International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 5, Sep-Oct 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Cybersecurity in Government

Matthew N. O. Sadiku[1], Matthias Oteniya[2], Janet O. Sadiku[3]

[1,2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Federal agencies and our nation's critical infrastructure, such as energy, transportation, communications, and financial services, rely on information systems to carry out fundamental operations. These agencies are the custodians of a vast array of personal and critical data, spanning from citizen welfare to public safety and national security. Cyberattacks against government are becoming more common and have more severe impact. Cyberattacks and security incidents can disrupt critical government and public services, leading to significant economic, social, and political consequences. These jeopardize not just data, but the very health, safety, and security of the citizens the government serve. This paper explores challenges, opportunities, and action points for security leaders across the government.

KEYWORDS: *technology, security, cybersecurity, government, public sector.*

How to cite this paper: Matthew N. O. Sadiku | Matthias Oteniya | Janet O. Sadiku "Cybersecurity in Government" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-5, October 2025, pp.719-728, URL: www.ijtsrd.com/papers/ijtsrd97596.pdf

IJTSRD97596

INTRODUCTION

The rapid digital transformation across sectors is accompanied by a high level of cyber threats and risks implying cybersecurity as one of the critical concerns for individuals, organizations, and government institutions [1]. As our society becomes more dependent on digital technologies for delivering important services, the impact of cyber incidents can go beyond just data loss. In the connected world, vulnerabilities of one organization can threaten its partners, clients, and even an entire industry. Attacks can scale dramatically, moving quickly between public and private networks. With organizations relying more and more on third-party providers for software and services, and attackers targeting suppliers directly, the risk of weak links in the supply chain is increasing. In an era where digital threats are evolving at an unprecedented pace, the role of government and public sector security professionals has never been more critical. The increased use of technologies such as social media, the Internet of things, and cloud computing by government agencies has extended the sources of potential cyber risk faced by those agencies. Not just state actors but also nonstate actors today have more technical prowess, motivation, and financial resources than ever before to carry out disruptive attacks on a country's critical infrastructure.

No longer are governments content just to protect their own networks; many are beginning to take larger roles in coordinating security across public-private ecosystems. Many governments across the world are already moving in this direction. But the shifting role of government in cybersecurity is not without friction. To become effective in these new roles, governments must shift how they manage relationships, talent, and even internal operations.

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 [2]. Figure 2 shows different components of cybersecurity [3].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their

target's computer system or network. Cybercriminals or ethical hackers are modern-day digital warriors, possessing extraordinary skills and knowledge to breach even the most impregnable systems. A typical cybercriminal is shown on Figure 3 [5]. 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]. These are known as the pillars of information assurance.

- *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.
- *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.
- *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.
- *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.
- *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.

Good practices for cybersecurity in construction companies should include all of these elements.

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]:

- *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.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *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.
- *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.
- *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 or threats are shown in Figure 4 [8]. Sources of cyber threats are displayed in Figure 5 [9].

The social and financial importance of cybersecurity is increasingly being recognized by businesses, organizations, and governments. 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 [10]. 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.

CYBERSECURITY IN GOVERNMENT

The public sector comprises all government agencies, organizations, and entities, ranging from federal and state to local government. It manages critical functions such as healthcare, education, public safety, and infrastructure. Unlike the private sector, which is motivated by profit and competition, the public sector's primary objective is to provide services to its citizens and uphold public welfare. The public sector has faced multiple cyber incidents, each with its own set of vulnerabilities and outcomes. These incidents highlight the importance of having strong public sector cybersecurity policies to safeguard sensitive information and maintain the public's trust [11].

Cyberattacks are inevitable, so every government needs to develop a national incident response and recovery plan to mitigate the effects of cyber incidents and improve recovery time. Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense. In March 2023, the White House issued the *National Cybersecurity Strategy*, describing five pillars supporting the nation's cybersecurity [12]:

- Defend critical infrastructure
- Disrupt and dismantle threat actors
- Shape market forces to drive security and resilience
- Invest in a resilient future
- Forge international partnerships

The Biden-Harris Administration released the *National Cybersecurity Strategy* to secure the full benefits of a safe and secure digital ecosystem for all Americans. The government cannot function in isolation. We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, local governments, and infrastructure operators, and onto the organizations that are most capable and best-positioned to reduce risks for all of us [13]. Figure 6 is a representation of cybersecurity in government [12].

Best-in-class countries give a single entity, usually referred to as a national cybersecurity agency, the overall responsibility of defining and driving the cybersecurity agenda of the entire country. Five common elements of successful national strategies have been identified. These strategies are [14]:

- a dedicated national cybersecurity agency (NCA)
- a National Critical Infrastructure Protection program
- a national incident response and recovery plan
- defined laws pertaining to all cybercrimes
- a vibrant cybersecurity ecosystem

Fulfilling these responsibilities requires the NCA to have adequate in-house technical skills and expertise. If an NCA could only focus on one aspect of cybersecurity, it should be protecting the critical infrastructure of the country, which is typically the most attractive target for hostile state actors. Typically, an NCA works with the regulator of each critical sector to prepare criteria for what should constitute critical assets in that sector.

COMBATING CYBERSECURITY IN GOVERNMENT

Against a backdrop of escalating geopolitical and geo-economic tensions, one of the biggest threats nations face today is from state-sponsored cyber warfare. More than 100 governments have developed national cybersecurity defense strategies to combat the cybersecurity risks that their citizens, businesses, and critical infrastructure face. Best-in-class countries use data from both active and passive sources to initiate actions to combat cyberthreats facing the country. As governments develop cybersecurity laws to prevent, investigate, and take actions against cybercrimes, they should focus on the following actions [11,14-16]:

- *Robust Cybersecurity Laws:* Governments need to decide which aspects of cybersecurity they want to legislate and which aspects they want to provide guidance on without necessarily imposing any legal penalties. Public sector entities must establish a comprehensive cybersecurity framework based on recognized standards such as NIST in the US or GDPR in Europe.

- *Cooperation:* In today's digital era, cybersecurity is a major concern for both public-sector entities and private-sector partners. The transnational nature of cybercrime makes it critical for governments to participate in global forums, establish intelligence- and threat-sharing partnerships with other countries, and collaborate on preventing and investigating cybercrimes. The security of all users—and the well-being of societies and economies around the world—depends on a concentrated effort to thwart the increasingly costly and threatening cyber risks that undermine the world order. With reduced government roles, it is likely that

American companies may increase their own proactive efforts. The US government's reduced posture also affects its international partnerships. The United States has historically played a significant role within the Five Eyes intelligence community (US, UK, Australia, New Zealand, Canada), which relies on extensive information sharing.

- *Awareness*: Cybersecurity has seen the government put great effort into ensuring skills in the field and awareness across the population and territory. Without help from citizens, professionals, and private-sector organizations, a government alone will not have the scale to improve the overall cybersecurity of its entire country. Best-in-class governments enable cybersecurity companies to thrive, develop the capabilities of cybersecurity professionals, and raise citizens' cyber awareness. They connect with students when they are young and encourage them to pursue a career in cybersecurity. For example, the United Kingdom government runs the Cyber Aware campaign to help individuals, families, and smaller organizations by providing simple guides on topics. It also runs accreditation programs to certify cybersecurity consultancies, training providers, and professionals in the country.
- *Employee Training:* When working in the public sector, where dealing with sensitive citizen information is a regular task, it is essential to have well-trained employees who follow cybersecurity best practices. The training programs should cover topics such as identifying phishing attempts, secure handling of confidential data, and compliance with internal security policies. Figure 7 shows some technicians using diagnostic tools to check car systems and find possible cybersecurity risks [17].
- *Risk Assessment:* Public sector organizations must regularly evaluate their cybersecurity risks in light of the constantly evolving nature of threats and the changing landscape of IT infrastructure. This process should involve identifying valuable assets, assessing vulnerabilities, and evaluating the potential impact of cyber threats. Effective risk management also requires creating a prioritized plan to address the identified risks. Regular security audits are crucial for public sector organizations to ensure the effectiveness of their cybersecurity measures and compliance with relevant laws and regulations.
- *Strict Access:* In the public sector, where sensitive information is handled, it is essential to implement strict access controls and robust user authentication mechanisms. This includes role-based access controls to ensure employees are given access only to the information necessary for their job functions. Network access control products enforce security policy by granting only policy-compliant devices access to network assets. They handle authentication and authorization functions and can control the data that specific users access, ensuring that users meet a certain safety standard before they can access any information. Additionally, multi-factor authentication should add an extra layer of security when accessing critical systems, especially if agencies utilize Internet of things (IoT) devices or other endpoints.
- *Intrusion Detection and Prevention Systems.* Known as IDS and IPS tools, these can help IT staff identify and protect their wired and wireless networks against several security threat types. IDS tools monitor and detect suspicious activity, while IPS tools perform active, in-line monitoring and can prevent attacks by known and unknown sources. Both IDS and IPS solutions detect threat activity in the form of malware, spyware, viruses, worms, and other attack types, as well as threats posed by policy violations. They can identify and classify attack types, improving overall computer security.

BENEFITS

The public sector is just one industry that benefits from a robust and rigid cybersecurity program. As governments roll out large-scale digital initiatives that benefit citizens, balancing cybersecurity concerns with convenience remains a top priority. Ensuring the security of cyberspace is fundamental to protecting America's national security and promoting the prosperity of the American people. The newest cyber tools use behavior analytics to stop bad actors in their tracks and prevent intellectual property and sensitive data from falling into the wrong hands. Other benefits include the following [18]:

- *Human Capital:* Greater collaboration in an ecosystem results in more and varied types of systems, data, and tools being used within an organization. That requires technology talent with broader skills than most single organizations can provide. Fortunately, ecosystems can also help governments gain access to the right talent with the right skills
- *Training:* Cybersecurity training initiatives in the United States have focused on higher education. The US Department of Homeland Security offers grants and partnership opportunities focused on

cybersecurity for both K-12 schools and institutes of higher education. US-based Cybersecurity Talent Initiative—a partnership between federal agencies, academia, and the private sector—chooses students drawn from relevant fields for two-year placements with federal agencies that have cybersecurity needs. Israel offers cybersecurity training at all levels of its educational system, starting in middle school and continuing through graduate school, where students can earn PhDs in cybersecurity. Figure 8 shows some students with technical talent, moral integrity, and leadership skill [19].

- *Competitions:* Governments use competitions to take advantage of cybersecurity capabilities outside their own workforces. One popular model is the bug bounty program, in which governments challenge hackers to find vulnerabilities in their networks, and reward them for each bug they find.
- *Cyber Crime Prevention for Women and Children:* The India's Cyber Crime Prevention for Women and Children (CCPWC) initiative aims to combat cybercrimes targeting vulnerable populations, specifically women and children.
- *Securing Healthcare:* Healthcare is just one of our 16 critical infrastructure sectors that is vulnerable to cyberattacks. In 2015, NSF-funded scientists at the healthcare security company Virta Labs introduced a cybersecurity system that protects vulnerable medical devices without requiring software installation or upgrades. The system can detect malware and anomalies on devices without disrupting patient care. Its developers are credited as pioneers in the field of medical device cybersecurity.

CHALLENGES

The challenges of securing sensitive data and critical systems have never been greater. While government organizations are aware of the risks inherent in critical infrastructure attacks, many are not well prepared. The distinction between the private and public sector's role in cybersecurity is ever changing. These sectors are interdependent, each contributing to national security and cyber defense. While both public and private sectors face cybersecurity challenges, the public sector tends to be more exposed in this ever-evolving threat landscape. Our government's approach to cybersecurity faces a period of uncertainty. Other challenges include [15,20]:

- *Skills Gaps:* Many critical infrastructure operators, especially smaller municipalities, lack the expertise or funding to implement comprehensive resilience strategies. The public sector is not immune to the global skills shortage in cybersecurity. The public sector tends to lose talent to the private sector, creating a vacuum of knowledge and expertise.
- *Automation:* In many countries, the public sector is constantly under pressure for being too big. By investing in security automation, public sector organizations can help improve operational efficiency, reduce manual errors and optimize resource utilization, ultimately enhancing overall productivity and effectiveness. For the public sector, enhanced security through automation is less a choice and more an imperative for multiple reasons.
- *Regulatory Compliance:* In response to increasing cyber threats, federal governments have implemented various regulations and compliance standards to safeguard public sector information systems and data. While challenging, regulatory mandates can drive investment in cyber security and resilience practices. To ensure compliance, sector committees typically audit sectoral entities on a periodic basis and may choose to apply incentives or penalties.
- *Standards:* To meet the unique needs of specific sectors, regulators in some countries may recommend additional sector-specific cybersecurity standards as well. Stronger cybersecurity standards must be built in at all levels of an agency's planning.
- *Sophistication of Threats:* Attackers are employing more advanced tactics, such as ransomware, Distributed Denial of Service (DDoS) and supply chain attacks, that target vulnerabilities unique to industrial systems.
- *Legacy Systems:* Public sector entities face a challenging environment when it comes to cybersecurity. They often operate with aging infrastructure and outdated systems, vulnerable to cyberattacks. Outdated legacy systems and insufficient funding for modernization efforts have hindered the ability of many government agencies to implement comprehensive resilience programs.
- *Government Limitations:* The US government cannot be the cyber defense force for all organizations. They are not structured to provide thorough investigations for all breaches or supply chain attacks. Direct response typically occurs when critical infrastructure is threatened. These critical industries remain a government priority,

even with budget and staff cuts, due to their impact on the health, safety and welfare of millions of Americans.

CONCLUSION

Cyberattacks have the power to bring our daily lives to a screeching halt. Nearly everything we use to work, play, and live relies on computer systems that are vulnerable to attacks. Federal agency information systems and national critical infrastructure are vulnerable to cyberattacks. As government agencies collect, store, and manage vast amounts of sensitive information, including citizen records, financial data and national security intelligence, cybersecurity is integral to public safety and national security. Countries have taken a wide variety of approaches to cybersecurity defense. These approaches vary even among leading countries but typically reflect a country's political philosophy, federal government structure, maturity of cyber capabilities, and overall cybersecurity aspirations. More information about cybersecurity in government can be found in the books in [21-26].

REFERENCES

[1] A. Priya, "List of cybersecurity initiatives by the government of India," October 2024, https://securityboulevard.com/2024/10/list-of-cybersecurity-initiatives-by-the-government-of-india/

[2] P. Singh, "A layered approach to cybersecurity: People, processes, and technology- explored & explained," July 2021, https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces

[3] M. Loi et al., "Cybersecurity in health – disentangling value tensions," *Journal of Information, Communication and Ethics in Society,* June 2019, https://www.emerald.com/insight/content/doi/10.1108/JICES-12-2018-0095/full/html

[4] M. Adams, "Unlocking the benefits of ethical hacking: The importance of ethical hackers in cybersecurity," April 2023, https://www.businesstechweekly.com/cybersecurity/network-security/ethical-hacking/

[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] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports,* vol. 7, November 2021, https://www.sciencedirect.com/science/article/pii/S2352484721007289

[10] Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation,* University of Toledo, 2015.

[11] "Guiding governance: Cybersecurity in the public sector," https://www.upguard.com/blog/cybersecurity-in-the-public-sector

[12] "Cybersecurity: Launching and implementing the national cybersecurity strategy," June 2023, https://www.gao.gov/products/gao-23-106826

[13] "The National Cybersecurity Strategy," https://bidenwhitehouse.archives.gov/oncd/national-cybersecurity-strategy/

[14] "Follow the leaders: How governments can combat intensifying cybersecurity risks," September 2020, https://www.mckinsey.com/industries/public-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks

[15] A. Berglas, "The future of U.S. cyber security depends on the private sector," September 2025, https://www.forbes.com/councils/forbestechcouncil/2025/09/17/the-future-of-us-cyber-security-depends-on-the-private-sector/

[16] "The importance of cyber technologies in government," September 2020, https://nitaac.nih.gov/resources/articles/importance-cyber-technologies-government

[17] "Cybersecurity: Safeguarding America's digital infrastructure," https://www.nsf.gov/impacts/cybersecurity

[18] "Government's broader role in cyber," March 2021, https://www.deloitte.com/us/en/insights/industry/government-public-sector-services/government-trends/2021/cybersecurity-and-the-government.html

[19] "Cybersecurity best practices," https://www.cisa.gov/topics/cybersecurity-best-practices

[20] "Government and public sector," 2025, https://kpmg.com/xx/en/our-insights/ai-and-technology/cybersecurity-considerations-2025/government-public-sector.html

[21] M. N. O. Sadiku, *Cybersecurity and Its Applications*. Moldova, Europe: Lambert Academic Publishing, 2023.

[22] D. V. Puyvelde and A. F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Polity, 2nd Edition, 2024.

[23] M. Erbschloe, *Threat Level Red: Cybersecurity Research Programs of the U.S. Government.* Boca Raton, FL: CRC Press, 2017.

[24] D. F. Norris, L. K. Mateczun, and R. F. Forno, *Cybersecurity and Local Government.* Wiley, 2022.

[25] G. Powers (ed.), *U.S. National Cybersecurity: Strategic Challenges and Opportunities*. Nova Science Publishers, 2014.

[26] J. Rollins, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations.* DIANE Publishing Company, 2009.

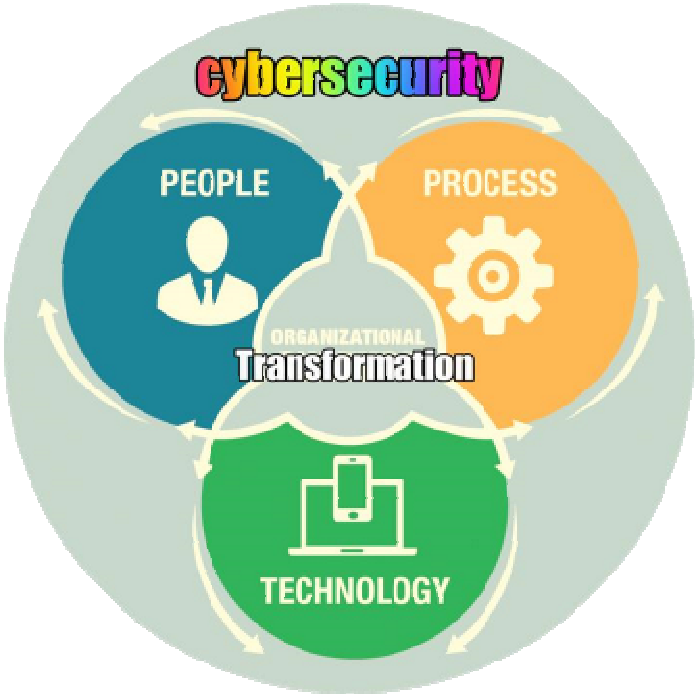

Figure 1 Cybersecurity involves multiple issues related to people, process, and technology [2].

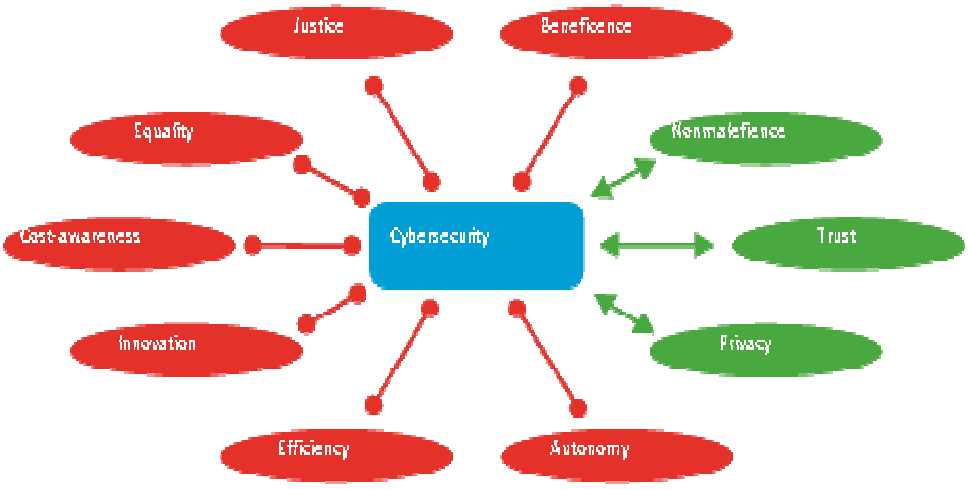

Figure 2 Different components of cybersecurity [3].(Green: supportive; red: in tension)

Figure 3 A typical cybercriminal [4].

Figure 4 Common types of cybersecurity threats [8].

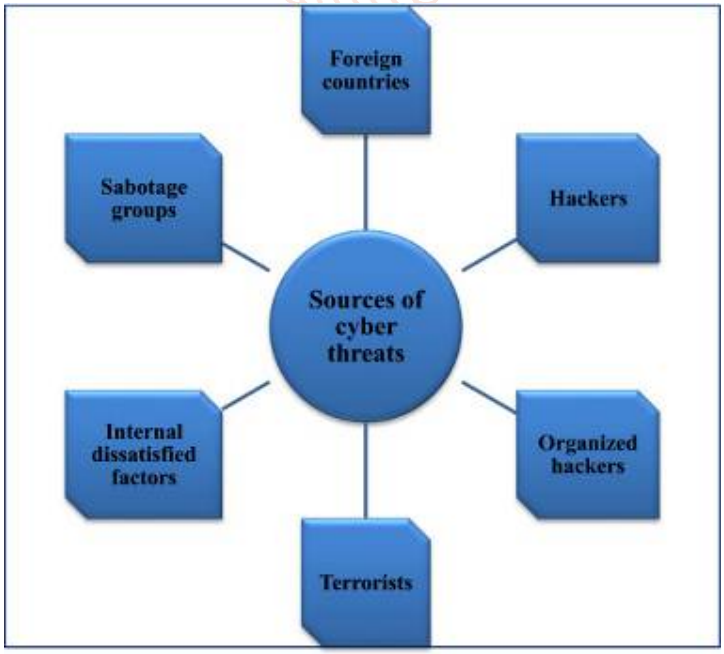

Figure 5 Sources of cyber threats [9].

Source: VideoFlow/stock.adobe.com.

Figure 6 A representation of cybersecurity in government [12].

Figure 7 Some technicians use diagnostic tools to check car systems and find possible cybersecurity risks [17].

Figure 8 Some students with technical talent, moral integrity, and leadership skill [19].