SOCIAL SCIENCE REVIEW ARCHIVES
https://policyjournalofms.com

ISSN Online: 3006-4708
ISSN Print: 3006-4694

# Digital Arms Race: U.S. - Russian Cyber Conflicts and their Impact on Global Financial Security

**Sumrah Ashiq[1], Dr Saddaf Sultaana[2]**

[1] School of Professional Psychology, University of Management and
Technology, Lahore, Pakistan
[1] Assistant Professor, Department of Political Science and International Relations
(DPSIR), University of Management and Technology, Lahore, Pakistan,
Email: sadaf.sultaana@umt.edu.pk

***DOI: https://doi.org/10.70670/sra.v3i3.889***

## Abstract

With the growth of cyber warfare, nations now use technology to retain power, obtain information and disturb their opponents. The influence of Realism in International Relations (IR) theory is investigated on the cyber confrontation between the United States and Russia for global financial stability. It investigates how cyberspace, apart from conventional warfare, is used for deterrence, power display and dealing with economic challenges. By looking closely at NotPetya and SolarWinds, the paper demonstrates that countries use financial targets in their national strategies. It also looks at the critical issues of identifying parties, managing activities and preventing attacks within the lawless digital environment. Finally, the article suggests strategies to help countries resist cyber threats, improve international cyber rules and stop future stress in the financial sector.

**Keywords**: Cyber Warfare, Interstate Relations, US-Russia Tensions, Cyber threat.

## Introduction

Things are developing at high speed around us. Wars today are settled with computers and code instead of soldiers and tanks. Investment in digital advancements by countries has made cyberspace the home of a competitive race that goes unseen to many people. People also call this race the digital arms race. It means more nations are competing to develop advanced means for cyber-attacks, eavesdropping and digital defense. As before, when countries competed to build nuclear weapons in the Cold War, today's powers aim to dominate cyberspace (Willet M. , 2023). The United States and Russia have been involved in a serious and continuous digital rivalry. Both countries are considered top global powers, and their cyber power is also strong. For the past twenty years, they have participated in cyber conflicts by attacking government, companies and critical infrastructure systems. It's not only about getting information or causing quick harm; these attacks also aim for future strategies, international clout and control online (Greenberg, 2019). The main aim in today's cyber wars is disrupting the global financial system. Banks, stock markets, online payments, payment networks and financial institutions play a part in the system that moves money around the globe. These days, most areas of the financial system rely heavily on the internet. That means trading can take place efficiently, but it also leaves it at risk. An attack on a bank or payment system can heavily disrupt the lives of many and negatively impact on the world's economies For this reason, cyber conflicts and financial stability go hand in hand. Competition between the U.S. and Russia in cyberspace tends to cover financial systems. State-sponsored cyberattacks have been used against U.S. financial institutions in the hopes of taking data, creating problems or delivering messages. These activities have the power to cost billions, damage people's faith in the system and put world trade in danger. During 2017, an attack named NotPetya was connected to Russian hackers and caused global financial damage. More than $10 billion in losses were caused to Maersk and FedEx by the hurricane. In the same way, the SolarWinds incident in 2020 let hackers (who seemed linked to Russian intelligence) penetrate U.S. government and company networks for a long time without being noticed (Willett, 2024). Cyberattacks on financial systems can harm the whole world, as the financial world is now global. A lack of faith in a financial institution society could lead to excessive worry, drops in the financial markets and economic losses. Due to these reasons, cyber-attacks from nations like the U.S. and Russia can affect the whole world.

## Historical Context of U.S.–Russia Cyber Rivalry

The cyber competition between the United States and Russia began several years ago and has kept adjusting to new developments. The start of the digital contest came during the Cold War era thanks to the constant investment of both superpowers in spying and signal techniques. While the analog background for cyber wars ended in the 2000s, more recently countries have shifted to conducting covert attacks online (Lewis, 2022). In 2007, Estonia was hit by a series of cyberattacks that experts linked to groups tied to the Russian government. As a result, Estonia lost the functionality of its banks, government and media sites which then became a blueprint for political coercion using cyber tactics. Similar cyber-attacks were recorded during the Russo-Georgian war in 2008 making it clear that cyber techniques could back up physical fighting (Connell, 2017). During the next years, Russia became more aggressive and advanced in its use of cyber tools. Attacking Ukraine with Black Energy and carrying out wide misinformation campaigns in NATO and EU countries demonstrated a new way of cyber-attack. It was after several hacking attempts which peaked with accusations of involvement in the 2016 U.S. election, that Americans began seriously considering Russian cyber abilities. They built the digital area into a key aspect of interactions between the United States and Russia and provided the basis for the lasting rivalry in place now. Many other noteworthy cases present cyber weapons, being systematically used in international affairs. Around 2010, the Stuxnet worm was identified, and it was not revealed by who, although the U.S. and Israel reportedly produced it to disable Iranian nuclear centrifuges. This was the first time any malware is recognized for causing physical harm (Zetter, 2014). Its result successfully showed that cyber tools can be used as offensive weapons which changed the Russian cyber policy and brought awareness to other nations about a new threat (Hassan, 2024) According to reports, Russian spy groups have entered Microsoft's email system and compromised accounts belonging to government agencies and businesses. The hack made many people concerned again about the possibility that important systems could remain open to attacks and that state-sponsored actors might keep spying for a long time. According to intelligence reports, Russian-connected actors have tried to use or possibly disrupt the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network in the last few years. These attacks are extremely risky because SWIFT handles a large share of transactions across borders. With global trade and banking at risk, even a small outage could disrupt the affairs of billions across the globe. Cyber-attacks of this nature demonstrate that modern cyber operations are more than just for spying or causing disruption; they are also designed to signal power, change how adversaries behave and help form new global rules.

## A Comparison of Two Approaches: Realism vs. Liberalism in Cybersecurity

Although Realism provides us with a clear view of why the U.S. and Russia are cyber enemies. Liberalism suggests that working together, building institutions and understanding that countries depend on one another is important for improving relations (Joseph, 2017). For Liberals, states should collaborate to deal with challenges that affect them all. Because of shared risks and how much online businesses work together, there are strong reasons for players in cyberspace to cooperate. By way of example, the 2015 agreement on cybersecurity between the U.S. and China caused a significant cutback in economic cyber espionage, implying that diplomacy is achievable between even the most competitive nations. At the same time, US–Russia relations add complexity to this picture. The ongoing challenges with dialogue, thin trust and conflicting beliefs about cyberspace prevent useful cooperation. Although Liberalism promotes the United Nations, the Tallinn Manual and similar structures, Realism points out that without concrete enforcement, these rules frequently break down. As a result, combining different forms of analysis is probably most realistic appreciating both diplomatic engagement and inter-institutional cooperation while also recognizing the ongoing impact of power politics, mistrust and deterrence on cyber behavior (Haizler, 2017).

## Proxy Warfare and Non-State Actors in Cyberspace

One aspect that makes cyber conflict especially difficult is the large number of non-government groups, like gangs, hacker networks and private personnel employed by states to carry out actions while hiding their involvement. There are frequent claims that Russia supports a community of cyber proxies. Fancy Bear (APT28) and Cozy Bear (APT29), groups related to the Russian government, carry out attacks according to the country's objectives unrelated with official law (Mearshiemer, 2001). There are occasions when Russian-spawned cybergroups do illegal cyberattacks to collect money, but their actions might be overlooked or praised since such actions are useful to Russia's government goals (Kirsch, 2011). Thanks to the proxy model, states can prevent direct detection, experiment with different tactics and respond to escalating or reducing tension within a conflict. The 2021 Colonial Pipeline attack was caused by Darkside, believed to be based in Russia and its consequences greatly affected both geopolitical and economic factors. Although Kremlin officials denied any roles, the event showed that tolerated individuals may still have large effects on foreign policy. The combination of crime and strategy in these threats is new and tough to spot, is often unclear under the laws and can greatly affect both world security and the global economy.

## A look at International Relations using the Realist perspective

No area in IR theory offers a better explanation of current cyber conflict between the United States and Russia than Realism (Mearshiemer, 2001). In realism, the idea that states are not subject to higher power foreign affairs is true. Consequently, countries find themselves in a situation where they need to depend on what they can do to defend themselves and what they care about. In such a situation, gaining power becomes the main aim and it is thought that rivalry among countries is sure to happen and cannot be stopped. Although early Realism mainly considered a country's weapons and borders, its beliefs concerning security are also relevant today in cybersecurity. (Gady, 2010). Realism gives us insight into why the U.S. and Russia behave the way they do in their cyber conflicts. In cyberspace, countries fight for power and strive to protect their national independence. Russia and the U.S. regard cyber technologies as a way to gain information, shape global events and create disruptions to enemies without the need for open warfare. With no worldwide authority to control cyber activity, these states depend on themselves to improve their cyber security and attack if such measures prove required. The idea here is that since the system is without authority, nations are mainly driven by self-interest and do not put full trust in one another. One can easily see the influence of the security dilemma, a main idea from Realism, in cyber scenarios. Growing cyber infrastructure in one country leads to another country to increase its cyber capabilities. Because of this, countries regularly spend money on new cyber systems to stop their opponents from overtaking them. One example is that when the U.S. works to improve their cybersecurity, Russia considers it an attack and raises their own digital capabilities. Like the classic arms race, this process begins with a lack of trust and ends with drama and larger online attacks. (Kirsch, 2011). According to this school of thought, why financial systems are a top choice for cyber attackers. Damaging a country's economic structure in today's world can affect their power abroad. The Not Petya attack in 2017 and the SolarWinds hack in 2020 demonstrate that cyberweapons are now being used to harm opponents both economically and in matters of policy. According to Realists such behaviors are carefully designed to help a country gain an edge, protect itself, show strength and adapt to a new warfare style. Additionally, since the rules of cyber activities are vague and there is no strong enforcement system, Realist assumptions become strengthened. Because a global organization cannot guarantee tough action against cyberattacks, the U.S. and Russia are able to act largely unchecked. Because of this area of uncertainty, countries can challenge each other in cyberspace without risking war. Realism believes that this is the right response since states must look after their own security and do not count on cooperation from others. (Khan, 2018). This conflict between the U.S. and Russia is well explained by Realist theory. Two powerful countries, operating in an unregulated internet space, are both trying to dominate the situation to make sure they dictate security and influence. Cyber conflicts are just a newer way for countries to compete in world affairs and Realism shows us why and how they keep increasing, mainly when global finances are at risk. Competing technology in the digital sphere is now driving a crucial shift in world conflict between the United States and Russia. Back then, armies determined wars by force; but today, the strongest countries depend on digital approaches and use cyberattacks, spying and disruptions. Unlike earlier times, the goal here is to gain an edge over time, extend global influence and win control over digital technologies, not just gather data or briefly derail actions. Since most parts of the world's financial system now depend on digital systems, the competition between the US and China has grown much greater. In today's world, cyberattacks are able to create economic problems, lower public confidence and risk upsetting markets worldwide (Sullivan, 2015)

## Research Questions

To analyze this phenomenon, this article applies the theory of Realism in International Relations (IR), focusing on two core research questions:

1. How does the cyber rivalry between the U.S and Russia serve as a deterrence strategy in global power politics?
2. In what ways have state-sponsored cyber operations between the U.S. and Russia undermined trust in global financial institutions?

## Theoretical Framework: Realism and Cyber Conflict

IR realists assume the international realm is anarchy, meaning no authority is in charge of nations. Most states are driven by their own needs and concentrate on growing stronger and more protected in the absence of universal help. Cyber strategies are power tools, just as military and territory were before, so the traditional ways of realism make sense in the digital age too. Primarily, realist thinking looks at cyber conflict in terms of:

The lack of worldwide rule in cyberspace reflects the anarchic system countries see in the world, so countries must look after their security by themselves. States aim to increase their power-now including online power-to remain safe and shape decisions. Because each country sees others improved cyber security as a threat, a race to build up cyber weapons begins. Since there are no strong international rules, countries rely on their own actions and resources to defend themselves in cyberspace.

## Cyber Rivalry as a Tool in International Contests

### *Realist Analysis of Cyber Deterrence*

Realists believe that deterrence means threatening our opponents with a firm response if they take actions we don't consent to (Nye, 2017). Today, trying to deter attacks through offensive actions in cyberspace is a growing competition between the U.S. and Russia.

Key points include:

- ➢ Denial-based deterrence is the primary approach in the US, to stop an attack before it happens; nevertheless, attacks in cyberspace are more commonly answered through retaliatory attacks.
- ➢ Either nation displays its cyber skills in different ways, using publications or leaks to signal (each other and possibly third parties) what they could do next.
- ➢ The military now concentrates on keeping the adversary away by continuously defending American networks, according to realist policy strategies aimed at blocking threats in advance. (Zarate, 2015)

Only by showing offensive cyber actions will the nation receive a strong deterrent impact. When nuclear weapons are combined with other means of national power, they usually become more powerful than their parts working on their own.

### *Security Dilemma and Digital Weapons Buildup*

The cyber competition scenario clearly shows what's meant by the security dilemma within realism. If the U.S. increases its cybersecurity or creates a new weapon, Russia interprets it as a threat and builds its own new cyber weapons138. This competition has many fewer limits and proceeds at a faster rate than what we would see in traditional military expansion.

### *State Interests and the Disorder in Cyberspace*

Because there are few international rules in cyber space, realist concepts remain valid. So, states depend on their own cyber power, not international law or cooperation, to make themselves secure. The approach to cyber deterrence by the U.S. and Russia is clearly self-help in nature.

## Breaking the Trust in Worldwide Financial Organizations

### *Destroying Financial Systems as Part of the Plan*

According to realists, the economy is a key support for a nation's overall power. So, financial systems are main priorities when cyber-attacks occur. Damage to an opposing country's financial system can hinder its ability to do business internationally, disrupt its economy and send a strong international statement (Sanger, 2021)

Notable incidents are:

- Many cyber security experts linked Not Petya (2017) to Russian actors, unwittingly costing companies over $10 billion and leading to Sing disorder in companies like Maersk and FedEx, as well as in the global supply chain.
- In 2020, hackers believed to be linked to Russia entered U.S. government and private networks, resulting in a data breach and lowering trust in cybersecurity2.
- Colonial Pipeline Attack (2021): The perpetrators of this ransomware attack were criminal groups associated with Russia, causing major disruption to fuel supplies on the U.S. East Coast, showing how at-risk critical infrastructure is from state-tolerated cybercrime.

### *Factors Harmful to Trust*

- By attacking banks, payment networks and financial exchanges, cyberattacks can cause banks to suspend their transactions, stop moving funds and disrupt trade globally.
- Cyber Espionage: Because organizations like APT28 and APT29 mainly rely on phishing and malware, the integrity of financial institutions' security is often at risk.
- Through actions involving the financial system, countries can artificially cause problems, control markets and lower global faith in the financial system.

## Global Consequences

Attacks on any part of the global financial system can harm other countries, causing market chaos, chopping confidence among investors and making the economy unpredictable. The lack of trust in financial institutions can jeopardize the condition of the world economy (Polyakova, 2018). These cyber-attacks are not simply random–they show that the attackers intend to gain power, weaken their opponents and prove what they can do, all without crossing the threshold for real warfare. Since the world lacks strong enforcement systems to ensure compliance, countries often resolve their issues on their own, sometimes using groups they deny responsibility for or what are known as "proxies." Due to legal and technical ambiguity, both countries are able to use cyberspace for actions considered acts of war elsewhere, but not meeting the traditional definition of war.

## Realism and What Lies Ahead for Cyber Conflict

An example that realism is still important in international relations is the US–Russia rivalry in cyberspace. Because the internet environment is so unregulated, every state can use cyber tactics to further its ambitions. This effort targets the financial system which is the main element of a nation's power (Marcus, 2023)

Key realist insights:

- The digital arms race is a natural outgrowth of the anarchic international system.
- Deterrence in cyberspace relies on credible threats, demonstrations of capability, and the willingness to act.
- Living organizations attack financial systems as a strategic way to decrease their rivals' power and reputation worldwide.
- Because there isn't strong global leadership in cyberspace, instability and escalation continue.

## Discussion and Analysis

The cyber challenge between the United States and Russia in recent years is one of the most important aspects affecting the world's present-day relations and means of protection. Thinking about Realism, this rivalry shows countries trying to become powerful and stay safe in a world that lacks authorities and where each nation is expected to rely on itself and its tactics to ensure security. This long-standing problem now occurs online as both the U.S. and Russia use complicated digital techniques to monitor rivals, weaken them and rise above the others in technology. The back-and-forth between these two nations trying to secure an edge in a digital security battle has led to many having the same technologies. When one side makes its security stronger or creates new offensive tools, the other side is made hesitant because of this, so they become more secure and perhaps create similar offensive capabilities as well. In other words, it follows the same pattern as traditional arms races happening in the world of cyber which is not governed by basic international rules or enforcement steps. (Billo, 2004). Among the key points in this competition is the grave effect on global monetary safety. At both national and international levels, the core of the modern economy is being targeted almost exclusively by cyber criminals. Nowadays, because things in finance overlap, an assault on any part of the system could quickly spread worldwide, harm markets, undermine people's faith in institutions and create problems for an area's economy. The country-wide damage of the 2017 Not Petya attack which targeted Ukraine and the SolarWinds breach alongside it which affected several countries, demonstrates just how far cyberattacks from Russia are able to affect both countries. If we follow Realist thinking, these attacks should not be considered only as vandalism, as real motives of these events are to hurt opponents and seek personal or national advantage apart from engaging in major fights. There are economic, political and moral results from an attack on a financial regime such as hurting an opponent's economy, showing off the power of a state in politics and lowering trust in the world's financial markets. Besides using other tactics, states may undertake cyber operations to achieve their economic ends. (Gady, 2010). But since countries deal with cyberspace differently, the competition becomes more complicated. While Russia pays special attention to cyber weapons, viewing them as major first strike weapons and emphasizing control over them, America stresses keeping the internet open, secure and ensures it can be used with other countries, identifying government's role from that of hackers. Such differences in ideas make people suspicious of each other and slow any agreement on how countries must act after being attacked in cyberspace. So, they engage in a constant state of uncertainty, each using proxies and claiming ignorance to reach their goals without facing an open war. However, this rivalry does not stay limited to those who take part in it. Outdated systems are now more likely to face sophisticated and repeated cyberattacks which challenge financial stability everywhere. The success or failure of one nation's banking system can set off panic in other countries, raising the likelihood of market shocks and upsetting the economies of millions worldwide. Concerns over potential cyberattacks and even more so those that might hit critical financial services, are seen as crucial in risk analysis and shape investment, country laws and diplomacy. Both countries hope that by making it clear cyber threats will cost attackers more than they are worth, they can discourage these attacks. It means you have to defend, yet show you are prepared to fight in return if the need arises. While cyber deterrence appears to function, it may not be completely reliable, because figuring out who carried out a cyberattack is challenging and because the rules for defining cyber warfare are unclear. There is always a chance that a situation might get out of hand, giving every meeting extra risk of leading to conflict (Khan, 2018). The contest between the U.S. and Russia in cyberspace is most likely to become a lasting security and financial stability challenge in coming years. Realism tells us that while the world is mainly state-to-state and states depend on their from-to cycle, cyber competition will likely continue and perhaps intensify. Given how strategically significant cyber abilities are to states and how mistrustful they are of their competitors, getting agreements, being more transparent and encouraging collaboration is necessary but very tough. In truth, the U.S.–Russia conflict in cyberspace follows the same strategy that traditional geopolitics has used. It brings serious effects to financial security everywhere and can destabilize markets, weaken big organizations and ruin the faith of citizens all over the world. Managing the risks requires governments to develop very strong defenses, reliable deterrence and a reliable promise from all United Nations members not to use the weapons. So far, the digital arms race is making changes to economic and political matters, and it might bring unforeseen and dangerous results.

## Conclusion

The way the United States and Russia compete in cyberspace is a main characteristic of current international conflict issues. Since it uses a Realist understanding of international relations, this competition highlights that power politics happen today across the internet. Through cyber power, states are able exert pressure, gather information, disrupt others and weaken important financial networks, all with little risk. What we see here is not only an effort to outsmart each other technologically, but also a sign of the global system's overall organization. Because cyberspace lacks order, like the international system, states respond by building capacities that help them stay safe and gain power. So, the U.S. and Russia are using both techniques: denial and punishment, to make it clear that particular actions will not be tolerated. Because there are no clearly accepted rules in cyberspace, trust is hurt, and the possibility of an unintended escalation grows. Since it is difficult to know who is behind cyberattacks and crestfallen representatives of states are used, cyber activities often remain unclear and unstable. If enforceable regulations are missing, acts that should be considered acts of war in the physical world are still considered legal grey areas and are used by both states and non-state groups. It has become even more obvious in attacks aimed at our financial systems. In the Not Petya virus, the SolarWinds data breach and the Colonial Pipeline attack, Russian-connected cyberattacks repeatedly showed the weaknesses in our financial and economic system. What appears to be attacks on U.S. companies typically leads to much broader effects, revealing how closely tied worldwide financial institutions really are and what can happen following a government-backed cyber-raid. (Haizler, 2017). It is important to see these strikes as purposeful weapons employed in political affairs, realists tell us. They want to weaken competitors, demonstrate expertise in cyberspace and adjust the balance of opinion without needing to fight a direct war. In this situation, financial systems function both as economic tools and as a result, they become appealing targets in the world's cyber fight. Brilliance in cybersecurity measures is still lacking because cooperation between nations is shallow and dispersed. The absence of legally enforced cyber agreements or shared rules on the internet is still preventing collective action. Moreover, because Russia wishes for a sovereign internet while the U.S. calls for an open and interoperable internet, it becomes even harder to build unity. In the near future, it is probable that there will be continued and even greater tensions in cyber space between the U.S. and Russia. As we see more advanced attacks, the introduction of new systems including AI and quantum computing and our growing reliance on the internet in finance all highlight the growing challenge to cyberspace's security. With little effective deterrence and effective diplomacy, the chances for strategic mistakes or much larger economic disruption are very high. For this reason, nations should secure their digital infrastructure, think of new ways to deter cyber threats and look for common frameworks with likeminded partners regardless of how widely these frameworks are adopted. Developing trust, setting up ways to share responsibility for attacks and ensuring safe communication channels can keep cyber escalation at bay and manage emergency situations. Arms control was formed to address nuclear threats in the Cold War, and we now need the same approach to cybersecurity. All things considered, the cyber conflict between the

U.S. and Russia is a sign of the larger changes happening in world security. As a result, new obstacles to financial stability around the world, new patterns in international competition and a focus on the main ideas of Realism in modern politics have appeared. Because strong governance is lacking, the digital arms race will keep having an impact on the future of the world's politics and economies across many sectors.

## References

Billo, C. &. (2004). Cyber Warfare. An Analysis of the means and motivation of selected nation states. *Dartmouth, ISTS.*

Connell, M. &. (2017). *Russia's approach to cyber warfare.* Retrieved from CNA analysis and solutions: http:/www.cna.org/reports/2017/russia-approach-to-cyber-warfare

Gady, F. &. (2010). *Russia, the United Statesand cyber Diplomacy.* Eastwest Institute.

Haizler, O. (2017). The United States' Cyber warfare history: Implications on modern cyber operationall structures and policymaking. *Cyber, Intelligence and Security, 1*(1), 31-45.

Hassan, Z. H. (2024). Digital Warfare: The Evolution of US and Russian Cybersecurity Strategies. *Review of Education, Adminisration and Law, 7*(1), 335-349.

Khan, S. (2018). Implication of cyber warfare on the financial sector. An Exploratory study. *International Journal of Cyber-security and Digital Forensics, 7*(1), 31-38.

Kirsch, C. (2011). Science Fiction no more: Cyber Warfare and the United States. *Denv. J. Int'l L & Pol'y, 39*(4), 620.

Kirsch, C. (n.d.). Science fiction no more: Cyber warfare and the United States. *Denv,.*

Lewis, J. A. (2022). Cyber war and ukraine. *Centre for strategic and International strategies*.

Marcus, W. &. (2023). The cyber dimensions of Russia-Ukraine war. In *In W. Marcus & G.Austin (Eds.), The Cyber dimensions of Russia-Ukraine war* (pp. 7-26). Routledge.

Mearshiemer, J. (2001). *The tragedy of great power politics.* W.W. Norton & Company.

Nye, J. (2017). Deterrence and dissuasion in cyberspace. *International security, 41*(3), 44-71.

Nye, J. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44-71.

Polyakova, A. &. (2018). *The future of political warfare: Russia, the West, and the coming age of global digital competition*. Retrieved from Brooking Institutions: http://www.brrokings.edu/research/the-future-of-political-warfare/

Sanger, D. (2021, December 20). *The SolarWinds hack: The quest for answers*. Retrieved from The New York Times: http://www.nytimes.com

Sullivan, J. &. (2015). Cyber War and Strategic culture: The Russian Integration of cyber power into grand Strategy. *Strategic Studies Quarterly , 9*(1), 85-111.

Willet. (2023). "The Cyber dimension of the Russia-Ukraine war." Survival: October-November 2022. *Routledge*, 7-26.

Willett, M. (2024). The Cyber Dimensions of Russia-Ukraine War. *Adelphi Series*, *64*(511-513), 105-124.

Zarate, J. (2015). *The Cyber Financial Wars on the Horizon. Foundation for the Defence of Democracies*. Retrieved from http://www.fdd.org

Zetter, K. (2014). Countdown to zero day: stuxnet and the launch of the world's first digital weapon. *Crown*.