

MONITORING IN THE MODERN DIGITAL ERA

Nabil Ahmad Sindhar *

Faculty of Arts, Virtual University of Pakistan.

Submitted January 2, 2024; Revised January 26, 2024; Accepted January 26, 2024; Published February 20, 2024

ABSTRACT

This research seeks to thoroughly review existing scientific literature, studies, and articles concerning the dangers of monitoring in the digital era. The difficulties in fighting monitoring will be emphasized throughout the paper. Electronic devices are becoming commonplace in all demographics due to technological advancements. For both personal and professional needs, people depend on devices like computers and cell phones on a daily basis. The purpose of this study is to find solutions that shield citizens from the danger of widespread surveillance and to examine the degree of digital monitoring that people encounter. People frequently utilize a variety of devices for a variety of functions these days, such as social networking and search engines. Many people aren't aware, though, that the information they post online frequently persists in cyberspace. This report makes clear how this data is gathered and used, as well as the possible dangers to mankind in the digital era if privacy is not sufficiently protected.

Keywords: Monitoring, Digital age, Cybersecurity.

*Corresponding Author. E-mail: nabilsindhar.10@yahoo.com

INTRODUCTION

Rapid technological advancements have led to the widespread adoption of electronic devices such as mobile phones and personal computers, which have become essential to daily life. It is challenging to envision a routine without these gadgets, as their versatility makes them indispensable for both personal and professional activities—ranging from communication and learning to business management, remote troubleshooting, and transferring funds. With a single mobile phone, users can browse the internet, access social media, send and receive emails, manage finances, and stay connected with

loved ones. This remarkable progress in technology has empowered individuals to achieve more than they ever thought possible, fundamentally transforming how they live, work, and interact with their surroundings. However, it is crucial to recognize that every action taken on a digital device leaves a trace that can reveal its purpose [1]. Like other digital actions, these traces are not immediately erased; instead, big corporations retain them on servers. Although many businesses guarantee data protection, multiple data breaches have shown that these guarantees are frequently deceptive. Big

IMS is published by [AMMANIF](#) Publisher. The authors retain the copyright without restriction. This article is an open access article published under the terms and conditions of [Creative Commons Attribution 4.0 International License](#).



companies like Facebook and Yahoo have not done enough to safeguard user privacy, which begs the question: Is personal information really safe online? There isn't a clear-cut or compelling response as of now [2-5].

Throughout the twentieth century, various local and international scandals have emerged, characterized by monitoring operations targeting entire populations rather than specific individuals or groups [6]. State agencies frequently carried out these actions, either alone or in cooperation. Regretfully, it becomes clear that these cases did not prioritize the defense of fundamental freedoms and human rights. The need to prevent crimes against the state and its inhabitants, such as espionage by hostile nations or other destructive acts, was often invoked by intelligence and counterintelligence services to justify their operations [7]. While protecting the state's and its citizens' interests is clearly crucial, particularly from threats from hostile intelligence agencies and other harmful organizations, abuses of individuals' fundamental rights jeopardize the well-being of society. Democracy collapses when people's fundamental rights are disregarded, leaving nothing to defend.

This research aims to explore the concept of monitoring, its various applications by government agencies, and the systems that were in place during the 20th century to monitor individuals or groups. The study will define surveillance, discuss its purposes, and examine the different ways government entities have implemented it. Furthermore, the investigation will highlight the technologies used to track people, both individually and collectively. The findings will provide insights into the evolution of monitoring systems and their societal impact. As humanity entered the new millennium, the digital world emerged as a new frontier for technological advancement. Each individual

found their place in this digital landscape, where progress continually pushed the boundaries of comfort and convenience—ranging from the concept of smart cities, where everything is interconnected [8], to the development of artificial intelligence that assists people across various fields, along with many other cyber technologies accompanying this progress. Consequently, monitoring the population became more accessible, increasing the temptation for state agencies to surveil individuals' activities. To mitigate this risk, it is essential to establish legal frameworks and protections for citizens against not only cybercriminals but also state monitoring.

This study's main goal is to show how monitoring techniques and systems have changed in response to technology developments and to look at the instruments used by different state agencies to monitor specific people or entire populations. The study will concentrate on contemporary monitoring technologies that are made especially for monitoring. Readers will learn a great deal about the scope of the state's power to examine digital behavior by investigating these platforms.

The study's final section will give a summary of the dominant viewpoints on digital surveillance. It will make important recommendations to protect people's fundamental rights and freedoms in the digital sphere based on the reviewed material. A backward move away from democratic values and toward a potentially dystopian future would result from the failure to uphold human rights in both the physical and digital realms, or from downplaying their significance.

MONITORING IN THE TWENTIETH CENTURY

Monitoring has long been recognized as a vital tool for maintaining the safety and security of the state. Over the centuries, various technological advancements have

improved the effectiveness and efficiency of monitoring practices. Throughout history, monitoring has played an essential role in preventing criminal activities, uncovering conspiracies, and protecting state interests [10-13]. The practice of monitoring individuals and groups dates back to ancient times, when officials would read the letters of certain individuals to gain insight into their intentions. Foreign visitors were also closely monitored to ensure they did not engage in activities harmful to the state [14].

Thorough research is vital for a comprehensive understanding of any topic. A notable example is the Ministry of State Security of the German Democratic Republic, or the Stasi, which implemented an extensive covert monitoring system monitoring not just individuals but the entire population [15]. When the Stasi records were made public following the collapse of the Berlin Wall and the reunification of Germany, it became clear that agents were closely observing almost every element of residents' life, including meetings, written content, correspondence, reading materials, and even listening habits. The Stasi's mass surveillance program was one of the most comprehensive in the 20th century. Nevertheless, this surveillance was not permitted by law and was not intended to uphold human rights. Because of the Stasi's constant surveillance, almost all East Germans were aware that they were being watched, which had a big influence on their day-to-day existence. The Stasi's actions are a clear warning of the risks associated with mass surveillance systems and the significance of protecting privacy and human rights [16-18].

The twentieth century marked an era of unprecedented monitoring. While the activities of the Stasi and Project SHAMROCK are frequently highlighted as notable examples, numerous other monitoring programs were implemented

during this time. These initiatives aimed to monitor citizens closely and collect information about their activities. Examining these cases helps clarify how monitoring operated in reality and underscores the significant power wielded by the agencies involved. However, as humanity entered the twenty-first century, the landscape shifted dramatically. The rise of the digital world introduced a new realm of monitoring accessible to many. This transformation has profoundly affected people's lives, as reliance on digital technologies for communication, work, and leisure has grown.

MONITORING IN THE DIGITAL WORLD

In today's digital age, individuals encounter a wide array of technological tools and opportunities that have transformed their lives. The ability to connect with people globally and send messages from the comfort of home is now commonplace. Innovative technologies have streamlined daily activities, enabling access to countless opportunities that once seemed unattainable. As a result, the boundaries of what can be achieved have expanded, allowing individuals to explore and accomplish what was previously considered impossible.

However, with the rapid advancement of technology and increased reliance on digital platforms, the world has also seen a rise in cybercrime. Cybercriminals present a significant threat to digital security. They exploit vulnerabilities in digital infrastructure using their technical expertise and advanced equipment to execute malicious activities. From stealing personal information to launching devastating cyberattacks, the consequences of cybercrime can be extensive and damaging. It is important to note that most cybercriminals are motivated by financial gain, employing various tactics such as cyber extortion and cyber fraud [19-22].

Cyber Terrorism

Concern over terrorist organizations that have moved their operations to cyberspace after realizing the enormous potential of the digital world has grown recently. Known as cyber terrorists, these individuals move their attacks from the digital to the physical world by using a variety of digital tools and technology to cause serious and irreparable harm. Their malicious actions can disrupt governmental agencies, interrupt essential services, and damage critical infrastructure, posing a substantial threat to national security. As these cyber threats evolve, protecting against them becomes increasingly challenging. Cyber terrorists employ advanced techniques such as hacking, phishing, and social engineering to access sensitive data and exploit vulnerabilities in computer systems. They also use malware and other harmful software to cause disruption and interfere with operations. Damage to metallurgical plants, disruptions in the electric power supply, and other criminal activities are a few examples of their effects.

Cyber Espionage

Traditionally, espionage activities relied on physical methods, such as breaking into facilities to intercept or steal information. These techniques frequently required a lot of resources and were complicated. However, a new kind of espionage known as cyber espionage has surfaced as a result of the quick development of digital technology and the growing digitalization of data. Cyber espionage differs from its conventional cousin in that it does not necessitate physical access or direct communication with the target. Rather, cyber spies use their access to the digital world and their understanding of computer systems to further their operations. They monitor communication channels, obtain sensitive information, and steal private data using a variety of methods and strategies. Because cyber espionage enables spies to function in ways that traditional spies

cannot, it has grown to represent a serious threat to both national security and the private sector. The use of sophisticated hacking tools and techniques facilitates these activities, while the risk of detection remains relatively low. Consequently, governments and organizations must be more vigilant and proactive in safeguarding their information and infrastructure against cyber espionage attacks [24].

Control of State Agencies

The digital landscape has become a haven for cybercriminals operating under the auspices of state agencies. This trend is particularly alarming, as these individuals execute activities dictated by their governments. Their operations range from large-scale propaganda efforts to hacking foreign agency websites and disseminating targeted information. Although classified as cybercriminals, their actions are uniquely orchestrated, with every move in cyberspace directed by state orders. This alignment with government interests renders them a formidable threat to digital security.

As the digital world evolves, so too do the associated dangers. Consequently, the need for vigilant monitoring of online activities has become increasingly critical, enabling state agencies to respond swiftly and thwart cybercriminal operations. However, a pressing question arises: to what extent can fundamental human rights and freedoms be safeguarded while combating cybercrime?

To better understand the capabilities of monitoring systems in the digital realm and to address concerns regarding the protection of human rights and freedoms, it is essential to conduct a comprehensive analysis of the programs employed for monitoring. By exploring the technical intricacies of these systems, we can gain insights into their operations and evaluate their potential implications for individual privacy and civil liberties [25-28].

MONITORING PROGRAMS IN THE DIGITAL WORLD

PRISM

In June 2013, whistleblower Edward Snowden disclosed classified documents detailing PRISM, one of the most significant monitoring programs in history. This revelation ignited a widespread debate about the protection of personal privacy in the digital age. Many individuals expressed concern that PRISM posed a serious threat to their privacy and civil liberties. Since 2013, no new information regarding the program's operations has surfaced, despite public uproar, making it unclear whether it has been suspended, changed, or repurposed. PRISM was a program created by the National Security Agency to gather and examine data on online activities, such as emails, chat messages, and communication logs, according to Snowden's. The capacity to access and retrieve data from the servers of big businesses like Google, Facebook, and Apple was its most important feature [29]. The PRISM program remains a highly controversial and secretive government initiative capable of gathering vast amounts of personal data. Its public exposure raised serious concerns about privacy and personal liberties in the digital era, with its current status still unknown.

Tempora

The U.K. Government Communications Headquarters runs the Tempora program. Edward Snowden disclosed in 2013 that the U.S. government had been conducting the covert PRISM program, which sought to gather copious amounts of data on Internet traffic from a variety of sources, such as emails, phone conversations, browsing history, and other online activity. According to reports, the program was created to give government intelligence organizations the ability to keep an eye on and follow possible threats to national security both at home and abroad. The establishment of a program

capable of collecting and analyzing personal data has sparked significant societal debate. This discussion revolves around whether such a program is acceptable and whether its benefits outweigh the potential risks. This ongoing debate raises critical questions about the necessity of such monitoring and the ethical implications of its implementation. While some argue that these measures are essential for safety and security, others view them as violations of privacy and threats to personal freedom. A consensus requires careful consideration of all perspectives [30-33]. The European Court of Human Rights deemed the Tempora program a violation of fundamental human rights and freedoms, highlighting the importance of protecting individuals' privacy and personal data in today's digital landscape.

Echelon

Since the Cold War, the covert intelligence collection program Echelon has been in existence. The United States, Great Britain, Canada, Australia, and New Zealand work together to manage it. Its main objective is to keep an eye on and regulate communications within these nations. Emails, phone conversations, faxes, and other electronic communications, both domestic and foreign, are among the many types of information that the program intercepts and gathers. Echelon processes vast amounts of data quickly, utilizing sophisticated algorithms and analytics to identify patterns and signals of interest. Its overarching goal is to manage public communication traffic and gather relevant information for intelligence, counterterrorism, and national security operations. For many years, the existence of Echelon was kept confidential, with developers taking significant measures to protect related information. Despite these efforts, investigative journalists and whistleblowers eventually revealed the program, leading to increased public awareness of its covert operations. As its

inner workings and purpose were disclosed, many individuals expressed concern about the implications and potential consequences of its ongoing activities [34].

MUSCULAR

The Government Communications Headquarters (GCHQ) of the United Kingdom and the National Security Agency (NSA) of the United States ran the contentious cooperative monitoring operation known as MUSCULAR. It was created especially to tap into the communication channels between data centers owned by Google, Yahoo, and others in order to harvest massive volumes of data. This made it possible to access user data—such as emails, documents, images, videos, and other types of information—that was kept on the servers of these businesses. Notably, the program could retrieve data without the involvement of Yahoo or Google, raising concerns about data privacy and security. In response to this incident, both companies implemented measures to enhance their safety protocols, including stronger security algorithms, improved data encryption techniques, and better overall safety standards to protect user information from unauthorized access or breaches. MUSCULAR was kept under wraps until Edward Snowden revealed it in 2013, which caused a great deal of indignation and condemnation from civil liberties organizations and privacy activists. They maintained that the program's operations constituted a major betrayal of confidence and infringed upon users' right to privacy. The partnership between two of the most potent intelligence organizations in the world intensified the dispute and stoked concerns about the extent and global reach of government monitoring initiatives [35].

SORM

In the Russian Federation, SORM is a comprehensive program that uses a range of technological instruments and methods for

the legal monitoring and interception of communication channels. In order to maintain public safety and fight crime, it enables authorities to monitor phone calls, internet traffic, and other types of communication. Law enforcement and other approved government agencies use this program. Regarding the SORM program, the European Court of Human Rights rendered a landmark decision in 2015. The court came to the consensus conclusion that people are left vulnerable since the current circumstances in which SORM functions do not guarantee the protection of human rights. Additionally, it found that the program infringes upon the right to privacy guaranteed by Article 8 of the Convention on Human Rights [36].

Central Monitoring System

In addition to monitoring email and social media activities on sites like Facebook, LinkedIn, and Twitter, the CMS program is a surveillance system that was put into place in India and has the ability to intercept and analyze phone conversations. It's noteworthy that the application runs inside Google's system and has the ability to monitor user behavior on the search engine, including past searches. Comparing the technology to the notorious PRISM program of the U.S. National Security Agency, some analysts think its capabilities are far more broad than what is known to the public. Furthermore, a report by Human Rights Watch has raised concerns that the CMS may threaten fundamental human rights and freedoms, highlighting the potential for abuse and its implications for privacy and freedom of expression. The report calls for greater transparency and oversight to ensure that the system is used in alignment with universal human rights standards [37].

The Great Firewall

The Great Firewall, or Golden Shield Project, is a comprehensive system in China that serves dual purposes of censorship and monitoring. As one of the largest systems of

its kind, it maintains strict control over the internet within the People's Republic of China. Its primary goal is to block access to foreign websites and applications deemed sensitive or inappropriate by Chinese authorities, including those related to democracy and human rights. Additionally, the Great Firewall restricts specific search terms, further controlling the information available to the Chinese populace. It is a powerful tool used by the government to limit the dissemination of ideas considered unacceptable. The Great Firewall's monitoring feature allows authorities to detect and eliminate possible security concerns by keeping an eye on all internet traffic within China. With the help of this system, the government can continue to regulate the internet and stop the flow of information that might be detrimental to the state [38].

As highlighted in the previous section, monitoring systems play a critical role in today's digital landscape. The rise of criminal syndicates, which aim to harm individuals and institutions through illegal means, underscores the need for such monitoring. However, it is significant that the European Court of Human Rights has ruled two of these systems in violation of the Convention on Human Rights. This decision has ignited a debate regarding the legitimacy of other monitoring systems, with many questioning their justification and potential infringement on individual privacy rights. It is essential to balance the necessity of monitoring with the fundamental human right to privacy, ensuring that any implemented system complies with legal standards and human rights conventions. In our contemporary digital environment, monitoring has become a fundamental aspect of daily life. To grasp its significance and implications fully, one must explore the legal and ethical considerations that surround it. These issues have sparked active debates across various fields, including

computer science, sociology, and philosophy. Researchers aim to understand how monitoring affects privacy, security, and freedom of expression, among other fundamental rights. This understanding can guide the development of policies and practices that balance the protection of individual rights with the safety and security of society as a whole [39].

ETHICAL AND LEGAL ASPECTS OF MONITORING

The world is becoming more digital, and with this transformation, criminals are exploiting technological advancements for malicious purposes. This creates substantial challenges for state agencies, which must swiftly respond to both cybercriminals and real-world offenders. However, these challenges come with serious consequences. The ethical, legal, and security implications are vast and complex. If not properly addressed, the fallout could be far more damaging to society than the criminal activities themselves. It is essential for any democratic state to design its monitoring systems to protect fundamental human rights and freedoms rather than infringe upon them. This is crucial for fostering a healthy and prosperous society for all.

Legal Basis

The need to update legal frameworks in response to technological advancements is critical. As new technologies emerge and impact fundamental human rights, it is essential for legislators at both local and international levels to establish specialized working groups to examine these developments. Existing laws, created before the advent of specific technologies, may no longer adequately address the associated risks. To effectively protect against cybercriminals and mitigate the adverse effects of monitoring programs, it is vital to regularly revise legal frameworks to ensure the safeguarding of fundamental human rights and freedoms. This proactive approach

will help maintain societal values while keeping pace with rapid technological changes.

Transparency

According to the report, surveillance programs are frequently unknown to the general public until they are made public by journalists and whistleblowers. These programs provide the government access to the information and conversations of its residents, which raises questions about possible rights and privacy violations. As a result, the state must provide a thorough and understandable justification for these surveillance programs, including their goal, necessity, and justification. People are more inclined to believe that the government is protecting their liberties and rights online and offline when they are aware of the rationale behind such initiatives. When seen as crucial to preserving a free society, initiatives like PRISM and ECHELON can allay public fears and foster confidence that citizens' rights are being upheld. The state must also carry out these initiatives in a way that is morally righteous, compliant with the law, and appropriate for the threats they are intended to counter. Transparent reporting, accountability procedures, and routine oversight can all help achieve this. By doing this, the government can maintain individual liberty while maintaining national security, promoting a fair and democratic society [40].

Encouraging Digital Education

Governments must prioritize equipping citizens with the knowledge needed to navigate the digital world and its associated risks. To achieve this, establishing specialized courses and training programs tailored to individuals' specific needs is essential. Furthermore, promoting fundamental cybersecurity education is critical, including teaching basic principles and minimum security standards necessary for online safety. Such initiatives will empower individuals to securely navigate the

digital landscape and protect themselves against potential threats.

Protection of Digital Rights

In a time when almost every part of life is impacted by digital technology, protecting human rights online is crucial. Governments must make sure that groups working to defend these rights have the resources and assistance they need to carry out their duties. Leading these groups requires someone with specialized training, a solid grasp of digital technology, and an awareness of basic human rights. More people can be shielded from online damage and their freedom of speech and privacy can be maintained by offering the required support [41, 41].

Development of Ethical Artificial Intelligence Systems

Artificial intelligence has advanced to previously unheard-of levels in recent years. These days, businesses and monitoring organizations use AI systems extensively to gather and examine enormous volumes of data. However, fundamental human rights and individual freedoms are seriously threatened by these technologies' unrestricted gathering and storage of personal data. Governments and the international community must thus give top priority to the creation of moral AI systems that safeguard private information and preserve citizens' liberties and rights in the digital sphere.

CONCLUSION

The twenty-first century is marked by unprecedented technological progress, with innovations developing at a pace that is challenging to control. While these advancements have provided humanity with many tools to simplify daily life, they have also been misused for harmful and criminal purposes.

States and international communities have developed strategies and mechanisms to effectively combat crime in the digital realm. One such mechanism is the monitoring system, which is employed by governments

and international entities to monitor human activity online. However, the use of monitoring systems has raised numerous questions and sparked ongoing debates, particularly regarding the protection of fundamental human rights and freedoms in the digital space.

The study's conclusion offers a number of important recommendations that governments and international organizations ought to follow in order to guarantee citizens' safety and security online. These suggestions seek to forge a close link between protecting fundamental human rights and freedoms and digital security. Citizens can exercise their rights without worrying about infringement or violation by adhering to these principles and having a safe online experience.

Humanity should expect amazing innovations that will improve everyday living

as long as technology advancements continue. However, the future will be far from the safe and easy paradise imagined if these developments are accompanied by human rights abuses, whether by state actors or cybercriminals. Rather, humanity runs the risk of realizing a dystopian, gloomy, and dictatorial world.

Author(s) Contribution: data collection and editing, S. A. Nabil.

Funding: This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Ethical Approval: Not applicable

Conflict of Interest: The authors declare no potential conflict of interest.

Consent for Publication: All authors approved the manuscript for publication.

REFERENCES

1. Akduman, B., 2023. From the Great Wall to the Great Firewall: A Historical Analysis of Surveillance. *Uluslararası Sosyal Bilimler Dergisi*, 7(28). 442-469.
2. Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., Walker, R.B., 2014. After Snowden: Rethinking the impact of surveillance. *International political sociology*, 8(2). 121-144.
3. Bowden, C., 2013. The U.S. surveillance programmes and their impact on E.U. citizens' fundamental rights. 10-14.
4. Brenner, S.W., 2010. *Cybercrime: criminal threats from cyberspace*. Bloomsbury Publishing. 9-38.
5. Bruce, G., 2010. *The firm: The inside story of the Stasi*. Oxford University Press. 142-161.
6. Bump, P., 2013. The UK Tempora Program Captures Vast Amounts of Data—and Shares with N.S.A. *The Atlantic Wire* 21(06). 23.
7. Cadwalladr, C., Graham-Harrison, E., 2018. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, 17(1). 22.
8. Chandel, S., Jingji, Z., Yunnan, Y., Jingyao, S., Zhipeng, Z., 2019. The Golden Shield Project of China: A decade later—an in-depth study of the Great Firewall. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*. 111-119.
9. Clayton, R., Murdoch, S.J., Watson, R.N., 2006. Ignoring the great firewall of China. In *International Workshop on Privacy Enhancing Technologies*. Springer Berlin Heidelberg. 20-35.
10. Deibert, R., Rohozinski, R., Manchanda, A., Villeneuve, N., Walton, G., 2009. Tracking ghostnet: Investigating a cyber espionage network. 5-49.
11. Dennis, M. and Laporte, N., 2014. *The Stasi: Myth and Reality*. Routledge. 25-34.
12. Ensafi, R., Winter, P., Mueen, A., Crandall, J.R., 2015. *Analysing the great*

- firewall of China over space and time. *Proc. Priv. Enhancing Technol.*, 2015(1). 61-76.
13. Ensafi, R., Fifield, D., Winter, P., Feamster, N., Weaver, N., Paxson, V., 2015. Examining how the great firewall discovers hidden circumvention servers. In *Proceedings of the 2015 Internet Measurement Conference*. 445-458.
14. Eremia, M., Toma, L., Sanduleac, M., 2017. The smart city concept in the 21st century. *Procedia Engineering*, 181. 12-19.
15. Friedewald, M., Burgess, J.P., Čas, J., Bellanova, R., Peissl, W., 2017. *Surveillance, privacy and security*. Taylor & Francis. 15-35.
16. Gibson, B., Townes, S., Lewis, D., Bhunia, S., 2021. Vulnerability in massive API scraping: 2021 LinkedIn data breach. *International Conference on Computational Science and Computational Intelligence (CSCI)*. 777-782.
17. Gordon, S., Ford, R., 2006. On the definition and classification of cybercrime. *Journal in computer virology*, 2. 13-20.
18. Greenwald, G., MacAskill, E., 2013. N.S.A. Prism program taps into user data of Apple, Google and others. *The Guardian*, 7(6). 1-43.
19. Johnson, L.K., 2004. Congressional supervision of America's secret agencies: The experience and legacy of the Church Committee. *Public Administration Review*, 64(1). 3-14.
20. Johnson, L.K., 2008. The Church Committee investigation of 1975 and the evolution of modern intelligence accountability. *Intelligence and National Security*, 23(2). 198-225.
21. Kalathil, S., 2017. Beyond the great firewall: How China became a global information power. Washington, DC: Center for International Media Assistance. 1-6.
22. Laidler, K., 2008. *Surveillance Unlimited: How we've become the most watched people on Earth*. Cambridge. 17-25.
23. Lanchester, J., 2013. The Snowden files: Why the British public should be worried about GCHQ. *The Guardian*, 3. 1-5.
24. Lee, R. M., Assante, M. J., Conway, T. 2014. German steel mill cyber attack. *Industrial Control Systems*, 30(62). 1-15.
25. Lewis, J.A., 2002. *Assessing the risks of cyber terrorism, cyber war and other cyber threats*. Washington, DC: Center for Strategic & International Studies. 1-12.
26. Liang, G., Weller, S. R., Zhao, J., Luo, F., Dong, Z. Y. 2016. The 2015 Ukraine blackout: Implications for false data injection attacks. *IEEE transactions on power systems*, 32(4). 317-318.
27. Lichter, A., Löffler, M., Sieglöcher, S., 2015. The economic costs of mass surveillance: Insights from Stasi spying in East Germany (No. 9245). *I.Z.A. Discussion Papers*. 741-789.
28. Lyon, D., 2001. Facing the future: Seeking ethics for everyday surveillance. *Ethics and information technology*, 3. 171-180.
29. Martin, J., 2014. Mafia in Florida and Cuba: F.B.I. Surveillance of Meyer Lansky and Santo Trafficante, Jr. *The Charleston Advisor*, 16(1). 23-25.
30. Miller, C.C., 2013. Angry Over U.S. Surveillance, Tech Giants Bolster Defences. *New York Times*, 31. 1-3.
31. Minnaar, A. 2019. Cybercriminals, cyber-extortion, online blackmailers and the growth of ransomware. *Acta Criminologica: African Journal of Criminology & Victimology*, 32(2). 105-125.
32. Mombelli, I., Piodi, F., 2014. The Echelon Affair: The E.P. and the global

- interception system 1998-2002. European Parliament History Series. 9-42.
33. Nicholls, J., Kuppa, A., Le-Khac, N.A., 2021. Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape. *Ieee Access*, 9. 965-986.
 34. Owen, M.D., 2012. A review of intelligence oversight failure: N.S.A. programs that affected Americans. *Military Intelligence Professional Bulletin*. 33-34.
 35. Polyakova, A., Meserole, C., 2019. Exporting digital authoritarianism: The Russian and Chinese models. *Policy Brief, Democracy and Disorder Series*. 1-22.
 36. Ponder, J., 2006. Operation Shamrock: N.S.A.'s First Domestic Spying Program Was Revealed by Congress in 1975. *Pensito Review*.
 37. Schwarz Jr, F.A., 2007. The Church Committee and a new era of intelligence oversight. *Intelligence and National Security*, 22(2). 270- 297.
 38. Soldatov, A. and Borogan, I., 2013. Russia's surveillance state. *World Policy Journal*, 30(3). 23-30.
 39. Sports, P.O.L., 2013. N.S.A. slides explain the PRISM data-collection program. 1-6.
 40. Tawil-Souri, H., 2016. Surveillance sublime: The security state in Jerusalem. *Jerusalem Quarterly*, (68). 56.
 41. Thielman, S., 2016. Yahoo hack: 1bn accounts compromised by biggest data breach in history. *The Guardian*, 15. 1-2.
 42. Verble, J., 2014. The N.S.A. and Edward Snowden: surveillance in the 21st century. *A.C.M. Sigcas Computers and Society*, 44(3). 14-20.