Journal of Social Political Sciences
JSPS
Vol. 1, No. 3, August, 2020

CYBERATTACKS AND DISINFORMATION CAMPAIGNS: LESSONS LEARNED FROM 2016 AND FOR 2020 U.S. PRESIDENTIAL ELECTION

Yudha Akbar Pally
Department of International Relations, Faculty of Social and Political Science
Universitas Nasional, Jakarta, Indonesia
[3]Email: yudhaakbar.pally@civitas.unas.ac.id

Abstract : Donald Trump's victory over Hillary Clinton in 2016 US Presidential Election is one of the most shocking political events of this decade. Various controversies and irregularities have been examined and led to alleged Russia's roles in the election results. Cyberattacks and disinformation campaigns run by Moscow and the weakness of US election security in preventing and mitigating such online intervention further confirm the failure of modern democracy in cyber and social media era. No one can guarantee that Russian cyberattacks and disinformation campaigns will not reoccur in US Presidential Election this year. The US preparedness and capability in dealing with election cyber threats will not only risk the legitimacy of US Presidency but also the sustainability of democracy to survive the today's information technology and social media advancement.

Keywords: cyberattack, disinformation campaign, social media, election security and democracy

Submission	:	May, 09th 2020
Revision	:	June 08th 2020
Publication	:	August 30th 2020

INTRODUCTION

The development of information technology has penetrated almost all aspects of modern human life. From simple things such as buying basic needs online, enjoying the flow of information that is fast and easy to grasp and even strategic matters such as influencing public policies to "intervening" in the process of changing political leadership. In the past, Government, as a result of a democratic election process, could dictate the change and information technology advancement to progress rapidly as it is now with policies and regulations flexibility. However, nowadays, the outcome of a democratic process can be influenced by information technology activism or misleading campaign. For example, in April 2018, the US Congress summoned Mark Zuckerberg, founder and CEO of Facebook, to attend the Congressional Hearing to clarify allegations of his company's role in Cambridge Analytica scandal. Facebook has reportedly provided access to around 87 million user data to be subject of political interests. The personal data exposed is used to influence political choices or election results. This scandal is not the first nor the last, there are many scandals of misappropriation of information technology used to intervene in election results. Russian hackers, for example, are accused of carrying out cyber-attacks and a disinformation campaign to disrupt 2016 US Presidential Election.

Many political researchers and even the US Intelligence Community such as The Central Intelligence Agency (CIA), The Federal Bureau of Investigation (FBI) and The National Security Agency (NSA) claimed Russia of being behind the surprising results of 2016 US Presidential Election. Russian agents are considered to have carried out a multipronged influence campaign through cyberattacks and disinformation campaigns with the aim of discrediting and delegitimizing the election results. They targeted Hillary Clinton, Democratic Presidential Candidate, and damaged her credibility and reputation and ultimately disrupted her electability and potential to become the 45th US President. Moreover, the ultimate goal is to undermine public confidence in US presidential election process and its result, US Presidency. It would also lead to lacks legitimacy so that in the end, a crisis of US public confidence in democracy will occur.

This multipronged influence effort with cyberattacks and disinformation campaign method began at least in 2014 when Russian hackers polarizing political perceptions through social media activism to display bias and mainstreaming sensitive issues such racial discrimination, immigration and Islamophobia as debated narratives in the election aiming to divide the unity of Americans. The campaign was carried out by fake social media accounts run by Russia's Internet Research Agency (IRA). After mastering the social media activism area, cyberattack targeted information technology infrastructure for US political institutions i.e. Democratic National Committee (DNC) and Democratic Congressional Campaign Committee (DCCC), through leaking of Hillary’s classified mails and documents. Although until now, no one has been able to prove that such information technology intervention and Russia's disinformation campaign against the 2016 presidential election had a direct impact on voter manipulation. Many argue that this intervention has significantly favored Presidential Election’s result, Donald Trump, as a leader of the second largest democracy in the world.

This article elaborates on some findings about the election, analyzes and examines the findings whether these cyber-attacks and disinformation campaign have discredited Hillary's reputation, influenced voters and ultimately helped Donald Trump to win the White House? And, has the US incapability to prevent and mitigate cyberattacks and disinformation campaign contributed to the controversial 2016 US Presidential Election result?

LITERATURE REVIEW

Cybersecurity has various definitions. The European Union defines cybersecurity as “safeguards and actions that can be used to protect cyber domain, both in civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure". This definition is in accordance with the reality that one of the barriers to be strengthened to mitigate cyber-attacks is to ensure that the barrier network and information infrastructure cannot be penetrated. Furthermore, in addition to these barriers, a comprehensive cybersecurity policy is also needed to analyze, prevent and mitigate all potential risks of cyber-attacks. US Policy Review, for that, also describes cybersecurity policy with a broader meaning where

> "Cybersecurity policy includes strategy, policy, and standards regarding the security of and operations in cyberspace, and encompasses the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure. The scope does not include other information and communications policy unrelated to national security or securing the infrastructure."

However, understanding cybersecurity is not easy, Maurer and Morgus as quoted in Nezir Akyesilmen's article underlines that

> "Threats in cyberspace are difficult to define as it is hard to identify the source of attacks and the motives that drive them, or even to foresee the course of an attack as it unfolds. The identification of cyber threats is further complicated by the difficulty in defining the boundaries between national, international, public and private interests and actors. Because threats in cyberspace are global in nature and involve rapid technological developments, the struggle to meet them is ever-changing and increasingly complicated. It requires high-level training, an advanced legal framework, effective organizational co-operation and the allocation of considerable resources."

Whereas several types of cyberattacks on election process, essentially in the case of Russian intervention in 2016 US Presidential Election, may include 5 types of information technology intervention, namely: (1) Infrastructure exploitation is a form of intervention by conducting surveillance, collecting and modifying data or functions of information technology systems or networks; (2) Strategic Publication is intervention in the form of releasing illegally obtained data. The data is usually gained through Infrastructure Exploitation intervention. It is aimed at discrediting a candidate by humiliating or exposing negative attitude of the candidate; (3) False-Front Engagement is intervention with the aim of communicating or even provoking a certain issue through interaction with other people using a false identity; (4) Sentiment Amplification is an intervention to increase the spread of certain sentiments as desired, either openly where the actor is clearly identified or covertly, and where the actor is deliberately obscured or exposed by false-front engagement with a false identity; and (5) Fabricated content is intervention in the form of disseminating written or broadcast untrue and misleading information of a candidate or a result of an election.

Disinformation campaign in election is the spread of false information to the detriment of a candidate, group, institution or the election process itself. Disinformation is not a new trick of manipulation. Sharing fake and misleading content is an ancient political tactic. However, what distinguishes it now is that the methods and media used are increasingly sophisticated through social media. The use of social media is aimed at reaching a larger audience so that the impact of disinformation campaign will be more massive.

Furthermore, cyberattacks and disinformation campaigns can be carried out by many parties and often even performed by certain regimes against candidate targets or elections in a country that is opposite to the campaign-host regime. There are at least three models of regime or state involvement in cyberattacks, namely (a) *State-Directed* where the campaign has been approved by state officials, who act in their capacity as a government representative or government leader; (b) *State-Encouraged* where the campaign is not ordered or given a direct signal by a state official, but also does not receive opposition from and is even considered favorable by the state; and, (c) *State-Aligned* where the campaign conducted by certain individuals or entities with the aim of supporting certain regime's goals.

METHOD

The research elaborated in this article applied a qualitative approach with descriptive analysis to answer aforementioned research questions. In addition, secondary data-based findings were sourced from relevant documents such as books, journals, reports, magazine articles and reviews, which were then evaluated and analyzed to examine the answers to the research questions.

DISCUSSION

These cyberattacks and disinformation campaigns were firstly echoed on 14 June 2016 when DNC reported hacking of their computer network and blamed Russian hackers for the hacking. After this incident, several cyberattacks were also frequently targeted at the Democratic Party. Wikileaks also published nearly 20,000 emails and 8,000 attachments belonging to several top DNC officials on 22 July 2016. Not only that, hackers continued to leak a large amount of sensitive campaign information in the days leading up to the US presidential election on 7 November 2016.

A hacker named Guccifer 2.0 claimed responsible for the hack. Crowdstrike, a US cyber security company immediately analyzed Guccifer's cyberattacks and released a preliminary report revealing the fact that on 22 July 2016, three days before the Democratic National Convention began, WikiLeaks published "part one" of the "New Hillary Leaks Series". The first part consisted of 19,252 emails and 8,034 attachments from senior DNC officials. The e-mails were distributed from January 2015 to May 2016 and contained a number of important conversations. For example, one email correspondence about a discussion of campaign strategy to undermine the reputation and integrity of Senator Bernie Sanders, Hillary's main contender in the Democratic Presidential Candidate nomination. The e-mails also exposed personal information to Hillary's campaign donors including addresses, credit card numbers, and even some passport and social security numbers. In addition, on 6 October 2016, DCLeaks published a leaked email belonging to Capricia Marshall. Capricia is former U.S Chief Protocol under President Barack Obama and senior advisor to Hillary's campaign team. The email leaked sensitive information about the campaign strategy, especially the media strategy and network enhancement.

The sequence of emerging cyberattacks, and disinformation campaigns reinforced the signals that there were parties orchestrating to target the credibility of Hillary's candidacy. This signal is strengthened by a report issued by US Intelligence Community publicly disclosing the results of their intelligence work on 7 October 2016 confirming their belief that the Russian Government was behind the cyberattack against DNC. The Intelligence Community's findings have triggered a comprehensive series of assessments with similar results and ultimately upset President Barack Obama who then on 28 December 2016 issued an Executive Order aimed at punishing Russia for their cyberattacks. The US government blocked five Russian entities and four Russian individuals from their involvement in businesses in the US and confiscated all their existing assets throughout US. Not only that, President Obama also instructed US State Department to "expel" thirty-five Russian diplomats with the label of "persona non grata" and close two Russian complexes on US territory. President Barack Obama believes that Russia used the two complexes as a hotbed for Russian intelligence activities.

Russia was furious and publicly condemned the sanctions and has insisted the complex should only be used as a vacation home for their diplomats. Russia argues the sanction is provocative and imposed just three weeks before President Obama left office, where they believe that a president who will leave office should not adopt a policy that damages bilateral relations between the two countries. Furthermore, Russian President Vladimir Putin's spokesperson stated that the Executive Order is nothing but a function of "a deal a blow on the foreign policy plans of the incoming administration." And, Russia is not responsible for any alleged cyberattacks and has promised to avenge against the US retaliation measures.

The US accusation that Russia had a hand in the cyberattacks and disinformation campaign seems plausible. Since the Cold War, Russia has often carried out intelligence operations targeting US elections, but this has only been limited to gathering foreign intelligence data. For decades, Russian and Soviet intelligence services have sought to gather insider information in US political parties that could help Russian leaders understand the plans and priorities of the US administration's new policies. In the mid-1970s, for example, *Komitet Gosudarstvennoy Bezopasnosti* (KGB), the Soviet Union's intelligence agency, recruited a Democratic Party activist who leaked information about the campaign and foreign policy plans of Jimmy Carter, who was the Democratic Party's presidential candidate.

Furthermore, in January 2017, the US Intelligence Community issued a joint report, attributing Russia's efforts to undermine the 2016 presidential election, although the report does not make an assessment of the impact of Russian activities on 2016 election results. In the summer of 2018, Special Counsel for the US Department of Justice, Robert Mueller, charged 12 GRU officials with hacking into the DCCC and DNC networks, and releasing documents and emails in an attempt to interfere with US presidential election. In this regard, media coverage initially focused primarily on leaked e-mail content after the DNC hack, particularly on DNC's preference for Hillary Clinton over rival Senator Bernie Sanders. In the run-up to the elections, the discourse on cyberattacks is increasingly being framed by the disinformation campaign machine as a national security issue, although media responses vary depending on political trends. The US right-wing media tends to deny or question the effects of hacking, while the left-wing media claims it is an attack on US democracy and institutions.

They further assess that Russian intelligence services have carried out intelligence work to establish the narrative war against US influential agencies such as think tanks and lobby groups which they consider having the ability to determine the direction of US future policies. The US Intelligence Community believes that the GRU uses the persona of Guccifer 2.0, DCLeaks.com, and WikiLeaks to release classified US data obtained in cyber operations and then publicly and exclusively to media outlets. Guccifer 2.0 covers his identity by claiming to be an independent Romanian hacker and making false claims about their Russian identity. Media reporting indicates more than one person has identified themselves as Guccifer 2.0. Furthermore, the US Intelligence Community claims that Guccifer 2.0 conveyed narrative obtained DNC and senior Democrat officials to WikiLeaks. WikiLeaks is used as a funnel for information leakage due to its reputation for the authenticity of its reports. The US public is considered to have a high degree of trust in WikiLeaks’ information. To link WikiLeaks' ties to this disinformation campaign, the US Intelligence Community states that RT (formerly Russia Today) chief editor visited WikiLeaks founder, Julian Assange, at Ecuadorian Embassy in London in August 2013, where they discussed renewing his broadcast contract with RT. Russian media later announced that RT had become "the only Russian media company" partnered with WikiLeaks and had received access to "a new leak of classified information." RT routinely provides a "pulpit" for Assange to attack the US with his leaked data.

The prolonged orchestra of cyberattacks and disinformation campaign has proven their results. In November 2016, 139 million Americans elected their president under the shadow of Russia's cyber operations and massive disinformation campaign designed to undermine the confidence of Americans in their democracy. Russia is spreading disinformation to American voters through YouTube videos, tweets and Facebook posts viewed by an estimated 126 million people on the Facebook platform alone. Russia also targets cyberattacks and a disinformation campaign of at least 21 states and seeks to infiltrate networks of voting infrastructure vendors and political parties. An unprecedented and successful information technology intervention exposing serious national security vulnerabilities in US election infrastructure.

DISCUSSION

As the US is currently preparing to convene 2020 presidential election. US might be very well prepared so that Russian cyberattacks and disinformation campaign in 2016 will not reoccur. In 2016, Russia had unprecedented opportunity and resources to carry out their intervention. The IRA activities, a troll distribution center based in St. Petersburg founded by Kremlin to spread disinformation during US elections, cost an estimated $ 1.25 million a month. It is just a cheap price for a cyber coup against another country. It is non-comparable to the election of a US president who "appears to be pro-Russia," a shocking and embarrassing defeat for Hillary Clinton, and, most importantly, an opportunity to expose US democracy as a dysfunctional old value. To make things even worse, US democratic infrastructure is unprepared and unresponsive to Russian cyber operation risks and seems incapable of mitigating such cyber incidents. The US has failed.

After four years, the emerging world problems and re-focusing of national interests have made the 2016 cyber tricks seem unworkable. The COVID-19 pandemic has required tremendous resources of all countries, including Russia, and decreasing oil prices have also hit the Russian economy. As a result, the level of domestic popularity of President Vladimir Putin has dropped dramatically. In the past, Russian presidents have taken foreign policy "dividends", namely the 2014 invasion of Crimea and years of intervention in Syria, to maintain political support at home. Now, Russian economy tends to be stagnant, the majority of Russians want their government to carefully focus on economic and domestic issues. Foreign policy activism is seen unattractive. In addition to domestic obstacles, if Russia still insists on intervening in the US presidential election this year, Moscow will need to work harder to manipulate US voters especially where social media companies are also becoming more aggressive in protecting their platforms by removing fake networks of accounts and bots. They have even dared to go head-to-head with the state in order to maintain the integrity of their platforms.

Social media companies have actually attempted to create policies to respond to disinformation campaign challenges. For instance, Twitter has banned all political advertising including limiting the visibility of some of Trump's tweets for violating his policy of abusive posts and behavior. Nonetheless, US First Amendment guarantees freedom of speech adding another set of complexities where social media company is often confronted with freedom of speech and access to information requirements.

Meanwhile, Google is fully committed to privacy of its users. Google always strives to comply with the applicable data protection laws where they operate. Apart from having qualified technical expertise and a well-trained cybersecurity team, Google cybersecurity system is also assessed by an independent auditor. Meanwhile, Facebook views that false news will damage trust and hinders flow of accurate information. Therefore, Facebook applies several strategies to combat disinformation campaigns including users-supported false news identification, third-party fact checking mechanism, strict policy enforcement of ads on buying to prevent false news posts, fraud and inauthentic spam accounts response and sustainable updated fake accounts detection capability.

Having learned that AS remains incapable of preventing and mitigating Russian cyberattacks and disinformation campaign, US needs to develop election cybersecurity initiatives and strategies covering, among others, identification and assessment of election cyber security risks which can provide a complete picture of US election cyber security capabilities and weaknesses. Then, the White House and Capitol Hill need to compromise to create a set of principles or norms and a national action plan based on the election cybersecurity risk assessment. US Government should also create an agency that specifically handles election cybersecurity and has authority to collect and manage cyber resources both nationally and internationally. It also needs to own expertise in establishing relationships with global cyber actors due to transnational and borderless nature of cyberspace. This agency should work in a high level of agility in order to manage complexity of election cyber threats in the most effective and efficient way considering that cyberattacks can occur in a fast, consecutive and massive fashion. It should also perform lobbying capabilities to convince stakeholders, such as the police, military, foreign ministry, defense ministry and other relevant counterparts, and gain their buy-in in the design and execution of election cybersecurity policies.

Technically speaking, U.S. Congress, in its report entitled Congressional Task Force on Election Security: Final Report, released in 2018, explained their findings and warned the Government to carry out strategies on how US should make self-improvement. The Report elaborates the need for (1) US intelligence community to carry out Pre-Election Threat Assessments before the actual elections are held; (2) Federal fund is prepared to replace outdated voting machines and rejuvenate IT infrastructure, including the sophisticated voter registration database system; (3) each state conducts post-election audits; (4) parties or vendors shall have capability to secure the voting system and collaborate with local officials to create a response system when a cyberattack occurs; (5) Federal Government develops a National Strategy and cybersecurity reforms to tackle cyberattacks and weaken attempts against US democratic institutions, including increased cybersecurity training; (6) making election infrastructure a critical infrastructure so that the security system and resource support are improved; (7) create and improve the capabilities of Channels for Sharing Threat and Intelligence Information with Election Officials.

Apart from increasing cyber capacity at home, US must end its isolationism approach. US should lead international collaborations to intensify global cyber cooperation. Facts on the ground show that not all countries have adequate cyber capabilities and shared cybersecurity-based national interests. It unfortunately results in the lack of quality of international collaboration. Pre-existing suspicion over the intended use of cyber capabilities has also contributed to the reluctance of international cooperation enhancement. Most countries are more inward-looking, nationalist and protective and see “international agreement” as an arena that focuses more on competition rather than collaboration. This condition inevitably fosters the practice of cyber arms race by several countries including the United States, European Union member states, Iran, Israel, China, and Russia.

Russia's attempt to intervene in 2016 US Presidential Election is “a new recipe in old menu” for Moscow and Washington continued competition. It is undeniable that Moscow has always had desire to "disrupt" US democracy. Moscow wants to show its leadership in cyber arms race and is currently seen as capable of performing the type, level of activity and scope of its "online" attacks, compared to the "offline" anti-democratic operations organized by the Soviet Union or Russia decades earlier. Russia has activated cyberattacks to undermine public confidence in the US democratic process, destroy Hillary Clinton's credibility and reputation, and simultaneously damage the electability and potential of her presidency. Russia also "has chosen" Donald Trump as President of the United States to replace President Barack Obama. Even if Hillary was elected, a Russian cyber strategy was prepared to focus on challenging the election result legitimacy and disrupting Hillary’s administration. In fact, a report produced by the US Intelligence Community underscores Russia's strategy prior to 2016 Presidential Election, Russian diplomats publicly criticized the election process and prepared to publicly question the result validity. Judging from their social media activities, pro-Kremlin bloggers have set up a Twitter campaign, #DemocracyRIP, on election night in anticipation of Hillary 's victory. This is Russian open propaganda campaign.

Successive cyberattacks carried out by Russian-run propaganda machines include its domestic media equipment, outlets targeting global audiences such as RT and Sputnik, and quasi-government troll networks have contributed to the campaign of influence by serving as a platform for Kremlin messaging to Russian audience and internationally. Russian-owned media made positive comments about President-elect Trump while consistently echoing negative coverage of Hillary Clinton. RT's coverage of Hillary during presidential campaign has persistently focused on leaked emails accusing her of corruption, poor physical and mental health, and her links to Islamic groups. In fact, the narrative was also formed to convince the public that if Hillary Clinton was elected, the potential for war between the United States and Russia would be even greater.

Would potential Russian cyberattack, and its actualization be well comprehended by US state election officials in the US? Yes, it would, but US lacks the resources to protect their election infrastructure. In most states, lawmakers are reluctant to increase their electoral security budgets. Some Governors also do not take strategic steps to improve the preventive and mitigation capacity of election security in their authorities. Congress fails to step in. In fact, the majority of state election officials surveyed by Politico at the end of 2017 indicated that they needed additional funding from the federal government to replace outdated electoral systems and technology that were vulnerable to cyberattacks from anywhere.

The dire state of US cyber capability is contrary to the readiness of Russia's resources and strategies. Alina Polyakova in her recent article in Foreign Affairs Magazine outlines the chronology of IRA’s cyberattacks. Initially and the most important first step is building an audience. In early 2014, IRA created fake social media accounts purportedly belonging to ordinary Americans. Using these accounts, they made general online content, not divisive or even political ones but is only designed to attract attention. After that, between 2015 and 2017, IRA purchased a total of more than 3,500 online advertisements for about $ 100,000 to promote its accounts. The second step is to make a strategy change. After IRA-run account gained a few followers, it suddenly began publishing divisive campaigns using racial, immigration and intolerance issues. Many accounts began publishing anti-Hillary Clinton content in 2015 and campaigning pro-Trump messages. The third step is to make it real. Later, fake IRA accounts sent private messages to their real-life followers, urging Americans to organize. IRA was able to reach millions of its social media followers. On Facebook alone, they have at least 126 million followers and around 1.4 million followers on Twitter. IRA's publication of thousands of Hillary campaign emails has also dominated headlines for months, tarnishing Democratic Party's image and eroding public support for her presidential campaign.

Unfortunately, just few weeks heading to2020 Presidential Election, US remains ill-equipped to potentially deal with Russian repetitive attacks. Since 2016, US Congress has not passed substantive laws targeting perpetrators of disinformation campaign in addition to limited sanctions against Russian officials and entities, nor does it oblige social media companies to take action on negative campaigns against US democracy. In fact, it is unclear which institution in the US government has a duty to deter cyberattacks against US Presidential Election. US Global Engagement Center is actually tasked with combatting state-sponsored disinformation; however, the Center is only part of the State Department and does not have domestic jurisdiction. Several government agencies have published guidelines on how the federal government should warn the American public about foreign interference, but the guidelines are not very specific. The good news is, the Cybersecurity and Infrastructure Security Agency, which is one of the agencies formed by the Department of Homeland Security, has been working to secure the physical machines of elections, update and replace electronic voting machines and strengthen security around voter data storage. It has also tried to improve information sharing among federal, state, and local authorities. These are important steps against cyberattacks and election hacks, but they cannot deal with foreign disinformation campaign operations. Things even get worse when President Trump continuously obscures facts and undermines US intelligence agencies making US and its people insecure and highly vulnerable to repeated cyberattacks. US democracy is indeed in a very fragile position.

CONCLUSION

During the twentieth century, democracy has confronted fascism, communism and other ideologies, and repeatedly proved itself a winner because of values that the world community considers more acceptable. Democracy determines the faith that everyone has the right to choose their leaders who can best regulate and meet their political needs. However, almost all over the world, the impact of social and economic inequality generated by globalization has led to widespread discontent and a rise in populism, the opponents have shown a clear intention to manipulate these unfortunate facts to discredit democracy. The emergence and advancement of social media and information technology, and their intersection with the political and social life is very encouraging and gives people ability to influence political decision-making processes and decide their future leaders. Yet, information technology and social media have also created new vulnerabilities such as exploitation of social issues by interested parties to undermine public trust in democratic institutions, exacerbate social problems and widen the gap through disinformation campaigns.

Russian hacking activism and disinformation campaigns have shown how information technology and social media become important actors in modern democratic process. If democracy does not heal its wounds, especially in modernizing its infrastructure, it is not impossible that democracy will collapse due to the loss of public trust in democracy itself. The question remains, if Russia will re-activate cyberattacks and disinformation campaign for this year US Presidential Election essentially when Putin has positioned himself as Russia's lifelong leader and, of course, determined to undermine public confidence in democracy. This call will always be a menu of foreign policy attractive to Moscow. At the same time, US heated domestic politics is hampering national collaboration to face Russia. Dictions of social issues revolving around racism, immigration and intolerance still dominates divisive atmosphere in the US.

REFERENCES

Adam Mosseri (2017). Working to Stop Misinformation and False News. Retrieved 25 August 2020, from Facebook website: https://www.facebook.com/facebookmedia/blog/working-to-stop-misinformation-and-false-news.

Adrian Shahbaz (2018). The Rise of Digital Authoritarianism. Washington D.C: Freedom House.

Alina Polyakova (2020). The Kremlin's Plot Against Democracy: How Russia Updated Its 2016 Playbook for 2020. Foreign Affairs Magazine 99 (5), p. 140-149.

Caroline Rossini and Natalia Green (2015). Cybersecurity and Human Rights. GCCS 2015 – Webinar Series Training Summaries (pp. 9-17).

Christina Lam (2018). A Slap on the Wrist: Combatting Russia's Cyber Attack on the 2016 U.S. Presidential Election. Boston College Law Review, 59 (6), p. 2167-2201.

Google (2020). We are committed to complying with applicable data protection laws. Retrieved 25 August 2020, from Google website: https://privacy.google.com/businesses/compliance/.

Laura Galante and Shaun EE (2018). Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents. Washington D.C: The Scowcroft Center for Strategy and Security, Atlantic Centre.

Lisa Reppell and Erica Shein (2019). Disinformation Campaigns and Hate Speech: Exploring the Relationship and Programming Interventions. Arlington, VA: International Foundation for Electoral Systems.

Nezir Akyesilmen (2016). Cybersecurity and Human Rights: Need for a Paradigm Shift? Cyberpolitik Journal, 1 (1), 38-61.

Office of The Director of National Intelligence Council (2017). Assessing Russian Activities and Intentions in Recent US Elections (2017). ICA 2017-01D.

U.S. Congress (2018). Congressional Task Force on Election Security: Final Report. Washington D.C.