SPCSJ

SCIENTIFIC AND PRACTICAL CYBER SECURITY JOURNAL

VOL7 No3
SEPTEMBER 2023

ISSN 2587-4667

Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 1 – 10 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

THE CRIMINALIZATION OF THE INTERNET AND CYBERCRIME IN GENERAL: A COMPREHENSIVE STUDY

Ayepeku O. Felix[1], Omosola J. Olabode[1], James K. Ayeni[2]

[1]Dept. of Mathematical and Computing Science, Thomas Adewumi University Oko-Irese
[2]Dept. Of Computer Science, Kwara State Polytechnic, Ilorin

ABSTRACT: The internet's rapid growth has revolutionized connectivity and convenience, but it has also led to a rise in cybercrime. This study explores the complexities, implications, and challenges of cybercrime, analyzing its evolution, forms, and socio-economic impact. It examines the legal framework surrounding cybercrime, including international agreements, national legislation, and emerging jurisprudence. The study also highlights the need for international cooperation and cyber forensics advancements. It also examines the ongoing cybercrime arms race between cybersecurity professionals and cybercriminals, emphasizing the importance of proactive defense strategies, threat intelligence, and incident response protocols. The study underscores the urgency of addressing the criminalization of the internet and cybercrime, emphasizing the role of public awareness, collaboration, and innovative technological solutions in mitigating threats and ensuring a secure digital future.

KEYWORDS: criminalization, internet, cybercrime, comprehensive, study

1. INTRODUCTION

The internet's widespread proliferation over the last two decades has undeniably transformed how we communicate, work, and go about our everyday lives. This digital metamorphosis has ushered in an era of unprecedented connectivity, convenience, and innovation. However, as the internet continues to evolve, so too does the shadowy underworld of cybercrime, raising profound concerns about the criminalization of the digital realm.

With the rise of the internet, cybercrime has emerged as a global epidemic, transcending geographical borders and infiltrating nearly every facet of our interconnected world. Cybercriminals exploit the boundless opportunities offered by the digital landscape, perpetrating a diverse range of crimes with far-reaching consequences. From financial frauds and data breaches to disruptive ransomware attacks and state-sponsored cyberespionage, the spectrum of cyber threats is both broad and ever-evolving.

As we embark on this comprehensive study, it is imperative to recognize the gravity of the situation. Cybersecurity Ventures estimates that by 2023, cybercrime will have cost the global economy $8 trillion. Cybercrime would have a larger economy than China and the United States combined, ranking third in the globe, the gross domestic product of many nations (yeoandyeo, 2023). Moreover, the implications extend beyond financial losses, encompassing the erosion of privacy, the disruption of critical infrastructure, and even the compromise of national security Rybicki, P. (2023).

To combat the criminalization of the internet and cybercrime effectively, it is paramount to understand its multifaceted nature. This study aims to dissect the intricacies of cybercrime, ranging from its historical roots to the modern-day landscape. We will explore the various forms of cybercrime, including hacking, malware, social engineering, and the ever-elusive dark web marketplaces. In doing so, we will delve into the motivations driving cybercriminals, the methodologies they employ, and the profound socio-economic impact these activities have on individuals, organizations, and society at large.

In parallel, this study will scrutinize the evolving legal framework governing cybercrime, spanning international agreements, national legislation, and emerging jurisprudence. It will also examine the persistent challenges associated with the attribution of cybercrimes to specific actors and jurisdictions,

emphasizing the pressing need for international cooperation and advancements in cyber forensics (Palmieri, M., Shortland, N., & McGarry, P. 2021)

Furthermore, we will investigate the perpetual cat-and-mouse game between cybercriminals and cybersecurity professionals. By analyzing the techniques employed on both sides of this digital divide, we will underscore the importance of proactive defense strategies, threat intelligence sharing, and the development of robust incident response protocols.

As we navigate this comprehensive study, it is our fervent hope that the insights gained will contribute to a broader understanding of the criminalization of the internet and cybercrime. Together, we can strive to safeguard the digital realm, ensuring that the boundless opportunities presented by the internet are not eclipsed by the shadow of cybercriminal activities.

1.1 MOTIVATION:

The criminalization of the internet and cybercrime in general is motivated by the need to understand, address, and mitigate the growing challenges posed by cybercriminal activities in our interconnected world. It serves as a means to inform, educate, and drive actions that enhance cybersecurity and promote responsible digital behavior.

1.2 HISTORICAL ROOTS OF CYBERCRIME

The origins of cybercrime can be traced back to the computing in its early days. As early as the 1960s and the 1970s, as computer technology began to emerge, the emergence of a new crime type started to take shape. Theft of private data and unlawful access to computer systems were early examples. Hacking as a concept, initially used to describe the activities of individuals exploring computer systems out of curiosity, began to evolve into a criminal enterprise.

One notable historical event was the first computer virus created in 1982 by Richard Skrenta, known as the Elk Cloner, which infected Apple II computers. This marked the beginning of malware as a tool for cybercriminals. As technology advanced, so did the sophistication and a wide range of cybercrimes, such as financial fraud and the dissemination of dangerous software.

1.3 TYPES AND EVOLUTION OF CYBERCRIME

Cybercrime encompasses a vast array of criminal activities, with hackers and cybercriminals continuously adapting to technological advancements. Some prominent categories of cybercrime include:

Hacking and Unauthorized Access: Unlawful entry into computer systems or networks with the intention of doing harm. Hacking has evolved from simple password guessing to more advanced techniques such as SQL injection, zero-day exploits , Brute forcing, Packet sniffing, Privilege escalation and Exploiting software vulnerabilities (Naidoo & Jacobs, 2023)

Malware Attacks: Malicious software, including viruses, worms, Trojans, and ransomware, is used to compromise systems and steal data. Modern malware is highly sophisticated, capable of evading detection and encryption (Naidoo, R., & Jacobs, C. (2023).

Social engineering and Phishing: Cybercriminals use deceitful methods to trick people into disclosing critical information. Phishing attacks often target email recipients with fraudulent messages, while social engineering exploits human psychology (Sekhar Bhusal, 2021)

Financial Cybercrimes: In the digital era, criminal activity including credit card scams, theft of personal information, and internet fraud has exploded, costing individuals and organizations billions of dollars (Mohsin, K. 2021).

Ransomware: An increasing danger, encrypts information belonging to a victim and demands payment to unlock it Ransomware attacks have disrupted critical infrastructure and led to significant financial losses

State-Sponsored Cyber Espionage: Nation-states engage in cyber-espionage for political, economic, and military purposes. Notable examples include the Stuxnet worm and the alleged Russian interference in foreign elections (Gulyás, O., & Kiss, G. 2023).

2.0 THE MODERN CYBERCRIME LANDSCAPE

The modern cybercrime landscape is characterized by its scale, complexity, and constant evolution. The advent of the dark web has provided cybercriminals with a clandestine platform for conducting illicit activities, including the sale of stolen data, hacking tools, and cybercrime-as-a-service offerings (Palmieri, M., Shortland, N., & McGarry, P. 2021)

Cybercrime is not limited to individuals; well-organized cybercriminal groups operate globally. These groups often employ sophisticated tactics, tools, and even conduct research and development to stay ahead of cybersecurity defenses (Lusher, 2018).

Additionally, as the Internet of Things (IoT) expands, new exploitative opportunities are opened up by hackers. Vulnerabilities in IoT devices can be targeted to gain unauthorized access or launching extensive distributed denial-of-service (DDoS) assaults (Zarpelão, Miani, & Kawakani, 2017).

2.1 HACKING

Hacking, broadly defined as unauthorized access to computer systems or networks with malicious intent, is one of the oldest and most pervasive forms of cybercrime (Naidoo & Jacobs, 2023). It includes:

Ethical Hacking: Ethical hackers, often referred to as "white hat" hackers, legally and ethically assess system vulnerabilities to improve security.

Black Hat Hacking: Malicious hackers, or "black hat" hackers, break into systems for personal gain, damage, or theft.

Gray Hat Hacking: A gray area where hackers may breach systems without authorization but not necessarily for malicious purposes, sometimes seeking rewards or recognition

2.2 MALWARE ATTACKS

Malware, or malicious software, is designed to compromise systems or steal data (Naidoo, R., & Jacobs, C. (2023). It includes:

Viruses: Self-replicating programs that attach to other files and require user interaction to spread

Worms: Self-replicating programs that spread independently and exploit vulnerabilities in networked systems

Trojans: Malware disguised as legitimate software, often used for data theft or providing unauthorized access

Ransomware: Data-encrypting malware that severely disrupts operations by encrypting victims' data and demanding a fee to retrieve it

2.3 SOCIAL ENGINEERING

Social engineering exploits human psychology to manipulate individuals into revealing sensitive information or performing actions they wouldn't otherwise (Sekhar Bhusal, 2021). Techniques include:

Phishing: Cybercriminals use fraudulent emails or websites that mimic trusted entities to trick victims into revealing personal information.

Pretexting: Attackers create fabricated scenarios or personas to obtain sensitive information or access.

Baiting: Malicious software or media is offered to entice users to download it, compromising their devices

2.4 DARK WEB MARKETPLACES

The dark web provides anonymity through tools like Tor (The Onion Router), making it difficult to trace users or monitor activities. This anonymity enables cybercriminals to operate with relative impunity, though law enforcement agencies have made efforts to combat illegal activities on the dark web (Palmieri, M., Shortland, N., & McGarry, P. 2021)

The dark web, special browsers are needed to access this hidden part of the internet, hosts various illegal activities, including cybercrime marketplaces This includes:

Stolen Data Markets: Platforms where hackers sell stolen credentials, credit card information, and personal data.

Malware and Exploit Markets: Cybercriminals offer malware, zero-day exploits, and hacking tools for sale

Drugs and Weapons Markets: Beyond cybercrime, the dark web hosts illegal marketplaces for drugs, firearms, and other contraband

3.0 MOTIVATIONS DRIVING CYBERCRIMINALS

Cybercriminals are driven by a range of motivations, including financial gain, ideology, and personal vendettas. They employ various methodologies, from phishing to malware, to achieve their objectives. The socio-economic impact of cybercrime is extensive, affecting individuals, organizations, and society through financial losses, data breaches, reputation damage, and even national security risks.

Cybercriminals are motivated by a range of factors, often intertwined. Understanding these motivations is crucial to addressing cybercrime (Palmieri, M., Shortland, N., & McGarry, P. 2021)

Financial Gain: A primary motivation for cybercriminals is financial profit. This includes activities like stealing credit card information, conducting ransomware attacks, and selling stolen data on the dark web (Mohsin, K. (2021).

Hacktivism: Some cybercriminals have political or ideological motivations, engaging in hacktivism to promote a particular cause or express dissent (Nershi & Grossman, 2023)

Espionage: Nation-states engage in cyber espionage to gain a competitive advantage, steal intellectual property, or gather intelligence

Personal Vendettas: Cybercriminals may have personal grudges or vendettas against individuals or organizations, leading to targeted attacks.

Thrill-Seeking: For some, cybercrime provides a sense of excitement and achievement, akin to a high-risk game

4.0 METHODOLOGIES EMPLOYED BY CYBERCRIMINALS

Cybercriminals employ a wide range of methodologies and techniques to achieve their objectives (Naidoo, R., & Jacobs, C. (2023).

Phishing: Sending deceptive emails or messages to trick recipients into revealing sensitive information or downloading malware.

Malware: Developing and distributing malicious software like viruses, Trojans, and ransomware to compromise systems.

Exploiting Vulnerabilities: Identifying and exploiting software or hardware vulnerabilities, such as zero-day exploits.

Social Engineering: Manipulating individuals into revealing information or performing actions against their best interests through deception and persuasion.
Denial-of-Service (DDoS) Attacks: Overloading a target's server or network with traffic to disrupt services or operations.
Insider Threats: Exploiting the trust of insiders, such as employees or contractors, to gain unauthorized access or steal data.

4.1 SOCIO-ECONOMIC IMPACT OF CYBERCRIME

The socio-economic impact of cybercrime is far-reaching and profound, affecting individuals, organizations, and society as a whole (Rybicki, P. 2023).

Financial Losses: Cybercrime costs individuals and organizations billions of dollars annually in financial losses, including theft, fraud, and the expenses associated with data breaches.
Data Breaches: Data breaches compromise the personal and financial information of individuals, leading to identity theft and financial fraud.
Reputation Damage: Organizations often suffer reputational damage following a cyberattack, which can erode customer trust and shareholder confidence.
Operational Disruption: Cyberattacks can disrupt critical infrastructure, leading to downtime and lost productivity.
National Security Risks: State-sponsored cyber espionage and cyberattacks on critical infrastructure pose significant national security risks (Gulyás, O., & Kiss, G. 2023).
Economic Impact: The overall economic impact of cybercrime includes costs associated with cybersecurity measures, legal proceedings, and insurance premiums.
Psychological and emotional effects: Individuals who fall victim to cybercrimes, such as online harassment or cyberbullying, may suffer emotional and psychological distress.

4.2 INTERNATIONAL AGREEMENTS AND CONVENTIONS

The legal framework governing cybercrime is evolving rapidly to address the complex and global nature of cyber threats. International agreements, national legislations, and emerging jurisprudence collectively form a multifaceted approach to combating cybercrime and protecting individuals, organizations, and society at large. International agreements and conventions play a significant role in shaping the legal framework for addressing cybercrime on a global scale Arnell, P., & Faturoti, B. (2022). Key agreements and organizations include:

Budapest Convention: The Council of Europe's Convention on Cybercrime, also known as the Budapest Convention, is a milestone international treaty that harmonizes cybercrime legislation and facilitates international cooperation (Council of Europe, 2001).
United Nations (UN) Resolutions: Various UN resolutions, such as Resolution 55/63 and Resolution 58/199, call for international cooperation in combating cybercrime and protecting critical infrastructure (United Nations, 2000, 2004)
Interpol: The biggest international law enforcement agency in the world is that facilitates cross-border cooperation and information sharing among law enforcement agencies to combat cybercrime (Interpol, n.d.).

4.3 NATIONAL LEGISLATIONS

National legislations are essential for addressing cybercrime within individual countries. These legislations define cybercrimes, penalties, and enforcement mechanisms (“A Study of Cyber Crime Awareness for Prevention and Its Impact,” 2017) some notable examples include:

USA - Computer Fraud and Abuse Act (CFAA): The CFAA criminalizes unauthorized access to computer systems and networks and has been used to prosecute various cybercrimes. (Cybercrime and the law, 2020)
European Union - General Data Protection Regulation (GDPR): While primarily focused on data protection, GDPR includes provisions related to data breaches and imposes significant fines for non-compliance (European Union, 2016).
China - Cybersecurity Law: China's Cybersecurity Law imposes strict regulations on data protection, critical infrastructure, and the operations of technology companies (National People's Congress, 2016).

4.4 EMERGING JURISPRUDENCE

Emerging jurisprudence refers to legal precedents set by court decisions in cybercrime cases. As cybercrimes evolve, courts are increasingly confronted with novel legal challenges Some notable cases include:

United States v. Ross Ulbricht (Silk Road): This case involved the prosecution of Ross Ulbricht, the creator of the Silk Road, a dark web marketplace. It set a significant precedent for the legal treatment of dark web activities (United States v. Ulbricht, 2015).
Facebook, Inc. v. Power Ventures, Inc.: In this case, Facebook sued Power Ventures for violating the Computer Fraud and Abuse Act by accessing Facebook's data without authorization. The court's decision clarified the boundaries of authorized access (Facebook, Inc. v. Power Ventures, Inc., 2016).
Google Inc. v. Equustek Solutions Inc.: This case involved a dispute between Google and Equustek Solutions over the removal of search results. It set a precedent for the extraterritorial reach of court orders in the context of online activities (Google Inc. v. Equustek Solutions Inc., 2017).

4.5 CHALLENGES IN ATTRIBUTION OF CYBERCRIMES

Attributing cybercrimes to specific actors and jurisdictions is challenging due to factors like anonymity and cross-border nature. International cooperation and advancements in cyber forensics are essential for addressing these challenges effectively. A collective effort among nations, law enforcement agencies, and technology experts is necessary to combat cybercrime in an increasingly interconnected world. Attributing cybercrimes to specific actors and jurisdictions is a complex task due to several challenges

Anonymity and Pseudonymity: Cybercriminals often hide behind anonymous or pseudonymous online identities, making it difficult to link actions to real individuals.
Proxy Servers and Tor: The use of proxy servers and the Tor network allows cybercriminals to obfuscate their IP addresses and geographic location.
IP Spoofing: Cybercriminals can manipulate IP addresses, making it appear as if the attack originates from a different location.
Cross-Jurisdictional Attacks: Cybercrimes can be launched from one jurisdiction but target victims in another, creating jurisdictional challenges.
Technological Complexity: Cybercriminals employ advanced techniques to cover their tracks, including using compromised systems as intermediaries.
State-Sponsored Attacks: Nation-states often engage in cybercrimes but attempt to conceal their involvement, further complicating attribution.

4.6 PRESSING NEED FOR INTERNATIONAL COOPERATION

Addressing the challenges of attribution requires international cooperation among nations, law enforcement agencies, and technology companies (Haataja, 2022):

Information Sharing: Countries must collaborate to share intelligence and cyber threat information. Initiatives like the INTERPOL Digital Crime Centre facilitate such cooperation (INTERPOL, n.d.).
Cross-Border Legal Assistance: International legal frameworks must be strengthened to allow for the efficient exchange of evidence and assistance in investigations (Council of Europe, 2001).
Bilateral Agreements: Nations can establish bilateral agreements to streamline cooperation in cybercrime investigations (UNODC, 2013).
United Nations and Regional Organizations: The United Nations and regional organizations can provide a platform for member states to cooperate in addressing cybercrime (UNODC, 2019).

4.7 ADVANCEMENTS IN CYBER FORENSICS

Advancements in cyber forensics are vital for improving attribution capabilities (Casey, 2011):

Digital Evidence Collection: Cyber forensic experts use advanced tools to collect, preserve, and analyze digital evidence, which can assist in attribution.
Machine Learning and AI: Machine learning and artificial intelligence can aid in identifying patterns and anomalies in large datasets, helping to trace cybercriminals.
Blockchain Technology: Blockchain can be used for secure and tamper-proof evidence storage, enhancing the credibility of digital evidence.
Cybersecurity Collaboration: Collaboration between cybersecurity professionals, law enforcement, and private sector organizations can improve the detection and attribution of cybercrimes.

5.0 CYBERCRIMINALS VS. CYBERSECURITY PROFESSIONALS

The competition between cybercriminals and cybersecurity professionals is a cat-and-mouse game which is relentless and dynamic. As cybercriminals develop increasingly sophisticated techniques, cybersecurity professionals respond with innovative approaches to protect systems and data. This ongoing struggle underscores the importance of constant vigilance, collaboration, and staying ahead of emerging threats in the ever-evolving digital landscape.
Cybercriminals and cybersecurity experts are engaged in a continual state of invention and adaptation. Each side employs techniques to outwit the other. Below, we explore these techniques:

5.1 TECHNIQUES EMPLOYED BY CYBERCRIMINALS:

Sophisticated Malware: Cybercriminals continually develop advanced malware, including polymorphic and fileless malware, which can evade traditional security measures (Naidoo, R., & Jacobs, C. (2023).
Zero-Day Exploits: Cybercriminals seek and exploit vulnerabilities in software and systems before they are patched. This gives them an advantage in launching successful attacks.
Social Engineering: Cybercriminals manipulate human psychology through techniques like phishing, spear-phishing, and social media manipulation to deceive individuals and gain access to systems (Sekhar Bhusal, 2021)
Ransomware Innovations: Ransomware attacks continue to evolve, with criminals using encryption and anonymous cryptocurrencies to demand ransoms (Chen, Su, & Chen, 2018).

Dark Web Collaborations: Cybercriminals leverage the anonymity of the dark web to collaborate, buy/sell tools, and exchange stolen data (Palmieri, M., Shortland, N., & McGarry, P. 2021)

5.2 TECHNIQUES EMPLOYED BY CYBERSECURITY PROFESSIONALS:

Advanced Threat Detection: Security professionals employ advanced threat detection technologies, including machine learning and artificial intelligence, to identify and mitigate threats in real-time (Alharbi et al., 2022).
Behavioral Analysis: Analyzing user and network behavior helps in identifying anomalies that may indicate a security breach or insider threat
Patch Management: Cybersecurity teams actively manage software updates and patches to mitigate vulnerabilities before they can be exploited
Cyber Threat Intelligence: Gathering and analyzing threat intelligence helps organizations proactively prepare for emerging threats and vulnerabilities
Incident Response Plans: Organizations develop incident response plans to quickly detect, contain, and mitigate cyberattacks when they occur (NIST, 2018).
Collaboration and Information Sharing: Public and private sector organizations collaborate to share threat information, enabling a collective defense against cyber threats (IC3, 2021).

5.3 PROACTIVE DEFENSE STRATEGIES:

Proactive defense strategies are crucial for preventing cyberattacks and minimizing their impact when they occur. These strategies include:

Vulnerability Management: Continuously identifying and patching vulnerabilities in systems and software
User Training and Awareness: Educating employees about cybersecurity best practices to reduce the risk of falling victim to social engineering attacks (Sekhar Bhusal, 2021)
Security by Design: Building security into software and hardware products from the outset to prevent vulnerabilities
Zero Trust Architecture: Adopting a zero-trust approach that requires verification of every user and device trying to access resources (Forrester, 2018).

5.4 THREAT INTELLIGENCE SHARING:

Threat intelligence sharing involves the exchange of information about cyber threats and vulnerabilities among organizations, government agencies, and cybersecurity experts. It plays an essential function in improving cybersecurity Manavi, M. T. (2018). Key benefits include:

Detecting threats early: Shared threat intelligence enables organizations to detect emerging threats and vulnerabilities at the beginning phases.
Contextual Information: It provides context around threats, helping organizations recognize the type and severity of of potential attacks.
Collective Defense: Collaborative efforts to share threat intelligence strengthen the collective defense against cyber threats (IC3, 2021).

5.5 ROBUST INCIDENT RESPONSE PROTOCOLS:

Effective incident response protocols are essential for minimizing the impact of cyberattacks and ensuring a swift and coordinated response. Components of a robust incident response plan include:

Preparation: Developing an incident response plan, defining roles and responsibilities, and ensuring that the organization is prepared for potential incidents (NIST, 2018).
Detection and Analysis: Monitoring systems for signs of an incident, investigating incidents when detected, and determining their scope and impact
Containment and Eradication: Taking immediate actions to contain the incident and prevent further damage, followed by efforts to eradicate the threat from the network (NIST, 2018).
Recovery and Lessons Learned: Restoring affected systems and data, analyzing the incident for lessons learned, and updating security measures to prevent future incidents (NIST, 2018).

6.0 CONCLUSION

The study highlights the growing internet, which has improved connectivity and convenience but also led to an increase in cybercrime. It explores its evolution, forms, and socio-economic impact. The study also discusses the legal aspects of cybercrime, emphasizing the need for international collaboration and advancements in cyber forensics. It also highlights the ongoing arms race between cybersecurity professionals and cybercriminals, emphasizing the importance of proactive defense strategies and robust incident response protocols. The study calls for increased public awareness, collaboration among stakeholders, and innovative technological solutions to mitigate cyber threats.

REFERENCES:

1. A Study of Cyber Crime Awareness for Prevention and its Impact. (2017). International Journal of Recent Trends in Engineering and Research, 3(10), 240–246. https://doi.org/10.23883/ijrter.2017.3480.jtu50
2. Alharbi, S., Attiah, A., & Alghazzawi, D. (2022). Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends. Sustainability, 14(23), 16002. https://doi.org/10.3390/su142316002
3. Arnell, P., & Faturoti, B. (2022). The prosecution of cybercrime – why transnational and extraterritorial jurisdiction should be resisted. International Review of Law, Computers & Technology, 37(1), 29–51. https://doi.org/10.1080/13600869.2022.2061888
4. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Retrieved from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
5. Cybercrime and the Law: Peter G. Berris, Computer Fraud and Abuse Act (CFAA) and the 116th Congress September 21, 2020
6. European Union. (2016). General Data Protection Regulation (GDPR). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj
7. Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016).
8. Forrester. (2018). The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q4 2018.
9. Google Inc. v. Equustek Solutions Inc., 137 S. Ct. 1744 (2017)
10. Gulyás, O., & Kiss, G. (2023). Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, 84–90. https://doi.org/10.1016/j.procs.2023.01.267
11. Haataja, S. (2022). Cyber operations against critical infrastructure under norms of responsible state behaviour and international law. International Journal of Law and Information Technology, 30(4), 423–443. https://doi.org/10.1093/ijlit/eaad006
12. IC3 (Internet Crime Complaint Center). (2021). 2020 Internet Crime Report. Retrieved from https://pdf.ic3.gov/2020_IC3Report.pdf
13. INTERPOL. (n.d.). Digital Crime Centre. Retrieved from https://www.interpol.int/en/Crimes/Digital-crime/Digital-crime-centre
14. Lusher, D. (2018). Organised cybercrime: Key findings from the UK and beyond. University of Surrey.

15. Manavi, M. T. (2018). Defense mechanisms against Distributed Denial of Service attacks : A survey. Computers & Electrical Engineering, 72, 26–38. https://doi.org/10.1016/j.compeleceng.2018.09.001
16. Mohsin, K. (2021). The Internet and its Opportunities for Cybercrime – Interpersonal Cybercrime. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3815973
17. Naidoo, R., & Jacobs, C. (2023). Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework. European Conference on Cyber Warfare and Security, 22(1), 311–318. https://doi.org/10.34190/eccws.22.1.1443
18. Naidoo, R., & Jacobs, C. (2023). Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework. European Conference on Cyber Warfare and Security, 22(1), 311–318. https://doi.org/10.34190/eccws.22.1.1443
19. National Institute of Standards and Technology (NIST). (2018). Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology. Special Publication 800-61 Revision 2.
20. National People's Congress. (2016). Cybersecurity Law of the People's Republic of China. Retrieved from http://www.npc.gov.cn/npc/c30834/201612/20de7ff8f7c9496b8fedf73d0f227643.shtml
21. Nershi, K., & Grossman, S. (2023). Assessing the Political Motivations Behind Ransomware Attacks. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4507111
22. Palmieri, M., Shortland, N., & McGarry, P. (2021). Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime. Computers in Human Behavior, 120, 106745. https://doi.org/10.1016/j.chb.2021.106745
23. Rybicki, P. (2023). Standardization In Combating Cybercrime Area. Cybersecurity & Cybercrime, 1(2), 109–130. https://doi.org/10.5604/01.3001.0053.8024
24. Scarfone, K., & Souppaya, M. (2006). Guide to Computer Security Log Management. National Institute of Standards and Technology (NIST)
25. Sekhar Bhusal, C. (2021). Systematic Review on Social Engineering: Hacking by Manipulating Humans. Journal of Information Security, 12(01), 104–114. https://doi.org/10.4236/jis.2021.121005
26. U.S. Department of Justice. (n.d.). Computer Crime & Intellectual Property Section (CCIPS) - Computer Crime & Intellectual Property Section (CCIPS). Retrieved from https://www.justice.gov/criminal-ccips
27. United Nations. (2004). Resolution 58/199: Creation of a global culture of cybersecurity. Retrieved from https://undocs.org/A/RES/58/199
28. United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2015).
29. UNODC. (2013). Model law against the illicit manufacturing of and trafficking in firearms, their parts and components and ammunition and explosives. Retrieved from https://www.unodc.org/documents/firearms-protocol/Model_Law_ENG_WEB.pdf
30. UNODC. (2019). Comprehensive Study on Cybercrime. Retrieved from https://www.unodc.org/unodc/en/cybercrime/study.html

Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 11 – 16 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

MATHEMATICAL MODELS AND ALGORITHMS FOR DETERMINING TIME DECISION-MAKING IN THE CYBER DEFENSE SYSTEM

Volodymyr Khoroshko[1], Mykola Brailovskyi[2], Yulia Khokhlachova[1], Natalia S. Vyshnevska[1]

[1] National Aviation University, Kyiv, Ukraine
[2]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

ABSTRACT: The article analyzes the literature, which shows the current lack of a unified approach to the comprehensive solution to the problem of synthesizing mathematical models and algorithms for determining the time of decision-making in the system of both protection and cyber protection of information. An analysis of the research stage was also carried out to determine the permissible terms of solving information-dependent problems of cyber information protection systems, taking into account the relationships between the directive terms of solving problems and the tasks of information dependencies between them, and determined the permissible intervals of processing and transmitting information over the network while ensuring the functioning of cyber information protection systems. Thus, the results that can be used in the development of effective algorithms for determining the time of decision-making based on mathematical models for decision-making support systems by the information cyber protection system, as well as for modeling complex technical systems and evaluating the effectiveness of the use of various information computing systems are given.

KEYWORDS: cyber security, cyber defense, cyber-attacks, cyber defense system, information protection, state protection, cyber space, communication channels.

INTRODUCTION

Today, the issue of cyber defense as a component of the state's information security is extremely relevant for Ukraine and the international community.

It should be borne in mind that the use of cyberspace [1, 2] expands people's ability to communicate, promotes the development of information technology, research and innovation, and stimulates the development of industry and the economy. At the same time, the advantages of modern cyberspace inevitably lead to new threats to people, society, national and international security. Along with initiatives of natural (unintentional) origin, the number and power of cyberattacks motivated by the interests of individuals, groups, states and associations of states is growing.

In addition, it should be noted that the industry of informatization and communication, information services at the present stage of society's development is one of the most developed areas of the world society. It has made information security systems more relevant for information and communication technologies and for the processing, storage and transmission of information in the global cyberspace.

The great complexity and at the same time vulnerability of these systems and the entire cyberspace on which the global, national and regional community is based functionally depend on their stable and reliable operation and protection from information influences and cyberattacks.

Therefore, it is necessary to apply various methods of counteracting them and use mathematical methods of modeling, building and analyzing models of both cyberattacks and cyber defense.

Increasing the efficiency of mathematical modeling of cyber security systems for state information can be achieved by modeling both the complex system and its subsystems. This necessity stimulates the development of models and algorithms that allow solving complex problems of system management and information flow processing.

Regarding the construction of the initial distribution of the total load of subsystems and communication channels of cyber information protection systems (CIPS) not only of the state, but also of society and individual enterprises and organizations [3]. In addition, it is necessary to determine the

tolerance interval of the solution for each task of the integrated cyber information security system, taking into account.

Setting directive deadlines for solving problems; Interrelated information processing and transmission tasks. It should be noted that cybersecurity is a priority area of state policy in the development of electronic space and the formation of the information society in Ukraine. Cyber security (cyber defense) should be understood as the protection of the state's cyberspace, which ensures the sustainable development of the information society and the communication environment, timely detection, prevention and neutralization of cyber-attacks.

The objects of cyber defense include: Communication systems of all forms of ownership that process national information resources; Critical information infrastructure facilities. Cybersecurity in Ukraine is based on the following principles: Openness, accessibility, stability and security of cyberspace, development of the Internet and responsible actions in cyberspace; Public-private interaction, broad cooperation with civil society in the field of cybersecurity and cyber defense; International cooperation to prevent the use of cyberspace for illegal purposes. Determining the tolerance intervals of the solution is carried out in several stages. At the first stage, the directive deadlines for solving problems are linked to the real-time moments defined for the IPSS tasks to the technological goals of control and management, the duration of which is determined by the period of time during which the data obtained on solving the problems of managing the facility's cybersecurity system reflect the objective reality with the specified accuracy, which allows making the right decision on managing the facility's IPSS.

The second stage involves resolving the relationship between the policy deadlines for solving cybersecurity tasks. Directive terms regulate the time of the possible start and the required completion of the task on the network and are determined by external factors. The interconnection of the directive terms of solution is carried out taking into account the information links between the tasks that are determined in the process of cybersecurity of information and the analysis of the information and logical structure of the set of tasks of managing the cybersecurity of the object.

At the third stage, taking into account the interrelationships of the directive deadlines for solving tasks and the task of information dependencies between them, the permissible intervals for processing and transmitting information over the network are determined while ensuring the functioning of IPSS.

PURPOSE OF THE WORK

The aim is to study the third stage to determine the acceptable timeframe for solving information-dependent tasks of IPSS.

THE MAIN PART

Analysis of the literature shows that there is currently no single approach to a comprehensive solution to the problem of synthesizing mathematical models and algorithms for determining the time of decision-making in the system of both information protection and cybersecurity [4,5,6]. This problem is an unresolved part of the general problem of ensuring information security in integrated systems of technical protection and cybersecurity of information.

Let us consider the formulation and solution of this problem. Given: an interconnected subset of Z_1, consisting of n tasks of information processing and transmission that involve the implementation of IPSI, requiring N subsystems and L communication channels $Z_1 = \{Z_j\}$.

The characteristics of each problem to be solved are known Z_j - the labor intensity of the solution W_j for information processing tasks and the amount of information transmitted V_j for information exchange tasks via communication channels, the directive coordination of the terms of possible start d_j^H and the required completion of the task d_j^K. The interconnection of tasks Z_1 is described by the set X_j and Y_j - respectively, the set of information inputs to the task $Z_j^{вх}$ and the set of information outputs from

Z_j^{aux}. It is required to determine for each , $Z_j \in Z_1$, $j = \overline{1,n}$ the following bounds of the admissible interval of its solution on the boundary of $t^H{}_j$ and $t^K{}_j$, that

$$\left[t_j^H, t_j^K\right] \subseteq \left[d_j^H, d_j^K\right]$$

And resolving all Z within the permissible $\left[t_j^H, t_j^K\right]$ interval requires a minimum of costs to create and operate secure component of the network's technical means.

The mathematical formulation of the problem is as follows.

Identify the following, $t^H{}_j t^K{}_j$, which reach the minimum gradually mail functionality

$$C = \min_{t_j^H, t_j^K} \left\{ \sum_{e=1}^{E} \Theta_{1e} \sum_{i=1}^{N} \sum_{j=1}^{n} \left(\frac{W_j \Pi_{ji}}{t_j^K - t_j^H} \right)^{\beta_{1e}} + \sum_{q=1}^{Q} \Theta_{2g} \sum_{i=1}^{L} \sum_{j=1}^{l} \left(\frac{N_j \eta_j}{t_j^K - t_j^H} \right)^{\beta_{2q}} \right. \quad (1)$$

With the following restrictions

$$d_j^H - t_j^H \le 0, \; j = \overline{1,n}, \quad (2)$$

$$t_j^K - d_j^K \le 0, \; j = \overline{1,n} \quad (3)$$

$$t_j^H - t_j^K \le 0, \; j = \overline{1,n} \quad (4)$$

$$t_j^K - \min_a \left\{ t_a^H \mid a \in Y \right\} \ge 0, \; j = \overline{1,n} \quad (5)$$

Constraints (2) and (3) take into account the given directive deadlines for solving problems $Z_{j\,j}$. Constraint (4) sets the conditions for a non-zero length of the tolerance interval of the solution Z_j . Constraint (5) imposes the requirement that the tolerance intervals of information-related tasks should not overlap if the j-th task is distributed for processing to the i-th subsystem, in the main case if the i-th task of information exchange of the l-th communication channel

$$\Pi_{ji} = \begin{cases} 1 \\ 0 \end{cases}$$ if the j-th task is distributed for processing to the i-th subsystem

, in the main case

And

$$\Pi_{ji} = \begin{cases} 1 \\ 0 \end{cases}$$ if the i-th task of information exchange of the l-th communication channel

, in the main case

Criterion C in (1) describes the total present value costs of creating and operating the technical means of a network designed to serve the tasks Z_1. E and $\Theta_{1e} > 0$; $\Theta_{1e} > 0$; ; $\beta_{1e} \ge 0$ $\beta_{2\,eq} \ge 0$ are constants.

Tasks (1)-(5) belong to the class of nonlinear mathematical programming problems. Known methods of nonlinear programming theory can be used to solve them. A characteristic feature of problems (1)-(5) is its large dimensionality, which is determined by the number of problems that are solved on the network and are in information interconnection. One of the effective approaches to solving nonlinear optimal problems of high dimensionality is the use of approximation methods of nonlinear programming theory [9, 10, 11], the essence of which is that the solution of the final nonlinear problem is carried out as a result of solving a sequence of problems of a simpler type, which require much less computational effort than the original problem.

Linear approximation is not always effective, as it only gives you a fairly approximate value.

Recently, scientific papers have proposed an approach to eliminate this drawback: solvable auxiliary quadratic problems. The minimization method used in [12, 13] occupies a special place among all such methods. This is due to the fact that, unlike other methods of my class, it converges from any initial approximation and does not require assumptions about the convexity of functions, does not require

strict positive definiteness of the matrix of second derivatives of Lagrange functions, and has a fairly simple structure of the auxiliary quadratic problem.

In general, the linearization method has a linear rate of convergence. However, there is a modification of the method [14,15], for which, at a considerable distance from the extremum point, the rate of ascent is linear, and at sufficient proximity to it, it is quadratic.

The peculiarity of solving quadratic problems is that they take into account only those constraints in which the violation of admissibility is the greatest [13]. This feature reduces the dimensionality of auxiliary problems and thereby reduces the computational complexity of the original nonlinear problem.

The advantages of the linearization method discussed above determine the definition of acceptable intervals in the statement of the problem (1)-(5).

For the algorithm of the linearization method to work, it is necessary to choose an initial approximation to the solution $t_j^K(0)$, $j=\overline{1,n}$ that satisfies the system of inequalities (2)-(5). Let the set of interconnected problems Z_1 be divided into R - information ranks by nr problems in the *r* -th rank, $r=\overline{1,R}$. The algorithm for the initial approximation is as follows:

Step 1 $r:=1$

Step 2 $j:=1$

Step 3 $t_j^H(0):=d_j^H+\Delta t\ t$

Step 4 $t_j^K(0):=t_j^H(0)+\Delta t$

Step 5 $j:=j+1$

Step 6 If $j\le n_r$, go to step 3, otherwise go to step 7

Step7 $r:=r+1$

Step 8 If $r\le R$, go to step 9, otherwise go to step 17

Step 9 $j:=j+n_{r-1}$

Step 10 $t_{\min}^H:=\min_a\left\{t_a^H(0)\mid a\in X_j\right\}$

Step 11 $t_j^H:=t_{\min}^H+2\Delta t$.

Step 12 If $d_i^H>t_j^H(0)$, go to Step 13, otherwise 14.

Step 13 $t_j^H(0):=d_i^H+\Delta t$

Step 14 $t_j^K(0):=t_j^H+\Delta t$

Step 15 $j:=j+1$.

Step 16 If $j\le n_r$, go to Step 10, otherwise go to Step 7.

Step 17 End.

The choice of the value Δ*t* is carried out depending on the task of the directive terms of solution d_j^H, d_j^K, $j=\overline{1,n}$.

Let $t_j(0)=\left\{t_j^H(0),t_j^K(0)\right\}$ and , $\bar{t}(0)=\left\{t_j(0)\right\}$, $j=\overline{1,n}$ be the initial approximation to the solution obtained by the algorithm described earlier, and let the accuracy of *E* , 0<E<1, be given. Consider the work of the algorithm of the linearization method [9] at the k-th step, when we have already obtained the *k-th* approximation $\delta>0$ to the solution *(k)*.

The construction of the *(k+1)*th approximation $\bar{t}(k+1)$ is carried out as follows:

1. The task of quadratic programming

$$\min_{\overline{P}}\left\{\left[\overline{C}^T(\bar{t}(k)),\overline{P}\right]+\frac{1}{2}\|\overline{P}\|^2\right\}. \qquad (6)$$

$\left[\overline{\varphi_S}(\bar{t}(k)),\overline{P}\right]+\varphi_S\left[\bar{t}(k)\right]\le 0$, $s\in S_\delta[\bar{t}(k)]$, is decided in relation to $\overline{p}$.

Here, $S_\delta(\bar{t}) = \left\{ s \in S : \overline{\varphi_S}(\bar{t}) \geq s^{\max} \in S \ \varphi_s(t) - \delta \ \right\}$, $\delta > 0$

$\Phi = \left\{ \overline{\varphi}_s(\bar{t}) \right\}$ - a set of functions such as

$$\overline{\varphi}_S = (t) \begin{cases} d_S^H - t_{S_1}^H, S = \overline{1,n}, \\ t_{S-n}^K - d_{S-n}^K, \ S = (\overline{n+1),2n}, \\ t_{S-2n}^K - t_{S-2n}^K, \ S = (\overline{2n+1),3n}, \\ t_{S-3n}^K - \min\limits_{a} \ \left\{ t_a^H \mid a \in \frac{1}{5} - 3n \right\}, \ S = (3\overline{n+1),4n}; \bar{t} = \left\{ t_j \right\}, t_j = \left\{ t_j^H, t_j^K \right\}, \ j = \overline{1,n}; \end{cases}$$

$\| \overline{p} \|$ is euclidean norm of a vector $\overline{p}$.

2. We find the first value of $S = 0,1,...,$ at which the following inequality is satisfied

$$\overline{\varphi}\left[\bar{t}(k) + \frac{1}{2^S} \overline{p}(k) \right] + N \max_{s \in S} \overline{\varphi}_S \left[t(k) + \frac{1}{2^S} \overline{p}(k) \right] \leq \overline{\varphi}\left[\bar{t}(k) \right] + N \max_{s \in S} \overline{\varphi}_S \left[\bar{t}(k) \right] - \frac{1}{2^S} \varepsilon \| \overline{p}(k) \|^2$$

If this inequality was first used in $S = S_0$, we note that

$$a(k) = 2^{-S_0}, \bar{t}(k+1) = \frac{1}{t}(k) + (k)\overline{p}(k)$$

Thus, at each step of the algorithm, the inequality is performed

$$\overline{\varphi}\left[\bar{t}(k+1) \right] + N \max_{s \in S} \overline{\varphi}_s \left[\bar{t}(k) + 1 \right] \leq \overline{\varphi}\left[\bar{t}(k) \right] + N \max_{s \in S} \overline{\varphi}_s \left[\bar{t}(k+1) \right] - a(k) \varepsilon \| \overline{p}(k) \|^2 \quad (7)$$

In [11], we show that the choice of $a(k)$ at each iteration takes a finite number of halving of the unit, and we prove the convergence of the algorithm. In particular, we prove that if the objective function and constraints are convex, the algorithm converges in a finite number of steps for any $a < 0$.

All the constraints (2)-(5) are linear, so they are convex. The above analysis of the objective function (1) shows that it is a convex function. Thus, for the problem (1)-(5), the linearization algorithm converges in a finite number of steps for any $a < 0$.

When using the linearization method, the main operation requiring significant computational costs is the solution of the quadratic problem (6). When choosing a method for solving it, it should be borne in mind that to control the correctness of the choice of the constant *N* in (7) when solving (6), it is necessary to obtain the corresponding Lagrange multipliers $\overline{U}(\overline{P})$ [11]. Therefore, when solving problem (6), it is advisable to move to a dual problem, which has the form

$$U = \left\{ \overline{U}^T \cdot G\overline{U} + h^T \overline{U} \mid \overline{U} \geq 0 \right\},$$

(8)

Where $G = A \cdot \overline{A}^T$, $\overline{h}^T = A\bar{b} + \overline{C}^T \left[\bar{t}(k) \right]$; A is amatrix, S is a string containing the components of the vector $\overline{\varphi}_S \left[\bar{t}(k) \right]$, $\bar{b}$ is a vector, $\overline{S}$ is a component equal to the value of the function $\overline{\varphi}_S \left[\bar{t}(k) \right]$.

To solve problem (8), it is advisable to use an iterative algorithm that represents some modification of the Gauss-Seidel method [16, 17]. The choice of this algorithm is due to the fact that, firstly, it is quite simple to implement on a computer, and secondly, its structure, calculation errors at individual iterations do not affect the convergence of the iterative process as a whole.

This algorithm for solving problem (8) has the following form

$$U_i^{(n+1)} = \max(0, \omega_i^{(n+1)}), \quad (9)$$

$$\omega_i^{(n+1)} = \frac{1}{g_0} \left(\sum_{j=1}^{i-1} g_{ij} U_j^{(n+1)} + h_i + \sum_{j=i+1}^{m} g_{ij} U_j^n \right), \quad (10)$$

Where U_i and the component of vector $\overline{U}$.

n - iteration number; g_{ij} - element of the matrix G;

m - the dimension of the vector $\overline{U}$.

The algorithm described is implemented in the form of a set of application programs for analyzing the effectiveness of algorithms for determining the decision-making time of cyber security systems.

CONCLUSION

Overall, these results can be used to develop effective algorithms for determining decision-making time based on mathematical models for decision support systems for cyber information security, as well as for modeling complex technical systems and evaluating the efficiency of using various information and computer systems.

In addition, the results of the study allow us to quantify the effectiveness of various computing systems and make it possible to choose the best system based on a specific practical task.

REFERENCES

1. Hryshchuk R.V. Fundamentals of cyber security / R.V. Hryshchuk, Y.G. Danik - Zhytomyr: ZhNANEU, 2016. - 636 p.

2. Brailovskyi M.M. Information security technologies / M.M. Brailovskyi, S.V. Zybin, I.V. Piskun, V.O. Khoroshko, Y.E. Khokhlachova - K: CC "Komprint", 2021. - 296 p.

3. Khoroshko V.O. Scientific tasks of synthesizing the organizational and technological scheme of creating software for computer networks with limited access / V.O. Khoroshko, N.F. Kazakova // Information Protection, No. 4, 2009.

4. Kozyura V.D. Choice of the moment for the operation of influence on information / V.D. Kozyura, I.V. Pikun, V.A. Khoroshko // Information security: human, society, state, No2, 2011.

5. Dakhno N.V. Calculation of the time of efficiency of the decision-making process in information security systems / N.V. Dakhno, E.O. Tiskina, V.A. Khoroshko // Modern Information Technologies in the Field of Security and Defense, No. 2 (5), 2011.

6. Zabolotsky V.P. Mathematical models in management / V.P. Zabolotsky, A.A. Ovodenko, A.G. Stepanov - St. Petersburg: St. Petersburg State University of Management and Administration, 2001.

7. Samarskiy A.A. Mathematical modeling: Ideas, Methods, Examples. 2nd ed. / A.A. Samarskiy, A.P. Mikhailov. - M: Fizmatlit, 2001. - 316 p.

8. Kelton V. Simulation modeling, 3rd ed: Piter, K: BHV Publishing Group, 2004. - 847 p.

9. Feldman L.P. Numerical methods in information / L.P. Feldman, A.I. Petrenko, O.A. Dmitrieva - K: BHV Publishing Group, 2006. 480 p.

10. Mathews D.G. Numerical methods / D.G. Mathews, K.D. Fink: SPb: K: Williams, 2001. - 713 p.

11. Samarskiy A.A. Numerical methods of mathematical physics / A.A. Samarskiy, A.V. Gulik - Moscow: Scientific World, 2003. 316 p.

12. Verzhbitskiy V.M. Osnovy numeral'nykh metodov [Fundamentals of numerical methods]: Vyssh.shk., 2002. - 840 p.

13. Hemming R.V. Numerical methods for scientists and engineers. 2nd ed: Nauka, 1998. 402p.

14. Tomashevsky V.M. Modeling of systems / V.M. Tomashevsky. - K: BHV Publishing Group, 2007. - 352 p.

15. Tomashevsky V.M. Solving practical problems by computer modeling / V.M.Tomashevsky, O.G.Zhdanov, O.O.Zholdakov - K: Korniychuk, 2001. - 267 p.

16. Knut D.E. The art of programming. - Vol. 2. Computed algorithms. 3rd ed: Izd.dom. "Williams, 2001. - 832 p.

17. Ryzhikov Y.I. Simulation modeling theory and technology / Y.I. Ryzhikov: Korona; M: Altex, 2004. - 384 p.

Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 17 – 20 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

HOW TO BUILD THE RESILIENCE AGAINST RUSSIAN CYBER OPERATIONS

Andro Gotsiridze[1]
[1]Business and Technology University, Tbilisi, Georgia

ABSTRACT: In the last two decades, Cyber has become the fifth domain of confrontation. Former US Secretary of State Michael Pompeo mentioned that "Huawei and other Chinese state-backed tech companies are Trojan horses for Chinese intelligence, Russia's disinformation campaigns try to turn our citizens against one another. Iranian cyberattacks plague Middle East computer Networks." Although China, Iran, and North Korea state and non-state actors have offensive cyber capabilities, Georgia remains most concerned about Russia. Cyber threats from Russia and their proxies will remain acute. Additionally, many capable hackers and profit-oriented cybercriminal groups maintain mutually beneficial relationships with the Kremlin that offer them safe haven or benefit from their activity. Cyber diplomacy activities, participation in small alliances for cyber capacity building, creating volunteer-based cyber defense units, and organizing joint governmental cyber exercises are the steps, Georgia can and should take to ensure resilience against cyber threats.

KEYWORDS: Cyber operations, cyber-attacks, resilience, cyber defense

1. INTRODUCTION

What is the geography of destructive Cyberoperations? Former US Secretary of State Michael Pompeo mentioned that "Huawei and other Chinese state-backed tech companies are Trojan horses for Chinese intelligence, Russia's disinformation campaigns try to turn our citizens against one another. Iranian cyberattacks plague Middle east computer Networks."

In the last two decades, Cyber has become the fifth domain of confrontation. The cyber operations today are an important part of any war, conflict, or confrontation. Many states use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure.

Iran's cyber capabilities may be a threat to Georgia insofar as the infrastructure of the states that Iran considers hostile to itself is placed on our territory. Also, it is entirely realistic for the Tehran-backed terrorist organizations to use the Georgian cyber network for recruiting and propaganda purposes. Cyber espionage is another tool for Iran to conducting a terrorist attack. It can be used both for determining real-time geolocation, resulting from surveillance through a cell phone company, as well as for tracking of a potential target to preparing a terrorist act.

China has been advancing its cyber-attack capabilities by integrating its military cyber-attack and espionage resources in the Strategic Support Force, which it established in 2015. Targets of China`s cyber-operations vary from national security related information to sensitive economic data and intellectual property. Furthermore, Georgia should pay significant attention to the cyber security of the national or commercial projects which involves US and other strategic partners, whom Beijing sees as adversaries.

Although China, Iran, and North Korea state and nonstate actors have offensive cyber capabilities, Georgia remains most concerned about Russia. Cyber threats from Russia and their proxies will remain acute. Additionally, many capable hackers and profit oriented cybercriminal group maintain mutually beneficial relationships with Kremlin that offer them safe haven or benefit from their activity.

2. INFORMATION AS A MAIN KEY TOOL OF CYBER OPERATIONS

The Kremlin views the information as a key domain for modern military conflict. Russia is successfully developing its offensive cyber capabilities to achieve political, economic, military goals, as well as geopolitical advantage. The Kremlin considers Georgia to be within its sphere of influence, which is why our country is a target for Russian cyberoperations. Therefore, Georgia's cyber defense policy must be "Russo centric".

How far, with what means and to what extent intentionally or unintentionally can Russia reach into information systems?

From the use of such tools as Not Petya to SolarWinds, or to Yandex and Kaspersky, what are the means of frustration?

Can the Kremlin score an unexpected success in cyber warfare if we are insufficiently prepared? When will we stop defining and start coping with the cyber challenges?

We can see how Russian cyber capabilities are becoming more and more sophisticated. Attack against Estonia, in 2007 was its political message and a punitive operation for the "bronze soldier" - aimed to provoke public unrest and mass disorder. This was the first attempt of using cyber to influence political processes. For the following year, the use of cyberoperations in the Russia-Georgia War was a well-organized complementary process to conventional military actions, aiming at creating an information vacuum, spreading disinformation, and closing the channels of international support for Georgia. Later, In the war with Ukraine in 2014-16 Russia managed to utilize the capabilities of large telecommunication companies to secretly eavesdrop on their clients, determine their locations and use this information to make psychological influence and to determine locations for artillery strikes. In addition, Russian Intelligence services for the first time, disabled part of the Ukrainian energy system by using sophisticated malware [1].

Soon, Russia's destructive cyber activities went beyond the post-Soviet area and Russian government connected hackers targeted elections in Europe and the United States. in recent years, Russian cyber enabled influence operations have been aimed at attacking to state democratic institutions and state sovereignty.

One good example for this was extensive GRU-organized cyberattack in 2019: thousands of Georgian websites—government, courts, media, NGOs —were defaced. Attackers replaced the landing pages with electronic graffiti. Images of former President Mikheil Saakashvili were saying "I'll be back!".

The attack was massive but less sophisticated. This could be an intelligence-by-attack-strategy: testing vulnerabilities, defenses, and resilience of the country; But above all it was to undermine Georgia's state sovereignty, turning citizens one against another. GRU-attack has success in terms of polarization.

We must consider that even low-tech Defacement could result quite high damage to weakly protected infrastructure.

Defacements and destructive wiper malware masquerading as ransomware - several cyber-attacks against Ukraine have made headlines before the Russia's unprovoked full-scale invasion in Ukraine, as military tensions along the Russian/Ukrainian border have escalated. Impacted Websites included the Ukrainian Foreign Ministry, the Ministry of Education and Science, and other state services.

The message "be afraid and expect the worst" was published. Even more additional malware was used to strike Ukrainian government websites and it had some similarities to the NotPetya wiper but was more capable to make additional damage [2-3].

Russia's cyber operations continue to be the serious threat for Georgia. Therefore, securing the cyber space is a priority. Compared to the cyber-attacks of 2008, the level of Russian cyber threats has grown due to several factors:

- First, Russia has not altered its aggressive cyber policy, but increased its offensive cyber capabilities even more.
- Second, Russia has been extending its cyber operations in both directions: Information-Technical and Information-Psychological.
- Third, Georgia's dependence on ICT is much higher now, which increases the scale of the expected damage.

Expected Consequences of Russian destructive cyber operations can be diverse:

- Various Levels of Disruption of Critical Infrastructure including Industry Control Systems (ICS).
- Cyber Espionage
- Cyber Attacks through sophisticated Malware
- Supply Chain Compromising
- Information Psychological Effect

On one hand, Information-technical effect could lead the country to the serious damage and/or casualties. On the second hand, the propaganda spread through cyber channels could cause the alteration of public perceptions in favor of the Kremlin, reduce pro-Western sentiments, and form or strengthen pro-Russian elite; And these might appear as a reason of possible conventional actions [4].

3. KEY STEPS TO ENSURE RESILIENCE TO CYBER THREATS IN GEORGIA

What Georgia as a small country can and should do to ensure resilience against cyber threats?
First, for Georgia it is important to participate in the development of a framework of responsible behavior in the Internet. In 2019 the US and 26 partner states signed a joint statement on the responsible behavior of states in cyberspace. The partners note that, if necessary, they will act jointly against the "irresponsible" countries in accordance with the norms of international law. Russia and China have not signed the document. It is important for Georgia to adhere to this document.
Second, Georgia should not limit itself to statements of attribution. Participation in small alliances for cyber capacity building would be strongly recommended. Annual exercises, organized by the US Department of Defense with the UK, Denmark, Estonia, and France, is based on a conception of a collective defense alliance in cyberspace and acts in accordance with the norms of responsible behavior of states in cyberspace. These Exercises enhance capabilities in terms of detecting malicious actions against critical infrastructure, synchronizing countermeasures and joint responses. Engagement in these events is very important not only for Georgia but for allies as well, as Georgia is a kind of testing ground, polygon for Russian cyber operations. These developments seem real, given the degree of Georgia's cooperation with the West in cyberspace.
Third, it is vital for Georgia to establish volunteer based cyber defense units and organize joint governmental cyber exercises.
Overwhelmed state agencies, unable to provide assistance, resource and talent constraints in the public sector, competitive private-sector salaries that the government cannot compete with, poor cyber habits and lack of awareness among the public – this is the problems landscape of Cyberdefence [5]. Establishing voluntary units similar to the Estonian model would help overcome existing obstacles.
A hypothetical case where volunteer cyber defense units might be involved would be a major cyber incident that involves declaring a state of emergency. This incident might be a disruption of Critical Infrastructure, or a major attack against government networks. In these scenarios, the state agencies may be unable to provide immediate assistance.

4. CONCLUSIONS

The cyber unit’s role is to improve readiness through trainings and exercises, and to be available when called upon for specific situations requiring additional help. Capability building and operations - two broad types of activities of units includes distributing awareness raising information, strengthening cooperation between Cyber security specialists in public and private sectors through the sharing of information, and participating in crisis management by protecting critical infrastructure.

In addition, the cyber unit might represent an opportunity for wounded warriors to reintegrate into the national defense, particularly for those unable provide service in a standard capacity. Georgia has about 1,500 wounded warriors from the 2008 Russo-Georgian War and ISAF and other international missions who cannot serve on active duty due to their health. It also can offer access to duty for those not ready to join the armed forces.

Even though the difference between our adversary and us is enormous in terms of military potential, cyber is a domain where a small country can truly resist a much more powerful aggressor. Cyber can become a successful element of an asymmetric response to destructive actions or a sort of on-going front of resistance. The response need not be devastating but it should at least be painful for Russian intelligence services and kremlin-sponsored criminal groups.

RESOURCES:

1. Janne Hakala, Jazlyn Melnychuk. Russia's strategy in Cyberspace. e NATO StratCom COE. Riga, June 2021. ISBN: 978-9934-564-90-1.
2. Joint Cybersecurity Advisory co-authored by authorities of the United States, Australia, Canada, New Zealand, and the United Kingdom. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. April 20. 2020.
3. Dr Andrew Foxall. Putin's Cyberwar: Russia's Statecraft in the Fifth Domain. Russia Studies Centre Policy Paper No. 9 (2016). The Henry Jackson Society May 2016.
4. Eneken Tikk, Kadri Kaska, Liis Vihun. International Cyber Incidents: Legal Considerations. CCD COE, 2010.
5. Cybersecurity and Infrastructure Security Agency. Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. 2022. Alert (AA22-110A).

Scientific and Practical Cyber Security Journal (SPCSJ) 7(3): 21 – 24 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

BGP (BORDER GATEWAY PROTOCOL) მარშრუტიზაციის პროტოკოლი და თანამედროვე საფრთხეები

არჩილი შენგელია[1]
[1]სოხუმის სახელმწიფო უნივერსიტეტი, თბილისი, საქართველო

ABSTRACT: It is difficult to imagine today's modern world without the Internet. The Internet has become very popular in the last 30 years and has changed many aspects of our daily existence. Our world has become highly dependent on Internet technologies and systems, and many essential services that billions of people use every day would simply not be available without Internet communications and networks. On the other hand, the almost continuous connection of billions of devices in Internet communications has led to an unhealthy interest of various types of cybercriminals in global computer networks, and for many organizations, the threat of hijacking, theft or destruction of their data and various values has potentially increased.

საკვანძო სიტყვები: *გლობალური მარშრუტიზაცია, მარშრუტიზაციის პროტოკოლების საფრთხეები და სისუსტეები*

1. შესავალი

BGP პროტოკოლი არის მარშრუტიზაციის ვექტორული პროტოკოლი, რომელიც ძირითადად გამოიყენება საშუალო და დიდი ზომის ინტერნეტ პროვაიდერების მიერ გლობალურ ქსელში მილიონობით მარშრუტიზაციის ჩანაწერის ურთიერთგაზიარებისათვის. პროტოკოლი იყენებს ეგრეთწოდებულ ავტონომიურ სისტემებს (AS – Autonomous Systems), რომელთა შიგნითაც ხდება განთავსება ხშირად ცალკეული ქვეყნისა და რეგიონის მრავალმილიონიანი ტრაფიკის დამმუშავებელი ე.წ. Border ანუ მოსაზღვრე მარშრუტიზატორებისა. თვით ავტონომიური სისტემა წარმოადგენს დამოუკიდებლად მოქმედ ქსელს,რომელიც იყენებს BGP მარშრუტიზაციის პროტოკოლს და მასში გამოცხადებული ყველა მარშრუტი ექვემდებარება საერთო წესებს. ყოველ ავტონომიურ სისტემას გააჩნია ავტონომიური სისტემის ნომერი ASN – Autonomous System Number, რომელიც ახდენს მასში წარმოდგენილი ქსელების უნიკალურობის იდენტიფიცირებას.

2. BGP პროტოკოლი და მისი სტანდარტები

საერთაშორისო სტანდარტიზაციის ორგანიზაციამ IANA – Internet Assign Numbers Authority, რომელიც მთელს მსოფლიოში ახდენს გლობალურ კოორდინირებას DNS Root, IP მისამართების დიაპაზონებისა და სხვადასხვა ინტერნეტ პროტოკოლების შემუშავება/იმპელენტაციაზე, შეიმუშავა წესების ნაკრები, რომელიც სავალდებულოა ყველა ქსელური თუ კომპიუტერული სისტემების მწარმოებელი კომპანიებისათვის [1-2]. IANA-მ მსოფლიოს 5 ძირითად რეგიონში (ARIN - კანადა, აშშ და რამოდენიმე კარიბის ზღვის კუნძული, LACNIC - ლათინური ამერიკა, RIPE NCC - ევროპა,შუა აზია და ცენტრალური აზიის ქვეყნები, APNIC - აზია, წყნარი ოკეანის ქვეყნები და AFRINIC - აფრიკის კონტინენტის ქვეყნები) ოპერირების მქონე ინტერნეტ სერვის პროვაიდერებს შესასრულებლად სავალდებულოდ დაუწესა მრავალფეროვანი ქსელური პროტოკოლებისა და მათი ნაკრებების დანერგვა/გამოყენების პარამეტრები. მათ შორის

IANA-მ 1994 წელს გამოაქვენა RFC 1654 სტანდარტის სახით დინამური მარშრუტიზაციის ვექტორული პროტოკოლი სახელწოდებით BGP – Border Gateway Protocol.
საერთასორისო ორგანიაზია IANA გასცემს ASN-ს ე.წ. RIR – Regional Internet Registries-ზე, რომელნიც თავის მხრივ სისტემის შიგნით თავიანთ ოპერირების ზონებში არეგისტრირებენ შიდა მოხმარების ავტონომიურ სისტემებს და ანიჭებენ მათ სერვისების გამომყენებელ ორგანიზაციებს. BGP პროტოკოლის ძირითადი დანიშნულება გახლავთ სწორედ AS-ს შორის კავშირის ხელმისაწვდომობაზე კონტროლი და მარშრუტების ურთიერთგაცვლა. მარშრუტები, რომელიც იცვლება სხვადასხვა ქვეყნის AS-შ შორის მუშავდება eBGP – External Border Gateway Protocol მიერ,ხოლო მარშრუტები ქვეყნის შიგნით განლაგებულ AS-ს შორის მუშავდება iBGP – Internal Border Gateway Protocol-ის მიერ [3-5].

3. BGP მოწყვლადობების ტაქსონომია

BGP პროტოკოლის სტრუქტურაში გამოვლინდა ქვემოთ ჩამოთვლილი სისუსტეები:

- **მარშრუტის გადაჭერა (Route Hijacking):** კრიტიკული სისუსტე,რომლის მეშვეობითაც შემტევ მხარეს შეუძლია გამოაცხადოს ყალბი მარშრუტები.შედეგად შესაძლოა განხორციელდეს რესურსებზე არაავტორიზირებული წვდომა,მათი მოდიფიკაცია ან სერვისების გაუმართაობა
- **მარშრუტების გაჟონვა (Route Leaks):** მარშრუტიზაციის ინფორმაციის შემთხვევითი ან განზრახ გამჟღავნება მისი დანიშნულების ფარგლებს გარეთ, რაც იწვევს მონაცემთა ნაკადში არასასურველ ცვლილებებს.
- **BGP პრეფიქსების დეაგრეგაცია (BGP Prefix Deaggregation):** ზედმეტად სპეციფიკური პრეფიქსების გავრცელება ხელს უწყობს მარშრუტიზაციის ცხრილის ინფლაციას, რაც ქსელებს დაუცველს ხდის DDos შეტევების მიმართ.
- **BGP სესიის გადაჭერა (BGP Session Hijacking):** დამნაშავეები გადაჭერილი სესიების მეშვეობით წარმოაჩენენ საკუთარ მოწოდებულ ინფორმაციას, როგორც კანონიერი მარშრუტიზატორებიდან მოწოდებულს, რითაც შესაძლებელი ხდება ქსელური ტრაფიკით მანიპულირება.
- **BGP სესიის განულება (BGP Session Reset):** სეანსების განულება მათი რეალიზებისას დამნაშავეების მიერ სპეციალურად დაშვებული შეცდომების გამო იწვევს ქსელის არასტაბილურ მუშაობას.
- **BGP პრეფიქსის მანიპულირება (BGP Prefix Manipulation):** BGP ატრიბუტებით მანიპულირებით, დამნაშავეებს შეუძლიათ ზემოქმედება მარშრუტების არჩევასა და ტრაფიკის მთლიანად გადამისამართებაზე.

4. BGP მოწყვლადობების პოტენციური შედეგები

- **მონაცემების გადაჭერა (Data Interception):** შემტევებს შეეძლებათ გადაამისამართონ ტრაფიკი საკუთარი ქსელების მიმართულებაზე, რაც აუცილებლად შექმნის საფრთხეს კონფიდენციალური ინფორმაციის გადაჭერისა.
- **მონაცემების მოდიფიკაცია (Data Modification):** შემტევებს შეეძლებათ გადასაცემი მონაცემების შიგთავსის შეცვლა, რაც აუცილებლად გამოიწვევს მონაცემების გაჟონვასა და მათზე არასანქცირებულ წვდომას.
- **მომსახურეობის დარღვევა (Service Disruption):** მარშრუტების გადაჭერა ან გაჟონვა აუცილებლად გამოიწვევს ქსელების მუშაობის ხარისხის დეგრადაციას.

- **DDos ამპლიფიკაცია (DDos Amplification):** BGP პრეფიქსების დეაგრეგაცია შესაძლოა გამოყენებულ იქნეს დამნაშავეების მიერ ქსელებზე DDos შეტევისას უფრო მეტი ზიანის მისაყენებლად.
- **სანდოობის დარღვევა (Trust Erosion):** უსაფრთხოების ხშირი დარღვევები მნიშვნელოვნად აქვეითებს ორგანიზაციების ნდობას ინტერნეტ მარშრუტიციის ინფრასტრუქტურის მიმართ,რაც პოტენციურად გამოიწვევს საერთო შემოსავლების დაქვეითებას უკმაყოფილო მომხმარებლებისა და ორგანიზაციების რაოდენობის გაზრდისას [6].

5. უარყოფითი შედეგების შერბილების სტრატეგია

BGP დაუცველობის აღმოფხვრა მოითხოვს ტექნიკური, ოპერატიული და უსაფრთხოების პოლიტიკის ზომების ერთობლიობას [7-9].

- **რესურსების საჯარო გასაღების ინფრასტრუქტურა (RPKI):** RPKI ეხმარება BGP პროტოკოლის ანონსების ავთენტურობის დადასტურებას, რაც ამცირებს მარშრუტის გატაცების რისკს.
- **მარშრუტის ფილტრაცია და დადასტურება:** ქსელის ადმინისტრატორებს შეუძლიათ მარშრუტების ფილტრების დანერგვა პოტენციურად მავნე მარშრუტების დასაბლოკად და BGP ანონსების დასადასტურებლად.
- **BGP მონიტორინგი:** BGP მარშრუტების რეგულარული მონიტორინგი საშუალებას იძლევა ქსელის უსაფრთხოების სპეციალისტებმა რეალურ დროში აღმოაჩინონ ანომალიები და პოტენციური თავდასხმები.
- **BGP პარტნიორის აუთენტიფიკაცია (Peer Authentication):** BGP სესიების დაცვა ისეთი მექანიზმებით, როგორიცაა TCP MD5 ხელმოწერები ან ტრანსპორტის ფენის უსაფრთხოება (TLS).
- **პრეფიქსის გაფილტვრა:** ქსელის უსაფრთხოების ადმინისტრატორებმა აუცილებლად უნდა გამოიყენონ ფილტრაციის ტექნიკა ზედმეტად სპეციფიკური პრეფიქსების გავრცელების თავიდან ასაცილებლად.
- **კოორდინაცია:** ქსელის ოპერატორებს, ISP-ებს და ინტერნეტის მართვის ორგანიზაციებს შორის მუდმივი კომუნიკაცია, ერთობლივი ძალისხმევა გადამწყვეტია საუკეთესო პრაქტიკის შემუშავებისა და განხორციელებისთვის BGP პროტოკოლის უსაფრთხოებისათვის [10].

6. დასკვნა

მიუხედავად იმისა, რომ BGP პროტოკოლი მხარს უჭერს თანამედროვე ინტერნეტის ფუნქციონირებას, მისი დაუცველობა ქსელს მნიშვნელოვან რისკებს აყენებს. ინტერნეტის დინამიური და ურთიერთდაკავშირებული ბუნებიდან გამომდინარე რთულია ყველა დაუცველობის აღმოფხვრა, მაგრამ ინდუსტრიის ერთობლივი ძალისხმევით, უსაფრთხოების ზომებისა და სტანდარტების განხორციელებით, შეიძლება მნიშვნელოვნად შემსუბუქდეს BGP შეტევებთან დაკავშირებული რისკები. მუდმივი სიფხიზლე, თანამშრომლობა და განვითარებადი ტექნოლოგიების მიღება სასიცოცხლოდ მნიშვნელოვანია BGP ინფრასტრუქტურის გასაძლიერებლად და გლობალური ქსელის მუდმივი სტაბილურობისა და უსაფრთხოების უზრუნველსაყოფად.

ბიბლიოგრაფია

1. S. Kent, C. Lynn and K. Seo, "Secure Border Gateway Protocol (S-BGP)," in IEEE Journal on Selected Areas in Communications, vol. 18, no. 4, pp. 582-592, April 2000, doi: 10.1109/49.839934.
2. G. Huston, M. Rossi and G. Armitage, "Securing BGP — A Literature Survey," in IEEE Communications Surveys & Tutorials, vol. 13, no. 2, pp. 199-222, Second Quarter 2011, doi: 10.1109/SURV.2011.041010.00041.
3. Iavich M., Iashvili G., Gnatyuk S., Tolbatov A., Mirtskhulava L. (2021) Efficient and Secure Digital Signature Scheme for Post Quantum Epoch. In: Lopata A., Gudonienė D., Butkienė R. (eds) Information and Software Technologies. ICIST 2021. Communications in Computer and Information Science, vol 1486. Springer, Cham. https://doi.org/10.1007/978-3-030-88304-1_15
4. M. Caesar and J. Rexford, "BGP routing policies in ISP networks," in IEEE Network, vol. 19, no. 6, pp. 5-11, Nov.-Dec. 2005, doi: 10.1109/MNET.2005.1541715.
5. B. Al-Musawi, P. Branch and G. Armitage, "BGP Anomaly Detection Techniques: A Survey," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 377-396, Firstquarter 2017, doi: 10.1109/COMST.2016.2622240.
6. Iavich, M. (2023). Post-quantum Scheme with the Novel Random Number Generator with the Corresponding Certification Method. In: Hu, Z., Wang, Y., He, M. (eds) Advances in Intelligent Systems, Computer Science and Digital Economics IV. CSDEIS 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 158. Springer, Cham. https://doi.org/10.1007/978-3-031-24475-9_7
7. Mitseva, Asya, Andriy Panchenko, and Thomas Engel. "The state of affairs in BGP security: A survey of attacks and defenses." Computer Communications 124 (2018): 45-60.
8. Butler, K., Farley, T. R., McDaniel, P., & Rexford, J. (2009). A survey of BGP security issues and solutions. Proceedings of the IEEE, 98(1), 100-122.
9. K. Butler, T. R. Farley, P. McDaniel and J. Rexford, "A Survey of BGP Security Issues and Solutions," in Proceedings of the IEEE, vol. 98, no. 1, pp. 100-122, Jan. 2010, doi: 10.1109/JPROC.2009.2034031.
10. Iavich, M., Gnatyuk, S., Iashvili, G., Odarchenko, R., Simonov, S. (2023). 5G Security Function and Its Testing Environment. In: Faure, E., Danchenko, O., Bondarenko, M., Tryus, Y., Bazilo, C., Zaspa, G. (eds) Information Technology for Education, Science, and Technics. ITEST 2022. Lecture Notes on Data Engineering and Communications Technologies, vol 178. Springer, Cham. https://doi.org/10.1007/978-3-031-35467-0_39