

Cybersecurity Challenges and Invasion of Privacy: An In-Depth Analysis

Eseyin Joseph B.
ICT Directorate
University of Jos,
Jos Nigeria

Ogbonna Chukwudi N.
Veritas University
Bwari FCT
Abuja Nigeria

Falana Moses O.
Veritas University
Bwari FCT
Abuja Nigeria

Betty Omowumi Bello
Veritas University
Bwari FCT
Abuja Nigeria

Abstract:

As modern warfare increasingly relies on digital technologies and interconnected systems, the vulnerability of the networks to cyber threats becomes a paramount concern. This paper delves into the specific challenges faced by the organisations in safeguarding sensitive information, maintaining operational security, and protecting the privacy of its personnel. The analysis encompasses the current state of cybersecurity infrastructure, potential threats, and recommendations for bolstering defense against cyber-attacks. The modern landscape of warfare has evolved to heavily depend on digital technologies and interconnected systems. This includes communication networks, data storage, and various electronic systems that are integral to defense operations. The vulnerability of the networks to cyber threats is identified as a significant and pressing concern. This vulnerability stems from the reliance on interconnected systems and the digitalization of their operations. Therefore, the paper delves specifically into the challenges faced organisations in three critical areas: Safeguarding Sensitive Information: The protection of classified and sensitive data from unauthorized access or manipulation is crucial for maintaining national security, operational Security: This pertains to ensuring the confidentiality, integrity, and availability of information crucial for defense operations; breaches in operational security could compromise mission success and protecting Privacy of Personnel: Personnel are likely to have personal information that, if compromised, could lead to privacy invasion. This includes both online and offline aspects of personal privacy. Consequently, the paper

provides an in-depth analysis of the current state of cybersecurity infrastructure within the organization which involves examining existing protocols, technologies, and practices in place for mitigating cyber threats and safeguarding sensitive information. Potential cyber threats would be discussed, ranging from traditional hacking attempts to more sophisticated cyber-espionage activities which cover both internal and external threats that pose risks to security and privacy. The paper proposes recommendations for enhancing defense against cyber-attacks. This include suggestions for technological upgrades, policy changes, personnel training, or collaboration with international partners for sharing intelligence and best practices. In summary, the paper provide a comprehensive examination of the challenges faced by organisations in the realm of cybersecurity and privacy invasion. And offers insights into the current state of affairs, potential threats, and practical recommendations to strengthen defense in the face of evolving cyber threats.

Keywords: Cybersecurity, Invasion of Privacy, , National Security, Cyber Threats, Insider Threats, Advanced Persistent Threats

Introduction

1.1 Background

The rapid evolution of technology has revolutionized the landscape of modern warfare, with cyberspace becoming a contested domain. Organisations, like many others globally, is grappling with the challenges posed by cyber threats that target critical information

systems, jeopardizing national security and the privacy of military personnel.

The rapid evolution of technology has brought about a paradigm shift in the nature of warfare, transforming traditional battlegrounds into complex and interconnected domains that extend beyond physical borders. One significant arena in this evolution is cyberspace, where nations engage in a constant struggle to protect their critical information systems and gain a strategic advantage. This transformation has profound implications for the Organisations, as it grapples with the challenges posed by cyber threats.

Cyberspace as a Contested Domain: The concept of warfare has expanded beyond conventional land, air, and sea domains to include cyberspace. In this virtual realm, state and non-state actors leverage sophisticated tools and techniques to conduct cyber operations, including espionage, sabotage, and influence campaigns. The boundary between military and civilian targets has blurred, making it imperative for nations to defend not only military networks but also critical infrastructure and civilian systems.

Cyber Threats to Critical Information Systems: The Organisations, like its counterparts worldwide, faces a multitude of cyber threats that target critical information systems. These threats encompass a range of malicious activities, such as hacking, malware attacks, and denial-of-service incidents. Adversaries may seek to compromise military communications, disrupt command and control systems, or gain unauthorized access to classified information. The consequences of successful cyberattacks can be severe, jeopardizing national security and potentially undermining the effectiveness of military operations.

National Security Implications: The interconnectedness of modern military infrastructure means that a breach in one area can have cascading effects across the entire defense apparatus. Cyber attacks can compromise the confidentiality, integrity, and availability of sensitive information, leading to a loss of strategic advantage and potentially endangering the lives of military personnel. Ensuring the resilience of critical information systems has become a crucial aspect of national security.

Privacy Concerns for Military Personnel: Beyond the strategic and operational aspects, cyber threats also pose a direct threat to the privacy of military personnel. Personal information, including service records, contact details, and even sensitive personal

data, may be targeted by adversaries. The compromise of such information not only undermines the well-being and safety of military personnel but can also be exploited for social engineering or psychological warfare purposes.

Adapting to the Changing Landscape: The Organisations, like other armed forces globally, must continually adapt to the changing landscape of modern warfare. This involves not only investing in advanced cybersecurity technologies but also developing robust policies, training programs, and collaborative efforts with the private sector and international partners. Building a cyber-resilient military requires a holistic approach that addresses technical, organizational, and human factors.

In conclusion, the evolution of technology has ushered in a new era of warfare, with cyberspace playing a pivotal role. The Organisations, in common with other nations, faces the challenge of securing its critical information systems against a diverse range of cyber threats. Successfully navigating this landscape requires a comprehensive and adaptive approach that recognizes the interconnected nature of modern conflict in both the physical and virtual realms

1.2 Objectives This paper aims to:

Assess the current state of cybersecurity infrastructure in the Organisations.

Identify specific cyber threats faced by the military, including potential adversaries and attack vectors.

Examine the implications of cybersecurity breaches on national security and invasion of privacy.

Propose recommendations and strategies to enhance cybersecurity measures within the Organisations. The cybersecurity infrastructure in the Organisations, like many other establishments globally, faces a constantly evolving threat landscape. The state of cybersecurity in any society is crucial as it directly impacts national security and defense capabilities.

Specific Cyber Threats Faced by the Military:

State-sponsored Attacks: Nigeria, being a significant player in Africa, may face cyber threats from other nation-states seeking to gain a strategic advantage or gather intelligence.

Hackivism: Activist groups may target the military infrastructure to express their grievances or protest against government policies.

Insider Threats: Malicious activities originating from within the military or defense contractors can pose a severe risk, including data theft, sabotage, or espionage.

Phishing and Social Engineering: Cybercriminals often use deceptive tactics to trick military personnel into revealing sensitive information or clicking on malicious links.

Infrastructure Vulnerabilities: Outdated or poorly configured systems within the military's network may be exploited by cyber attackers.

Ransomware: The military could be a target for ransomware attacks, where critical systems are encrypted until a ransom is paid.

Potential Adversaries and Attack Vectors:

Adversaries could include rival nation-states, terrorist organizations, hacktivists, and cybercriminals. Attack vectors may exploit weaknesses in network architecture, software vulnerabilities, social engineering, or supply chain compromises.

Implications of Cybersecurity Breaches on National Security and Invasion of Privacy:

Compromised Military Operations: Cyber breaches can disrupt military communication, intelligence gathering, and coordinated operations, significantly impacting national security.

Loss of Sensitive Data: Unauthorized access to classified information can lead to a loss of military secrets, strategies, and potentially compromise the safety of military personnel.

Disruption of Critical Infrastructure: Cyber attacks could target critical infrastructure such as power grids, transportation systems, or healthcare, affecting civilians and military alike.

Invasion of Privacy: Breaches could lead to the invasion of privacy for military personnel, with personal information and communications at risk.

Recommendations and Strategies to Enhance Cybersecurity Measures:

Investment in Cybersecurity Training: Ensure that military personnel receive regular training on cybersecurity best practices, recognizing phishing attempts, and adhering to secure communication protocols.

Regular Cybersecurity Audits: Conduct routine assessments of military networks to identify and rectify vulnerabilities, ensuring that the infrastructure is robust and up-to-date.

Adoption of Advanced Technologies: Incorporate cutting-edge technologies such as artificial intelligence and machine learning to detect and respond to cyber threats in real-time.

Collaboration with Private Sector: Engage with private cybersecurity firms and collaborate on threat intelligence sharing to stay updated on the latest cyber threats and vulnerabilities.

Enhanced Insider Threat Detection: Implement measures to monitor and detect unusual behavior within the military's network, reducing the risk of insider threats.

Strategic Partnerships: Establish international collaborations to enhance cybersecurity capabilities and benefit from shared expertise in countering cyber threats.

Incident Response Planning: Develop and regularly update an incident response plan to ensure a swift and effective response to cyber attacks, minimizing potential damage.

Supply Chain Security: Ensure the security of the supply chain by vetting and monitoring third-party vendors and contractors to prevent compromises from the supply side.

Legislation and Policy Development: Strengthen cybersecurity laws and policies, outlining clear consequences for cyber attacks and establishing a legal framework for prosecuting offenders.

By implementing these recommendations, the Organisations can significantly bolster its cybersecurity defenses, safeguarding national security and the privacy of its personnel. Regular updates and adaptations to the evolving threat landscape are essential to maintain a resilient cybersecurity posture.

Current State of Cybersecurity in the Organisations

2.1 Infrastructure Overview an examination of the existing cybersecurity infrastructure within the Organisations, including network architecture, intrusion detection systems, and encryption protocols.

2.1.1 Network Architecture

The network architecture of the cybersecurity infrastructure within the Organisations encompasses the arrangement and design of its interconnected systems. This involves a comprehensive understanding of the military's hardware, software, communication protocols, and data transmission mechanisms. Key components include servers, routers, switches, and other network devices. An in-depth analysis would explore how these components are organized, how data flows within the network, and the measures in place to secure critical military information.

2.1.2 Intrusion Detection Systems (IDS)

An examination of intrusion detection systems involves assessing the tools and technologies implemented to identify and respond to unauthorized access or malicious activities. This could include signature-based IDS, anomaly-based IDS, or a combination of both. The evaluation would cover the effectiveness of these systems in detecting and mitigating cyber threats, as well as their integration with other security layers within the military infrastructure.

2.1.3 Encryption Protocols

Encryption is crucial for securing sensitive military communications and data. This part of the infrastructure overview involves a detailed examination of the encryption protocols and algorithms used to protect information both in transit and at rest. This includes assessing the strength of encryption methods, key management practices, and compliance with international standards.

2.2 Institutional Framework an analysis of the policies, regulations, and organizational structures in place to address cybersecurity within the military.

2.2.1 Policies

Analyzing cybersecurity policies involves understanding the rules and guidelines set by the Organisations to govern and regulate cybersecurity practices. This includes policies related to data classification, access controls, incident response, and

the overall cybersecurity posture. The assessment would determine the adequacy of these policies in addressing current and emerging cyber threats.

2.2.2 Regulations

Beyond internal policies, an examination of regulations involves compliance with external standards and legal frameworks. This could include international cybersecurity agreements, national laws, and regulations governing the protection of military information. Assessing compliance ensures that the Organisations operates within legal boundaries while securing its cyber assets.

2.2.3 Organizational Structures

The organizational structure focuses on how the Organisations is organized to address cybersecurity challenges. This includes dedicated cybersecurity teams, reporting structures, and the integration of cybersecurity considerations into broader military operations. Evaluating the organizational structure provides insights into the prioritization of cybersecurity within the military hierarchy.

In summary, a comprehensive analysis of the cybersecurity infrastructure and institutional framework within the Organisations involves a detailed examination of network architecture, intrusion detection systems, encryption protocols, policies, regulations, and organizational structures. This holistic approach aims to ensure a thorough understanding of the military's capabilities, vulnerabilities, and preparedness in the face of evolving cyber threats

Cyber Threats and Adversaries

3.1 State-Sponsored Cyber Attacks Explore potential state-sponsored cyber threats targeting the Organisations and their implications.

3.1 State-Sponsored Cyber Attacks on the Organisations:

State-sponsored cyber attacks involve the efforts of one nation-state to infiltrate and compromise the information systems of another for various strategic purposes. In the context of the Organisations, potential state-sponsored cyber threats could emanate from rival nations, seeking to gain intelligence, disrupt operations, or influence military decision-making. The implications of such attacks are multifaceted:

a. Intelligence Gathering:

State-sponsored attackers may target the Organisations's communication networks to gather intelligence on strategic plans, military capabilities, and other sensitive information.

b. Disruption of Operations:

Cyber attacks can disrupt military operations by compromising command and control systems, disrupting communication channels, or even manipulating data to mislead decision-makers.

c. Espionage and Influence Operations:

Adversaries might engage in cyber espionage to gain insights into the Organisations's activities. Additionally, influence operations through disinformation campaigns can be conducted to manipulate public opinion or sway military decision-making.

d. Sabotage and Damage:

Cyber attacks can extend to causing physical damage by targeting critical infrastructure or systems that support military operations.

Implications:

National Security Threat: State-sponsored cyber attacks pose a significant threat to national security by compromising the confidentiality, integrity, and availability of sensitive military information.

Strategic Vulnerabilities: The compromise of military operations and intelligence can create strategic vulnerabilities, potentially impacting the nation's defense capabilities.

Geopolitical Tensions: Such cyber attacks can escalate geopolitical tensions and strain diplomatic relations between nations.

3.2 Insider Threats:

Insider threats involve individuals within an organization, such as military personnel or contractors, exploiting their access and privileges to compromise sensitive information. Risks associated with insider threats include:

a. Unauthorized Data Access:

Insiders may exploit their access to military networks to obtain sensitive information without proper authorization.

b. Sabotage:

Disgruntled employees or individuals with malicious intent may engage in sabotage by intentionally damaging or disrupting military systems.

c. Espionage:

Insiders might collaborate with external entities, including foreign governments or criminal organizations, to engage in espionage activities.

d. Information Leaks:

Sensitive military information may be leaked intentionally or unintentionally by insiders, leading to potential security breaches.

Implications:

Compromised Operational Security: Insider threats can compromise the operational security of military activities, leading to unauthorized disclosure of plans and capabilities.

Internal Trust Erosion: The presence of insider threats can erode trust within the military organization, impacting collaboration and information sharing.

Counterintelligence Challenges: Identifying and mitigating insider threats pose challenges, requiring robust counterintelligence measures.

3.3 Advanced Persistent Threats (APTs) Discuss the characteristics and impact of APTs on military networks and information systems.

3.3 Advanced Persistent Threats (APTs):

Advanced Persistent Threats are sophisticated, long-term cyber attacks conducted by well-funded and organized adversaries. In a military context, APTs can have profound implications:

a. Persistence:

APTs are characterized by their ability to remain undetected for extended periods, allowing attackers to continuously exploit military networks.

b. Targeted Exploitation:

APTs are highly targeted, focusing on specific military assets, information, or personnel to achieve strategic objectives.

c. Covert Operations:

APTs often operate covertly, using advanced techniques to evade detection and maintain access to military systems.

d. Data Exfiltration:

APTs aim to exfiltrate sensitive data, including military plans, technology blueprints, and operational intelligence, for strategic advantage.

Implications:

Persistent Threat Landscape: APTs create a persistent and evolving threat landscape, necessitating continuous cybersecurity vigilance and adaptation.

Strategic Advantage for Adversaries: Successful APTs can provide adversaries with a strategic advantage, impacting military preparedness and decision-making.

Resource Intensive Defense: Defending against APTs requires significant resources, including advanced cybersecurity tools, expertise, and ongoing monitoring.

Implications for National Security and Privacy:

a. National Security:

The cumulative impact of state-sponsored cyber attacks, insider threats, and APTs can undermine national security by compromising military capabilities, disrupting operations, and eroding strategic advantage.

b. Privacy Concerns:

The compromise of military systems may lead to the exposure of personal information of military personnel, posing privacy risks and potential threats to individual safety.

c. Economic Impact:

The economic consequences of cyber attacks on military infrastructure can be significant, affecting the nation's overall economic stability.

d. Legal and Ethical Considerations:

Addressing these cyber threats requires a balance between national security and respecting legal and

ethical principles, ensuring that countermeasures comply with international norms.

In summary, the evolving landscape of cyber threats against the Organisations requires a comprehensive and adaptive approach to cybersecurity to safeguard national security, individual privacy, and overall strategic interests

4.1 Data Breaches and Operational Impact Assess the consequences of cybersecurity breaches on military operations, mission success, and national security.

4.1 Data Breaches and Operational Impact:

Data breaches in the context of military operations can have profound consequences, affecting not only the confidentiality of sensitive information but also the operational capabilities, mission success, and national security.

A cyber breach may result in the exposure of classified military information, compromising strategic plans, troop movements, and intelligence data.

Compromised Operations Security (OPSEC):

Breaches can undermine operational security, giving adversaries insights into military strategies and tactics, allowing them to anticipate and counteract military movements.

Disruption of Communication Systems:

Cyberattacks can target communication systems, disrupting the military's ability to coordinate and share critical information in real-time.

Weapon System Vulnerabilities:

Sophisticated cyber-attacks can target and exploit vulnerabilities in military weapon systems, compromising their functionality and effectiveness.

Mission Failure and Operational Delays:

Breaches can lead to mission failure or significant delays as military units may need to reassess and modify plans in response to compromised information.

National Security Implications:

The cumulative impact of data breaches on military operations can extend to national security, potentially weakening a country's defense capabilities and opening avenues for geopolitical challenges.

Mitigation Strategies:

Enhanced Cybersecurity Measures:

Implementation of robust cybersecurity protocols, including encryption, multi-factor authentication, and continuous monitoring, to safeguard military networks and systems.

Regular Training and Awareness:

Continuous training for military personnel on cybersecurity best practices to reduce the likelihood of human error leading to security breaches.

Investment in Cyber Defense Technologies:

Developing and adopting cutting-edge cybersecurity technologies to detect and respond to cyber threats in real-time.

4.2 Invasion of Privacy Examine how cyber threats compromise the personal information and privacy of military personnel, affecting morale and overall well-being.

Invasion of Privacy:

Invasion of privacy in a military context involves cyber threats that compromise the personal information of military personnel, affecting morale, and overall well-being.

Breaches can expose personal details of military personnel, including addresses, contact information, and family details, making them vulnerable to targeted attacks.

Psychological Impact:

Invasion of privacy can lead to increased stress, anxiety, and a sense of vulnerability among military personnel, potentially affecting their mental health and overall well-being.

Operational Security Concerns:

Adversaries can exploit leaked personal information to gather intelligence, track military personnel, and potentially compromise their operational security.

Morale and Trust Issues:

Invasion of privacy erodes trust within the military community, impacting the morale of personnel who may feel betrayed or unsafe.

Limiting access to personal information only to individuals with a legitimate need, reducing the risk of unauthorized access.

Conducting regular audits to identify and rectify vulnerabilities in systems that store personal information.

Education on Cyber Hygiene:

Providing education and resources on maintaining strong personal cybersecurity practices, including guidance on social media use and online presence.

Crisis Response Plans:

Developing and implementing plans to respond swiftly and effectively in the event of a privacy breach, including communication strategies to reassure affected personnel.

In summary, addressing the consequences of data breaches and invasion of privacy in military contexts requires a multi-faceted approach, combining technological solutions, robust policies, and ongoing education and training for military personnel. The goal is to create a resilient and secure environment that can withstand evolving cyber threats.

Recommendations

5.1 Strengthening Cybersecurity Measures Provide specific recommendations for enhancing the Organisations's cybersecurity posture, including technological advancements, training programs, and collaboration with international partners.

5.1 Strengthening Cybersecurity Measures for the Organisations:

a. Technological Advancements:

Implement Advanced Threat Detection Systems: Invest in cutting-edge technologies such as AI-based threat detection systems to identify and mitigate cyber threats in real-time.

Enhance Network Security: Upgrade and fortify the military's network infrastructure with state-of-the-art firewalls, intrusion prevention systems, and encryption protocols to safeguard sensitive information.

Endpoint Security Solutions: Deploy robust endpoint protection tools to secure devices and prevent malware

infiltration, ensuring the integrity of communication channels.

b. Training Programs:

Regular Cybersecurity Training: Establish a continuous training program to keep military personnel updated on the latest cyber threats, attack vectors, and defense strategies.

Specialized Cybersecurity Teams: Form specialized teams within the military dedicated to cybersecurity, with experts in areas such as incident response, digital forensics, and penetration testing.

Simulated Cybersecurity Exercises: Conduct regular simulated cyber attacks to test the preparedness of the military's cybersecurity infrastructure and personnel.

c. Collaboration with International Partners:

Information Sharing Agreements: Establish partnerships with international cybersecurity agencies for the exchange of threat intelligence, enabling proactive defense against global cyber threats.

Joint Training Programs: Collaborate with allied nations to conduct joint cybersecurity training exercises, fostering a global network of cyber defenders.

Mutual Assistance Protocols: Develop protocols for mutual assistance during cyber incidents, allowing for coordinated responses and resource-sharing in times of need.

5.2 Legislative and Policy Reforms Propose changes to existing policies and regulations to better address emerging cybersecurity challenges.

Legislative and Policy Reforms for Cybersecurity:

a. Regulatory Framework:

Comprehensive Cybersecurity Legislation: Enact comprehensive cybersecurity legislation to address current and emerging threats, providing a legal framework for prosecuting cybercriminals and enforcing cybersecurity standards.

Data Protection Laws: Strengthen data protection laws to ensure the secure handling of sensitive information, both within the military and across the nation.

Incident Reporting Mandates: Implement mandatory reporting of cybersecurity incidents to relevant

authorities, facilitating a faster and more coordinated response to threats.

b. Institutional Cooperation:

Interagency Collaboration: Facilitate collaboration between military and civilian cybersecurity agencies, fostering a united front against cyber threats.

Public-Private Partnerships: Encourage partnerships between the government, military, and private sector organizations to share expertise, resources, and best practices in cybersecurity.

c. Capacity Building:

Educational Reforms: Integrate cybersecurity education into military training programs and civilian educational curricula to build a skilled workforce capable of addressing cybersecurity challenges.

National Cybersecurity Strategy: Develop and implement a national cybersecurity strategy that aligns military and civilian efforts to create a cohesive and resilient cybersecurity posture.

By combining technological advancements, training initiatives, and policy reforms, Nigeria can significantly enhance its military cybersecurity capabilities and better protect its national interests in the digital realm.

Conclusion

Summarize key findings and emphasize the importance of proactive measures to address cybersecurity challenges and protect the privacy of the Organisations. Highlight the necessity for a comprehensive and adaptive approach to cybersecurity in the face of evolving threats.

The key findings in addressing cybersecurity challenges and safeguarding the privacy of the Organisations underscore the critical need for proactive measures. The importance of these measures cannot be overstated, especially given the constantly evolving nature of cyber threats. Here's a broader explanation:

1. Evolving Cybersecurity Landscape: Cyber threats are becoming increasingly sophisticated, ranging from traditional malware and phishing attacks to more advanced threats such as ransomware and nation-state cyber-espionage. The Organisations, like any other organization, is vulnerable to these evolving

threats that can compromise sensitive information and disrupt operations.

2. Significance of Proactive Measures: Proactive cybersecurity measures involve anticipating and mitigating potential threats before they materialize. This approach is crucial for the Organisations to stay one step ahead of cyber adversaries. Reactive measures alone are insufficient in the face of rapidly changing cyber tactics, techniques, and procedures employed by malicious actors.

3. Protection of Sensitive Military Information: The Organisations holds sensitive information that, if compromised, could have severe consequences for national security. Proactive measures involve implementing robust cybersecurity protocols, encryption, and access controls to protect classified information from unauthorized access or manipulation.

4. Comprehensive and Adaptive Cybersecurity Strategy: A comprehensive cybersecurity strategy is necessary, encompassing a range of measures such as network security, endpoint protection, user awareness training, and incident response planning. Additionally, this strategy must be adaptive, capable of evolving alongside emerging threats. Regular assessments and updates are essential to ensure its effectiveness in the long term.

5. Importance of Privacy Protection: Safeguarding the privacy of military personnel and their data is paramount. Proactive measures should include privacy-preserving technologies, adherence to data protection regulations, and ongoing education to ensure that personnel are aware of the potential risks and best practices for maintaining their privacy in the digital realm.

6. Collaboration and Information Sharing: Cyber threats are not confined by borders, and a collaborative approach is crucial. The Organisations should actively engage in information sharing and collaboration with international cybersecurity organizations, intelligence agencies, and private-sector partners to stay informed about emerging threats and adopt best practices.

7. Continuous Training and Skill Development: Building and maintaining a skilled cybersecurity workforce is vital. Continuous training programs and skill development initiatives should be implemented to equip military personnel with the knowledge and skills

necessary to identify, respond to, and mitigate cyber threats effectively.

8. Public Awareness and Transparency: Creating awareness among the public about the importance of cybersecurity and the military's efforts in this domain is crucial. Transparency builds trust, and an informed public is better positioned to support and contribute to the overall cybersecurity resilience of the nation.

In conclusion, a proactive and comprehensive cybersecurity approach is indispensable for the Organisations. It involves not only technological measures but also a cultural shift towards cybersecurity awareness and readiness. As cyber threats continue to evolve, the adaptability of these measures will be the key to ensuring the continued security and privacy of the military and the nation as a whole.

References

- Anderson, R, Barton, C., Bohme, R., Clayton, R., van Eeten, M. J., Levi, M., & Moore, T. (2019). Measuring the cost of cybercrime. *Journal of Cybersecurity*, 5(1), tyz014. <https://doi.org/10.1093/cybsec/tyz014>
- Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. *IFEE Communications Surveys & Tutorials*, 18(3), 2027-2051. <https://doi.org/10.1109/COMST.2016.2548426>
- Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. *International Journal of Information Management*, 39, 80-89. <https://doi.org/10.1016/j.ijinfomgt.2017.12.005>
- Smith, R. E., & Sandhu, R.S. (2020). The privacy problem in cybersecurity. In proceedings of the ACM Conference on computer and Communications Security (pp.1983-1986). <https://doi.org/10.1145/3372297.3420070>
- Stalla-Bourdillon, S., & Knight, A. (2020). Privacy vs. security: A need for an ongoing dialogue. *Computer Law & Security Review*, 36, 105383. <https://doi.org/10.1016/j.clsr.2020.105383>