Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2023, 10(6):219-227**

Review Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Cybersecurity around the world

Matthew N. O. Sadiku[1], Chandra M. M. Kotteti[2], Janet O. Sadiku[3]

[1]Department of Electrical & Computer Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]School of Computer Science and Information Systems, Northwest Missouri State University, Maryville, MO, USA
[3]Juliana King University, Houston , TX, USA
Email: sadiku@ieee.org; chandra@nwmissouri.edu; janetsadiku1@gmail.com

Abstract Security of the cyberspace is of great societal importance. Cybercrimes or cyberattacks are impacting users across the globe. A series of high-profile attacks has brought cybersecurity to the forefront of the world's attention in recent years. Cybersecurity is now a global priority as cybercrime and digital threats grow in frequency and complexity. Cybercrime has now become a business in online fraud, identity theft, and lost intellectual property, affecting millions of people around the world. This paper introduces readers to cybersecurity activities around the world.

Keywords world, cyberattacks, cybercrimes, cyber threats, cybersecurity around the world

1. Introduction

Our modern life is increasingly dependent on a multitude of interconnected and interdependent infrastructures such as computer networks and satellite systems. The Internet has been characterized as borderless and a medium through which we all can communicate. Today, the Internet has crossed national boundaries and changed the way we talk, play games, work, shop, make friends, listen music, see movies, order food, pay bill, etc. Internet has become one of the most important inventions of the 21st century [1]. Through this medium, many people have been able to access services and basic human needs such as education and commerce. Public safety, military, and security professionals depend more and more on a secure digital infrastructure including the Internet. Unfortunately, the growth rate of the Internet has outpaced cybersecurity capacity, lowering the barriers of entry for illicit activities. The unprotected system connected to the Internet is compromised within a few seconds.

With the increase in Internet usage, there has been a growing interconnectedness between society, technology, and the economy. This has caused national governments to consider how to protect their citizens and critical infrastructure from threats in the digital environment. Government and business leaders are now aware that the gains to be obtained from digital connectivity must be balanced by the need to manage cybersecurity risks and resilience in the face of cyber threats [2].

The top three most attacked industries in 2022 were education/research, government, and healthcare. Academic institutions have become a popular feeding ground for cybercriminals. Many education institutions have been ill-prepared for the unexpected shift to online learning, creating ample opportunity for hackers to infiltrate networks. The healthcare sector is so lucrative to hackers as they aim to retrieve health insurance information, medical records numbers, and social security numbers. Hackers like to target hospitals because they perceive them as short on cyber security resources [3].

2. Overview on cybersecurity

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 1, cybersecurity involves multiple issues related to people, process, and technology [4].

Figure 1: Cybersecurity involves multiple issues related to people, process, and technology [4].

A typical cyber-attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [5].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [6].

i. Availability: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
ii. Authenticity: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
iii. Integrity: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.

iv. Confidentiality: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
v. Nonrepudiation: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [7]:

i. Malware: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
ii. Phishing: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
iii. Denial-of-Service Attacks: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
iv. Social Engineering Attacks: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
v. Man-In-the-Middle Attack: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks are shown in Figure 2 [8].

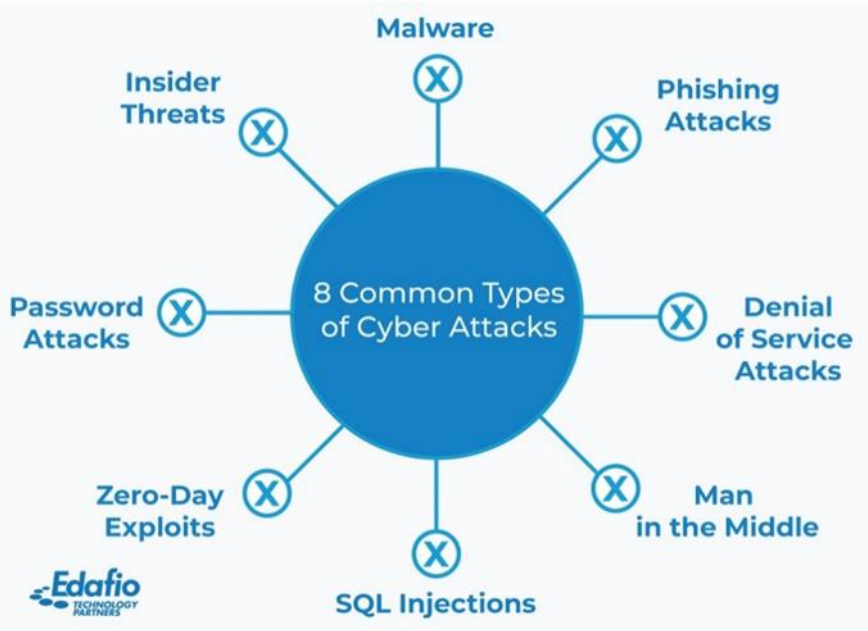

Figure 2: Common types of cyber attacks [8].

Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [9]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

3. Global cybersecurity

The top four short-term risks to the world are infectious disease, income inequality, extreme weather events, and cybersecurity. Like pandemics, income inequality, and extreme weather caused by climate change, cybersecurity is a global problem. The Global Cybersecurity Index took a look at defense capabilities in 134 countries, focusing on five factors: technical, organizational, legal, cooperation, and growth potential. Half of the countries investigated do not have a cybersecurity strategy. Figure 3 shows countries best prepared against cyberattacks [9]. Figure 4 shows the average security spending as a percentage of a company's IT budget [10].

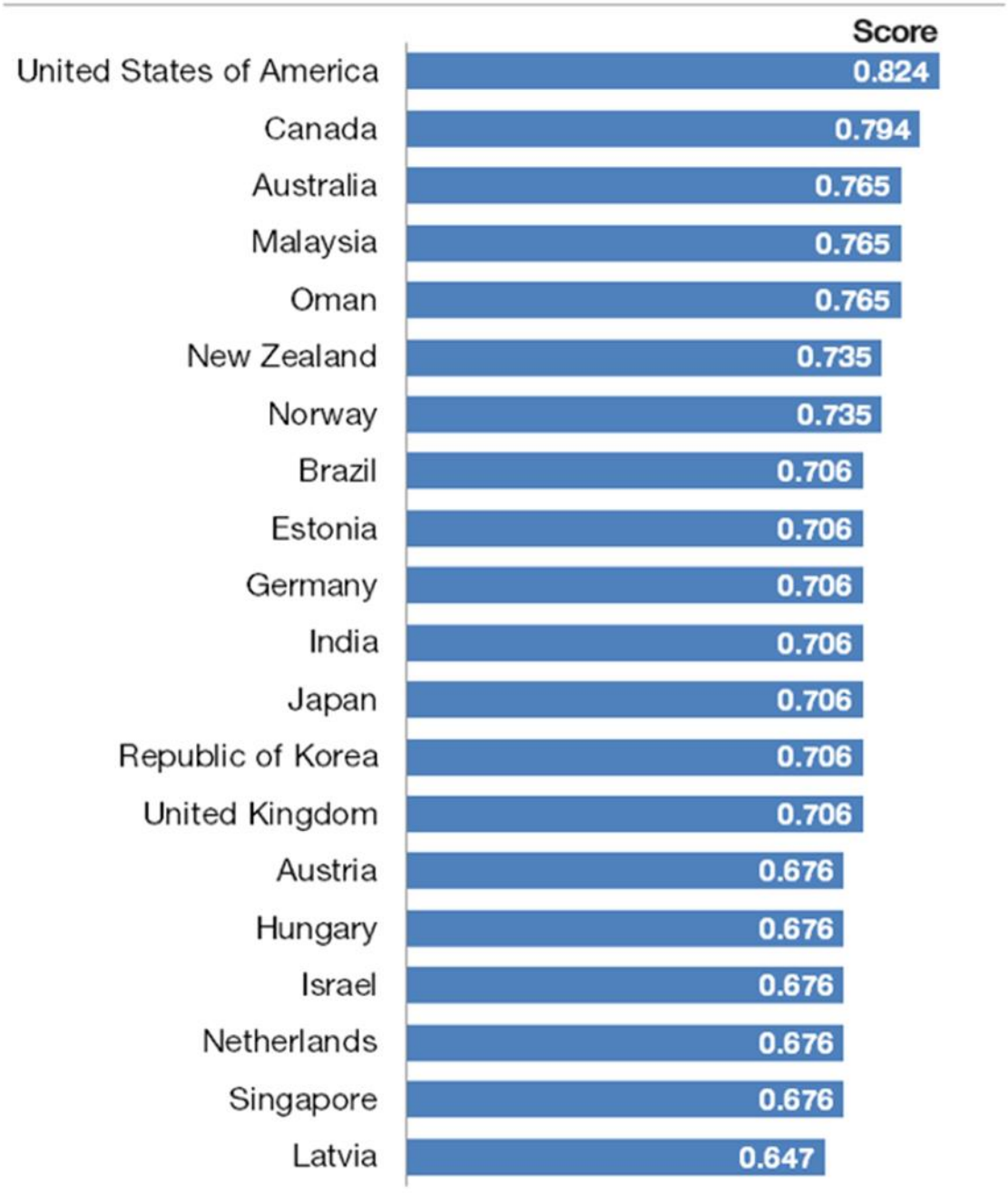

Figure 3: Countries best prepared against cyberattacks [9].

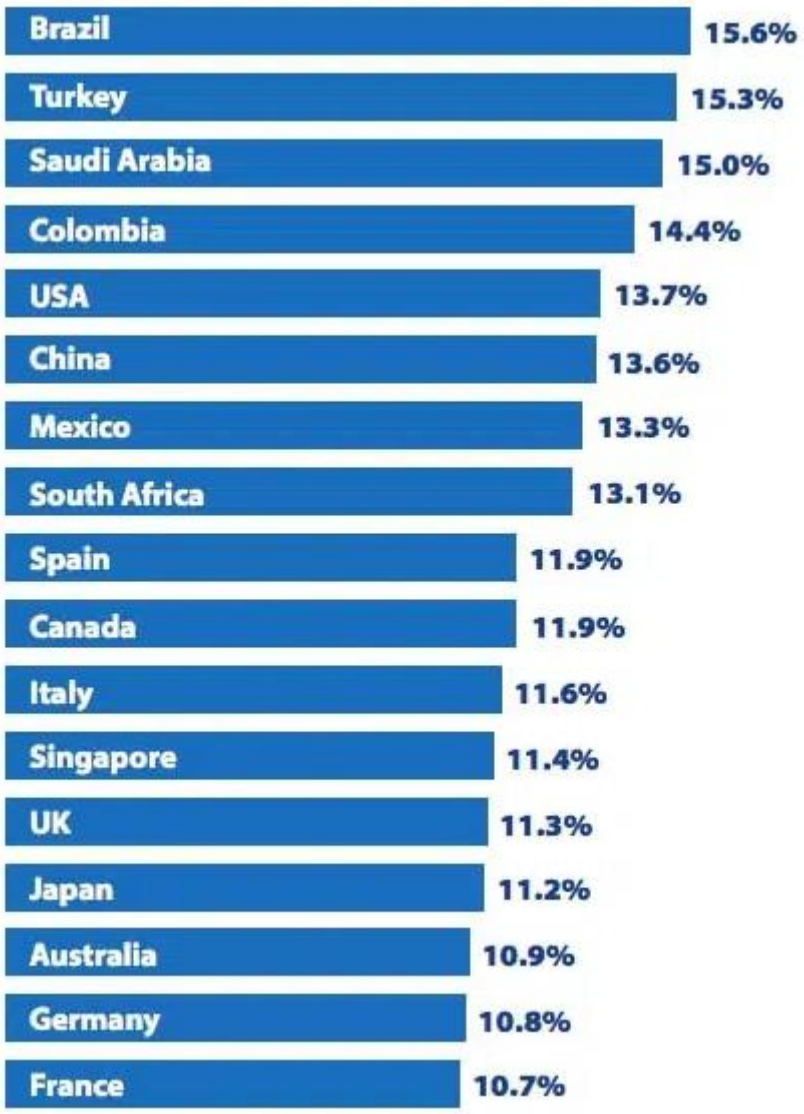

Figure 4: The average security spending as a percentage of a company's IT budget [10].

Cybersecurity is no longer just an IT issue: it is now a core area of risk for business and government. Cybercrimes or digital cyberattacks are not only harmful to people, but also affect government and organizations in negative ways. With recent nation-state attacks, it's time to stop talking and start acting. Now is the right time for business leaders to rethink their security deployments and take their cybersecurity to the next level.

Cybersecurity is a major issue for national governments and organizations. Russia's invasion of Ukraine is the latest example of the growing importance of cybersecurity. Some cybersecurity experts believe that President Putin will retaliate for the sanctions and social isolation being levied against Russia and that the retaliation will involve cyberattacks. Russian threat actors and government agencies should not be underestimated.

4. Cybersecurity in United States

The United States and other Western democracies have been under siege by foreign and domestic cyber threat actors since the existence of computer networks. From the theft of business intellectual property to military secrets, the impacts have been growing. The resulting interruptions come at a high cost in both human and financial capital. The attacks erode our technological advantages and national security [11]. The Federal Reserve Chairman Jerome Powell said that the greatest risk facing US economy is cyber risk, not inflation, not

another financial crisis, and not even a pandemic. Online security has become a major concern for national defense. The US Department of Defense (DoD) released the Cybersecurity Maturity Model Certification (CMMC), which acts as a unified standard for implementing cybersecurity across the 300,000 companies.

President Joe Biden has recently proposed a $2.1 billion allocation for the Cybersecurity Infrastructure and Security Agency (CISA). State governments are also jumping into the game, taking legislative action to demand a higher level of cybersecurity. For example, the Georgia Cyber Center is the largest single investment in a state-owned cybersecurity facility. Figure 5 shows total job openings in the US [12].

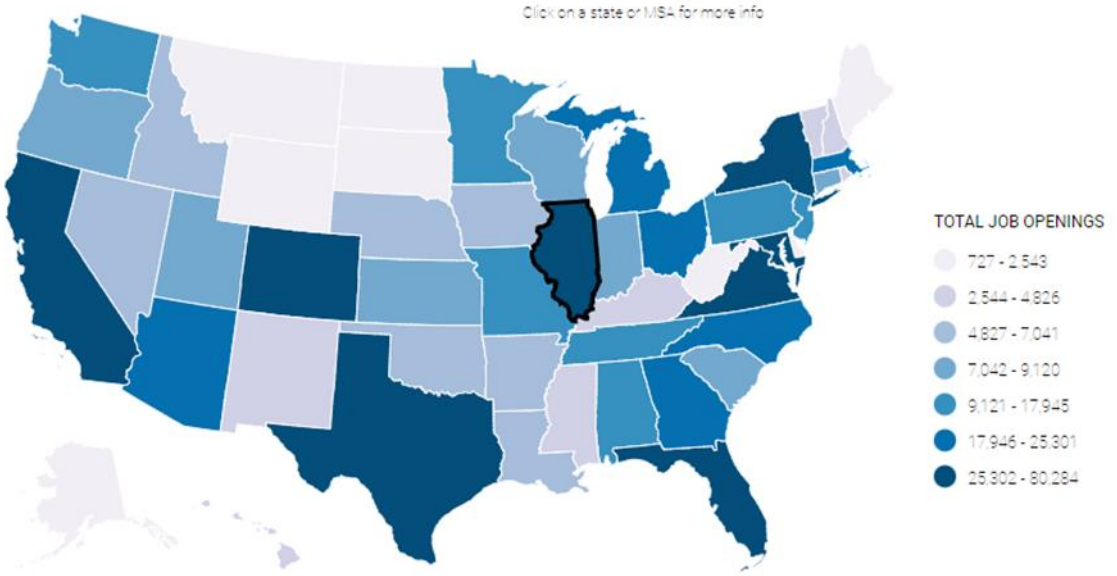

Figure 5: Total job openings in the US [12].

5. Cybersecurity in United Kingdom

Cybersecurity is top of mind for individuals and businesses in the United Kingdom.

Cybersecurity activity in London is the strongest in Europe. Launched in 2016, the United Kingdom's National Cyber Security Centre (NCSC) was created to provide a unified national response to cyberthreats and cyberattacks. This is UK's cyber security mission. The center supports the public and private sectors on matters pertaining to cybersecurity. It helps protect the UK's critical services from cyber attacks, manages major incidents, and improves the underlying security of the UK Internet. When incidents occurs, the NCSC provides effective incident response to minimize harm to the UK, helps with recovery, and learns lessons for the future [13]. In 2020, the UK government launched a new National Cyber Force (NCF) to tackle the growing problem of cybercrimes.

6. Cybersecurity in Europe

Although the European Union is often criticized for being cumbersome, it has been solid as far as cybersecurity is concerned. One of the main strengths of the European Union is that Europe can create laws that are subsequently implemented over the entire European Union. As a result, all members of the European Union will implement minimal cybersecurity standards. Countries in Central and Eastern Europe run regular drills of their cyber defenses, which have been extensively tested in recent cyberattacks [13].

The European Union Agency for Cybersecurity (ENISA) is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. It was established in 2004 to help Europe prepare for the cyber challenges of tomorrow. In partnership with regional and international organizations, ENISA hosted the first International Cybersecurity Challenge (ICC), a Cyber World Cup in June 2022. ICC is not just a competition, the ultimate aim is to assist in addressing the shortage of IT security professionals by attracting and bring together top cyber talent from all over the world [14,15].

7. Cybersecurity in Africa

The continent needs a comprehensive agenda to address its low cyber resilience and deal with the scale of cyber threats. The region's growing strategic relevance, due to its economic development and evolving digital landscape, makes it a prime target for cyberattacks. It is estimated that Africa loses more than $3.5 billion annually due to direct cyberattacks. African nations lack the strategic mindset, policy preparedness, and institutional oversight needed to address cybersecurity issues. Regional businesses do not have a comprehensive approach to cybersecurity. The region's cybersecurity industry faces shortages of homegrown capabilities and expertise. Addressing these cybersecurity challenges must be comprehensive and collaborative. It will require an active defense mindset that sees nations collaborating to defend and leverage the continent's resources [16]. The African Union (AU) has taken steps to increase collaboration on cybersecurity across the region by establishing the African Union Convention on Cyber Security. A few African countries have already defined their national cybersecurity strategy and implementation road map [17].

8. Cybersecurity in China

In the People's Republic of China (PRC), cybersecurity is recognized as a basic law. The Chinese Cybersecurity Law was enacted by the National People's Congress with the aim of increasing data protection and cybersecurity ostensibly in the interest of national security. The law is part of a wider series of laws passed by the Chinese government in an effort to strengthen national security legislation. The cybersecurity law is applicable to network operators and businesses in critical sectors [18]. China has recently expanded its cybersecurity capabilities due to concerns about the security of its national data and the need for more personal information protection in the digital economy. Currently, China probably represents the most active and persistent cyber espionage threat to US Government and private-sector networks. China is capable of launching cyberattacks that could disrupt critical infrastructure within the US. The Cybersecurity Infrastructure and Security Agency (CISA) and US partners around the world should provide timely and actionable information about the PRC cyber threats [19].

9. Cybersecurity in India

India has witnessed rapid digitalization in almost all spheres of public life. The country has over 1.15 billion phones and more than 700 million internet users, and this number is growing. Missions like Make in India and Digital India are creating a positive ripple effect across the national economy. India is progressing quickly into digital adaptation as a result of the Digital India Initiative. However, its dependence on interconnected networks and systems means that cyber security is a major challenge. Technology experts are of the opinion that as the economy becomes more digitized in India, cyberwars and cyberterrorism become bigger risks [20]. Some doubt the country's ability to protect itself from cyber attacks. India is already one of the most attacked countries in cyberspace. For example, in May 2021, the national airline Air India reported a cyber-attack in which the data of 4.5 million of its customers across the world was compromised. India has taken several legislative and organizational measures to bolster its cyber defense and effectively respond to cybercrime. India's cybersecurity budget is still inadequate. To improve the cyber security posture of the nation and its assets, a whole-of-nation approach must be followed. The nation must be a part of international cooperation efforts to promote responsible behavior in cyberspace [21].

10. Cybersecurity in Israel

Globally, three geographical regions stand out as the largest clusters of cybersecurity innovation: the San Francisco Bay Area, Greater Washington D.C., and Israel. Israel is a leading country in the middle east on cybersecurity. It may be regarded as the center of the global cybersecurity ecosystem. Tel Aviv is the heart of cybersecurity and the broader tech industry in Israel. Israel's cybersecurity business has continued to surge. Israeli companies have a crucial position in the global cybersecurity ecosystem and are readjusting to the changing landscape. For example, CyberArk is one of the largest Israeli cybersecurity firms with a market capitalization of $6.4 billion as of April 2022. Israel's cybersecurity sector amassed $8.84 billion in funding

during 2021. There is the increased awareness that cybersecurity requires a cooperative effort. As a cybersecurity powerhouse, Israeli companies are in a position to play a leadership role in that effort. Israel and the United States signed agreement in March 2022 to bolster cybersecurity cooperation [22].

11. Conclusion

As cybersecurity threats continue to evolve, companies must make a security-first commitment; they must adapt or risk getting left behind. As governments and organizations worldwide face increasing numbers of cybersecurity incidents, they must turn their focus to how to manage cybersecurity threats and deal with the aftermath of cybersecurity incidents. To take cybersecurity to the next level, many organizations are implementing a risk-based focus to cybersecurity on top of their maturity approach.

National government should encourage local players to research and develop solutions which can be used nationally and subsequently globally. Since there is no future that does not involve cyberspace, understanding how to ensure effective cybersecurity to protect our assets is critically imperative. More information about cybersecurity around the world can be found in the books in [24-27] and the following related periodicals:

i. Journal of Cybersecurity
ii. Cyber Security Journal
iii. Security Magazine
iv. United States Cybersecurity Magazine

References

[1]. J. Pande, "Introduction to cyber security (FCS)," 2017, https://www.uou.ac.in/sites/default/files/slm/Introduction-cyber-security.pdf

[2]. "National cybersecurity strategies: Lessons learned and reflections from the Americas and other regions," https://www.gp-digital.org/publication/national-cybersecurity-strategies-lessons-learned-and-reflections-from-the-americas-and-other-regions/

[3]. "Check Point Research reports a 38% increase in 2022 global cyberattacks," January 2023, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

[4]. "Eliminating the complexity in cybersecurity with artificial intelligence," https://www.wipro.com/cybersecurity/eliminating-the-complexity-in-cybersecurity-with-artificial-intelligence/

[5]. M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[6]. M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

[7]. "FCC Small Biz Cyber Planning Guide," https://transition.fcc.gov/cyber/cyberplanner.pdf

[8]. "The 8 most common cybersecurity attacks to be aware of," https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/

[9]. "Cybersecurity around the world," January 2017, Unknown Source.

[10]. "Cybersecurity supply/demand heat map," https://www.cyberseek.org/heatmap.html

[11]. Unknown Source

[12]. K. McDonald, "Three ways that global conflicts are impacting cybersecurity in the business world," March 2022, https://connect.comptia.org/blog/3-ways-global-conflicts-impact-cybersecurity-in-business

[13]. "Cyber security," https://www.gchq.gov.uk/section/mission/cyber-security#:~:text=The%20NCSC%20helps%20protect%20the,advice%20to%20citizens%20and%20organisations.

[14]. "A cold war is raging in cyberspace. Here's how countries are preparing their defenses," https://www.zdnet.com/article/a-cold-war-is-raging-in-cyberspace-heres-how-countries-are-preparing-their-defenses/

[15]. "Cyber teams from across the globe to compete in 1st International Cybersecurity Challenge," February 2022, https://www.enisa.europa.eu/news/enisa-news/cyber-teams-from-across-the-globe-to-compete-in-1st-international-cybersecurity-challenge
[16]. "Cybersecurity in Africa—A call to action," June 2023,' https://www.kearney.com/service/digital/article/-/insights/cybersecurity-in-africa-a-call-to-action
[17]. "Cybersecurity efforts in Africa need a massive boost," June 2023, https://african.business/2023/06/apo-newsfeed/cybersecurity-efforts-in-africa-need-a-massive-boost#:~:text=The%20paper%2C%20%E2%80%9CCybersecurity%20in%20Africa,Fortify%20the%20ecosystem.
[18]. "Cybersecurity law of the people's republic of China," *Wikipedia*, the free encyclopedia, https://en.wikipedia.org/wiki/Cybersecurity_Law_of_the_People%27s_Republic_of_China
[19]. "China cyber threat overview and advisories," https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/china
[20]. "Cybersecurity: How does India perform at the global stage?" https://cio.economictimes.indiatimes.com/news/digital-security/cybersecurity-how-does-india-perform-at-the-global-stage/99628852
[21]. "India's cybersecurity and its impact on the economy," August 2022, https://www.gatewayhouse.in/indias-cybersecurity-and-its-impact-on-the-economy/
[22]. D. Jaghory, "Cybersecurity in Israel: Fortifying digital defenses amid elevated risks," August 2022, https://www.etfstream.com/articles/cybersecurity-in-israel-fortifying-digital-defences-amid-elevated-risks
[23]. "Cybersecurity futures 2025: Insights and findings," February 2019, https://cltc.berkeley.edu/wp-content/uploads/2019/02/Cybersecurity-Futures-2025-Insights-and-Findings.pdf
[24]. F . Liu et al., *Science of Cyber Security.* Springer, 2018.
[25]. B. Zukis, *Digital and Cybersecurity Governance Around the World.* Now Publishers, 2022.
[26]. M. J. Carey and J. Jin, *Tribe of Hackers: Cybersecurity Advice from the Best Hackers in the World.* Wiley, 2019.
[27]. N. Kshetri, *Cybercrime and Cybersecurity in the Global South.* Palgrave Macmillan, 2013.

About the Authors

Matthew N. O. Sadiku is a professor emeritus in the Department of Electrical and Computer Engineering at Prairie View A&M University, Prairie View, Texas. He is the author of several books and papers. His areas of research interest include computational electromagnetics and computer networks. He is a life fellow of IEEE.

Chandra M. M. Kotteti received a Ph.D. degree in Electrical Engineering from Prairie View A&M University, TX, in 2020. He currently works as an Assistant Professor in the School of Computer Science and Information Systems at Northwest Missouri State University, MO. His current research interests include machine learning, deep learning, data science, and computer science.

Janet O. Sadiku holds bachelor degree in Nursing Science in 1980 at the University of Ife, now known as Obafemi Awolowo University, Nigeria and Master's degree from Juliana King University, Houston, TX in December 2022. She has worked as a nurse, educator, and church minister in Nigeria, United Kingdom, Canada, and United States. She is a co-author of some papers and books.