White-Grey-Black Hat Hackers Role in World and Russian Domestic and Foreign Cyber Strategies

Mikhail A. Shlyakhtunov
Senior Lecturer, Department of General Military Training, Military Training Center
Moscow Aviation Institute (National Research University)
4 Volokolamsk Highway, Moscow, 125993
Russian Federation

***Abstract*—The article aims at establishing the role of three different types of hackers in the domestic cyber space, policy and welfare, international relations and warfare of the Russian Federation compared to the situation in the world as for the beginning of 2020 year. The character and structure of hackers' participation in the information policy and cybersecurity are characterized in connection with the intensity and duration of their intervention, national interests, technical and political outcomes. The new role of cyberwarfare as the fifth sphere of military activity is highlighted and proved. Positive and negative influence of hackers' activities, methods of their detection and control on the level of an individual Internet user, company, government and international organization are differentiated. Examples of certain criminal groups of hackers' activities are given. Main organizational measures, tools and cryptography techniques for the protection against hackers' invasion are proposed. The article reveals and analyzes the specifics of various hacker attacks: white, gray and black. The article emphasizes that cybersecurity in the world is now the object of hacker attacks, which can affect the functioning of not only national or private corporations: but also, the work of government agencies.**

Keywords*—Cyber wars; cybercriminals; disinformation; espionage; hackers; information security; military technology

I. Introduction

Peace and the war states in the modern era are separated by the thin line. There is no longer need to declare a certain and to follow a certain template. For organization of the anti-government protests, misguideness of adversaries, disorganization of the governance, public opinion influence, and reducing an opponent's resistment the disinformation is used; intelligence, military, and agencies of law enforcement prioritizing IT security for investing and recruiting [1].

At NATO Summits in Bucharest (2008) and Lisbon (2010), cybersecurity was first included in the strategic concept of position on cyberspace as new fifth sphere of military activity alliance. This direction was dynamically developed at the NATO summit in Wales (2014) and has become one of the keys on subsequent, including parliamentary, assembly organizations [2].

In the modern war it is impossible to achieve the set goals without constant implementation of information fighting measures. In peacetime, information warfare becomes an important component of the deterrent potential of the enemy. The strategies and motivations of those involved in cyberwarfare are often hidden by its technical nature, rapid evolution, and covert methods of use. Russia also succeeded in integrating cyber warfare into the state strategy for political domination [3].

In US cyber strategy, Russia, China, Iran and North Korea are treated as opponents using cyberspace to challenge the United States, its allies and partners. Donald Trump repealed the rules on the implementation of cyber-attacks, approved by the directive of B. Obama, wherein the United States prioritizes strengthening information component of the potential of hybrid warfare, the creation of a global electronic surveillance system and robotic on social networks, aimed at inspiring "cyber rebellion" in Russia [3]. Cyberwarfare no longer concerns only computer ports and protocols. Professional trolls are able to create misleading content and share it worldwide. Kevin Mitnick, famous hacker, stated: "it's easier to manipulate people rather than technology." Military operations now are usually preceded by information operations for the potential battle space preparing [1].

Hacker attacks are usually technical in nature (for example, malicious ads that inject dangerous objects onto a computer in the shadow mode and do not require user participation). However, hackers can also use psychological methods to trick users into opening malicious attachments or providing sensitive data.

At the end of 2020, Sunburst launched a stunning hacking attack on US and global targets, including SolarWinds, a leading US network management company, launching a monitoring platform that provides IT support staff with access to devices on which it is installed) allowed to break the function of updating its program. According to representatives of the cybersecurity company FireEye, which helped expose the hacker attack, said that many organizations around the world could be at risk, although the main target of this attack, apparently, were US authorities.

At the same time, it should be noted that throughout 2020, cybersecurity experts around the world have seen a surge in hacker attacks on critical infrastructure, including organizations involved in the fight against the COVID-19 pandemic.

II. Literature Review

With the development of Internet technologies, the development of artificial intelligence - hacker attacks, hacking as a phenomenon and cybersecurity are becoming the object of scientific research.

In particular, it is worth starting a review of scientific accentson different types of hat hacker. According, Banda, Phiri, Nyirenda, Kabemba, computer crimes have been in existence for a long time now and hacking is just another way or tool that hackers are now using to perpetrate crime in different form. In their opinion, the following are some of the consequences of network attacks: 1) Intermittent Business: Even small cyber-attacks can disrupt business. This may result in financial information and interrupted inventory to a complete digital shutdown. This may result in the denial of service (DOS); 2) Data Loss: Data lose may result in compromised consumer privacy and agency. Fines and Legal Consequences: Apart from properly reporting the depth and breadth of a cyber-attack, your business could face specific government-mandated “mishandling” fines, plus lose compliance or standard certifications; 3) Overall Loss of Business: Technology consumers will least trust a company whose resume is tarnished with digital maladministration. This directly affects the company’s ability to stay open [4].

If we are talking about the study of white hat hackers, it is worth mentioning the study Goel, Gupta, Garg. In their opinion, white hat hackers these are ethical hackers. They try to find out weaknesses of the computer system or the network with the help of penetration testing and vulnerability assessments. Their main intention of doing so is not to harm the system but to help. A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. White hat hacker’s job is one of the demanding jobs available in IT industry and its ethical hacking. White hat hackers these are Ethical Hackers. They try to find out weaknesses of the computer system or the network with the help of penetration testing and vulnerability assessments. Their main intention of doing so is not to harm the system but to help. A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software [**5**]. White hat hacker’s job is one of the demanding jobs available in IT industry and its ethical hacking.

Nanda think, that the white hat hacking plays a significant role in securing the information systems that is crucial in our computer driven world. That is not to say that it does not present some ethical problems in itself but if it is used correctly, it has tremendous potential in helping to secure information. Much of its success will come down to the morals and ethics that are at the core of the individual hacker. The more ethical-minded the individual, the more trust-worthy and beneficial that individual white hat hacker will prove to be [6].

The study Goel, Gupta, Garg "Ethical Hacking and Its Countermeasures," described above also the phenomena of black and gray hat hackers. Grey hat hackers, in their opinion, are a combination or blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner’s permission or knowledge. The intention behind their work is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners. A grey hat hacker is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example [5].

If we talk about black and gray hat hackers, mentioned above Goel, Gupta, Gar, that they are people who hack the system illegally. When they gain unauthorized access to a system their intentions are to harm its operations or steal sensitive corporate data or secret information. They can also violate privacy block the system network communication, overload the system so that it becomes too slow, etc. A black hat hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" [5].

Pelton, Indu B. Singh believe that the problem of cyber-attacks, invasion of privacy, stolen data, and identity theft will become ever more difficult to block, because the torrent of information exchange will only become larger and faster and more internationally diverse. The new cyber world that unfolds ever more rapidly each day will bring new opportunity for education, training, business, global economic exchange plus gaming and amusement, but it would be misleading to suggest that there is likely to be a silver bullet to stop cyber-crime and cyberterrorism. If you operate a business, it would be very prudent to follow the five-step program in the new U. S. cybersecurity framework. This means taking action to: “Identify, Protect, Detect, Respond and Recover.” [7].

Black-hat hackers in darknet are often on the borderline between cyber-libertarians and outlaws. Regardless of different views on their rightfulness, there is a consensus about the importance of understanding organizational workings in their communities [8].

Considering the current research on hockey attacks, it is worth making a number of emphases on scientific developments in the context of cybersecurity. Cybersecurity has emerged as a global challenge and is becoming a tier one security threat for nation states. Cyber incursions are complex and difficult to detect. They are extremely subversive. These challenges are even enhanced by developing AI, which bring new tasks for cyber security specialists. It is the cyber attacks that pose the biggest challenge to states and personal data [9].

According to Sharma, artificial Intelligence (AI) is a popular expression in the digital world. It is as yet an emerging science in various features as indicated by the difficulties experienced in the 21st century. Nowadays one can't imagine a world without AI as it has had a gigantic impact on human life. Computer-based intelligence is in almost every sphere of human life, including gaming, language preparation, discourse acknowledgment, insight robots, money-related exchanges, and so forth; every movement of human life has become a subset of AI. Security issues have become a significant threat for governments, banks, and associations due to online ambushes by software engineers. AI and cyber security have expanded and become more essential in the progressing events but AI is suffering also as it is a dynamic and fragile issue associated with human life [10].

Information security becomes a cornerstone of creation of communication networks of future generations and how data and communication networks will be protected safety of Society and State will depend. If today objects, potentially vulnerable from the Internet, are computers and the maximum harm which hacker attack can cause is a temporary suspension of work of automated control systems and access to information, any element of Digital economy can become object of attack in networks of the Industrial Internet of things. [11].

III. Methodology

Statistical reports and recent time historical backgrounds are implemented into each part of the article, discussed and compared for identifying the conceptually important patterns and responses. The character and structure of hackers' participation in the information policy and cybersecurity are characterized in connection with the intensity and duration of their intervention, national interests, technical and political outcomes.

In this article, the main scientific methods used are search, comparative, analytical methods. From the point of view of the specifics of the article - cybersecurity and hacker attacks, as well as its nature - the review article took into account and analyzed the materials of specialists in cybersecurity, countering hacker attacks and hacking in general as a phenomenon in cyberspace, which certainly affects government data protection policies.

IV. Result and Discussion

A. Hackers Activities for Peaceful Purposes

The attitude in the software industry for the term "hacker" has shifted from a positive "smart programmer" to a negative meaning "a person who uses computers to gain unauthorized access to data." (Fig. 1).

Nevil Maskelyne in 1903 managed to perform one of the earliest examples of hacking. It was the disruption of wireless telegraphy technology (invented by Guglielmo Marcony) by John Ambrose Fleming during its public demonstration. Maskelyne used auditorium's projector to send insult Morse code messages. Maskelyne drew attention to the technology's flaws and showed that interference is possible. He organized his Royal Institution hack with the use of a simple transmitter and Morse key at the West End music hall owned by his father [36].

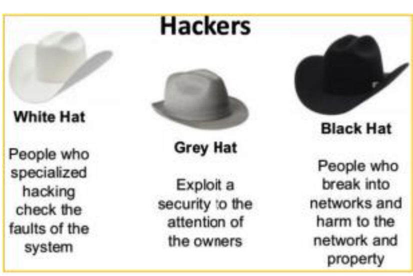

Fig. 1. Three main Types of Hackers.

1) White hat hackers or cybersecurity experts: In a professional environment there are "white" (or ethical, or white hat) hackers. Thanks to them a chance to gain access to customer data is reduced significantly. Some of hackers earn considerable sums of money from "bug bounties" from giant software corporations. For example:

- U.S. Army, Google, Microsoft, Pentagon pay them for breaching their security and exposing vulnerabilities. To identify vulnerabilities in their products Apple and Microsoft (e.g., Pwn2Own) encourage and sponsor hacking competitions. Vulnerability Rewards programs (VRP) from PayPal, Firefox, Google and others encourage hackers to disclosing and testing vulnerabilities [12].
- Most developers of information security systems of Rostelecom are white hat hackers. They are not inferior to grey and black hat hackers in either knowledge, experience, or ingenuity. They apply their talent in the legal field, in the interests of the law and the protection of information [13].
- For the first time, some companies (Zerodium and others) used an advertisement for the purchase of security vulnerabilities in order to transfer them to government clients for use in espionage. Zerodium payed $2million to white hackers in January 2019.
- Apple offered ethical hackers more than $1m for iOS kernel weakness discovering. And if the bug is found in pre-release software, company pays for a single bug 50% more [14].

2) Grey hat hackers: This type of hacking is illegal in most instances, though not inherently malicious. They expose vulnerabilities in systems without any permission given from the owners. Fee is requested by a gray hat for not disclosing it. And, if the organization doesn't fix the problem quickly enough, they will publicly disclose the vulnerabilities. In recent years, these hackers put much attention to the Internet of Things security issues due to such devices' growing ability to affect people's everyday life on macro and micro level and, therefore, the catastrophic repercussions of the IoT system violation [15]. For example:

- Thousands of Asus routers' users were left text warnings reminding to make patches when they were hacked by grey hats in 2014.
- A malware to close security vulnerabilities in several Linux routers were released by a group of grey hackers self-proclaimed as "White team" in 2015.
- A malware program able to delete firmware or brick the unpatched IOT gadgets was released by a grey hat in 2017. Later this year, more than 100,000 printers printed warnings about the leaving the devices exposed online being dangerous.

- In 2018 Catalin Cimpanu by ZDNet reported: grey-hat hacker Alexey had broken into and patched over 100,000 MikroTik (Latvian-based company dealing with routers and wireless ISP systems) routers to close the exploit that could be used by crypto-miners. Most hacked devices' owners were angry at invasion. Only near 50 people have contacted him to thank. Later this year, to make thousands of owners update their MikroTik and Ubiquiti routers another grey hat renamed them "HACKED" [16].

Grey hackers make the software market more competitive. Since grey hackers are working with largely used platforms, all users will benefit from their actions. Moreover, such activity can help the population of developing countries where governments often implement electronic documentation systems with little to no regard to their security [17] by increasing public awareness of such situation's potential risks and dangers.

However, grey hackers' actions are debated regarding their outcomes:

- Andrew Aurnheimer' charge of disclosing (exploiting website vulnerability) 114 thousand emails of iPad owners to AT&T;
- Downloading articles without subscription containing JSTOR research leaded to the prosecution of Aaron Swartz.
- Mathew Keys was charged for providing a website account's password of Los Angeles Times [18].

An act of discovering a vulnerability in a software could be acknowledged as criminal activity according to CFFA law.

B. *Hackers Activities for The Criminal, Political and War Purposes*

1) Black hat hackers or cybercriminals: Black hackers are ranged from amateurs to experienced criminals. Sometimes they are supported by goverment or terrorists or the employees or former employee of the attacked organization. They exploit information or sell it on the black-market to gain money. Such group like Fancy Bear, for example, is government employed and a group like Magecart acts independently. Among organized worldwide known groups such as "Swagg Security", "LulzRaft", "the Hacker Encrypters", "Team Appunity", "Lulz security", etc can be distinguished.

Due to the fact of having a developing economy, great wealth in Russia and countries of East Europe is monopolized. Also, the heritage of Soviet Union, made people used to free of charge products. A great gap between the quantity of educated in math, science and computers people and work opportunities pushes them towards illegal activities. Hackers originated from Russia and East Europe is known among the best in the world, so other states hire them for cyberattacks.

2) Features of russian hackers: Hacktivists from Russia and cyber-criminal syndicates became famous worldwide due to such features as:

- anonymity;
- easy to hire;
- crowdsourcing utilized by hackers and criminal networks;
- support by government agencies [1].

3) Interference into the election process in the own country: For such purpose hackers use different methods to disrupt voting trough Internet:

- Spoofing attack method. It is a legitimate message or resource imitation that is offered to voters. The fake voting website and the official website are visually functioning and look similarly. The attacker receives voter's identification data and can use it on the real voting website.
- Pharming attack method. It is a traffic redirection from one website to another. One way is to change voter's computer settings; another way is to exploit DNS (domain name server). Another name of attack of this type is DNS poisoning, falsifying DNS records so that a voter is directed to a fake voting website.
- Attacking against the website. It is a type of a hybrid attack achieved by inserting website-dependent malicious code that leads to lose of the voting possibility [19].

4) Examples of hackers activities for the war and foreign policy purposes

- In Europe. DDoS (Distributed denial of service) attacks like one that happened in Estonia against NATO-related cyber security center website [1]. Near 2,5 thousand confirmed attacks and 147 million "suspicious events" happened every day on computers at Mons (Belgium) cyber defence centre of NATO in 2013 [20]. TV5 Monde French television network and German Parliament were also subject to hacking attacks.

World disinformation: Since 2013 in St. Petersburg IRA (Internet Research Agency) was developed, also known as a 'troll factory'. Propaganda for both domestic and international social media such as Facebook, Instagram, Twitter and YouTube are created there. IRA's ad volume on Facebook peaked in April 2017, the same month as the introducing of tax reform plan and when ISIS tunnels in eastern Afghanistan were striked by Syrian missile [21].

World espionage: During the MH17 Belgian, Malaysian, Dutch, Australian, and Ukrainian authorities' investigation Russian cyber espionage campaign derailed.

In Georgia: The first known wide-scale offensive cyber operations in conjunction with conventional military operations were conducted by Russian hacktivists websites, such as stopgeorgia.ru on the first day of war in Georgia. Lists of Georgian sites to attack and downloadable malware, instructions and after-action assessments were made public. Most perpetrators traced to Russian and Turkish servers. Right before air attacks on the city of Gori their news websites and government websites were affected. Georgian government had to reroute most traffic through servers of other countries, such as Estonia, Poland and the United States due to IT infrastructure limitations in 2008 [1].

In Ukraine: During the Russian-Ukrainian conflict Russian hackers conducted malware attacks, spear phishing (sensitive information stealing), DDoS attacks, along with the actions of Russian military forces: TDoS (telephone denial of service) attacks, seizing an IXP (Internet Exchange Point), Internet cables' damaging, getting access to public CCTV cameras in the East of Ukraine, etc. Ukraine's military, government, private-sector, information technology infrastructure and telecommunications were targeted [22]. For example, CyberBerkut hacktivist group made public stolen, sensitive information against Ukrainian independency and proclaim themselves as defenders of Ukrainian national interests against aggression of West. On the eve of President of Ukraine elections in 2014, the group CyberBerkut damaged the IFES system of the Central Election Commission of Ukraine [19].

In USA: As US researchers state, the Main Directorate of the General Staff of the Armed Forces of the Russian Federation, abbreviated G.U. applied coordinated hacking to attack over 5 hundred institutions and people in US by exposing hidden information via WikiLeaks and other aliases such as "DCLeaks", "Guccifer 2.0." In March 2016, G.U. sent deceiving emails to more than 3 hundred people related with the Democratic Congressional Campaign Committee, Democratic National Committee, and Hillary Clinton's presidential campaign. Campaign chairman John Podesta was affected, as a result, more than 50 thousand secret messages were unwittingly handed over to the Russians [23]. North Korea's hack of Sony Pictures was also suspected of being conducted by Russian hackers.

Cyber-attacks against RF: The country ranked second in number of cyberattacks — 10% of all world cyberattacks accounted for Russia. According to international cyber experts, Russia suffered as a result of WannaCry cyber-attack in May 2017: most damage have been brought to the work of computer systems of the Ministry of Internal Affairs, Ministry of Emergencies, Russian Railways, Sberbank and "Megafon". Another massive virus attack was in June 2017: ransomware virus Petya blocked access to data, demanding for the unlock US$300 in Bitcoins. Individual versions of Petya disguised as a resume. Though the Petya virus is powerless without gaining administrator rights, its improved version — the Misha virus — is vested with administrator rights in advance [24].

C. Current State of Cybersecurity

1) Number of breaches by years

- In 2013, there were near 4 million records stolen from breaches every day; near 160 thousand per hour; about 3 thousand per minute or 44 every second. It takes about 6 months to detect data breach for most companies [25].
- In 2016, retail, government and technology are targeted in 95% of breached records. It is a 126% more than in 2017. In January 2016 it estimated 500 million Yahoo users accounts targeted.
- In May 2017, according to Equifax, data on 143 million Americans was exposed [18].
- In 2018, half a billion of personal records were considered stolen.
- 2019 year was proclaimed the year of data breach. Breaches used for exposing the records have risen by 54% (to near 4 billion) as for the second quarter of the year. 71% breaches were made for money gain and 25% – for espionage. 28% applied malware and 32–33% with phishing or social engineering, and 52% of hacking-related breaches.
- By 2021, according to Cybersecurity Ventures, the cybercrime damage can reach up to $6 trillion [26].

2) New vulnerabilities and possibilities: New vulnerabilities appeared at the beginning of 2020 year in world social network. Twitter has revealed details of cyberattacks, during which third parties used the company's official API to map phone numbers to social network user names. Security researcher Gal Weizman from PerimeterX has revealed a potentially dangerous Open Redirect vulnerability that allowed an XSS attack to be sent by sending a specially crafted message. If the victim views a malicious message, the attacker will be able to execute arbitrary code in the context of WhatsApp domain [27].

The weakest link in the security chain is considered the human factor. It results in 95% of cybersecurity breaches. Transferring personal data during an incoming call from an unknown number, a PIN code stored with a bank card, a password from an account on the work network glued to the monitor screen, clicking on random links from an office computer — all this creates ideal conditions for cybercrime.

As possibility to track and visualise global hacking real-time malicious activities the Kaspersky Cyberthreat is used [18].

D. Methods of Increasing Cybersecurity

1) Cryptography techniques: Digital image security has now attracted extra attentiveness. Cryptography and steganography techniques (permutation of pixel position, pixels value conversion etc.) were proposed to overcome the problem of information protection [28]:

- scan patterns,
- quantum chaotic maps,
- linear hyperbolic chaotic systems,
- quantitative cryptanalysis,
- chaotic nonlinear adaptive filtered,
- a linear quad tree compression etc.

Also, there are various math methods used:

- Lagrange interpolation to guess the value of the unknown values, use of nonlinear distortion cancellation for nonlinear compensator synthesis;
- Quadratic number spirals used in key image to create other types of spirals [29].

E. Main Organizational Measures, Tools and Software for Cybersecurity

1) Detecting unrecognized individuals and not letting people without appropriate accreditation into secure areas.

2) Restrict not required use and access of applications to the Internet.

3) Using Userfocus tool for mapping of attacker's procedures, monitoring attack methods for understanding the offenders' actions and for their prevention by individual techniques and tools [30].

4) Antivirus software use with updated signature databases and licensed, updated operating system and software.

5) Use of differential privacy when analyzing data to minimize the risk of users' sensitive information disclosure [31].

6) Clear explanation of every change taking important role for big corporations. For example, dual-factor authentication [32].

7) Hosting regular education sessions, but avoiding information overload which can be dangerous. It's better to use humor, repetition, short films, quizzes or collaborative workshops for better perception of complex material.

8) Due to the modern situation when people of different age groups work together under the same roof, company managements should use for training purposes the channels appropriate for every type of learner: audio, visual materials or practical activity.

9) Use of new tools for fake sources detection. For example, Alphabet-owned Jigsaw has released a free tool that allows journalists to detect fake photos, including those created using artificial intelligence [33].

*10)*Provide companies with the ability to retrieve and analyze information about their databases without profile tracking or invasive identity. These measures can also help to mitigate data breaches since sensitive data contained with other noise. In September 2019, Google announced set of libraries (open source) that offer the equations and models to set boundaries and limits on data identification and interface for developers to implement security [34].

*11)*The iOS platform is slightly less vulnerable to hacks compared to the Android platform [18].

*12)*Financing of cyber security sector and providing it with more responsibility. For example, in Canada two organizations are responsible for cyber security: PSC (Public Safety Canada) oversees the CSE (Communications Security Establishment) and the new CCCS (Canadian Centre for Cyber Security). The RCMP (Royal Canadian Mounted Police) is in the process of creating a National Cybercrime Coordination Unit. The Canadian government have decided to spend more than $500 million in five years beginning from 2018-2019 for realizing the National Cyber Security Strategy (28). It is better to invest in marketing campaigns to encourage competing software users to switch, than invest in developing more secure software, according to Sen, Verma and Heim (2020) investigation.

*13)*Provision of e-voting security procedures. For example: ensuring that voters receive an authentic electronic ballot and voter's information is destroyed immediately after receiving valid voting results; restricting connection to the e-voting system after the end of elections and integrity of the received data checked [35].

*14)*Special network access controlling systems use: 802.1x standart (checks profiles on the server and grants them access rights), Demilitarized zone tool (DMZ) (ensures public servers' security, establish two-step), Public Key Infrastructure, Intrusion Detection System, Web Application Firewall, TLS 1.2 (secure protocol latest version with symmetric and asymmetric encryption methods) along with well-developed PKI [19].

V. Conclusion

The year 2020 showed unpreceded number of data breaches and new vulnerabilities appeared at the beginning of 2021. The expenses on cybersecurity are growing. The cybersecurity process itself is based on a risk-oriented approach that identifies cyberspace assets and stakeholders, threats, recommendations and risk management measures, moreover, coordination guidelines are used as a specific measure actions and information sharing.

Human factor is considered to be the main problem for e-security. Supply of essential services can be affected by Cyber security incidents (providing healthcare, mobile network, electricity, water) and the critical infrastructure can be damaged.

The use of new tools for fake sources detection, special network access controlling systems, provision of e-voting security procedures, financing of cyber security sector and providing it with more responsibility, using appropriate channels to educate every learner, new steganography and cryptography techniques, mapping of attacker's procedures, constant implementation of information fighting measures, using the white hat expertise via bug bounty programs and responsible disclosure policies are the main sources to survive in a cyber war that continues to expand worldwide.

References

[1] M. Connell and S. Vogler, "Russia's Approach to Cyber Warfare," CNA Analysis and Solutions Publ. 2017. Retrieved November 24, 2020, from https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf.

[2] A. Smirnov, "Latest cyber strategies of USA – Preamble of war?" International Processes, vol. 16, No. 4(55), pp. 181-192, 2018. doi: 10.17994/IT.2018.16.4.55.11.

[3] J. J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy," in Cyber War in Perspective: Russian Aggression against Ukraine, K. Geers (Ed.). Tallinn: NATO CCD COE Publications, 2015, pp. 29-37.

[4] R. Banda, J. Phiri, M. Nyirenda and M. M Kabemba, "Technological paradox of hackers begetting hackers: a case of ethical and unethical hackers and their subtle tools," Zambia ICT Journal, vol. 3(1):1, 2019. doi:10.33260/zictjournal.v3i1.74.

[5] S. Goel, K. Gupta and M. Garg, "Ethical Hacking and Its Countermeasures," International Journal of Advance Research and Innovation, vol. 2, no. 3, 2014, pp. 624-629.

[6] S. Nanda, "World of White Hat Hackers," International Journal of Scientific and Engineering Research, vol. 10(5), 2019.

[7] J. Pelton and I. B. Singh, "Who Will Control the Future, Black Hat Hackers or the Hacked?", in Digital Defense, 2015, pp.127-144. doi:10.1007/978-3-319-19953-5_7.

[8] K. H. Kwon and J. Shakarian, "Black-Hat Hackers' Crisis Information Processing in the Darknet: A Case Study of Cyber Underground Market Shutdowns," in Networks, Hacking, and Media – CITA MS@30: Now and Then and Tomorrow. Studies in Media and Communications, vol. 17, 2018, pp. 113–135 doi:10.1108/S2050-206020180000017007.

[9] R. Walters and M. Novak, "Cyber Security," in Cyber Security, Artificial Intelligence, Data Protection and the Law, 2021, pp.21-37. doi:10.1007/978-981-16-1665-5_2.

[10] S. Sharma, "Role of Artificial Intelligence in Cyber Security and Security Framework," in Artificial Intelligence and Data Mining Approaches in Security Frameworks, B.Neeraj, B. Ritu, P. Singh and A. Rashmi (Herausgeber), Eds. John Wiley & Sons, 2021, pp.33-63. doi:10.1002/9781119760429.ch3.

[11] N. Ulpe and S. Melnik, "CyberSecurity Concept For New Generation Telecommunication Networks," pp. 72-75, January 2019 [Conference: International Conference Technology and Entrepreneurship in Digital Society].

[12] A. Hamilton, "Here's what it's like being a hacker millionaire under the age of 25," Business Insider, September 2019. Retrieved March 4, 2021 from https://www.businessinsider.com/how-2-white-hat-hackers-became-millionaires-before-the-age-of-25-2019-9.

[13] Information Agency "Region 29", "Information wars: "white" Rostelecom hackers are counting," 2019. Retrieved April 7, 2021 from: https://region29.ru/2019/11/11/5dc967ac764de97cd127f722.html.

[14] A. Hern, "Bug bounty: Apple to pay hackers more than $1m to find security flaws," The Guardian, 2019. Retrieved November 4, 2021 from https://www.theguardian.com/technology/2019/aug/12/apple-hackers-black-hat-conference.

[15] D. J. Devadass and E. S. Juliet, "A Survey on Security Issues in IoT," International Journal of Emerging Technologies in Engineering Research, vol. 7 (12), 2019.

[16] P. A. Nohe, "Mysterious Russian Grey Hat Vigilante has patched over 100,000 routers," Hashedout, October 2018. Retrieved March 26, 2021 from https://www.thesslstore.com/blog/mysterious-russian-grey-hat-vigilante-patched-over-100000-routers/.

[17] B. Haque, A.K.M. and T.H. Pranto, "Health Data Security: A Privacy-Preserving Proposed Strategy for Bangladesh," International Journal of Emerging Technologies in Engineering Research, vol. 8, issue 7, 2020.

[18] R. Sen, A.Verma and G. R. Heim, "Impact of Cyberattacks by Malicious Hackers on the Competition in Software Markets," Journal of Management Information Systems, vol. 37, issue 1, pp. 191-216, 2020. doi: 10.1080/07421222.2019.1705511.

[19] T. Limba, K. Agafonov, L. Paukštė, M. Damkus and T. Plėta, "Peculiarities of cyber security management in the process of internet voting implementation," *Entrepreneurship and Sustainability Issues, vol. 5*, issue 2, pp. 368-402, 2017. doi: 10.9770/jesi.2017.5.2(15).

[20] A. Croft and P. Apps, "NATO websites hit in cyber attack linked to Crimea tension," Reuters, March 2014. Retrieved April 13, 2021 from https://www.reuters.com/article/us-ukraine-nato/nato-websites-hit-in-cyber-attack-linked-to-crimea-tension-idUSBREA2E0T320140316.

[21] Ph.N. Howard, "The IRA and political polarization in the United States," *Homeland Security News Wire, LLC News Wire Publications, New York,* December 2018. Retrieved March 31, 2021 from http://www.homelandsecuritynewswire.com/dr20181221-the-ira-and-political-polarization-in-the-united-states.

[22] L. Jaitner, "Russian Information Warfare: Lessons from Ukraine," in Cyber War in Perspective: Russian Aggression against Ukraine, K. Geers, Ed. Tallinn: NATO CCD COE Publications, 2015, pp. 87-94.

[23] S. Lobo, "DCLeaks and Guccifer 2.0: How hackers used social engineering to manipulate the 2016 U.S. elections*," Packt*, July 2018. Retrieved April 1, 2021 from: https://hub.packtpub.com/dcleaks-and-guccifer-2-0-how-hackers-used-social-engineering-to-manipulate-the-2016-u-s-elections/.

[24] D. M. Berova, "Kiberataki kak ugroza informatsionnoy bezopasnosti" [Cyberattacks as a threat to information security], Gaps in Russian Law. A Law Journal, vol. 2, pp. 186-188, 2018.

[25] D. Milkovich, "15 Alarming Cyber Security Facts and Stats," *Cybint*, September 2019. Retrieved April 8, 2021 from: https://www.cybintsolutions.com/cyber-security-facts-stats/.

[26] Cyber Observer, "*29 Must-know Cybersecurity Statistics for 2020,"* 2020. Retrieved April 16, 2020 from https://www.cyber-observer.com/cyber-news-29-statistics-for-2020-cyber-observer/.

[27] A. Hashim, "WhatsApp Desktop Platform Security Flaw Allowed Access to Local File System," *Latest Hacking News*, February 2020. Retrieved April 6, 2021 from https://latesthackingnews.com/2020/02/07/whatsapp-desktop-platform-security-flaw-allowed-access-to-local-file-system/.

[28] S. A. Thajeel and M. Sh. Al-Tamimi, "An Improve Image Encryption Algorithm Based on Multi-level of Chaotic Maps and Lagrange Interpolation," Iraqi Journal of Science, vol. 59 (1A), pp. 179-188, 2018. doi: 10.24996/ijs.2018.59.1A.19.

[29] E. B. Solovyeva, (2014). "Neural networks as nonlinear compensator models for digital communication system," IEEE [International Conference on Computer Technologies in Physical and Engineering Applications (ICCTPEA)]. Saint Petersburg, Russia, 2014, pp. 174-175. doi: 10.1109/ICCTPEA.2014.6893342.

[30] S. Šišulák, "Userfocus – tool for criminality control of social networks at both the local and international level," Entrepreneurship and Sustainability Issues, vo. 5, issue 2, pp. 297-314, 2017. doi: 10.9770/jesi.2017.5.2(10).

[31] R. J. Wilson, C. Zhang, W. Lam, D. Desfontaines, D. Simmons-Marengo and B. Gipson, "Differentially Private SQL with Bounded User Contribution," Sciendo: Cornell University, 2019. Retrieved April 6, 2020 from https://arxiv.org/abs/1909.01917.

[32] G. Beuchelt, "Security Is a Process, Not a One-Time Project," *Buzz news*, February 2020. Retrieved April 2, 2021 from https://www.informationsecuritybuzz.com/articles/security-is-a-process-not-a-one-time-project/.

[33] D. Alba, "Tool to Help Journalists Spot Doctored Images Is Unveiled by Jigsaw," The New York Times, February 2020. Retrieved April 10, 2021 from https://www.nytimes.com/2020/02/04/technology/jigsaw-doctored-images-disinformation.html.

[34] M. Deshazo, "Just Let Those Tech Companies Know Less about You, Google is Here," Techchums, September 2019. Retrieved April 9, 2021 from https://techchums.com/2019/09/08/just-let-those-tech-companies-know-less-about-you-google-is-here/.

[35] H. Solomon, (19). "Federal Budget 2019: More money for cyber security," IT World Canada, March 2019. Retrieved April 11, 2021 from https://www.itworldcanada.com/article/federal-budget-2019-more-money-for-cyber-security/416155.

[36] P. Marks, "Dot-dash-diss: The gentleman hacker's 1903 lulz," NewScientist, December 2011. Retrieved March 6, 2021 from https://www.newscientist.com/article/mg21228440-700-dot-dash-diss-the-gentleman-hackers-1903-lulz/.