Liberal Arts & Social Sciences International Journal (LASSIJ)
eISSN: 2664-8148 (online)
https://www.ideapublishers.org/index.php/lassij
Vol. 5, No. 1, (January-June 2021): 648-666
Research Article | Original Research https://doi.org/10.47264/idea.lassij/5.1.42

Cyber hegemony and information warfare: A case of Russia

Asma Rashid*[1] | Anum Yar Khan[1] | Syed Wasif Azim[2]

1. Department of Politics & International Relations, International Islamic University, Islamabad, Pakistan.
2. Department of Political Science, School of Political & Social Sciences, University of Innsbruck, Austria.

*Corresponding Author Emails: asmawaqar87@gmail.com | asma.rashid@iiu.edu.pk

Abstract

The world has shifted to a digital landscape in the recent decade with both its perks and underlying threats. Russia, throughout history has experimented with its information along with cyber channels and have been able to generate fruitful results that are manifested in the contemporary era. Russian expertise towards merging cyber domain into its military capabilities is praiseworthy to the point that its Western adversaries, despite the fact being economically and technologically advanced compared to Russia, have not been able to effectively counter Russian aggression. This research examines the essentiality of cyber security as a mere software or cyber command can create instability and drastic consequences requiring millions for clean-up by examining Russian cyber-attacks on Estonia, Georgia, Ukraine, US and Western Europe and concludes that the first steps towards Cyber and Information Warfare have been made, it is now to be made sure this does not escalate into a Cyber Arms Race. The research recommends that cyber security should be treated as an international issue with rules established for cyber governance and databases identifying cyber criminals and the software used by them or can be used by them and requires cooperation rather than competition amongst states particularly global superpowers.

Article History

Received:
March 13, 2021

Last Revised:
June 13, 2021

Accepted:
June 18, 2021

Published:
June 30, 2021

Keywords: CISA, NATO, crowd strike, cyber-attacks, cyber espionage, cyber security, fifth generation warfare, malware, Russian report, Solar Winds, unconventional warfare.

How to Cite:
Rashid, A., Khan, A. Y., & Azim, S. W. (2021). Cyber hegemony and information warfare: A case of Russia. *Liberal Arts and Social Sciences International Journal (LASSIJ), 5*(1), 648-666. https://doi.org/10.47264/idea.lassij/5.1.42

1. Introduction

The advent in technology and current trends of globalisation has indeed served as a massive tool to revolutionise the world. Practices that were common decades ago are not seen nor heard of in the current age, whereas there are number of novel practices that have become the norm of today. This revolution has extended its web to various areas such as economy, politics, science, health, education, infrastructure and even warfare. However, this revolution in modern warfare is not only a threat but also an opportunity for nations to grasp. Another novel practice is the evolution in means of warfare giving rise to the terminology of the 5th Generation of Warfare that includes hybrid and cyber warfare which have come to existence owing to the present status of diminishing territorial boundaries among states. In this aspect, Cyber warfare is something that has not been given its due attention and is emerging as a silent yet deadly threat. Cyber warfare is the type of warfare that includes the usage of computer technology and attacking the cyber-space of nations, their important institutions and there are various reasons as to why these types of attacks are carried out, such as:

- To carryout cyberespionage i.e., to retrieve important strategic military, economic or political information that is kept in confidential files on computers of nation's institutions.
- To disrupt functions such as water supplies, transportation systems, power grids, critical infrastructure, and military systems by the usage of viruses.
- To disable authorized and legitimate users to access respective cyber-space and important documents known as DoS or "Denial of Services".
- To hold or confiscate important government or organisational documents in exchange for ransom (Hanna *et al.*, 2019).

Apart from these activities attack on cyber-space can also lead to disrupting functioning of government functions as well in a bid to destabilise it or to elect an official that is favourable with respect to a particular nation or group, the prominent example of that of being Russia when it was speculated that Russian intelligence had hacked into the electoral procedure of the US that led to Donald Trump's victory in the 2016 elections despite the fact that he had clearly lost the popular vote. In the modern-day scenario, several nation states have engaged in this type of Warfare predominantly US, China, North Korea, Israel, India and Russia. This has led to highlighting of developing Cyber Security seen in the national policies of many states that are working towards it which in previous years was neglected.

In the Russian context it tends to focus more upon the "information" factor in terms of its Cyber Strategy and Warfare. Its Information doctrine has clearly stated the gathering of information and manipulating this said information to inflict damage in the form disruptions and creating Havoc by establishing controversial or hoax knowledge and theories. The cyber military capabilities of Russia are highly advanced and have expressed their desire to engage their adversaries in terms of both offensive as well as defensive cyber confrontation. However, when explaining cyber warfare, Russian's does not tend to use the terminology of "cyber" and refers it in broader terms that as "Informationiasation". In the Russian context, cyber is considered as one of the means to acquiring information that are to be coupled with traditional efforts of gaining information such as disinformation operations, PsyOps, electronic warfare, and political subversion (Connell & Vogler, 2017).

The usage of cyber and Information networks of Russia is not new. These activities have been

carried out prior the second world war and have only escalated during the Post-Cold War Era, in order for Russia to maintain its control over former Soviet States such as in Chechnya in 2000, Estonia in 2007, Georgia in 2008 and in recent have been more active since the conflict in Ukraine in 2014 and emerge as a global super power by taking advantage over the lack of strength of its rivals in the cyber and information domain.

This research seeks to shed light on Russian usage of cyber and information technologies in the past to indicate that while some consider this new, it has existed in Russian military policy making since decades and now has come to exist as such a powerful weapon at Russia's disposal. The research also further seeks to highlight the level of impact of Russia's cyber prowess and how its victim states are coping with such threats by asking important questions such as What has been the response of NATO to deal with Cyber aggression from Russia? And The US is the world's current reigning superpower, why has it not been able to effectively counter Russian Cyber-attacks? The study also seeks to understand Russian motivation behind utilizing such means of unconventional warfare considering theoretical perspective to understand the nature of cyber and information warfare in the realm of international relations theories and perspectives. In the end the research also seeks to provide recommendations regarding how relations can be improved between Russia and its Adversaries as well as advises to take collective action to tackle the emerging unconventional threats.

1.1. Historical background

The cyber and information warfare that is termed as Russia's strategy of the contemporary era has its roots even before World War 2 i.e., to say that only contemporary situations have prompted Russia to behave this way would be an understatement. The development of Russia's cyber operations can be dated back to 1920s when the first kind of these cyber operations manifested in the form of "radio-reconnaissance stations" that were used to propagate Soviet agenda in the USSR and abroad. These stations played an increasingly important role in securing Russian victory in the Sino-Soviet conflict of 1929. By 1939 there were advancements in Russian technical intelligence activities such as Soviet Military Signals Intelligence and cryptography that even surpassed the capabilities of the West. After the Second World War, there was considerable growth in Soviet technical intelligence and in 1942 military cryptologists were able to hack into German Enigma machine granting them the ability to decipher and intercept German signals and communications.

During the pre–World War II era, the Spetsprop, units came into existence and were responsible to carryout functions such as broadcasted messages and distributed leaflets and products to enemy forces to reduce their morale and entice surrender. As of 1991 these units rebranded under the GRU that divided them in to 8 'psychological operations groups' and were dispersed into Russia's military districts. Under the influence of the KGB government these intelligence activities were able to flourish significantly during the Cold War era and by the Gorbachev era the Soviet military possessed 40 signals intelligence regiments, 170 battalions, and over 700 companies.

In the 1990s and 2000s the Federal Security Service built a network of independent Russian hackers and specialists to carryout Cyber operations, respectively. The 'Siberian Network Brigade', under the guidance of the FSB, were responsible for the Chechen website attacks in 2000s. During the late Cold war, the 85th Main special centre unit came into existence and with its advent led to the "Bulat Computer System". After the 2000s Chechen website attacks, the

most prominent cyber-attacks that occurred were against Estonia in 2007 followed by Georgia in 2008 and Ukraine in 2014, with occasional attacks on the US and EU financial and security systems by Russian hackers (Lilly & Cheravitch, 2020).

1.2. The Estonia cyber-attacks (2007)

The Estonia 2007 cyber-attack impetus was that the Estonian government carried out eradication of the Soviet Union monument i.e., the Tallinn and were moving it to a military cemetery. This was termed by the Russian leadership as an act of vandalising historical monuments. The Estonian leadership viewed these monuments as a symbol of oppression when they were under the Red Army's aggression. Russian cyber and information agencies propagated to the masses that the Estonian leadership was not only eradicating the monuments but also the graves of Soviet military personnel and honourable citizens and, as a result, were undermining and carrying out offensive actions against the ethnic Russians in Estonia. Russian information channels worked to their full extent to instigate unrest among the youth that were pro-Kremlin.

Technologies were used to send text messages, internet spams, inability of government officials communicating with each other via emails, breakdown of Estonian online banking services leading to a damage worth 415,000 euros, DNS services were offline, mobile communication operators experienced disruption, the government was unable to communicate with the media due to the fact its briefing room was shut down. These were later identified to be the work of non-state hackers with pro-Russian sentiments and the IP address used was of Russian governments and the President's administration established the fact that it was indeed sponsored, instigated, and supported by the state itself. According to CERT, Russian language websites had already begun to propagate information to instigate country wide protests calling for volunteers to cyberattack Estonian websites. These actions led to hindrance of communication amongst state institution creating a feeling of unrest, havoc, panic, and psychological terrorism (Pernik *et al.*, 2018a).

1.3. Georgia cyber-attacks (2008)

The Georgia cyber-attacks were carried out in a similar manner i.e. Russian language websites propagated the goals, plan of action and targets. DoS was the primary course of action targeting a total of 54 Georgian websites including government websites and similar techniques of that of Estonia were employed such as massive email spams, website defacements and payloads on web application. The attacks were later identified to be carried out by the Russian Business group affiliated with the Russian security agency. It was distinct from that of Estonia in a way that for the first-time cyberspace was used to carry out military operations. Georgia was already involved with Russia in a military conflict over Ossetia. Georgian intelligence was able to detect a Malware in 2011 known as WIN32/Georbot that was involved in cyberespionage and had gathered confidential information regarding Georgian state institutions, economic and non-governmental institutions. It was attributed by Georgian experts that this was carried out by Russian security services (Pernik *et al.*,2018b).

2. Literature review

Russia's emerging status as a cyber superpower cannot be ignored. To compete with its adversaries and to emerge as a key player in international politics Russia seeks to introduce a

new realm of competition where it has been investing for a vast majority of years, and now has culminated itself as a giant, seems to be almost unstoppable and has emerged as a constant source of ire. The cyber capability of Russia continues to grow from simple information espionage attacks to extreme kinetic manifestation, serving as a reminder that, if worked upon more, can generate dire consequences and cause mass scale destruction.

In the book "Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers", Greenberg (2019) provides a detailed account of the Ukraine hacking attacks that occurred from a time period of 2014-2017 and not only highlights the technicalities of the attack in detail by explaining the kinds of software that can be used but ultimately provides a clear-cut evidence as to why it is clear that the group of Hackers that identified them as Sandworm are affiliated with Russia state intelligence GRU. This book serves as an excellent reminder as to why there is a need for caution regarding each software used and how the concept of a full-scale cyber war is not imagination but has come to exist as a reality by explaining in detail the minute working of software painting a horrifying picture of the future. Furthermore, this book also sheds light towards the fact that how little there is preparedness and attention given to the looming threat of cyber warfare and Russia's growing strength as a cyber nation as well as emergence of non-state actors and the growth in their strength despite not having military prowess can cripple nations with a mere click of a button.

The article "The past, present, and future of Russia's cyber strategy and forces written by Lilly and Cheravitch (2020) explores the detailed evolution of Russia's GRU intelligence units and provides an eye-opening account to analyse that what steps Russia undertook to modernise its warfare capabilities from traditional espionage activities to cybernetics. The article raises an important point by discussing the need to create a form of deterrence to Russian offensive aggression by the US. This article explains Russian motivation behind utilizing such methods of warfare. According to the article 'these weapons can help an adversary achieve information supremacy without crossing borders or establishing physical presence on the enemy's territory' and offensive cyber capabilities can be considered as asymmetric actions that can help a technologically and economically weaker state to neutralize a stronger opponent'.

Article Russia's Approach to Cyber Warfare written by Michael Connell and Sarah Vogler published in the CNA Analysis and Solutions explain the concept of offensive cyber activities and defensive cyber activities categorising Russia in the former. It provides a list of the activities that are carried out by Cyber groups as well as highlights that Russia establishes that cyber operations be used alongside other traditional methods of warfare, something actively seen in Estonia (2007), Georgia (2008) and Ukraine (2014-2017). The article also indicates Russia's familiarity of usage of such means to propagate agenda and create havoc and upheaval in rival states by the manipulation of information bringing insight to why Russia terms cyber warfare as 'Informationiasation'. The article further provides a new direction for Russia's employment for non-state hacker groups so frequently for two major reasons namely Cost effective and anonymity.

In the book Understanding Cyber Conflict: Fourteen Analogies, Stephen Blank in Chapter 5 titled Cyber War and Information War à la Russe discusses the inner working mind-set of Russian motivation and establishes that Russia like all autocratic and dictatorial states envisions itself in a constant state of conflict and threat predominantly by the US and hence feels the need to engage each and every aspect of the country in a state of war and feels the needs to modify each element in a military sense. The Russian leadership establishes that

information wars have the capability to generate results which direct military confrontations are not able to. The article notes that Russia heavily stresses upon the techniques of 'framing' regarding media and seeks to diminish any public opposition to its military operations by propagating Pro-Russian agenda and believes that it has been done by the US for years.

The article "Russia's latest land grab: How Russia won Crimea and Lost Ukraine" written by Mankoff (2014). The article explores the concept of "frozen conflicts" which states that the division of the Soviet Union was done based on ethnic distribution that gave Russia an opportunity to install its enclave within the territory which would be eventually used to stir up conflicts ultimately leading to the revival of the Soviet Union. Furthermore, by focusing on the concept of "ethnic divisions" this article provides a new and rather overlooked overview to the conflict, the article also discusses the exploitation of the ethnic communities by the independent Soviet states painting the picture that Russia is not always the ultimate oppressor while highlighting the injustices of the former Soviet States leading to Russia intervention in support of Russian ethnic minorities in the first place.

The article "Uncertain security community: Building western cyber security order" by Tumkevič (2018) highlights cyber security postures of the US, UK, France, and Germany regarding their priorities and whether they prefer multilateral or bilateral means to address the evolving cyber scenario. It establishes the point that there is a need for a common ground and to undertake the matter collectively. The article highlights the difference in viewpoints regarding the nations as the UK and US prefer a rather offensive means to tackle the growing threat, Germany is rather defensive, and France has not been able to decide whether it opts an offensive and defensive approach and hence creates a dubious scenario for the leading NATO states for them to devise common practices regarding how NATO is to engage the Cyber aggression by not only Rogue states but non-state actors.

In the report "Hacks, leaks and disruptions: Russian cyber strategies, Russian cyber activities in the EU discusses offensive cyber activities that have taken place throughout the years in various EU countries. The nature of the attacks has been inherently similar and centralised on parliaments and government personalities. The article discusses this as a way of Russia to dispose of any possible anti-Russian governments and to install regimes that are either pro-Russian or using social media to generate Pro-Russian sentiments, respectively. It also proposes possible solutions as well as criticizes EU approach to dealing with cyber aggression to be inadequate and recommending that more work is needed in this regard.

The CRS published Russian Armed Forces: Military doctrine and strategy explores Russia's military doctrine related to be cyberspace and establishes that it was first mentioned by Gerasimov in 2013 to revolutionise the means of warfare with the changing aspects of technology and Russia recognises the need for it. The report describes that Russia extends its capability of deterrence to not only nuclear but also "strategic conventional weapons, and non-military measures—including concepts such as NGW—across both peacetime and conflict". One interesting aspect of the article is that it provides a comparison between the events of Arab Spring and propagation of Western ideology of Democracy as two similar phenomenon and further provides reason as to why Russia considers its cyber activities defensive.

The book "Cyberwar: How Russian trolls and hackers helped elect a President" by Jamieson (2018) explores the details of the 2016 US presidential election that led to the surprising victory of Donald Trump who had lost the Popular vote. Despite the majority of US public against the

regressing sexist and racist views of Trump, his overnight victory shocked the nation. The turning point was the leaks of Clinton's controversial Emails that tarnished her electoral campaign. The book explains the tricks through social media that were used by the Russian trolls disguising themselves as American citizens and using references from the American constitution was enough for fooling common Americans to pay mind to their propaganda. The book excellently raises the question of incompatibility of US laws that are not in accordance with the overall nature of Cyber aggression, and hence, further solidifies the need for laws dictating cyber governance.

The article "Unpacking US cyber sanctions" by Peters and MacConaghy (2021) provides a detailed analysis of the sanctions imposed by the US in response to cyber aggression by Rogue States such as Iran, North Korea, and Russia as well as non-state actors. It highlights a variety of activities carried out by the US administration from imposing sanctions to freezing financial assets and travel restrictions. However, the article raises serious questions regarding how effective such measures are as well as whether the US should rely only on such means or should work towards more practical approaches into dealing with this threat establishing that alternative means to counter sanctions exists. The article serves as an eye opener for the realisation that how traditionalist approach of the US that has always generated results in its favour has not been able to produce similar fruitful results against non-traditional threats.

3. Theoretical framework

The "theory of realism" has been advocated by various scholars throughout the ages the most prominent ones of them being Thucydides, Machiavelli, Thomas Hobbes, and Emmanuel Kant that laid the foundations of various division in the realism school of thought such as classic realism and neo realism. The essence of realism is that man by nature is selfish, nasty, egoistic and seeks power and the international system is anarchic which prompts its actor to behave in a way that would ultimately satisfy its end goals. The stronger states or 'the prince' according to Machiavelli is free to do anything while the weaker states suffer and must compromise. To gain hegemony and to battle the uncertain nature of the anarchic international system, man seeks to establish power by any means deemed significant. Anarchy is the status quo, and it impacts the actions of the state and states in turn act to maintain a balance of power (Wohlforth, 2008). Hence, realism supports the notion that any means necessary to gain power can be undertaken establishing that there is no morality when it comes to international relations and therefore offers explanation along with justification of Russian utilisation of Unconventional along with Conventional means to gain power. Since, the world has shifted to a digital and cyber landscape one reality that cannot be ignored is that there is no central governing authority in the realm of cyber space that dictates rules and monitors abidance by said rules, in this way we can say the Cyber Space is indeed anarchic in nature where every state is for themselves (Craig & Valeriano, 2018).

The theory of Realism also states that man or states seeks to manipulate each and everything to gain power and authority over the weaker states and this is what we can see in Russian military and political agenda that how Russia has manipulated cyber technology to gain superiority over its adversaries that are not much advanced in the respective field i.e., it valued competition over cooperation. It has transformed its cyber and information capabilities as a sort of weapon that extends far beyond that of espionage purposes and directly attacks key institutions of various states such as the electoral systems whereby Russia seeks to elect pro-Russian leaders to gain and maintain its power an example of which would by US president

Donald Trump (Jamieson, 2018) It continues to carry on with its purpose and in the future, there might be even stronger cyber-attacks. This falls perfectly under the realist principle of States seek to gain, maintain, and expand power. This also lies in accordance with the realist principle of immoral nature of international system and how states would go to any extent to gain supremacy. Russia is aware of its strength in the realm of Cyber and Information warfare thus establishing itself as the "Prince" hereby doing whatever Russia seems right to dictate the rules of international politics according to its will. Russia could've used its expertise to assist other states against this threat of cyber aggression and non-state actors in this regard, but it resolved to realist nature and used it as a means of warfare and establishing control meaning that States by nature are antagonistic.

To counter Russian cyber aggression, its adversaries have taken more aggressive approaches such as sanctions and working on their own cyber military postures and cyber security, this can also be covered the umbrella of defensive realism. This branch of realism advocates that in the face of offensive realism, states must take defensive actions to maintain the balance of power and protect themselves and their interests from aggressive actors (Lobell, 2017). As the US and Western European states come to terms with Russian growing strength as a cyber Nation, they're currently working towards to first detect how much Russia has infiltrated their cyber networks and how much information is influenced by Russia, furthermore the US is actively seeking to engage Russia in this regard by the establishment of CISA in 2018 as well as imposing sanctions but the US approach is rather flawed owing to the fact that one cannot tackle unconventional threats via conventional means and henceforth in order to maintain the balance of power, other states need to do more while the threat of possible escalation towards cyber and information warfare remains.

Russia on the other hand defends itself by stating that it rather is following the defensive realism paradigm and its activities cannot be considered as 'offensive' by arguing that US and its Western Allies have long worked to not only spread misinformation regarding Russia being a hegemonic, power-hungry and oppressive nation but also have been involved in instigating Russia's youth against the Putin government and spreading the ideology of democracy via social media and hence it is the US and its Allies that have carried out the offensive realist stance. By examination of the stances of both parties one thing is evident i.e., according to realism, states are always suspicious of one another and will always expect hostility. Henceforth we see that cyber has integrated itself in International Relations Theory, at first which was not considered a domain of competition in the realistic perspective as anything that generates military actions can only be constituted as realist. Analyst that refers themselves as Cyber Realists have now begun to see how cyber fits into the realist criteria and as an alternative means of power propagation to the Morgantheusian concept. With case studies of Russian aggression, similarities have been observed between cyber space and realist principles owing to a paradigm shift in realist politics and taking into consideration threats and power aside from conventional military forces and weaponry (Rocha & Fonseca, 2019).

4. Methodological approach

The research is based upon qualitative analysis of both primary and secondary resources such as research reports, articles, journals, books and news webpage and analysis is carried out under the content analysis method. The rationale for using this method was that it is the widely used method in social sciences as well as the fact that this study does not deal with any numerical figures or statistics for quantitative analysis to be used. The research design follows the

comparative historical event research method from a period of 2014-2021 and various events from that period are analysed to indicate similarity of Russian attacks to establish evidence to support their motivation, case studies that are undertaken during said time period have almost similar pattern of results ranging from Cyber Espionage and false information propagation, there was only one unique case of Ukraine where Physical attacks manifested. The research conducted is reliable in the sense that all resources consulted are reliable and published with authentic and justified information.

Limitations to the study include unintentional biasedness towards Russia and against US and European states or vice versa as the main basis of this research is only directed towards highlighting Russian growing hegemony and the threat cyber-attacks pose to state security and stability of international system under the shadow of potential cyber arms race however, whilst exploring Russian strength biasedness of the researchers might be observed by certain readers leading to Interpretation of information provided through this research and Time restriction regarding the exploration of case studies and literature analysed that might've led to certain aspects ignored by certain readers of this research.

The significance of the research is such that to identify the evolution in means of warfare and to study how it is carried out in the digital space and to dictate why there is a need for rules regulating cyber activity and why there is need for cybersecurity policies. The research also seeks to shed light on how global hacktivist elements work, why they are an immense threat to national security and why strict steps be taken to tackle this ongoing threat as well as to see how nation states manipulate this threat into such a powerful force that cannot be countered. The research also seeks to explain Russian ultimate motivation behind these attacks as well as to bring into Focus how Russia has couple conventional and non-conventional means of warfare to emerge as a formidable threat. This research also tends to bring into focus that why cyber warfare is not a far reality but is currently a sword hanging above the head.

5. Current timeline of events (2014-2021) and responses

5.1. Ukraine cyber-attacks

In 2014 Ukraine and Russia have been involved in a conflict that led to the annexation of Crimea instigated by the speculations of Ukraine becoming part of the EU that would result in Russian loss of access to the warm waters in the Crimean coast. It was also speculated that Ukraine would also become part of NATO. It has been Russia's longest desire to carry out revival of the Soviet Union and if not possible then to maintain its stronghold on the former Soviet Countries and hence we see Russia often instigating acts of violence towards former Soviet States in the form of either. Apart from the military conflict that ensured amongst the belligerent states there was a sort of hybrid war present among them as well along with cyberattacks carried out by Russia to dismantle state functioning of Ukraine and to cripple their response mechanism creating psychological pressure. The first cyberattack carried out by Russia was in 2014 when a Russian based hacking group 'Cyber Berkut' (Baezner & Robin, 2018) was involved in hacking the election system of Ukraine three days before the presidential election to rig the election so that their preferred pro-Russian candidate would win. In 2015 another attack was carried out on a power grid that resulted in power shortages. Hackers used certain malware such as black-energy and used spear phishing for employees to download data from mock emails resulting kill disk malware to destroy part of the grid.

Similar attacks were also carried out in 2016. 2017 saw one of the deadliest attacks carried out in Ukraine with the usage of malware "Petya" resulting in the malware "Not Petya" which provided access to commercial institutions such as utility companies, banks, airports, and government agencies along with multinational companies such as Maersk the Danish shipping giant, FedEx the logistics giant and Merck pharma company. A total of 10 billion USD was required for clean-up. However, against Russian desire this has attracted a vast amount of involvement and interest in the domain of cybersecurity from the West. While the US is actively exchanging intelligence with Ukraine along with US tech related companies such as Microsoft, cyber firm Crowds trike and Cisco's cyber intelligence unit known as Talos are more actively engaging in Ukraine. USIAD attributed to Ukraine for the development of its IT system amounts up to 10 million USD. Furthermore, EU and the US have been conducting seminars across Ukraine for awareness regarding Cybersecurity and policy (Cerulus, 2019). Russian support of Insurgent elements in Crimea along with hacktivists provided the necessary leverage for Russia to win the Crimean war. The strategy was important as it enabled access to location of Ukrainian artillery subjected to destruction (Flynn, 2019).

5.2. Cyberwar against the US

The rivalry between the US and Russia has extended from the end of the Second World war to the contemporary era with both countries engaging in competition in various fields of military, nuclear, economy, space, and technological innovations. This competition has also made its way to the cyber domain as well. The belligerent states have carried out cyberespionage and attacks against one another. After the Cold War Era, US emerged as the sole superpower and retained the status quo of unipolarity throughout many years. Russia, however, did not give up and continued its struggle for hegemony. In recent years there has been a shift in the status quo as some have speculated the shift to multipolarity and in this scenario Russia is actively engaging with the global world both offensively and cooperatively and has been termed as "Revisionist power". Over the years many small and large cyber-attacks have been carried out by Pro-Russian groups. Some of the prominent ones include The Democratic National Committee Cyber Attacks and the Solar Winds hack.

The DNC attack was carried out in the years of 2015 and 2016. Indicated by US intelligence reports along with cybersecurity firms, Crowd strike, Fedilis and Mandiant that two Russian intelligence agencies were found responsible for these attacks by the names Cosy Bear in 2015 and Fancy Bear in 2017. They used techniques such as spear phishing and sent emails to important government officials in which contained links when clicked enabled hackers to access the files stored in their computer and email passwords. This enabled hackers to not only gain access to Hilary Clinton's controversial emails that were then given to WikiLeaks smearing her electoral campaign but also carried out hacking of the electoral system that resulted in Donald Trump's victory in the 2016 elections. The tactic used in this regard was that while Russian trolls actively participated in propagating Pro-Trump Agenda on Social media sites with the hacking of Hilary Clinton's mail, this provided as the final straw on the camel's back leading to tarnishing of Clinton's image and Trump winning the election (Jamieson, 2018). This was confirmed by CIA officials (Kelly & Bowman, 2016) however, severely denied by the Trump administration after all at the end of the day it ultimately benefitted the Trump administration.

The most recent cyber-attack that took place was the of the Solar winds hack in which a US cybersecurity company, Fireye detected. The Solar Winds is a network management company

and because of this hacking, several areas were impacted due to breach such as Microsoft to US government agencies, including the US Treasury and departments of Homeland Security, State, Defence, and Commerce as well as research data related to COVID-19, NATO, European Parliament. It was later articulated to one of Russian intelligence agency SVR which Russia has denied. As to why Russia has been accused is that it has carried out similar attacks in the past as well (Vaughan-Nicholas, 2021). This has been called as a Supply Chain attack since rather than targeting private sources, service provider was hacked (Korolov, 2021). This attack is considered more of a cyberespionage rather than cyberattack.

Following these events, the Biden administration responded with strict actions such as expelling ten Russian diplomats along with imposing sanctions upon Russia (Soliman *et al.*, 2021). However, it is the need of the hour that due attention to be paid towards US cybersecurity policies and actions so that the data of millions of Companies and individuals are compromised. The important question here is to note that how were Russians able to hack into such critical areas of US state agencies and retrieve information so easily? For years there has been neglect in cybersecurity posture which only as of recent years have been considered. US has tended to focus more on traditional means of warfare rather than non-traditional means of warfare. Whilst its economic and military capacity exceeds that of Russia in great ways, the cyber domain is a front where we see Russia winning.

Irrespective of the fact Cybersecurity and Infrastructure Security Agency (CISA) was able to stop Russian meddling in the 2020 elections this year as well as was able to detect Russian hacking in the case of Solar winds (Phillips, 2019) going as far as to expel Russian diplomats along with sanctions but these are actions taken post the attacks not prior. Another argument for this is that the types of attacks carried out are not merely 'attacks' but taken more in the context of espionage. The US cannot use its advanced technology or nuclear capabilities against such events as they have resulted in no loss of life. Also, one key aspect is to note is that CISA did not even exist prior to 2018. Only in Biden's presidency there have been thinking to improve policies in cyberspace and to focus more on cyber deterrence approaches. So, it is questionable for US as the world's strongest nation to start thinking of cyber strategy even though Russian threat has been in looming for years.

Even though a vast number of sanctions have been imposed upon individuals that have been involved in cyber terrorism and cyber espionage both state and non-state, the question here to ask is that how practical and effective these sanctions are? As well as if assistance and financial systems are blocked what guarantee is there that no other means will be undertaken by these individuals to transfer finances. Furthermore, if these sanctions prove themselves to be ineffective, this can ultimately impact foreign policy tool of the US and hence create a doubt over the credibility of economic sanctions to control rogue states and individuals (Peters & MacConaghy, 2021).

5.3. Attacks against Western Europe

Russia has also been responsible in carrying out cyber-attacks and cyberespionage against various countries of the Western Europe such as Germany, Norway, Denmark, Italy, and France as well as the UK. In 2017, Germany was under severe cyberattacks from Russian group ATP28 that was able to infiltrate both the government as well as foreign ministries. Russia was also accused of cyberespionage by Norway, Denmark, and Italy. In Norway, the Norwegian security services highlighted targets of cyberattacks that were democratic institutions, the

Police Security Service and the country's Radiation Protection Authority. France was also under cyberattacks by Russia in the years 2015 and 2017. In 2015, Russian affiliated hacking group ATP28 was involved in hacking of French TV network taking down all their 12 channels (Limnell *et al.*, 2018a) while in 2017, were involved in hacking of French President Emmanuel Macron email account and leaking over 20,000 of his emails to smear his electoral campaign (Vilmer *et al.*, 2018). After Brexit, it was also speculated that Russia was ultimately behind the decision of UK exiting the European union as it ultimately supported Russian interests in 2016, following the Russian Report that was released in 2020.

However, experts have denied these accusations stating that the polling was a physical process rather than electronic, so it is impossible such an act could have taken place which is answered by the report that it is uncertain whether Russia via the use of social media did or did not influence public opinion and lent support to certain prominent UK officials. Further speculations have also come to existence that Russia was also ultimately behind the 2014 Scotland referendum. Despite all these statements the report does confirm that Russia indeed plays an active role in UK politics, and it is far greater than how the UK officials want to admit, and it seems that they are giving Russia a sort of an easy hand when it comes to investigations (Ellehuus & Ruy, 2020). However, the UK highlights that in the future it will take deterrent and self-defence activities and hints at tackling threats in five domains that include maritime, land, air, space and cybernetics (Lester & Moore, 2020) that further confirm the fears of a possible escalation of a cyber war or military confrontation. Just like the US, even in Europe we see there is vulnerability and weakness regarding cyber policies. Russian hackers are easily able to infiltrate and acquire confidential and crucial information. There are steps to prevent these attacks but are only taken place when said attack is carried out i.e., there are no pre-emptive measures.

The thing here to note is the lag in the intelligence agencies of these countries in detecting any possible activity to take place, even if the hackers are just non-state actors that work independently with no connections to the Russian Government, why have not adequate steps have been taken to ensure safety of not only individuals but also key political figures' cyber rights. This highlights further how little state governments take into consideration the Cyber security interests of their respective nationals. Even though the cyberattacks on the German elections of 2017 were predicted (Tumkevič, 2018), fruitful actions were not undertaken to prevent the action. This serves as an example of how little preparedness is observed by the states that presume themselves under Russian threat. The question here is to ask if the enemy was known, the kind of offense was known then what caused inadequacy? Furthermore, why haven't there been undertaking of adequate measures in order to capture these so-called independent hacker groups, yet there is even lack of recognition of the associated persons and hence raises a serious question on not only the security and intelligence agencies of these countries but also highlights the need for dictation of cyber space rules and regulations as well as databases that identify not just groups but also individuals that are involved in cybercrimes and hence require greater level of commitment from national intelligence agencies to monitor state individuals activities regarding cyberspace as well as to take into consideration private Social Media sites such as Gmail, Facebook, Twitter etc.

To see what kind of groups can access data of individuals through these sites, how these companies protect private information of individuals and whether no background business is occurring where information is sold to the hacking groups by these private websites and what kind of information or agendas can be propagated through these sites. Furthermore with the

recognition of the zero day phenomenon , this raises scrutiny over each and every software used and hence calls for stricter attention towards Cybersecurity, the fact that this phenomenon provides a leverage to hackers and even companies developing the software do not know how to cure this phenomenon creates a situation in which the time bomb is in the pocket and the person is waiting for it to blow up as it is a software defect that only hackers know about and are subject to exploitation as seen in the case of the Ukraine Black energy case (Greenberg, 2019). Furthermore, the attacks of Ukraine have openly manifested themselves as Cyber operations are not only limited to information manipulation but can manifest kinetic damage and hence of modified in the future could lead to full scale destruction by setting off machinery and weaponry to self-destruct only by entering a simple code.

5.4. NATO response

The word 'cyber' first entered the NATO's vocabulary at the Prague Summit the Heads of State and Government in 2002. However, in the years to come responses dealing with cyberattacks and cyber threats were considered as more domestic measures rather than to be undertaken by international organisations. Something that should not have been done so as Russia had a vast developed information and cyber network and had demonstrated its capabilities enough times. Cyber security was not considered eminent as compared to other issues such as terrorism. A major reason why as to no proper response by the NATO member states can be seen is since until now cyber aggression by Russia does not include itself in the kind of threat that would prompt NATO military action (Blank, 2017) and hence explains why NATO felt the need to modify itself in the face of emerging Cyberwar like scenario. Following the attacks of Estonia and Georgia, NATO focused to strengthen its cybersecurity policy and on the emerging cyber security landscape respectively because of which NATO adopted its first cyber policy which urged its member states to share information with each other as well as practice and capabilities.

Following the Wales summit of 2014, the NATO members extended Article 05 of the charter which states that any attack to one NATO member will be seen as an attack to all states to the realm of cyber. Since Russia's annexation and cyber activities in Ukraine almost all NATO members have responded to imposing sanctions on Russia, but these seem to have little to no avail as Russia continues to carry out strong attacks that are potentially more dangerous in the years to come. This suggests that NATO needs to develop effective cyber related policies rather than relying on traditional approaches. Furthermore, these actions cannot work since Russia already has the technology and software it needs. Economic sanctions would do little than to impact as in this type of competition, the damage done is rather abstract.

In 2016 at the WARSAW summit there was a consideration to develop an independent doctrine to cover cyber related issues. It was agreed that cyber domain and operations will be given as much attention as that of traditional operations along with a cyber pledge was taken by member states to develop maximum range of capabilities aimed to protect national networks and infrastructures. However, all these attempts seemed to be futile following the 2017 attacks of Russia on German and French governments. This served to highlight even, yet NATO countries were all talk, and no concrete action was undertaken.

It was only in 2017 that the NATO agreed to launch a cyber operations capability at the Supreme Headquarters of Allied Powers in Europe. However, this would take eminent efforts for it to become reality. In 2018 at the Brussel's Summit, it was also decided that a Cyberspace

Operations Centre would be setup as well as NATO can draw support in terms of cyber capabilities from member states (NATO, 2021). One thing that NATO member states have stated that due to complex global scenario and hyper connectivity of the world they have not been able to undertake fruitful efforts however, here it is key to note that Russia singlehandedly has been able to subdue almost all major nations of the globe this is indeed an embarrassing point for NATO (Alatalu *et al.*, 2018).

5.5. Russian approach

While providing analysis to the actions taken by the Russian government towards directly and indirectly infiltrating cyber and information space of the states it is necessary to understand Russian motivation and viewpoint regarding how they view the cyber confrontation. Even though Russia does not have a specific doctrine that addresses cyber security and warfare, their actions however project openly their desire of integrating cyber offensive and defensive capabilities within their military as well as information sphere. In the 2015 military doctrine it was openly stated that Russia recognised the threats it faces in the information space and what actions it will take to address or counter these threats. The interesting thing to note here is while Russia uses the terminologies such as websites, telecommunication networks, internet, and information technologies etc. as cyber connotations, Russia refers them as a part of its "information infrastructure" (MFA Russia, 2016) and this terminology explains how these activities have been used to distort, gather, manipulate, and disseminate information.

Upon closer analysis of its information, military and cyber postures, the respective doctrines project a rather 'defensive approach' which is somehow contradictory to Russian offensive action. If viewed from the point of view of Russian leadership, they term these action as 'retaliatory actions' and argue that the west is responsible for projecting Russia in a negative light globally as well as have meddled in internal matters of the Russian state and have propagated their ideologies that led to weakening of relations amongst the Soviet states and continue to do so in former Soviet States (McDermott, 2016) which even till today Russia views under sovereignty and recognises as a breach of Russian national interests which are so vital that Russia would do anything necessary for their safeguard. In this regard Russian state officials often compare their condition similar to that of the Arab spring where propagation of Western ideology of democracy was carried out via social media and establish that similar activities must've and are occurring in former Soviet territories and within Russia as well (Bowen,2020). Henceforth, is endangering Russian Ideology and deems as a direct attack on Russian sovereignty believing that the US and its allies are instigating Russia's own citizens against the state. Furthermore, it also recognises its control over former Soviet territories in matters of their decision-making owing to ethnic features, something eminent in the case studies of Georgia, Estonia, and Ukraine that where decision was not made favourable to Russian interests, Russia reacted.

Russian President Vladimir Putin recognises that the breakdown of the Soviet Union was one of the biggest tragedies to occur (Nbc News, 2005) and hence his ideology is based upon revival of the Soviet Union (Popovici, 2018). We see aggressive approaches towards former Soviet States if it is deemed by the leadership that they aim to break the connection with their past. When the breakdown of the Soviet Union took place, it was carried out in such a manner whereby a large fraction of Russian populace would be a part of the newly independent Eastern Europe states thus giving rise to the terminology of 'Frozen Conflicts' (Mankoff, 2014). If Russia's national policy is assessed, it clearly establishes that it will come to the aid of ethnic

Russians distributed in Eastern Europe countries foregoing territorial constraints and will take any measures it deems necessary. If seen in the case studies of Estonia, Georgia, and Ukraine, Russia has laid the foundation of threat to ethnic Russians and their heritage sites or territories to act offensively what they term as defensive. As to why there is a pattern for Russian hackers to target US and its western Allies can be attributed to the facilitate it seeks to install pro-Russian governments that will easily enable Russian integration in International Politics and ultimately would not raise many concerns over Russian activities a major example of the is Donald Trump who openly exhibited Pro-Russian and Pro-Putin sentiments in the 2016 elections. It could be considered that Russia seemed to take a similar approach in European countries.

6. Conclusion

Russia has worked towards the expansion of its information and Cyber capabilities even before the concepts of hybrid warfare and cyber space gained familiarity. At first Russia relied on traditional means of information and media, now it relies on cyber espionage and spreading propaganda via the new media i.e., social media i.e. it has modified its technology with the coming trends. The attacks carried out by Russia further highlight that Russia not only limits cybernetics to the area of only acquiring, manipulating and transmitting information rather it has great expectations form said technology. There could come a time when it will control physical action of states from within its territory, clearly observed in the case of Ukraine where it was able to carry out physical acts to instigate unrest and instability. It can be said that the case of Ukraine was a test bed and there can be expected future cyber-attacks coupled with physical attacks expected such as this.

By closer analysis it observed by majority policy analysts that in recent developments in the post-Cold War era, Russia has tended to carry out a more non traditionalist approach to maintain its stronghold in world politics while seeking revival of the glory it once sought. The Russian policies if assessed drive towards one conclusion that Russia views every action from the West as a threat and seeks to manipulate every opportunity in the global arena to challenge the hegemony of the West. Even prior to the world war era it has sought usage of information acquisition via espionage and now what we see currently are the fruits because of that long process of development, something that was neglected globally in the wake of more traditional problems such as Terrorism and territorial conflicts. Russian cyber-attacks highlight two global realities, the first of them being that how the world is shifting from conventional means of warfare to non-conventional means of warfare such as Cyber warfare and hybrid warfare as analysts have included cyber warfare under the umbrella term of Hybrid warfare and another reality of that how dangerous can technology be and, in some scenario, have prompted analysts to even consider de-digitalisation of societies (Limnell *et al.*, 2018b).

Another important thing to see is that with respect to the emerging nonconventional forms of warfare the preparedness of the West is quite minimal even until now it is considered that Cyber threats cannot led to any dire consequences and have no motivation towards created an international unit dealing with the said issue and only domestic feats made by states. However, the question to not here is that if one hacking group comprised of only a handful of individuals can hack into national security systems the time is not far where they will soon hack into weaponry systems as well and to be able to control said weaponry via codes to cause self-destruct or attacks on the state territory within the state itself. Furthermore, in the present era even terrorist and non-state militias have also shifted their scope to the cyber domain with the

emergence of cyber caliphate. Furthermore, Russia's cyber warfare also creates a threat towards the ideology of democracy as in many cases of the attacks we see that mostly Russia has carried out attacks for the election of their preferred candidates and hence undermines the democratic ideology of 'choice of the majority and free'.

In a nutshell, Russia is regarded as a 'revisionist power' meaning that it was a former superpower seeking to establish its prior status as such. In recent years we have seen Russian activities transform into a rather aggressive and assertive stance. From Russia's active involvement in the Syrian conflict to its growing ties with China and the role they are playing in Afghanistan. Russia is actively giving out the message that it is a key player in international politics and should be regarded as such. It is also trying to secure a favourable world opinion of itself so that it could build connections however, the US and NATO's active involvement in its backyard has been a constant source of ire for Russia. Henceforth, Russia realises that while the US can effectively counter its conventional and nuclear prowess, it throughout the years has seen that the same cannot be said for the realm of cybernetics and information.

The problems that need to be pondered here are that will these minor cyber activities result in a full scale cyber war? What areas of national security will be threatened by such activities? Will this new emergent threat create a security dilemma and instigate a Cyber Arms race? How viable or trustworthy are the non-state actors Russia employs (Sandworm) and are these non-state actors really linked with the Russian government? And is there a possible middle way for the belligerent states to address this situation? Furthermore, what can be done by the US and European countries under Russian threat to establish deterrence? Last but not the least is that does the world require large scale events such as the Japan Nuclear attacks, 911, climate change and COVID to realise the importance of Nuclear, Terrorist, Environmental and Health related issues and for cyber security to be recognised as a legitimate concern what criteria should current cyber aggression by states fulfil to prompt action of the International Community? The case study of Russia proves that cyber warfare is not a farfetched reality and has shown what can be done by cyber capabilities and should be treated as dangerous military tool as the damage inflicted covers various domains such as economy, ideological and individual privacy and should not be confined to only entertainment purposes. Key recommendations of the study are as follows:

- Continuous Russian attacks may prompt retaliation from the West as well and hence could instigate a full-scale cyberwar that could further result vulnerability of key information of individuals easily accessible to terrorist groups such as the cyber-caliphate. Instead of fighting with each other the adversaries should work together towards sharing knowledge and capabilities to battle global cyber threats and capturing international cyber criminals.
- Russia has a weak economy that tends to bear the burden of its conflicts and is also under international isolation to some extent predominantly from the Western Europe and North America. It seeks to form relations with countries to boost its economy. It can attract a more cooperative and integrated role in international community by offering its technical expertise and cyber technologies as well as sharing knowledge.
- The global community needs to have more comprehensive approaches towards dealing with non-traditional problems rather than considering them as something inevitable. Following the changing scenario of global warming, COVID-19, global economic crisis, refugee crisis as well as energy crisis it is imminent that focus be shifted from conflicts

as well as states should aim towards not creating conflicts and work towards absolute and collective gains.

- The US and EU countries have long since employed an isolationist and un-cooperative approach towards Russia tending to limit its approach in the global arena that has prompted Russia towards behaving aggressively towards them. Instead of constant enmity channels of cooperation should be established amongst them.
- Presently we see that there is no involvement from international organisations such as the UN regarding the growing threat, it is necessary that proper rules and regulations be dictated to govern activities in cyberspace like the Chemical and Biological Weapon Conventions, the nuclear treaties such as NPT, CTBT and PTBT and the UNCLOS.

References

Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Pernik, P., Reinhold, T., Reshetnikov, A., Soldatov, A., & Vilmer, J.-B. J. (2018). NATO's responses to cyberattacks. In N. Popescu & S. Secrieru (Eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies* (pp. 95–102). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21140.13

Baezner, M., & Robin, P. (2018). Cyber and information warfare in the Ukrainian conflict. *CSS Cyber Defense Project*, 5–24. https://www.researchgate.net/publication/322364443.

Blank, S. (2017). Cyber war and information War à la Russe. In G. Perkovich & A. E. Levite (Eds.), *Understanding Cyber Conflict: 14 Analogies* (pp. 81–98). Georgetown University.

Bowen, A. S. (2020). Russian armed forces: Military doctrine and strategy. *Congressional Research Service*. https://fas.org/sgp/crs/row/IF11625.pdf

Cerulus, L. (2019, February 14). How Ukraine became a test bed for cyber weaponry. *Politico.eu.* https://www.google.com/amp/s/www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/amp/

Connell, M., & Vogler, S. (2017, March). Russia's approach to cyber warfare. *CNA Analysis and Solutions*. https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

Craig, A., & Valeriano, B. (2018, February 3). Realism and cyber conflict: Security in the digital *age. E-International Relations*. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

Ellehuus, R., & Ruy, D. (2021, March 5). Did Russia influence Brexit? *Centre for Strategic and International Studies (CSIS)*. https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit

Flynn, M. J. (2019). Strategic cyber: Responding to Russian information warfare. *The Cyber Defense Review Special Edition: International Conference on Cyber Conflict (CYCON U.S.)*, 193–208. https://www.jstor.org/stable/26846128.

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.* Knopf Doubleday Publishing.

Hanna, K. T., Ferguson, K., & Rosencrance, L. (2019, May 28). What is cyberwarfare? *Searchsecurity*.https://www.google.com/amp/s/searchsecurity.techtarget.com/definition/cyberwarfare%3famp=1.

Jamieson, K. H. (2018). *Cyberwar: How Russian hackers and trolls helped elect a President what we don't, can't, and do know*. Oxford University.

Kelly, M. L., & Bowman, E. (2016, December 10). CIA Concludes Russian Interference Aimed to Elect Trump. *NPR.* https://www.npr.org/sections/thetwo-way/2016/12/10/505072304/cia-concludes-russian-interference-aimed-to-elect-trump.

Korolov, M. (2021, February 4). What is a supply chain attack? Why to be wary of third-party providers. *CSO Online.* https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html.

Lester, P., & Moore, S. (2020). Responding to the cyber threat: A UK military perspective. *Connections: The Quarterly Journal, 19(1),* 39-44. https://doi.org/10.11610/connections.19.1.04

Lilly, B., Cheravitch, J. (2020). The past, present, and future of Russia's cyber strategy and forces. *12th International Conference on Cyber Conflict (CyCon),* 129–155. https://doi.org/10.23919/cycon49761.2020.9131723

Limnell, J., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Pawlak, P., Pernik, P., Reinhold, T., Reshetnikov, A., Soldatov, A., & Vilmer, J.-B. J. (2018). Russian cyber activities in the EU. In N. Popescu & S. Secrieru (Eds.), *Hacks, leaks and disruptions: Russian cyber strategies* (pp. 65–74). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21140.10

Lobell, S. E. (2017). Structural realism/offensive and defensive realism. *Oxford Research Encyclopedia of International Studies.* https://doi.org/10.1093/acrefore/9780190846626.013.304

Mankoff, J. (2014). Russia's latest land grab: How Russia won Crimea and lost Ukraine. *Foreign Affairs, 93(3),* 60–68. https://www.jstor.org/stable/24483406.

McDermott, R. (2016, November 18). Russia's 2015 National Security Strategy. *Jamestown.* https://jamestown.org/program/russias-2015-national-security-strategy/.

MFA Russia. (2016, December 5). Doctrine of Information Security of the Russian Federation. *MFA Russia.* https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163.

NATO. (2021, May 26). Cyber defense. https://www.nato.int/cps/en/natohq/topics_78170.htm

Nbc News. (2005, April 5). Putin: Soviet collapse a 'genuine tragedy'. *nbcnews.com.* https://www.google.com/amp/s/www.nbcnews.com/news/amp/wbna7632057.

Pernik, P., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Reinhold, T., Reshetnikov, A., Soldatov, A., & Vilmer, J.-B. J. (2018). The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine. In N. Popescu & S. Secrieru (Eds.), *Hacks, leaks and disruptions: Russian cyber strategies* (pp. 53–64). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21140.9

Peters, A., & MacConaghy, P. (2021). *Unpacking US cyber sanctions*. Third Way. http://www.jstor.org/stable/resrep30835

Phillips, M. (2019, December 18). Russia hack claims: What is the cybersecurity and Infrastructure Security Agency (CISA)? *foxnews.com.* https://www.google.com/amp/s/www.foxnews.com/politics/russia-hack-claims-what-is-the-cybersecurity-infrastructure-security-agency-cisa.amp.

Popovici, A. (2018, July 12). Why Russia wants Crimea. *history.com.* https://www.google.com/amp/s/www.history.com/.amp/news/crimea-russia-ukraine-annexation.

Rocha, M., & da-Fonseca, D. F. (2019). The cyber issue and realist thinking. *R. Esc. Guerra Nav, 25(2),* 517-543. https://doi.org/10.21544/1809-3191.v25n2.p 517-543

Soliman, T. A., Simon, D. A., De, R., Hungerford, J., Ito, Y., Lev, O., Nadadur, A. D., & Silverstein, J. M. (2021, A*pril 20). Biden Administration Announces Expansion of Sanctions Against Russia and Signals Potential Additional Restrictions Following SolarWinds Cyber-Attack: Perspectives Events*. Mayer Brown. https://www.mayerbrown.com/en/perspectives-events/publications/2021/04/biden-administration-announces-expansion-of-sanctions-against-russia-and-signals-potential-additional-restrictions-following-solarwinds-cyber-attack

Tumkevič, A. (2018). Uncertain security community: Building Western cyber security order. *Journal of Information Warfare, 17(1),* 74–86. https://www.jstor.org/stable/26504130.

Vaughan-Nichols, S. J. (2021, January 4). SolarWinds: The more we learn, the worse it looks. ZDNet. https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/?_amp_linker=1%2Ac37si5%2Aid%2ASFJxYS0yVnlsSjc4RW1MQllyVnhBWkxXekwzZmM5eHl2aXo1QkJVc1RnQXNHZWZDUy0zRGRPWURXWFRGSmZCRA..#ftag=CAD-00-10aag7e.

Vilmer, J.-B. J., Alatalu, S., Borogan, I., Chernenko, E., Herpig, S., Jonsson, O., Kurowska, X., Limnell, J., Pawlak, P., Pernik, P., Reinhold, T., Reshetnikov, A., & Soldatov, A. (2018). Lessons from the Macron leaks. In N. Popescu & S. Secrieru (Eds.), *Hacks, leaks and disruptions: Russian cyber strategies* (pp. 75–84). European Union Institute for Security Studies (EUISS). http://www.jstor.org/stable/resrep21140.11

Wohlforth, W. C. (2008). Realism. *Oxford Handbooks Online.* https://doi.org/10.1093/oxfordhb/9780199219322.003.0007