Journal of International Relations (JoS)
E-ISSN 2828-1667 Vol 1 No 1, Maret 2026
DOI PREFIKS 10.36232

The Implementation of Cybersecurity in United States Foreign Policy After the Russian Hack (2016–2020)

Dini Septyana Rahayu [1]*, Ibaadur Rahman Azzahidi [2]

[1] Universitas Darussalam Gontor, Indonesia
[2] Universitas Muhammadiyah Yogyakarta, Indonesia

Email Korespondensi: dinirahayu@unida.gontor.ac.id

Abstract
This paper aims to analyze the implementation of cyber security in US foreign policy as a response to Russian cyber threats from 2016 to 2020. The development of internet-based information technology is a new form of power for various countries, this includes ushering in a new era in defense policy development by utilizing cyber technology to support state progress and military modernization. The United States and Russia are two countries that are progressively developing cyber technology as their defense and security strategy. In this case, the two assume each other asrivals and threats. Thus, the development of cyber technology, one of them, was responded to as aform of threat to the security and defense of each country. To analyze, this study uses a descriptive qualitative research method to describe how cyber security is implemented in US foreign policy against Russian cyber crimes. The type of data used is secondary data obtained through data collection techniques of literature documentation. Using foreign policy and cyber security concepts, this research found that United States formulates Security Policy country through the Development of Defense (DoD) and US Cyber Command belonging in the American National Defense Agency (National Security Agency) as a means to improve national security defense to respond hacking attempts made by Russia against the United States government.
Keywords: ***Cybersecurity, Foreign Policy, United States, Russia***

Abstrak
Tulisan ini bertujuan untuk menganalisis implementasi keamanan siber dalam kebijakan luar negeri Amerika Serikat sebagai respons terhadap ancaman siber Rusia pada periode 2016 hingga 2020. Perkembangan teknologi informasi berbasis internet menjadi bentuk kekuatan baru bagi berbagai negara, termasuk dalam menghadirkan era baru dalam pengembangan kebijakan pertahanan dengan memanfaatkan teknologi siber guna mendukung kemajuan negara dan modernisasi militer. Amerika Serikat dan Rusia merupakan dua negara yang secara progresif mengembangkan teknologi siber sebagai bagian dari strategi pertahanan dan keamanan mereka. Dalam konteks ini, keduanya saling memandang sebagai rival dan ancaman. Oleh karena itu, pengembangan teknologi siber dipersepsikan sebagai bentuk ancaman terhadap keamanan dan pertahanan masing-masing negara. Untuk menganalisis hal tersebut, penelitian ini menggunakan metode penelitian kualitatif deskriptif guna menggambarkan bagaimana keamanan siber diimplementasikan dalam kebijakan luar negeri Amerika Serikat terhadap kejahatan siber Rusia. Jenis data yang digunakan adalah data sekunder yang diperoleh melalui teknik pengumpulan data berupa studi dokumentasi literatur. Dengan menggunakan konsep kebijakan luar negeri dan keamanan siber, penelitian ini menemukan bahwa Amerika Serikat merumuskan kebijakan keamanan negaranya melalui pengembangan Departemen Pertahanan (DoD) dan Komando Siber Amerika Serikat (US Cyber Command) yang berada di bawah Badan Keamanan Nasional Amerika (National Security Agency), sebagai sarana untuk meningkatkan pertahanan keamanan nasional dalam merespons upaya peretasan yang dilakukan Rusia terhadap pemerintah Amerika Serikat.
Kata kunci: Keamanan Siber, Kebijakan Luar Negeri, Amerika Serikat, Rusia

Journal of International Relations (JoS)
E-ISSN 2828-1667 Vol 1 No 1, Maret 2026
DOI PREFIKS 10.36232

Introduction

This paper aims to analyze the implementation of cyber security in US foreign policy as a response to Russian cyber threats from 2016 to 2020. The development of information technologyalso has implications for the development of issues and threats in the international structure. One of the implications felt by countries is the increasing popularity of using cyber technology in defense and security strategies. The existence of cyber technology is an alternative for the international system to guarantee the security of each actor, when military capabilities areconsidered insufficient to guarantee their security[1]. At a certain level, the existence of this technology automatically brings a new face in international security, which is marked by the emergence of non-traditional threats. The form of security required by countries is clearly also changing, not only about how to guarantee security in a military context but also about the importance of guaranteeing their cyber security from possible threats. In the military world, the term cybersecurity has been a part of defense and security practices for more than a decade. The term has also become popular in various contexts, including in the study of international relations[2]. Cybersecurity is part of the fluctuations in interactions between countries, the context is more in the development of new forms of threats andappropriate strategies to overcome them.

One form of threat to cyber security appears in the form of hacking that occurs in cyberspace, and is faced by local governments, companies, and citizens as well. The problem is that hacking, espionage or other cyber-attacks can be very damaging without causing death or destruction in the real world. This has become a new focus in national security and defense including the United States[3]. As a superpower that has many interests as well as opponents, the USis faced with the threat of cyber-attacks that have the potential to cause losses. Cyber warfare has become a threat that is as dangerous as the threat of physical war for the United States. Attacks launched through cyber space can paralyze vital infrastructure such as information systems, so that it can attack the government's credibility and ultimately threaten national sovereignty. The demand for cyber security has increased due to the threat of cyber

[1] Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and Cyber Defence: National Level Strategic Approach. *Automatika, Journal for Control, Measurement, Electronics, Computing and Communications*, 273- 286.
[2] Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. *International Security, 45*(1), 97–134.
[3] Rid, T. (2020). Cyber war and political warfare. *Journal of Strategic Studies, 43*(2), 245–267.

warfare. Therefore, state needs a securitypolicy in the field of cyber to protect the security and sovereignty of the state. America's Cyber Security Vulnerabilities began with events that occurred in 2013, America was shocked by the case of Edward Snowden, a former intelligence agent for his country, who leaked classified information belonging to the United States[4]. This problem was resolved by Barack Obama's policy that year on limiting the NSA's operations. However, these events heighten US sensitivity to cybercrime threats to US sovereignty and security. In 2016, the US again experienced cybersecurity problems, where US Intelligence suspected that there was an email hack carried out by the Russians. USIC believes that the hacking of emails aimed at US political institutions and organizations was carried out by Russia with the aim of interfering with US elections[5]. This event indirectly caused chaos again incyberspace security that Barack Obama had anticipated and coordinated well. At the same time, this problem also has implications for the future of US democracy which is actually threatened bythe existence of external entities. A study conducted by David P. Fidler assumes that during the administration of President Trump, cyber policies aimed at protecting US democracy, law and sovereignty were not a priority. This is evidenced by President Trump's initiative to establish betterdiplomatic relations with Russia (Fidler, 2016). Therefore, this research seeks to see how the implementation of policies related to US cyber security was in 2016, when President Trump was still in office until 2020. The US has a series of new cyber security policies that were issued afterthe hacking incident discovered by US Intelligence in 2016.

Research Method

This study uses qualitative research methods to present a picture of a social situation and explain why something happens, and in its method does not use numerical data as an analytical tool but rather words[6]. This method will be used to describe how cybersecurity elements are implemented in US foreign policy in the 2016-2020 period after the hack by the Russians. The data used in this study were collected through documentation data collection techniques. Related literature and

[4] Klimburg, A. (2020). The geopolitics of cybersecurity. *Strategic Studies Quarterly, 14*(1), 28–47.
[5] Ashford, E. (2020). The US response to Russian cyber operations: Lessons from 2016. *Journal of Cyber Policy, 5*(2), 189–205.
[6] Patton, M. Q., & Cochran, M. (2002). *A Guide to Using Qualitative Research Methodology.* London: Research Officer MSF.

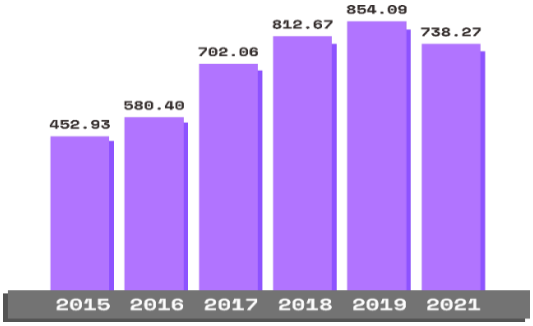
documents are US Intelligence press releases, websites, journals and scholarly articles related to US cybersecurity, reviews of Russian hacking of US elections, and literature related to US foreign policy.

Result and Discussion

US Security Network Vulnerability

The United States is a country with the highest level of technology use in the world and this is evidenced by the many giant IT companies that are there. This actually has implications forif there is a slight weakness in information technology security, it can trigger other security network vulnerabilities on various sides. This weakness allowed hackers to inject malware into US cybersecurity networks. Malware, stands for "malicious software", which refers to intrusive software. This software is developed by hackers, who are also categorized as cybercriminals, to steal data, damage or destroy computer systems[7]. Types of malware include computer viruses, trojans, spyware, ransomware, adware, worms, fileless malware, or hybrid attacks. Malware attacks have recently become more sophisticated with the advent of machine learning and targeted spear phishing emails. Triggered by a more sophisticated enemy, the spread of this modern threat is also more massive and causes more damage. The image below shows how the issue of malware is increasingly dominating information security and technology in the US[8].

Figure 1: increasing number of malware threats in the US[9]



[7] Cisco. (2022, December 20). *What is Malware?* Retrieved from Cisco: https://www.cisco.com/c/en/us/products/security/advanced-malware- protection/what-is-malware.html#~related-topics
[8] Lindsay, J. R. (2020). Cybersecurity and the problem of strategy. *Contemporary Security Policy, 41*(3), 321–344.
[9] Statistics, C. S. (2021, October 15). *Cyber Security Statistics*. Retrieved from Cyber Security Statistics: https://purplesec.us/resources/cyber-security-statistics/

The data on increasing malware threats is actually an indicator that US cyber security has experienced a significant weakening, even though Barack Obama's policies are considered effective in ensuring US cyber security. This network weakness is clearly a great opportunity for Russian hackers to find methods of hacking the US government's vital infrastructure. So it's no wonder that many reports coming from the United States government have been hacked by foreign parties, especially Russia and have continued to increase over the past year. The data on increasing malware threats is actually an indicator that US cyber security has experienced a significant weakening, even though Barack Obama's policies are considered effective in ensuring US cyber security. This network weakness is clearly a great opportunity for Russian hackers to find methodsof hacking the US government's vital infrastructure. So it's no wonder that many reports coming from the United States government have been hacked by foreign parties, especially Russia and have continued to increase over the past year. This weakening was also influenced by the low number of IT technicians in the US who understand that intrusion detection, hacking, including cyber attack mitigation are part of the skills they must have[10]. These facts point to US cybersecurity vulnerabilities, so it is not surprising that Russia managed to carry out a hack in 2016 that was considered to interfere with the US election process at that time.

The United States Election Information Hacking Case in 2016 and Department of Finance and Commerce hacks in 2020

The United States has a high level of vulnerability when it comes to cyber security. This can be proven by hacking aimed at the information and technology system of one of the US government agencies. In 2015, the FBI discovered a Russian hack into the Democratic National Commission's IT department, but after an inspection, nothing was found[11]. A series of hacking acts occurred within a year, right at a time when the US was in the general election. In March 2016, Hillary Clinton received phishing emails during her campaign, and this incident was reported by Hillary Clinton's campaigner, John Podesta. Hacking after hacking that occurred simultaneously on US government institutions, organizations, and even participantsin

[10] McDermott, R. (2021). Russia's cyber strategy and the evolving threat to the United States. *Parameters, 51*(2), 25–40.
[11] Research, C. E. (2022, October 20). *2016 Presidential Campaign Hacking Fast Facts* . Retrieved from CNN: https://edition.cnn.com/2016/12/26/us/2016- presidential-campaign-hacking-fast-facts/index.html

the US election throughout 2016 caused disruption to the US election process. This was identified as a Russian cyber crime against the US, and the US felt the need for resolution and prevention of similar crimes in the future. Rod Rosenstein, Deputy US Attorney General, reported that 12 Russians were indicted for hacking acts during 2016 that interfered with the conduct of elections in the US[12]. Thehacking triggered internal conflicts during the election period, because as a result of the hacking, some information related to election participants, presidential preferences, and other important information was leaked to the public. In 2020, The United States Department of Treasury and Commerce during the administration of President Donald Trump was hacked by foreign parties. The Trump administration has almost confirmed that Russian intelligence agencies were the actors behind the hack.

According to federal and private experts, the hacks breached key government networks, including those at the Departments of Finance and Commerce, and opened up free access to their e- mail systems[13]. In the span of 4 years the US has experienced several hacking acts carried out by external parties, and it has been proven that of all the hacking acts, Russia is the main actor. Based on the above data on the security vulnerabilities of US IT systems, it can be concluded that because the US is very vulnerable to cyber-attacks, it is easy for hackers to enter US cyber systems to obtain certain information or simply cause chaos to national security.This action is categorized as a cyber-attack by the US, and the US needs to review and even restructure cyber security policies. This is necessary to ensure IT security in the US domestic sphere, as well as a firm response to Russian threats in cyberspace.

United States Cybersecurity Policy

Against the backdrop of the increasing threat of cyber-attacks by Russia, the US feels the need to restructure and strengthen cyber security policies. Automatically, cyber security becomes the top priority of the US government, because a large vulnerability in cyberspace will increase the potential threat to the security and sovereignty of the country. During President Barack Obama's administration, the US

[12] Valeriano, B., & Maness, R. C. (2020). Cyber conflict and US–Russia relations in the digital age. *Journal of Strategic Studies, 43*(6–7), 1002–1024.
[13] Sanger, D. E. (2021, December 13). *Russian Hackers Broke Into Federal Agencies, U.S. OfficialsSuspect*. Retrieved from The New York Times: https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us- government- treasury-commerce.html

issued an international cyber security policy that not only served as protection for cyber security at the domestic level, but also as a foreign policy to respond to theincreasing threat of cyber attacks on international structures[14]. The US explained thatthe cyber security policy was not only part of domestic policy, but the US also emphasized that this policy was part of norms and foreign policy related to cyber security. President Barack Obama considers this policy important to overcome actions from the international environment that are detrimental to the US[15]. The existence of Russia as the actor behind the hacking thatis often experienced by US domestic institutions and agencies, is a disturbance to US democracy. Therefore, the US feels the need to emphasize its cyber strategy policies as part of international norms. This US foreign policy is a response to Russian crimes that violate international norms related to cybersecurity.

Following the hacking that occurred, this policy was then restructured during the administration of Donald Trump. This strategy was issued by the US to create interconnectednessbetween the US and all countries in the world in the context of cyber security. Apart from that, this policy is also a guide for the US in dealing with all the challenges of information technology security in the cyber world. Increasing competition with China and Russia is an indicator for creating changes in foreign policy, especially in the field of cybersecurity. Therefore, US restructured the Obama administration's cyber security policies through the US Department of Defense (*DoD*), by issuing The 2018 Department of Defense Cyber Strategy. This policy was also stated to replace the national cybersecurity policy issued by the US in 2015[16]. Cybersecurity priorities in the Donald Trump administration include:

1. Protecting the country's infrastructure and information systems from cyber threats
2. Improve the ability to identify and report incidents related to cybersecurity so that it can beresponded to in a timely manner
3. Call on the world to promote internet freedom and build support for open, easy-to-operate,secure, and reliable cyberspace.

[14] Borghard, E. D., & Lonergan, S. W. (2021). The logic of coercion in cyberspace. *Security Studies, 30*(2), 283–310.
[15] *ibid*
[16] Department of Defense. (2023). *Cyber strategy of the United States Department of Defense*. U.S. Department of Defense.

4. Securing central government networks by setting clear security targets and placinggovernment agencies responsible for meeting these targets Building cyber-strength and communicating via passwords in partnership with the privatesector[17].

Technically, the strategic steps that have been prepared by the Department of Defense (DoD)for cyber security are as follows:

1. Strategic Goal I, *Build and maintain ready forces and capabilities to conduct cyberspace operations*, To operate effectively in cyberspace, DoD requires the support of individual personnel and high standard trained soldiers. Therefore, DoD must invest heavily by providing training to soldiers and building an effective organization
2. Strategic Goal II : *Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions*, DoD must start identifying, prioritizing and maintaining the most important networks and data, so that it can carry out its mission objectives effectively. DoDalso needs to continue to develop technology so that it is more at the forefront of dealing with threats by increasing cyber defense capabilities
3. Strategic Goal III *: Be prepare to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyber-attacks of significant consequence*, DoD must cooperate with various partners, starting from the private sector, including forming alliances with other countries to prevent or disable cyber-attacks that have a significant impact on US interests.
4. Strategic Goal IV *: Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages*, DoD mustbuild cyber systems that are sustainable and integrated with the plans of related agencies, developing cyber capabilities to achieve national security goals.
5. Strategic Goal V *: Build and maintain robust international alliances*

[17] White House. (2023). *National cybersecurity strategy*. Executive Office of the President of the United States.

and partnerships to deter shared threats and increase international security and stability, DoD requirescollaboration with foreign allies and other partners. In engagement with the international cyber world, DoD must build cooperation capacity in cyber security and defense[18].

Cybersecurity in US Foreign Policy

The awareness to develop cyber security and prepare strategies in dealing with threats andchallenges in the digital world has long been recognized by the US. However, the intensity of developing cyber power is very visible in the policies of the US government from 2016 to 2020.

Table 1. U.S. International Strategy for Cyberspace[19]

No	Year	Documents	Agencies
1	2016	Department of State International Cyber Policy	US Department of Defense
2	2017	U.S International Strategy for Cyberspace	US Department of Defense
3	2017	National Security Strategy : Cyberspace	The White House
4	2018	National Security Strategy : Cyberspace	The White House
5	2019	The Cyber 9-Line	U.S Cyber Command
6	2020	Authority of the Intelligence Community to Collect Certain Intelligence Regarding United States Persons Held Captive Abroad	National Security Presidential Memorandum

The series of US policies listed in the table, which are closely related to Foreign Policy is "U. S International Strategy for Cyberspace". This strategy is a special formulation issued by the White House as the US international code of conduct in international cyber issues. The US really understands that the world still does not have clear regulations regarding cyber space. This situation was eventually exploited by

[18] *ibid*
[19] U.S. Department of Defense. (2023). *Cyber strategy of the United States Department of Defense*. U.S. Department of Defense.

several countries such as Russia to act arbitrarily in cyber space. One of the US foreign policies as well as a cyber security policy that is used to defend its cyber security from cyber-attacks, especially threats from Russia, namely, the United States Cyber Command (USCYBERCOM). This policy is realized through the establishment of a security institution as a military command that operates globally and fights against state enemies that damage United States cyber space (Warner, 2020). The reinforcement of this institution in 2020 is also inseparable from the various forms of cyber security policies described above. USCYBERCOM or United States Cyber Command is a sub-command of the US StrategicCommand created by the US Secretary of Defense in 2009, Robert Gates. The existence of this sub-command was specifically formed to complement the Department of Defense's strategic tasks in the military, intelligence and information technology fields. This sub-command also operates globally with its field of operations primarily in cyberspace, USCYBERCOM is tasked with directing, synchronizing, and organizing cyber defense and security strategy planning (Command, 2021). In other words, this institution is a US strategic institution that was formed specifically to secure and defend the US from cyber-crimes, including what Russia did in 2016 to 2020 through hacking. Since 2018, following the increasingly massive cyberattacks the US has received from Russia, USCYBERCOM has increasingly engaged in cybersecurity and defense missions. USCYBERCOM strengthens its vision and mission, implements cyber security policies that have been formulated by the Department of Defense and the White House, as a form of their firm and progressive action against enemies in cyberspace.

> *"Defending forward as close as possible to the origin of adversary activity extends our reach to expose adversaries' weaknesses, learn their intentions and capabilities, and counter attacks close to their origins. Continuous engagement imposes tactical friction and strategic costs on our adversaries, compelling them to shift resources to defense and reduce attacks. We will pursue attackers across networks and systems to render most malicious cyber and cyber-enabled activity inconsequential while achieving greater freedom of maneuver to counter and contest dangerous adversary activity before it impairs our national power"* [20].

[20] Command, U. C. (2021, December 12). *Our History*. Retrieved from U.S. Cyber Command: https://www.cybercom.mil/About/History/.

USCYBERCOM together with the NSA formed a small commission that specifically deals with Russian intervention in the US election process in 2018. This commission then continues to work together to secure the US from cyber threats coming from Russia. To secure the 2020 elections, USCYBERCOM and NSA jointly formed The Election Security Group(ESG), as a preventive measure against Russian hacks[21]. These actions are interpreted as the US response to Russia targeting US security through cyberspace by hacking the election process and hacking information on US government agencies, such as the Department of Treasury and Commerce. Therefore, this paper concludes that the US implements cybersecurity aspects in its foreign policy more intensively, because the hacking carried out by Russia has clearlyviolated state sovereignty even though it came from cyberspace.

Conclusion

Guarantees for the protection of information and freedom in cyberspace are sought by the US government, and are getting stronger after the hacking that repeatedly occurred during the USelection and during the administration of Donald Trump. The US policy in response to Russia is contained in more than one set of cybersecurity policies compiled by the US Department of Defense. The Russian hack prompted the US to restructure its cyber security defense strategy and policy. These two things are then collaborated on policies which also become a new strategic reference for USCYBERCOM. Cybersecurity for the US needs to be part of the focus ofinternational structures, so that even the national policies they make are emphasized in the systemas part of international norms. In this case, US foreign policy does not only show US actions against Russia, but in a more distant context this policy is US efforts to create new norms in the system regarding cyber security.

Referensi

Ashford, E. (2020). The US response to Russian cyber operations: Lessons from 2016. *Journal of Cyber Policy, 5*(2), 189–205.

Borghard, E. D., & Lonergan, S. W. (2021). The logic of coercion in cyberspace. *Security Studies, 30*(2), 283–310.

Buchanan, B. (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics.

[21] *Ibid*

International Security, 45(1), 97–134.

Cisco. (2022, December 20). *What is malware?* Retrieved from https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html

Command, U. C. (2021, December 12). *Our history*. Retrieved from https://www.cybercom.mil/About/History/

Department of Defense. (2023). *Cyber strategy of the United States Department of Defense*. U.S. Department of Defense.

Galinec, D., Možnik, D., & Guberina, B. (2017). Cybersecurity and cyber defence: National level strategic approach. *Automatika, Journal for Control, Measurement, Electronics, Computing and Communications*, 273–286.

Klimburg, A. (2020). The geopolitics of cybersecurity. *Strategic Studies Quarterly, 14*(1), 28–47.

Lindsay, J. R. (2020). Cybersecurity and the problem of strategy. *Contemporary Security Policy, 41*(3), 321–344.

McDermott, R. (2021). Russia's cyber strategy and the evolving threat to the United States. *Parameters, 51*(2), 25–40.

Patton, M. Q., & Cochran, M. (2002). *A guide to using qualitative research methodology*. London: Research Officer MSF.

Research, C. E. (2022, October 20). *2016 presidential campaign hacking fast facts*. Retrieved from https://edition.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html

Rid, T. (2020). Cyber war and political warfare. *Journal of Strategic Studies, 43*(2), 245–267.

Sanger, D. E. (2021, December 13). Russian hackers broke into federal agencies, U.S. officials suspect. *The New York Times*. Retrieved from https://www.nytimes.com/2020/12/13/us/politics/russian-hackers-us-government-treasury-commerce.html

Statistics, C. S. (2021, October 15). *Cyber security statistics*. Retrieved from https://purplesec.us/resources/cyber-security-statistics/

U.S. Department of Defense. (2023). *Cyber strategy of the United States Department of Defense*. U.S. Department of Defense.

Valeriano, B., & Maness, R. C. (2020). Cyber conflict and US–Russia relations in the digital age. *Journal of Strategic Studies, 43*(6–7), 1002–1024.

White House. (2023). *National cybersecurity strategy*. Executive Office of the President of the United States.