (Lam 2018, 2172-2173). One would think that this would result in greater intensity of cyber defense, but while there was some intensification of talks with China and reprisal attacks against North Korea there was very little overarching structural change in how these things would be handled in the future. Instead, the United States relied on the older ideas of International relations "specifically, the U.S. response involved the doctrine of retorsions, economic sanctions law and practice, and the Vienna Convention on Diplomatic Relations" used by many states around the world (Lam 2018, 2182). There are many who consider this framework to be not applicable anymore and that current efforts are not enough to discourage future attack. This argument is made by the likes of Dóra Dévai, who consider the current strategy to be outmoded by current frameworks used by states like Russia. To him "the U.S. is lacking a working cybersecurity policy largely because its perception of cyber threats is self-centered and still deeply rooted in the strategic thinking of nuclear or traditional military attacks" and not in the realm of cyberspace (Dévai 2019, 59).The problem specifically lies in how complex the situation is over this kind of technology and how the security establishment of the United States has not adapted well to the new battlefield it finds itself in.

However, others in the Liberal group say that say that the material threat is relatively small in comparison to the other idea of threats posed by those looking to move towards war measures. Experts like Troy Smith argue that blowing the kinds of attacks, like the 2016 hack, out of proportion will end up backfiring when we really need to get serious about it. He argues that "after people continue to hear 'wolf' cried for too long they might dismiss the threat of cyber war and, unfortunately, the reality of the cyber threat along with it" when these attacks are used

to drum up political hysteria (Smith 2013, 85). He is not arguing that the attack was not serious but that the escalation of rhetoric could have us end up in a place where we cannot de-escalate and our governments are therefore forced to make grave decisions. There have been similar calls for measured approaches by others within the technology industry who are wary of government intervention into their programs (Peck 2017, 8). It has also been argued that viewing Russia as an adversary in the traditional sense is not helpful and may be guided by bias instead of rational thought. Some scholars argue that the Russian government is less interested in a direct conflict with the West is more concerned with prestige within its own neighborhood of Eastern Europe and Central Asia (Gunitsky AND Tsygankov 2018, 387). Overall the argument this part of the school presents is that while it is important to combat the threat, we must do it in a way that does not risk greater conflict.

One could view the primary variable that this school uses to be the failure of the International system to properly engage with cyber security affairs and it being primarily a case of lack of shared definitions and minutia. This can be measured in the lack of enforced international mechanisms to actively combat cyber attacks.

IV. Comparison and analysis

We will now apply these concepts to both how the effects of the lack proper cyber defense and vested interest theory make the case for why Russia conducted these attacks. This research design will be a qualitative analysis using congressional findings, academic journals, and other sources to build a picture of how the variables of the “Vested Interests” and cybersecurity failures had an impact on both cases. The cases selected will be the 2016 DNC cyber attack and another hack that took place during Britain’s referendum to leave the European

Union in 2016. This is a convenient case as both the vote and the election of Donald Trump were both events that were widely covered by the media, both involved cyber espionage and sometimes explicit cyber attacks, and both were influenced by parties outside of their respective countries (Peck 2017, 8). The targeting of a database echoes greatly the attack on the DNC database as well. There were many within the British government who were not plussed at the idea of this happening to them but considering the evidence, it appears that it was so.

To start, a brief description of the details of both attacks. The Brexit referendum had seen numerous irregularities as vested interests from both the European Union and others had been established in the run up to the election including several members of the leave campaign visiting several Russian sources (Cadwalladr and Jukes). The cyber-attack in question happened during the 2016 Brexit referendum but was not detected until 2017. This attack concerned a website used by UK citizens to register to vote and had crashed due to a suspected Distributed Denial of Service (DDOS) attack from elsewhere (Reuters). This was initially suspected to be due to millions of young voters looking to register last minute, but a government panel in the UK had determined that the signs were more in line with a conventional cyber-attack. Although the interference was not determined to have impacted the outcome, the attack was very troubling and drew eyes on whether the UK could stand up to these kind of attacks that could happen in future elections that could happen. It has been determined that the foreign elements who engaged the attack were most likely from Russia and originated from the Internet Research Agency (US Congress 2018, 39). Overall, the attack was much more of a minor affair as compared with the one that took place in the US, but it provides a good comparison as another nation that subject to a cyber attack by Russian government agents.

The cyber-attack on the United States in 2016 has been quite well documented since the event and with the actual event being conducted in the same year as the database DDOS attack in Britain it provides a convenient comparison case. The environment of the 2016 United States election has been well documented with both candidates emerging as some of the most unpopular in history and with many decrying the democratic process. It was in this environment that a breach occurred in the DNC database on June 14, 2016. It was not widely published or known about at the time but the effects of it would be extremely noticeable with many decrying the allegations that the DNC was favoriting certain candidates over others. On July 22, 2016, the infamous website Wikileaks published nearly 20,000 emails and eight thousand different attachments with more coming in waves up till the actual day of the election on November 7, 2016. Donald Trump won the election in what many saw as an upset. Soon after, it was determined by the Central Intelligence Agency that the Russian government had participated meaningfully in the attack on the DNC database with the intention of influencing the outcome (Dévai 2019, 47). There were tit-for-tat expulsions of diplomats, closure of diplomatic compounds and eventually a new round of sanctions but more could not be enacted due to the forthcoming change in power between the Obama and Trump administrations. It should be noted that these intrusions were not into the voting process it self but instead were directed at the apparatus of a major political organization that was fielding candidates for the election (Lam 2018, 2170). Despite the lack of actual vote manipulation, it was quite apparent in the aftermath that the attack and subsequent leak had a substantial effect on the election as evidenced by the many who point to it shifting the favor of the election to Donald Trump (Jameson 2018). Now

that the details of each incursion have been established, we can now provide a comparison and see which variable are significant.

Let us first view these attacks through the lens of what Russia's vested interest might be in both. The report on Russian hacking during the Brexit referendum, along with reporting during the aftermath of the referendum, and since then can reveal some key clues, as well as recognizing the UK's place within world politics. While it is not the economic and military powerhouse it once was, the United Kingdom still has a substantial part to place in the NATO military alliance and as the location of London, one of the most economically significant cities in the world. It is with this in mind that we can look at some of the connections which contribute to a vested interest in Russia caring about the referendum. It has been established that there were significant financial relationships between some of the most ardent pro-leave campaigners and numerous Russian, both state and private, entities prior to the referendum thus opening levels of communication between one side of the referendum and Russia (Cadwalladr and Jukes 2018). These open lines of communication could allow for coordination with elements of the campaign and with many meetings had between both the investors and the Russians we can assume this is the case. This plays well into Russian strategies for causing disunity in Europe and eroding commonly held truths throughout the amplification of existent social discord (US Congress 2018, 39). This has been identified as one of Russia's main goals and is a vested interest as Russia seeks to rearm and reaffirm their strength as a major social power with the added bonus of having substantial financial ties with political and economic interests on one side of the contentious political argument. It is here where one can see the vested interest as being tied to

causing social discord in Britain because of its status as a NATO member and as an ally of the US. Russia's vested interest is to see the US and its allies not have influence and clout.

There are similar threads in the case behind the vested interest that Russia has in influencing the results of the US election. The United States and Russia have been traditional adversaries since the inception of the cold war and even in the post-soviet age there are still tensions between the two countries which cannot be easily ignored. Recently that has manifested in tensions over Russia's intervention into Crimea and their support for separatists in Eastern Ukraine (Tchandourize 2018, 17). This is compounded with US intervention in Syria on behalf of the Anti-Assad Rebels, international condemnation of the treatment of LGBT individuals, and the historic military rivalry that these nations have had in the race to acquire ballistic missiles and nuclear arms.These reasons have resulted in a new round of tensions between the two and more reason than ever to interfere in each-others businesses. Now the domain is in cyberspace with the Russians looking to build up their intelligence and cyber security arsenal to counteract any US efforts to do the same. It is in looking at the broader rivalry between the US and Russia that we could maybe see the long game that the Russian government is playing here. According to some researchers, the 2016 attack was not only an attempt to influence the outcome of the election but also "it gave the Russian government access to data of American government officials, and that data was then used during a wider information war" that Russia is currently waging (Shuya 2018, 4). Ultimately, the vested interest is the desire to see the US and its allies wane in terms of influence and status within the world. Therefore, using a cyber-attack to sway American votes in a particular way is a valid tactic that they could use.

When one looks at the cyber security failures of the UK, one can look at many different avenues, but it is obvious that they possessed an overall better state of preparation and awareness than the United States. The cyber attacks against Britain, specifically the one against the voter database, attacked a broad range of British governmental interests including but not limited to the media sector, the telecommunications sector, and the energy sector (US Congress 2018, 118). The attacks were varied and included an online influence campaign directed by the Russian Internet Research Agency but certain measures did help prevent even more major attacks. These include measures to deter bad actors, prepare the online infrastructure for DDOS-style attacks, and to determine appropriate response measures. These measures mentioned int the congressional report allowed the UK to remain relatively unscathed from an espionage style attack from Russian government like done to the US. However, because these attempts were only enacted in 2016 and there is still little in the way to know the true extent of Russia's attacks on the UK population's financial information, personal information, and other parameters (US Congress 2018, 119). If the defenses could have been enacted sooner Russia might have not been able to act in the way they want and could have even prevented the state from even the idea of a DDOS style attack. Ultimately the failure, and thus the variable in question, is in the timing of the institution of broader cyber security efforts and how they were not instituted in time to prevent attacks like the DDOS on the voter database.

The US attack has been widely document and the Failures of the US cyber security have been even more widely documented. However, the failures of the prior administrations can be broken down into methodological, administrative, and timing failures. Prior to the attack, there had been growing concerns within the intelligence branches of the United States going back to

2011 and earlier citing the need for better cyber security against state and independent actors. Following the recommendations back in 2011 where we can see one of the large issues that seems to rear its head in the preparation of cyber defenses is the issue of how they are viewed. For those operating in the defense sector, cyber security is often viewed in terms of quantity and is viewed in the same way as conventional weapon systems like missile batteries or naval vessels (Dévai 2019, 45). This mindset has its benefits, but it also places limitations kinds of strategies that those in Washington endorse and who gets material support. This is where resource management and distribution comes into the argument as the United States federal government has a duty to distribute funding in many different directions and too many sources that are hard to direct. These include state governments, the Federal Bureau of Intelligence, Homeland Security, and numerous other agencies and governmental units which cannot act in unison the same way that the UK or other governments can act (Dévai 2019, 49). This results in a certain amount of fragmentation and lack of decisiveness. While there has been efforts to implement more forward thinking policy in this field, it has often seen criticism for their lack of legality (Cook 2018, 208). This in particular allowed for the attack to happen the way it did and even after the attack there were still “naming and shaming” of New York for allowing it to happen due to the DNC database being located there (Dévai 2019, 60) With this in mind, it appears that the failures of the US cybersecurity apparatus can be mostly understood through the decentralization of cyber security efforts and the dated viewpoint on cyber security by the United States Department of Defense and others.

Now that it has been shown how each of these variables manifest in both cases, it is important to compare and contrast. In terms of vested interest it appears that both attacks had

relatively the same variable of a vested interest, in seeing the United States and its allies become weaker and less capable against Russia and its foreign policy goals. The variable is the weakness as represented by the public response to each event. Both the media in the UK and the United States labeled these attacks as major failures and incredible missteps on the part of both governments as shown by reporting from *The Guardian* and other news sources with the United States being more widely discussed due to the public nature of the attack. These attacks have called into question the reliability of both governments and have given rise to the idea that these governments are less legitimate, and therefore weaker, because of them. The weakness, as represented by the distrust in each government from the press and the public at large, can be identified as the independent variable and as a commonality in both cases.

However, unlike the other variable, the failures of the cybersecurity apparatuses of both states are on different scales and thus can lead to a greater possibility for the US attack to be more easily seen as ebbing subject to both a vested interest by Russia and failure of cyber defense. The UK attacks were not as destructive, though still dangerous, due to the UK's National Cyber Security Centre (NCSC) to handle all cyber security matters creating a proverbial one stop shop for cyber security needs within the country (US Congress 2018, 119). This centralized process, along with a more visible response from the United Kingdom's government, created less damage and less of a negative response from the public and the press. This limited the loss of prestige and potentially defused a toxic situation. Regardless of the outcome, the Brexit debate was not swayed specifically by this attack and its fallout. This is something that cannot be about the attack on the DNC database. Because of the diffuse, non-centralized, and seemingly stale outlook of the Department of Defense on the implementation of cybersecurity

measures, the Russian agents were able to retrieve countless documents and sensitive information regarding the DNC and the candidates themselves. The revelation of the documents publication in WikiLeaks created an image that the United States was weak on cybersecurity and that the system was falling apart. The United States was not able to put up a truly effective cyber security defense prior to the attack and therefore the attack ended up blossoming into something dire. Many have analyzed how the attack helped sway members of the public to vote for Donald Trump due to the bad image propagated by the leaked documents. Due to content of the leaked documents, many became very unenthusiastic about a Hilary Clinton presidency and in time the election proved this true as Donald Trump won the electoral college vote and became president (Dévai 2019, 69). Overall, the failure of cyber security can be seen as a significant variable as it was the main reasoning behind why the attacks took on different characteristics and were on separate levels of effectiveness.

The conclusions that one can make from this comparison can be seen as follows. While Russia's vested interest was present in both cases and took on a similar character of an attempt to weaken the United States and its allies, it was the failure of cybersecurity that can be seen as the primary and most significant Independent variable. If the United States had centralized their cyber security apparatus like the UK to better defend against cybersecurity attacks, Russia would have most likely would have not seen the United States as being as much of a target and thus would have not tried something as daring as the DNC attack. It is not that they did not possess any defenses, but instead that the organization elements including the states, the FBI, the OMB, and numerous other authorities, did not In this we find the independent variable as the organizational, structural, and ideological issues that prevented a better cyber security defense

apparatus from coming about prior to the US election. As this was the factor that determined the severity of the attack and the aftermath, this is the significant aspect and the main factor into why Russia believed it could impact the US election and weaken the US government in the eye of both the public and the media.

V. Conclusion

Given the research that about Russian foreign policy, the United States's cyber defense, and its effects on 2016 election, there is a significant amount of evidence that the lack of centralized and effect cyber-warfare defense policies is the reason for attack on the DNC database. Through a comparative study showing the similarities between the situation in the UK and the United States, it is clear that the most important aspect is the lack of an up-to-date and solvent cyber security strategy that could prevent intrusions into databases like the kind at the DNC. This variable is significant and shows that without proper mechanisms enacted by both the United States and the international community, there will be further attacks from The Russian Federation and other powers willing to exploit internal political tensions. If foreign powers were able to get into a major political party's database with that much ease, imagine what else they could accomplish. The urgency of the issue should be understood as the political climate in the United States right now points towards future polarization which could lead to more illicit measures by other governments who have a vested interest in the outcome of future elections. With an overall lessening of respect for sovereignty, peace, and self-determination of government in general we could potentially see the concept of Westphalian sovereignty disappear and something far more sinister take its place. The infrastructure of elections are incredibly reliant on databases like the one that was attacked and the gathering of large quantities of personal data.

The knowledge that this technology to safeguard people identities and documents can be manipulated is concerning and should be acted upon. Without policies that can better protect against cyber-attacks, we could potentially see harm come to both the United States and its citizens. However this research is limited to the national scale and it would be prudent for individual states to fund and consider their own studies to find out their own vulnerabilities. Overall, if a broader cyber-security initiative is not presented by federal government before the next major election, there are likely to be more attacks like this from an even greater number of hostile actors from abroad.

Bibliography

- Cadwalladr, Carole, and Peter Jukes. 2018. “Revealed: Leave.EU Campaign Met Russian Officials as Many as 11 Times.” *The Guardian*.https://www.theguardian.com/uk-news/2018/jul/08/revealed-leaveeu-campaign-met-russian-officials-as-many-as-11-times (July 8, 2018)
- Cook, Chris. 2018. “Cross-Border Data Access and Active Cyber Defense: Assessing Legislative Options for a New International Cybersecurity Rulebook.” S*tanford Law & Policy Review* 29 (Febuary): 205–36.
- “The Consequences of Cyber Attacks.” 2016. *Journal of International Affairs* 70 (1): 175–78.
- Dévai, Dóra. 2019. “The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace: (Part 1).” *AARMS: Academic & Applied Research in Military & Public Management Science* 18 (January): 59–77.
- Dévai, Dóra. 2019. “The U.S. Response to the 2016 Russian Election Meddling and the Evolving National Strategic Thought in Cyberspace: (Part 2).” *AARMS: Academic & Applied Research in Military & Public Management Science* 18 (January): 59–77.
- Deyermond, Ruth. 2016. “The Uses of Sovereignty in Twenty-First Century Russian Foreign Policy.” *Europe-Asia Studies*, no. 6 (July):957- 983.
- Godinez, Johnathan J. 2018.“The Vested Interest Theory : Novel Methodology Examining US-Foreign Electoral Intervention.” *Journal of Strategic Security* 11, no. 2 (2018): 1-34.
- Gunitsky, Seva, and Andrei P. Tsygankov. 2019. “The Wilsonian Bias in the Study of Russian Foreign Policy.” *Problems of Post-Communism* 65 (June): 385–93.

- Hamilton, Logan. 2017. “Beyond Ballot-Stuffing: Current Gaps in International Law Regarding Foreign State Hacking to Influence a Foreign Election.” *Wisconsin International Law Journal* 35 No.1 (July): 182-204.
- Jamieson, Kathleen Hall. 2018. “How Russia Cyber Attacks Helped Trump to the US Presidency | Kathleen Hall Jamieson.” *The Guardian*. https://www.theguardian.com/commentisfree/2018/oct/22/russia-cyber-theft-trump-us-election-president-clinton.
- Jensen, Eric Talbot. 2017. “The Talinn Manual: Highlights and Insights.” Georgetown Journal of International Law 48: 735–78.
- Karaganov, Sergei A., Kristina I. Cherniavskaia, and Dmitry P. Novikov. 2016. “Russian Foreign Policy: Risky Successes.” *Harvard International Review*, no. 3 (March): 74-79.
- Kelsey, Jeffrey T.G. 2008. “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare.” *Michigan Law Review* 106 (July): 14-27.
- Lam, Christina. 2018. “A Slap on the Wrist: Combatting Russia’s Cyber Attack on the 2016 U.S. Presidential Election.” *Boston College Law Review* 59 (June): 2166–2201.
- Libman, Alexander, and Anastassia V. Obydenkova. 2018. “Regional International Organizations as a Strategy of Autocracy: The Eurasian Economic Union and Russian Foreign Policy.” *International Affairs* 94 (May): 1037-1058.
- March, Luke. 2012. “Nationalism for Export? The Domestic and Foreign-Policy Implications of the New ‘Russian Idea.’” *Europe-Asia Studies*, no. 3 (May): 401-425.
- Ohlin, Jens David. 2017. “Did Russian Cyber Interference in the 2016 Election Violate International Law?” *Texas Law Review* 95 (July): 1579–98.

- Peck, Stuart. 2017. “Cybersecurity in World Politics.” ISSA Journal 15 (7): 8.
- Petro, Nicolai N. 2018. “How the West Lost Russia: Explaining the Conservative Turn in Russian Foreign Policy.” *Russian Politics* 3 (3): 305–32.
- *Reuters*. 2017. “Brexit Referendum Website Might Have Been Hacked: UK Lawmakers.” April 12, 2017.
- Sadłocha, Jarosław. 2019. “Heterogeneity of the Notion of Interest in Accordance with the International Relations Theory: A Study of Russia’s National Interests.” *International Studies: Interdisciplinary Political & Cultural Journal* 23 (1): 235-256.
- Sinclair, Michael R. 2018. “The Rising Dragon and the Dying Bear: Reflections on the Absence of a Unified America from the World Stage and the Resurgence of State-Based Threats to U.S. National Security.” *Syracuse Journal of International Law & Commerce 46* (1): 115–81.
- Shuya Mason. 2018. “Russian Cyber Aggression and the New Cold War.” *Journal of Strategic Security* 11 (1): 1–18.
- Smith, Troy E. 2013. “Cyber Warfare : A Misrepresentation of the True Cyber Threat.” *American Intelligence Journal* 31 (1): 82-85.
- Tchantouridze, Lasha. 2018. “The Black and the Caspian: Russia’s Warm Seas.” *Central Asia & the Caucasus* 19 No.4 (2018): 16-24.
- US Congress. Senate. 2018. *Putin’s asymmetric assault on democracy in Russia and Europe: implications for U.S. national security: a minority staff report prepared for the use of the Committee on Foreign Relations*, United States Senate, One Hundred Fifteenth Congress,

2018 Sess., January 10. https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf (April, 1,2020).

- Zittrain, Johnathan & Molly Sauter, Everything You Need to Know About Wikileaks, *MIT Tech Review(*Dec. 9, 2010), https://www.technologyreview.com/s/421949/everything-you-need-to-know-about-wikileaks/ [http:// perma.cc/R2WH-9284].