Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2, 2018

Cyber warfare – New threat for national and international security and transformation of the conflicts under the conditions of the new geopolitical order

* Nika Chitadze

Abstract

This research paper, based on the methodology of political realism, will be discussed the transformation of conflicts in the context of the new geopolitical order and how important this methodology is in international cyber politics.

Within the paper, virtual threats are discussed where not only cyber-attacks and cyber wars are considered. Information, propaganda and disinformation manipulations, brief history, and development in cyberspace are analyzed. The focus is on fake news and these issues are supported by various examples. It analyses how all this works in relation to Georgia and cites the 2016 NDI survey. Furthermore, the research presents the classification of cyberspace and discusses the black market, which is a major threat worldwide. From the book by Kenneth Knapp, a cyber-security specialist the information provided on “Cyber Security and Global Information Assurance - Threat Analysis and Response Solutions”, published by the US Air Force Academy in Colorado, deals with the black market in cyberspace.

At the same time, the research is devoted to the analysis of the impact of modern high technologies on international security processes. It is noted that the development of technology and the Internet has had an impact on international security processes. It is discussed in the framework of the force balance method, or force balance methodology. Numerous examples are given of Russia’s cyber-technological capabilities, as well as those of the United States, China, and the Islamic Republic of Iran. Attempts by Russian hackers to intervene in various elections, including the 2016 US presidential election, as well as examples of Chinese cyber-attacks, which are of great political importance internationally and an important element in the balance of power, are discussed.

Keywords:

Cyberwarfare, cyber security, Surface Web, Deep Web, Dark Web, Darknet.

* Prof. Dr. of International Relations, Head of International Studies Research Center, International Black Sea University
E-mail: nchitadze@ibsu.edu.ge

Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2, 2018

Introduction

The social and economic well-being, health, and life of each citizen are significantly dependent on the security of information systems and electronic services. Cyber-attacks have a great impact on all sectors of the economy, hinder the proper functioning of the economic space, reduce public confidence in e-services and threaten the development of the economy through the use of information and communication technologies. Against the background of the existing global cyber threats, when cyber attacks, cyber espionage, cyber terrorism, and disinformation are carried out on a daily basis, the development, introduction, and development of new defense mechanisms is an important issue. It is noteworthy that NATO plays an important role in this direction and together with the EU is a kind of security umbrella for both member and partner countries.

Each century is accompanied by its own problems. Cybercrime has become one of the most dangerous events in the 21st century, with many people, private companies, and government agencies being harmed on a daily basis. Billions of dollars are already being spent on defense.

All NATO concepts and doctrines emphasize that, based on basic principles, no member state should be forced to rely solely on its own forces. The Alliance Strategy allows each Member State to pursue national security objectives through collective means.

Every leading country in the world has a national cyber security strategy, which is a determining factor of state policy. The National Security Strategy aims to identify, prevent, reduce and eliminate existing threats. Cooperation with partner countries and organizations is of great importance for Georgia.

Although Georgia is not in a leading position at this stage (as evidenced by numerous studies), there is an effective defense system - there is a cyber security bureau and a data exchange agency. As stated in the National Security Strategy of Georgia, Georgia aims to become a regional provider of cyber security services and to develop the necessary infrastructure for the operation of communication systems of other countries located on its territory. It is impossible to do this without the help of partners. According to the reports of the Security Service of Georgia, a significant risk to the security of the country is posed by hacker groups controlled by foreign special services, cyber-attacks on government infrastructure, and cyber-intelligence operations.

Threats cannot be avoided without modern technology, professional staff, and cooperation with leading states. Consequently, international cooperation is the only way. For Georgia, in terms of security, it is necessary to strengthen cooperation with NATO and the security services of leading countries in order to take timely preventive measures. There is also a need for closer cooperation with the security services of neighboring states.

NATO is the only organization that has the technical, financial, or human resources to withstand cyber threats. Therefore, it is important to study, analyze, research the current situation and future plans from a practical point of view. Researchers claim that if the scientific approach is correct, cyberbullying results will not be as devastating as they were in previous years.

Specific objectives and objectives of the study can be identified in order to better identify new types of threats, which are reflected in the impact that cyberwarfare has on world politics, as well as to analyze and evaluate new political conflicts.

The main objectives of the research are:

Identify cyber warfare as a new threat factor and discuss it in the context of a specific political conflict

Study and analysis of countries' security issues within the framework of cyber security format

Identify the authorial definition of civil cyberwarfare and explain its impact on political processes

Research and analysis of the impact of cyber threats on the national security of Georgia

The main research questions of the paper:

1. To what extent can cyber warfare be perceived as a new reality of political conflict?

2. What impact can cyber warfare have on the international community?

3. What are the action plan and components of the military strategy in cyber warfare?

4. What is the importance of Georgia's strategic partners in ensuring cyber security?

Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2, 2018

Research Methodology

Theory of Political Realism - According to science, political realism was the answer to liberalism, the basic premise of which was that states should not seek cooperation. Early realists Edward Carr and Hans Morgenthau believed that states were selfish rational actors seeking power because of their own security concerns. Any kind of cooperation between countries is perceived as random. For the realists, World War II was a kind of confirmation of their ideas. According to the theory of political realism, international relations are fierce competition between countries that have no reason to trust each other when the essence of their existence is self-preservation in an environment where the loss of one is the gain of the other. The methodology used is that of the founder of realism, Thucydides, and the followers of this theory, Morgenthau, Vasquez, and so on. Based on the considerations, as well as the examples presented in terms of the development of cyber technologies, we discuss the transformation of conflicts into a new geopolitical order. The methodology of political realism occupies a large place in 21st-century cyberpolitics.

Cyberwarfare and Political Realism

We discuss the topic based on the theory of political realism. Realism has long dominated the paradigm of international relations and is based on general assumptions about international politics. For example, the fact that states are the most important actors as independent entities in the international system has no centralized authority and have their own interests to ensure power and security. The essence of this methodology is important in the field of cyber security.

The importance of the theory of political realism is great in international cyberpolitics. In this case, it is uniquely related to cyber security. Historically, the foundations of the theory of political realism can be found in Thucydides' description of the Peloponnesian War (5th century BC), where he emphasized the immoral nature of international politics and the importance of power for survival. The development of this theory in international relations may be mainly due to Hans Morgenthau (1948), who focuses on the struggle for power between independent states (Stanford Encyclopedia of Philosophy, 2017).

Paul D., a follower of the theory of political realism. Senezi and John A.. According to Vasquez (Paul D. Senese and John A. Vasquez), there are factors that increase threats - e.g., military units, alliances, unions, alliances, are often unproductive and increase the likelihood of conflict (Paul, 2018).

Nevertheless, with a focus on security and conflict issues, realism seems to be a natural theory in addressing the acute issues of cybersecurity. In general, the study of the cyber conflict began when John Arquilla and David Ronfeldt developed the concepts of "cyber warfare" and predicted the transformation of war into the rapid advancement of ICT (Arquilla, 2000).

Proponents of realism Brandon Valeriano and Ryan C. Maness view the issue in this way: This form of conflict takes place in cyberspace and involves "the use of computing technologies in cyberspace for evil and/or destructive purposes. For the purpose "(Brandon, 2015).

We focus on these politically motivated relationships because they have a direct impact on national security. Joint military units or the conclusion of treaties are often perceived as a threat by other states, which then take similar measures to enhance their own security. This process is often referred to as the spiral model. The spiral model represents an escalation that causes a rapid shift in the balance of power, as well as an increase in international tensions and the risk of conflict. The cyber domain lacks effective global institutional governance.

Relevant organizations include the International Telecommunication Union (ITU) and the Internet Corporation for Assigned Names and Numbers (ICANN), but their functions and competencies do not extend to conflict management. The security dilemma is more acute when offensive and defensive capabilities do not differ from each other. In this case, the development of cyber security by states and increased funding for technology improvements are considered a potential threat. It is difficult to distinguish capabilities in cyberspace. Moreover, cyber-military organizations such as the US Cyber Command have both defensive and offensive roles, and if they say they are raising budgets or personnel, it is clear that this is both defensive and offensive reinforcements, which exacerbates uncertainty and competition between states - they seek security. In cyberspace.

In the classical sense of political realism, improving armaments increases the likelihood of war, but Barney Glaser argues that military savings are a necessary means of restraining revisionist power (Glaser, 2011), in which case the question arises: Will security competition escalate into real conflict? Will the increase in cyber armaments lead to new conflicts?

Christine M. Lord and Travis Sharp (Kristin M. Lord and Travis Sharp) argue that conflict in cyberspace is uniquely driven by escalation (Lord, 2011).

According to political realism, power is of great importance, it can ensure the independence and survival of the state. As Morgenthau (Morgenthau 1948, 80-108) puts it: "Whatever the ultimate goal of international politics, power is always its closest companion" (Rösch, 2020).

Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2, 2018

Realists often equate power with state property - natural resources, industrial capabilities, military armaments, and population size. Although there is no theory of cyber-power in the realist literature, it still offers a framework for the distribution of power among actors. In general, the information revolution calls into question the primacy of states, as often non-state actors threaten the dynamics of traditional power, they become more important over time. However, when it comes to cyberconflict, states are still dominant.

There is a perception that in relation to cyberspace, weak states further empower strong states and configure distribution in the system. For example, a major scandal has erupted over the training of thousands of hackers in North Korea, as well as the activism of China, which has been accused of stepping up its cyber-espionage campaign against the United States and refining its cyber-tactics against the Islamic Republic of Iran. Naturally, advanced countries are most dependent on digital infrastructure and are therefore most vulnerable to devastating cyber-attacks (Popescu, 2018). However, John Lindsay argues that only the technological superpower has the ability to develop the most sophisticated cyberweapons (Lindsay, 2020).

Cyberspace has become a new international battlefield. The Internet fits perfectly with the realistic model of security. In this setup, every state is alone or with its allies, whom it can never trust, and tries to build its cyber industry and defense for fear that any breach by another state will directly threaten their security. The best example of this is Russia, which has so-called Allies (China, Islamic Republic of Iran), but in reality, no one trusts. This country attacks every state for its own chauvinistic interests.

There are norms of international law in the 21st century. International organizations try to solve problems by civilized methods. Democracies operate on the principle - freedom, sovereignty, law. Peaceful resolution of conflicts, as well as coexistence, is the essence and basis of the current world order, although this does not exclude the possibility of wars. Every state is trying to ensure the security of the country and at the same time is ready for war - economic, informational, biological, and cyber.

Recent observations and examples show that economic pressure on any country is easier than a military campaign. A clear example of this is the imposition of sanctions by the United States and Great Britain on Cuba, Serbia, and Belarus, and even the imposition of sanctions on Russia by the European Union. It is no longer necessary to engage in hostilities to achieve political goals. However, there is also a goal, if the goal is to occupy the territory or create a buffer zone, then this will not happen without the use of armed forces. We have examples in this regard in Ukraine and Georgia, where Russia annexed the territories with the help of military forces and cyber warfare.

Virtual threat and asymmetric military challenges

There are five war zones in the world - air, land, sea, space, and cyberspace. Our research topic is cyberspace. Virtual threats include not only cybercriminals, psychological terror, digital viruses, and hacker attacks, but also virtual information and disinformation manipulations, as well as the global Internet market known as the Black Market (Darknet). Let us first highlight information warfare, which involves the use of information technology and management to gain an advantage over an adversary. It can be used to gain tactical information, disseminate misinformation and propaganda in order to demoralize the public or the adversary. Can be used for manipulation as well as prevent the dissemination of real information.

The phenomenon of information-propaganda war is not new, it is as old a method as the most ancient craft. It was just changing and will probably change (progress) in the future with the development of technology. Propaganda - means the systematic use of any form of communication to influence people's minds, behaviors, and emotions. This means is considered by many to be the most effective and common means of persuading people to engage in political activity. Intelligence services have historically used propaganda for a long time. The full strength of the propaganda war was revealed during World War II and is still relevant today. It is hard to believe, but the fact is that when World War II ended, many in Germany said, "Yes, Adolf Hitler is to blame, he exaggerated a little, but he did a lot of good, restored dignity and built highways" (Deusche Welle, 2020). Moreover, in post-Hitler Germany the influence of Goebbels's ideology and propaganda was so strong that witnesses did not appear at the Nuremberg trials in 1948 (History Extra, 2020). Even three years after the end of the war, people believed (many feared) that the Nazis would return to power. Then there was no internet, there was no computer, but there was radio, there was ideology, there was agitation in the population, there were pressure underarms. In this regard, we can say that Russia has a long history of information, propaganda, and disinformation, but in the era of technological revolutions, this activity has become more effective. Russian propaganda is not truth-oriented, but that does not mean that everything is a lie. Here we have a mixed-method when mixed misinformation is spread in truth. There are cases when we are dealing with complete disinformation and "fake news". For example, a fake report on September 11, 2014, informed us that a chemical plant in Louisiana had exploded (Manufacturing, 2015).

At the time this information seemed credible, it covered almost every social network. Generally, fake news spreads quickly and is easily believed. Especially when the information is spread by not one, but several media outlets. In this case, it is important to warn the public about impending misinformation. We are generally called upon to verify the facts, to look at several sources, but in relation to the masses it is ineffective - verifying the facts requires time and knowledge when it is proved that the information was false, a story already told, self-justification or simply denial is relatively ineffective. However, there is no other way. The mainstay of Kremlin propaganda in Georgia is the media and social networks. At least one TV station, several Internet TV stations, a print edition, and a Web site feature anti-Western "message boxes" that rely heavily on Russian sources for information. The active use of social networks by Russian propagandists is also noticeable when viral dissemination of disinformation or anti-Western narrative material

Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2, 2018

is viral. Numerous public opinion polls show that the main source of information in Georgia is television. According to a 2016 poll by the National Democratic Institute (NDI), 77% of the Georgian population names television as the primary source of information on politics and current events. Surveys also show that almost half of the Georgian TV viewers (47%) watch foreign channels in addition to Georgian ones. The most popular foreign channels are Russian (HTB, ORT, and RTR) (IDFI, 2016). It should be noted that there are countries where they actively control the Internet space and communication networks. For example, China, which also controls television and social media. It is known that the Chinese government has hired up to two million people, they write comments according to the instructions and influence, manage public opinion. A study by Carrie King, Margaret Roberts, and Jennifer Pan, based on leaked government emails on the Internet, has also been published. The study says the Chinese government fabricates 448 million comments a year. Employees in social networks often glorify China and the Chinese Communist Party, they try to divert people's attention to other, less important issues (Waddell, 2017).

What should we do to counter misinformation, fake news, false news, information warfare? Defining this is not so simple. In this case, it is important to attend, ie to disseminate real information. In case of delay, it is necessary to spread an alternative option. As mentioned above, the threats in cyberspace are multifaceted - one of which is the black market, which is not available to everyone on the Internet. In this case, we need to distinguish four areas of the Internet:

1) **Surface Web** - means a surface network. Also referred to as the Clear Web. This network is searched by standard web search systems. The network is indexed by search engines. This network includes Google, Facebook, Yahoo, Wikipedia, Instagram, etc.

2) **Deep Web** - Deep network, its content can be found directly in the URL or IP address. However, you may need to go through a password or other security mode to view websites. However, implies normal use. For example, when a user has limited access to various websites where they need to register to view content. On sites where you need to pay to download a magazine or newspaper. This space includes Paypal, Facebook, Twitter, Whatsapp, Gmail, etc.

3) **Dark Web.** This is a system that is not indexed by web search engines. You need a special program, configuration, or authorization to get here. It is possible to communicate anonymously, protect privacy, communicate privately, obtain illegal information, trade illegally, for example, in drugs, weapons, etc.

4) **Darknet - Dark Network**. Also known as a "hidden network". This is a system available using non-standard ports. Darknet differs from other networks in that file sharing is done anonymously, i.e. IP addresses are not publicly available. Communication in this space is uncontrolled and contains various dangers. We can draw a parallel between underground illegal activities that take place in real space and Darknet, which takes place in virtual space. Getting into this system is not easy, specific software and authorization are sacrificed. Darknet can also be considered as an alternative internet, or the dark side of the internet, it is a huge network that brings together thousands of unlicensed and illegal websites. There are many things available here - buying weapons illegally, buying cloned cards, buying fake passports, subscribing to slaves, buying drugs, renting a killer, and so on. Darknet has lots of illegal forums, social networks, and non-standard websites. We do not deliberately discuss the instructions for entering this system in the paper, it can be understood as an incentive. In his book, Cybersecurity and Global Information Security - on Threat Analysis and Response Solutions, published by the US Air Force Academy in Colorado, Knauf Kenneth emphasizes that one of the major shortcomings of the software is the black market. In his view, the defenses of cyberspace users usually lag behind cyber-attacks. Kenneth also explains that the possible growth of black markets increases the chances of vulnerabilities in software. It is difficult to obtain statistics on black markets for vulnerable users and related transactions. Our observation is expressed as a dynamic model of the system. We conduct simulations to observe whether the number of users increases or decreases. From our observations, we can say that the rate is increasing. However, it is difficult to say what causes it. Kenneth writes that the simulation scenario of their operations causes the market to temporarily shrink:

"Security companies such as IBM ISS X-Force (2007), PandaLabs (2007), and Symantec (2008) report an increase in cyberattacks. , Criminals and criminal organizations, trade in a variety of products. Their ultimate goal is to steal personal data. The Symantec report makes it clear that black markets pose a serious threat, both on a personal and global level. Using the black market poses a serious threat to the protection of personal information. Hackers also use cyber-attacks against specific users and specific sites to launch cyber-attacks on browsers and websites "(Kenneth, 2009).

The impact of modern high technologies on international security processes

The development of technology and cyberspace has changed the way countries make decisions, create policies, and interact with each other. The development of technology brings efficiency and success in almost every field. However, today it is unclear how much modern technology has changed the balance of global forces, or the balance of power in cyberspace. We have a slightly different picture in this regard.

Balance of forces, or balance of power, is one of the oldest and most important issues in the theory of international relations. According to this concept, the main task of states is to fight for self-preservation and self-determination, they care about security and independence. Often states come together to confront a state, or group of states, that poses a threat. It turns out that the international system, let's say cooperation, is divided into several groups of states, which determines peace for them. The high possibility of

Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2, 2018

asymmetric use of cyber opportunities in the modern era has made it possible for small countries to influence the ongoing proletarian processes in the world. Nevertheless, the general trend is to show that power is still in the hands of large and powerful countries. Since cyber warfare has become the standard tool of international politics, we can say that modern technologies have somewhat changed the approaches to global security. In this regard, it is important to define the concept of balance of power and the conditions for strengthening cyber technologies, which implies the cyber capabilities, development, and balancing of states. This refers not only to the strengthening or dominance of one state in terms of cyber technologies but also to the various stages of cooperation.

The concept of balance of power implies: if one state is strengthened, it will take advantage of the weakness of other states, which will lead to the unification of weak states for defense. It is a chain reaction that has evolved against the background of the development of technology and has facilitated the production of cyber warfares. This has put the security of some countries in question.

It should be mentioned, that the United States continues to spend lame-doubled funding to enhance cyber capabilities. This is not surprising, since the United States created the Internet and introduced many new technologies in this country. In general, a wide range of cyber-instruments in politics also provide different options for strategic flexibility, which was previously almost unthinkable. The Russian factor is also noteworthy, which is also in the leading position in terms of cyber capabilities. What is Russian Cybercrime and what is its role in terms of the balance of power? Russia really works innovatively in various conflicts. Due to the specific geopolitical environment, Russia has successfully adapted cyber-attacks to expand its own interests. In the paper, we have discussed numerous examples in relation to Russia. One of the 2007 cyber attacks against Estonia. It was a simple DDoS attack that did not cause significant damage but had a positive impact on strengthening Estonia-NATO relations in terms of security. The same thing happened in 2008 during the Russian-Georgian war, which we have already mentioned many times. Also - in relation to Ukraine, where the cyber attacks turned out to be more “sophisticated” and damaging. We have many examples that point to Russia’s enhanced cyber capabilities. Cyber-attacks carried out by Russia are mostly used in conditions of asymmetric conflict. Although hackers intervened in the 2016 US presidential election in a different way in the sense that Russia did not use cyber-attacks, it was not a punitive measure, it was intended to test cyber-capabilities to influence the election. Naturally, Russia’s capabilities also have a limit. When carrying out a cyberattack with a certain strategy, potential opponents have the opportunity to prepare in a defensive direction. Russia’s cyberattacks on Georgia and Ukraine may be considered experiments, but it allows leading countries to fully explore the so-called Russian methods in technological terms. And then it becomes easier to improve defense mechanisms. For example, the interference of Russian hackers in the elections in France, Italy, the Netherlands, and Germany was not as effective as it may have been in previous cases. China’s role in cybersecurity is also noteworthy. The intensive use of Chinese cyber espionage has extremely irritated the White House administration. It was at the expense of these attacks that secret materials were leaked by Chinese intelligence. One of the most damaging was when the US Administration Office of Personnel Management system was attacked - the personal data of more than 20 million people were obtained (Zengerle, Cassella, 2015).

Along with Russia, it is a powerful cyber player of the Islamic Republic of Iran not only in the region but also in the world. The Islamic Caliphate of Iran, like Russia, is not a predictable state, especially since its cyber doctrine is built on asymmetric warfare tactics and is largely based on hacker attacks. Every detail of the cyber doctrine is controlled by the government of the Islamic Caliphate of Iran, which includes the High Council of Cyberspace, which includes the highest representatives of the same government, starting with the president and ending with the ministers.

These countries are joined by the North Atlantic Alliance, which plays an important role in terms of cyber security worldwide and cooperates with member and non-member countries. NATO, with the help of the European Union, is trying to deal with the threats posed in cyberspace, which further balances the situation, reduces risks and threats. It is clear that today, in terms of cyber technologies, the system is not single-pole. In this case, the number of potential allies is greater and it is easier to make policy. Today’s international environment is multipolar in different dimensions. No one spends as much money as the United States, nor does anyone form a military alliance, not even China and Russia, but they still strengthen military cooperation and coordinate foreign policy. It should also be noted that the US has redoubled its efforts to counterbalance China around the world, especially in East Asia. Generally, China is considered the number one threat to the US. It is about American supremacy in global politics.

Conclusion

The review presented in the paper reveals how highly active different countries are in using cyber technologies in their international policy-making. The importance of the cyber element has a positive effect on maintaining the balance of power, as there is no single dominant force here. Yet the ability of cyber technologies to be easily used for asymmetric attacks reveals what risks and challenges the world faces.

Journal of Social Sciences; ISSN: 2233-3878; e-ISSN: 2346-8262; Volume 7, Issue 2, 2018

References:

Stanford Encyclopedia of Philosophy, 2010. Political Realism in International Relations. Retrieved from: https://plato.stanford.edu/entries/realism-intl-relations/

Paul D. Senese and John A. Vasquez. 2018. The Steps to War: An Empirical Study.

John Arquilla, David Ronfeldt. 2000. Swarming and the Future of Conflict. RAND National Defense Research Institute. Retrieved from: http://www.analytictech.com/mb021/swarming%20db311.pdf.

Brandon Valeriano and Ryan C. Maness. 2015. Cyber War versus Cyber Realities. Oxford University Press. Retrieved from: https://global.oup.com/academic/product/cyber-war-versus-cyber-realities-9780190204792?cc=ge&lang=en&#

Barney Glaser, 2011. Grounded Theory: The Philosophy, Method, and Work.

Kristin M. Lord and Travis Sharp, 2011. America's Cyber Future: Security and Prosperity in the Information Age, Center for a New American Security. Retrieved from: https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNAS_Cyber_Volume-I_0.pdf?mtime=20160906081238&focal=none

Felix Johannes Rösch. 2011. Hans J. Morgenthau, the "marginal man" in International Relations. A "Weltanschauungsanalyse", Newcastle University School of Geography, Politics, and Sociology. Retrieved from: https://core.ac.uk/download/pdf/40019366.pdf

Nicu Popescu and Stanislav Secrieru. 2018. Hacks, leaks and disruptions Russian cyber strategies, European Union Institute for Security Studies Paris, CHAILLOT PAPER № 148, Retrieved from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

Jon R. Lindsay. 2020. The Impact of China on Cybersecurity, Fiction and Friction. Retrieved from: https://www.belfercenter.org/sites/default/files/legacy/files/IS3903_pp007-047.pdf

Deusche Welle, 2020. The myth of Hitler's role in building the autobahn. Retrieved from: https://www.dw.com/en/the-myth-of-hitlers-role-in-building-the-autobahn/a-16144981

History/Extra. 2021. Forgotten trials: the other side of Nuremberg. Retrieved from: https://www.historyextra.com/period/second-world-war/forgotten-trials-the-other-side-of-nuremberg/

Manufacturing, 2015. Report: Russian 'Internet Trolls' Behind Louisiana Chemical Explosion Hoax. Retrieved from: https://www.manufacturing.net/operations/news/13099148/report-russian-internet-trolls-behind-louisiana-chemical-explosion-hoax,

Kaveh Waddell, 2017. Look, a Bird' Trolling by Distraction". Retrieved from: https://www.theatlantic.com/technology/archive/2017/01/trolling-by-distraction/514589/

J. Knapp Kenneth, 2009. Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions, U.S. Air Force Academy, Colorado, USA.

Patricia Zengerle & Megan Cassella, 2015. Millions more Americans hit by government personnel data hack, Retrieved from: https://uk.reuters.com/article/us-cybersecurity-usa/millions-more-americans-hit-by-government-personnel-data-hack-idUSKCN0PJ2M420150709.

"ინფორმაციის თავისუფლების განვითარების ინსტიტუტის" (IDFI).*"კრემლის საინფორმაციო ომი საქართველოს წინააღმდეგ: პროპაგანდასთან ბრძოლის სახელმწიფო პოლიტიკის აუცილებლობა", პოლიტიკის დოკუმენტი.* 2016.22.08. გვ. 5-23. მოპოვებული idfi.ge: https://idfi.ge/public/upload/Meri/Russian%20Propaganda%20in%20Georgia%20-%20Policy%20Paper.