Wachemo University College of Engineering and Technology Department of Software Engineering Course: Fundamentals of Software Security B.Sc. In Software Engineering

Group Name: ID

Gurmesa Ayele_____ 150091

Tut Gatwech Tut_____1501376 Marefu Abebe_____150107

Tewodros Kifle_____150134

Niguse Derribe_____150119

Advisor MS. Fozia Abako (MSc)

April 11, 2025 GC

Hosanna, Ethiopia

Table of contents

1.1 Overview

Cyberattacks targeting defense and military organizations have shown a marked increase in frequency and sophistication between 2021 and 2025. These attacks, often attributed to supported by governments actors or advanced persistent threat (APT) groups, are designed to exfiltrate sensitive data, disrupt crucial operations, and undermine national security. General trends observed during this period include an

increased focus on important important systems such as energy, communications, and defense systems, with attackers aiming to cause widespread disruption. Ransomware has also emerged as a significant threat to the defense industrial base, where sensitive data is encrypted and held for ransom, potentially severely impacting operations and data confidentiality. Furthermore, supply chain attacks, exemplified by the SolarWinds incident, have become more prevalent, allowing attackers to compromise targets through trusted third-party vendors. Geopolitical tensions have fueled the use of cyberattacks as a tool for spying, sabotage, and disinformation campaigns by state actors to achieve their strategic objectives. The integration of artificial intelligence (AI) into cyberattacks presents a growing concern, as AI can be leveraged to automate attacks, evade detection mechanisms, and create more convincing phishing attempts.

1.2 Incident

Notable cyberattack incidents between 2021 and 2025, while often classified, illustrate these trends. In 2024, Ukraine experienced a surge in Russian cyberattacks, increasing by nearly 70% to 4,315 incidents targeting important important systems, including government services, the energy sector, and defense entities. These attacks aimed to steal sensitive data and disrupt operations through malware, phishing, and account compromises. By 2025, Chinese cyberattacks on Taiwan doubled to 2.4 million daily attempts, primarily targeting government and telecommunications firms with the goal of data theft and important systems disruption, with successful attacks increasing by 20% from the previous year. Also in 2025, suspected Russian hackers conducted spearphishing attacks against Kazakh diplomatic entities, embedding malicious code in diplomatic documents for spying.

The impact of these cyberattacks on defense and military targets is substantial. They can lead to the loss of classified military plans, intelligence data, and technological secrets. Military operations can be disrupted through attacks on command and control

systems, communication networks, and weapons systems. Compromises of defense-related important important systems can disrupt essential services and undermine national security. Financially, recovery from these attacks is costly, requiring significant investments in security upgrades and incident response. Moreover, cyberattacks can damage the reputation of defense organizations and erode public trust. Looking forward, the threat is expected to persist and intensify, necessitating continuous vigilance and investment in robust computer security measures to safeguard important assets.

1.3 Attacker Profile

The profile of cyberattackers targeting defense and military organizations between 2021 and 2025 typically includes advanced actors with considerable resources and expertise, primarily falling into two categories: supported by governments actors and non-state actors.

State-sponsored Actors

State-sponsored actors are groups or individuals operating on behalf of nation-states, conducting cyberattacks to achieve strategic objectives such as spying, sabotage, or disruption. These actors often possess advanced capabilities, extensive resources, and significant patience for complex and persistent attacks. Examples include China, with groups linked to the PLA and MSS targeting defense contractors and government agencies for intellectual property theft and spying. Russia, with groups associated with the GRU and FSB, has engaged in attacks against NATO countries and Ukraine, aiming to disrupt important systems and spread disinformation. Iran has increased its cyber capabilities, with groups linked to the IRGC targeting entities in the Middle East and the US for spying and sabotage. North Korea's cyber program, while primarily focused on financial crimes, has also shown involvement in attacks against defense and important important systems. The motivations of supported by governments actors are typically

geopolitical, including spying, sabotage, deterrence, and political influence.

Non-State Actors

Non-state actors, on the other hand, are not directly affiliated with a nation-state and may be motivated by financial gain, ideological beliefs, or personal agendas. This category includes cybercriminal groups that conduct attacks for financial profit through ransomware and data theft, potentially targeting defense contractors for sensitive information. Hacktivists are individuals or groups who use cyberattacks to promote political or social causes, sometimes targeting defense organizations to protest military actions. The motivations of non-state actors can include financial gain, ideology, revenge, or notoriety. Attributing cyberattacks to specific actors remains a significant challenge due to attacker anonymity, the use of false flags, and the lack of direct evidence, particularly in supported by governments attacks. Despite these challenges, computer security researchers and government agencies are increasingly able to attribute attacks with reasonable confidence through the analysis of technical indicators, attack patterns, and other intelligence.

1.4 Compromised Data /System

Cyberattacks on the defense and military sector between 2021 and 2025 have compromised/Affected a wide array of sensitive data and important systems, leading to significant consequences for national security and operational effectiveness. Sensitive data that has been affected

includes classified information related to military operations, defense strategies, and weapons systems, the compromise of which can provide enemies with important advantages. Weapons systems data, detailing the design and capabilities of advanced technologies, has also been targeted, potentially allowing enemies to develop countermeasures. Personnel data, including PII of military personnel, has been compromised, posing risks of identity theft and phishing attacks. Research and

development data concerning cutting-edge defense technologies has been lost, potentially hindering technological progress. Secure communications between military units have also been targeted, risking interception or disruption. Additionally, computer security policy data itself has been compromised, as seen in the 2024 Russian targeting of Romania's election systems and subsequent credential leaks, which can further facilitate unauthorized access.

Critical systems that have been affected

include command and control systems, essential for directing military forces and operations, whose disruption can lead to confusion and impaired decision-making. Intelligence, surveillance, and gathering information (ISR) systems, vital for situational awareness, have been compromised, degrading mission planning capabilities. Modern weapons systems, heavily reliant on computer networks, are also potential targets for disabling or manipulation. Communication networks, crucial for military coordination, have been disrupted by cyberattacks. Logistics and supply chain systems, managing the movement of troops and equipment, have been affected, impairing military readiness. Furthermore, defense operations' reliance on civilian important important systems, such as power grids and transportation networks, makes these systems indirect targets with cascading effects on military capabilities.

The impact of compromised data and systems in the defense and military sector is severe. It can lead to the loss of military advantage by providing enemies(opponnents) with sensitive information. Disruptions to important systems can impair operations and jeopardize mission success. The theft of classified information or disruption of important important systems can compromise national security. Increased risk to personnel can result from compromised communication or weapons systems. Moreover, cyberattacks can erode trust in the military and defense establishment. Examples of affected systems include Telecommunications Systems, where Chinese hackers breached US

providers in 2024, defense contractors, leading to compromises of weapons designs and supply chain information, and government agencies, such as the US office assessing foreign investments, which was breached by Chinese hackers in 2025.

1.5 Detection and Response

Detection and response to cyberattacks in the defense and military sector between 2021 and 2025 have relied on a range of advanced methods and structured strategies. Detection methods include Intrusion Detection Systems (IDS), which monitor network traffic and system activity for malicious patterns, with both network-based (NIDS) and host-based (HIDS) variations. Security Information and Event Management (SIEM) systems aggregate and analyze security data from various sources to identify potential incidents and complex attacks. Log analysis, both manual and automated, helps reveal suspicious activities. Regular vulnerability scanning identifies potential entry points for attackers. Anomaly detection uses statistical and machine learning techniques to spot deviations from normal behavior. Incident reports from users or external parties, counterintelligence efforts, and third-party notifications, such as CISA's warning about Medusa ransomware in 2025, also contribute to detection.

Once an attack is detected, defense and military organizations typically follow an incident response plan that outlines procedures for control, removal, and recovery. Containment is the immediate priority, aiming to prevent the attack from spreading by isolating affected systems or blocking network traffic. Eradication involves identifying and removing the threat, which may include removing malware or patching weaknesses. Recovery focuses on restoring affected systems and data to a secure state, often through backups. A thorough investigation is conducted to understand the scope and cause of the attack and identify the perpetrators. Depending on the severity, notification to affected parties, law enforcement, or regulatory bodies may be required. International cooperation, particularly within organizations like NATO, is crucial in

addressing supported by governments attacks through information sharing and coordinated response efforts.

1.6 Consequences

The consequences of cyberattacks in the defense and military sector between 2021 and 2025 extend to significant financial, legal, and operational impacts.

Financial impacts include direct costs such as recovery expenses, investigation costs, and control and removal costs. Indirect costs arise from operational disruptions, loss of productivity, reputational damage, and increased insurance premiums. Mitigation costs involve increased computer security spending in the aftermath of attacks. Reports indicated that global cybercrime costs were projected to reach $10.5 trillion in 2025, underscoring the financial magnitude of these threats.

Legal impacts include potential legal liability under data breach notification laws and contractual obligations, especially in defense contracts with specific security requirements. International law implications can arise if cyberattacks are deemed acts of aggression. Regulatory fines may be imposed for failures to protect sensitive data. Litigation from affected parties seeking compensation is also a possibility. Furthermore, cyberattacks could compromise legal proceedings. The EU's Cyber Resilience Act, effective in December 2024, introduced computer security standards and incident reporting mandates with legal implications for defense contractors operating within the EU.

Operational impacts are severe, potentially leading to mission failure and the loss of operational capabilities by disrupting important military systems. Compromised intelligence can undermine ongoing and future operations. Disrupted communications can hinder coordination between military units. Eroded trust in military systems and leadership can weaken alliances. Responding to and recovering from attacks strains resources, diverting them from other important activities. In some cases, cyberattacks

can escalate international tensions and potentially lead to armed conflict, as highlighted in a 2025 report by the Canadian Centre for Cyber Security warning about supported by governments actors aiming for disruptive effects to support military objectives.

1.7 Security failures

Cyberattacks against the defense and military sector between 2021 and 2025 have exploited a range of technical security failures. Common weaknesses leveraged include zero-day exploits, which are unknown flaws(defect) exploited before patches are available, and known weaknesses in unpatched(unfixed) systems. Malware, including ransomware, spyware, and Trojans, has been a significant tool for compromising systems. Phishing and spearphishing social engineering techniques have successfully deceived individuals into revealing sensitive information. Insider threats, whether malicious or negligent, have also led to breaches. Misconfigurations in systems and software create exploitable weaknesses. Supply chain attacks have compromised targets through their vendors. Lack of coding data for data at rest and in transit, weak login check practices, and software and network weaknesses such as code injection, buffer overflows, DDoS attacks, and man-in-the-middle attacks have all been exploited. A recent report noted a surge in zero-day vulnerability exploitation in 2023, targeting high-value organizations. Specific examples in the defense and military sector, while often classified, include compromised networks, stolen credentials through phishing (as seen in the 2024 Russian campaign targeting Ukrainian forces), and malware infections aimed at disrupting operations or stealing classified information.

1.8 Prevention and Solution

Preventing and mitigating cyberattacks in the defense and military sector between 2021 and 2025 requires a multi-layered approach encompassing proactive measures and advanced strategies. Proactive measures include implementing a a rule that no one

is trusted by default:

which assumes no user or device is inherently trustworthy and enforces strict verification and least privilege access.

Strong login check:

particularly multi-factor login check (MFA), is crucial for all users accessing sensitive systems.

Robust vulnerability management practices:

including regular patching and vulnerability scanning, are essential.

Network security measures

involve deploying advanced firewalls and intrusion detection/prevention systems (IDS/IPS), along with network segmentation to limit breach impact.

Data protection strategies:

include encrypting sensitive data both in transit and at rest and implementing Data Loss Prevention (DLP) solutions.

Regular security awareness training for all personnel is vital to mitigate phishing and social engineering attacks. Supply chain security measures, such as vetting vendors, are necessary. Comprehensive and regularly tested incident response plans ensure effective recovery from attacks. The use of AI-powered security tools can enhance threat detection and automate security tasks. A 2025 report by Cynet emphasized network security, endpoint protection, regular updates, employee training, and access control as key preventive measures.

Advanced strategies include leveraging cyber threat intelligence to proactively anticipate and defend against potential threats. Red teaming exercises simulate real-world attacks to identify weaknesses. Deception technology uses decoys to detect attackers within the network. Zero Trust inspection, a important component of the Zero Trust strategy, involves deep inspection of all traffic and access requests to ensure

security.

Sources and related content:

Source: https://digital-strategy.ec.europa.eu/en/policies/computer security-policies 1

Source:
https://www.csis.org/programs/strategic-technologies-program/significant-cyber-inciden
ts

Source:
https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Source: https://www.cm-alliance.com/computer
security-blog/january-2025-recent-cyber-attacks-data-breaches-ransomware-attacks

Source: https://www.cisa.gov/news-events/computer security-advisories/aa25-071a

Source: https://www.act.nato.int/activities/cyber/

Source: https://www.upguard.com/blog/the-impact-of-cybercrime-on-the-economy

Source: https://www.cisa.gov/topics/computer security-best-practices

Source:
https://www.cynet.com/advanced-threat-protection/top-6-cyber-attack-prevention-strat
egies-in-2025/

Source: https://www.edstellar.com/blog/how-organizations-prevent-cyber-attacks