IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 27, Issue 2, Ser. 2 (Mar. – Apr. 2025), PP 38-48
www.iosrjournals.org

Advanced Persistent Threats (APTs) and U.S. National Security: A Multi-Layered Defense Strategy

FEYISAYO MARIAM YUSSUF

ABSTRACT
Advanced Persistent Threats (APTs) represent an important and evolving cybersecurity challenge to U.S. national security, targeting government institutions, critical infrastructure, and private sector entities. Characterized by stealth, persistence, and sophistication, APTs are often orchestrated by nation-state actors, cyberterrorist organizations, and financially motivated cybercriminals. These adversaries employ advanced exploitation techniques, including zero-day vulnerabilities, social engineering, and lateral movement within networks, to compromise sensitive data and disrupt essential services. Given the limitations of traditional security measures in countering such threats, this study examines the integration of Security Information and Event Management (SIEM) systems with honeypot technology as a proactive cyber defense mechanism. Furthermore, this study explores policy recommendations for reinforcing national cyber resilience against APTs. Strengthening public-private partnerships, enforcing mandatory threat reporting, and adopting AI-driven threat detection models are imperative for a more adaptive and strong cybersecurity framework. The findings emphasize the necessity of deception-based defense mechanisms in the advancing threats in cyber warfare, positioning SIEM-honeypot integration as a strategic imperative for safeguarding U.S. national security.

Keywords: *Advanced Persistent Threats, SIEM, Honeypots, U.S. Cybersecurity, Threat Intelligence, National Security, Critical Infrastructure Protection.*

Date of Submission: 14-03-2025 Date of Acceptance: 27-03-2025

I. INTRODUCTION

The increasing sophistication of cyber threats presents a serious risk to U.S. national security, with Advanced Persistent Threats (APTs) emerging as one of the most formidable challenges in modern cybersecurity. Olubudo (2024) noted that APTs are created to discreetly enter networks, establish a strong presence, and operate unnoticed for long durations. Unlike conventional cyberattacks that often rely on opportunistic exploitation, APTs are characterized by their long-term strategic objectives, advanced infiltration techniques, and persistent access to targeted networks. Advanced persistent threats (APTs) employ various attack techniques, ranging from social engineering to technical exploits (Sfetcu, 2024). These threats are typically state-sponsored or orchestrated by well-funded cybercriminal organizations, making them highly resistant to traditional security measures (Kinzar, 2023). The ability of APTs to operate undetected for extended periods allows adversaries to conduct cyber espionage, intellectual property theft, and disruptive operations against vital national infrastructure.

A key distinction between APTs and conventional cyber threats lies in their operational methodology. While traditional cyberattacks may be executed rapidly for immediate financial or disruptive gain, APTs employ stealth, reconnaissance, and strategic patience to achieve long-term infiltration (Jeevaneswaran 2023). Threat actors leverage zero-day vulnerabilities, sophisticated phishing campaigns, and advanced command-and-control (C2) frameworks to move laterally within networks, escalating privileges and exfiltrating sensitive data over time. The persistent nature of these threats means that once an APT successfully embeds itself within a system, it can remain undetected for months or even years, continuously adapting to security countermeasures (LegitSecurity, 2025).

The gravity of APTs extends beyond individual organizations, threatening the stability of important U.S. infrastructure. As cyber operations become integral to geopolitical conflict, state-sponsored threat groups have increasingly targeted sectors essential to national security and economic resilience. The energy sector for example, has faced alarming vulnerabilities, as seen in the 2021 Colonial Pipeline ransomware attack, which disrupted fuel supplies across the Eastern United States (CISA, 2023). While specific figures on APT intrusions in the energy sector remain classified, the frequency of such incidents has steadily increased. The financial system has also become a key target, as seen in December 2024 when a Chinese state-sponsored APT actor breached the U.S. Treasury Department by exploiting vulnerabilities to access remote government workstations and obtain unclassified documents as reported by Financial Times (2024). The healthcare industry has seen a surge in

ransomware attacks since 2022, leading to the compromise of vast amounts of patient data and significant operational disruptions. The American Hospital Association (AHA) in 2024 highlighted that, with 386 healthcare cyber-attacks reported to date, data theft and ransomware incidents targeting the sector and essential third-party providers continue at the same elevated rate as in 2023, which marked the worst year on record for healthcare breaches (AHA, 2024). In 2024, the U.S. aviation sector faced severe cyber disruptions, including a software-induced IT outage at Delta Airlines that canceled 7,000 flights (Alison et al.,2024) and a suspected cyberattack on Seattle-Tacoma International Airport (New York Post, 2024), which caused 247 delays and multiple cancellations, highlighting vulnerabilities in essential infrastructure.

Given the progressive nature of Advanced Persistent Threats (APTs) and their increasing impact on U.S. national security, this study aims to investigate the Tactics, Techniques, and Procedures (TTPs) employed by APT groups to infiltrate and persist within vital infrastructure networks. Also, it will explore the integration of Security Information and Event Management (SIEM) systems with honeypot technology to enhance real-time threat detection and response capabilities. Analyzing these strategies will enable the research to formulate policy recommendations that strengthen national cyber resilience, ensuring a more proactive and adaptive defense against sophisticated cyber adversaries.

THE EVOLUTION OF APTs AND THEIR THREAT LANDSCAPE

The emergence of Advanced Persistent Threats (APTs) as a formidable challenge to U.S. national security can be traced to highly coordinated cyber operations conducted by both state and non-state actors. According to the US-CISA, APT actors are well-resourced and conduct sophisticated, targeted cyber activities designed for prolonged network/system intrusions with goals such as espionage, data theft, and network/system disruption or destruction (CISA, 2023). These sophisticated campaigns, often aimed at infiltrating essential infrastructure, government networks, and private-sector entities, have evolved in complexity over the years.

One of the earliest and most persistent APT threats against the U.S. government comes from APT29 (Cozy Bear) and APT28 (Fancy Bear) both of which are Russian state-sponsored hacking groups linked to the Foreign Intelligence Service (SVR) and the military intelligence agency GRU, respectively (CISA, 2022). These groups have targeted multiple U.S. agencies, including the Department of State, the White House, and the Democratic National Committee (DNC). Notably, in 2014, APT29 gained prolonged access to unclassified email systems of the State Department and the Executive Office of the President, demonstrating the group's long-term infiltration tactics and persistent reconnaissance efforts (Picus Security, 2024). Upon infiltrating the network, Cozy Bear employed sophisticated methods like custom backdoors and remote-access tools to ensure continuous access, compromising high-level communications and raising alarms about sensitive national security and diplomatic information being exposed.

APT28 played a central role in the 2016 U.S. election interference, using spear-phishing and malware-based intrusions to compromise high-profile email accounts and exfiltrate sensitive data. The group, also known as Fancy Bear, targeted Democratic National Committee (DNC) email servers, stealing sensitive emails that were later leaked to the public in what was seen as an attempt to influence the election (Cyware, 2024). Paudel (2021) noted that the operation began as early as 2015, with a spear-phishing campaign targeting key individuals, and by June 2016, both APT28 and APT29 had gained full access to the DNC's computer systems.

A more recent and far-reaching example is the SolarWinds supply chain attack, an operation attributed to APT29, which compromised multiple federal agencies and private firms, with the possibility that adversaries employed additional initial access vectors and TTPs yet to be discovered (CISA, 2021). In 2020, Russian operatives infiltrated the update mechanism of SolarWinds Orion software, a widely used IT management platform, enabling access to networks across the U.S. government, including the Department of Homeland Security, the Treasury, and major Fortune 500 companies (Vaughan-Nichols, 2021; Lucian, 2020). This attack underscored the vulnerability of supply chains, as adversaries exploited trusted software vendors to establish deep and persistent access to important networks.

Key Characteristics of APTs

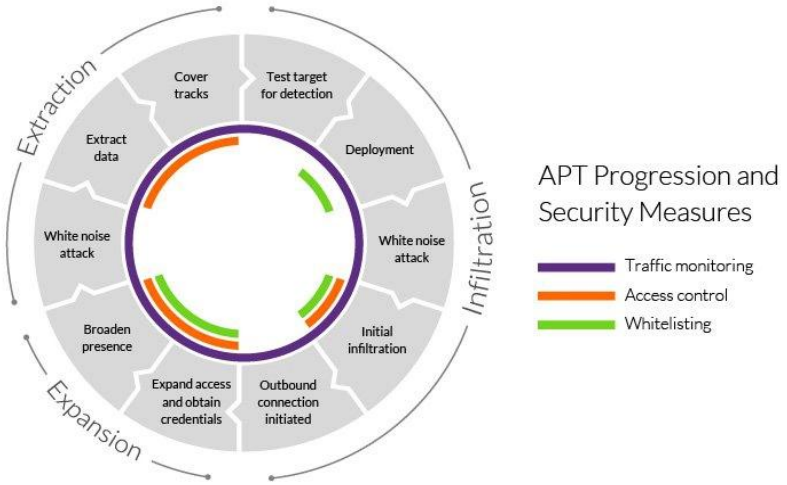
Unlike conventional cyber threats, APTs are characterized by their sneakiness, persistence, and ability to operate within compromised environments for extended periods without detection. They employ a variety of advanced tactics, including:

- Stealth and Persistence: APTs remain undetected by using fileless malware, encrypted communication channels, and sophisticated evasion techniques that circumvent traditional security measures.
- Sophisticated Command-and-Control (C2) Tactics: They utilize custom malware, proxy networks, and multi-stage payloads to establish long-term access and maintain operational security.
- Lateral Movement and Deep Network Penetration: Once inside a target network, APTs escalate privileges, compromise additional systems, and move laterally to exfiltrate sensitive data or manipulate necessary processes.

NATION-STATE ACTORS AND CYBERTERRORIST GROUPS

APTs are largely driven by geopolitical and strategic objectives, with nation-state actors playing a dominant role in cyber espionage and sabotage. APT attacks involve highly customized and sophisticated methods executed by well-funded, skilled cybercriminal teams targeting high-value organizations, with objectives such as cyber espionage, financial gain, hacktivism, or destruction (Kurt, 2025). APT attacks unfold in three key stages - infiltration, expansion, and extraction. Attackers compromise entry points through methods like social engineering or malicious uploads, establish backdoors for stealth operations, broaden their access by targeting sensitive personnel and data, and ultimately use distraction tactics, such as DDoS attacks, to extract stolen information without detection (Imperva, 2024).

Figure 1: APT Progression and Security Measures
Source: Imperva, 2024



The People's Republic of China, through groups such as APT41 and Hafnium, has engaged in sustained cyber campaigns targeting U.S. intellectual property, military systems, and research institutions. Operation CuckooBees was a multiyear cyber espionage campaign by APT 41, the group linked to DOJ indictments in 2020 against five Chinese nationals for hacking over 100 companies (Benjamin, 2023). Leveraging APT28 and APT29, Russia has actively targeted democratic institutions and important infrastructure, with APT28 conducting operations in the United States, Argentina, Armenia, Azerbaijan, Belarus, Georgia, Kazakhstan, Poland, and Ukraine, using free hosting providers to deploy backdoors targeting Windows Operating Systems, while APT29 has employed diverse infection methods, including BURNTBATTER and DONUT, and as of February 2024, expanded its arsenal with WINELOADER to enhance its capability for stealthy and persistent network infiltration as described by Flashpoint, 2024. Also, Iranian-backed APT33 and North Korea's Lazarus Group have been involved in financially motivated attacks and disruptive cyber warfare tactics, targeting U.S. financial institutions and defense contractors. According to OSL (2025), the Lazarus Group, a North Korea-linked hacking organization, has carried out sophisticated cyberattacks and high-profile cryptocurrency heists, including the theft of nearly $500 million from a cryptocurrency exchange, using malware like WannaCry and DTrack, phishing campaigns to steal credentials, and exploiting software and hardware vulnerabilities to infiltrate targeted systems. Iranian nation-state hacking group APT33 (Peach Sandstorm/Refined Kitten/Holmium) has been deploying a newly discovered FalseFont backdoor malware to conduct espionage operations against U.S. defense industrial base (DIB) workers, with Microsoft's Threat Intelligence team first detecting this activity in November 2023, noting that FalseFont enables remote system access, file execution, and data exfiltration to command-and-control (C2) servers, reinforcing APT33's ongoing refinement of its cyber capabilities with Mandiant highlighting special interest of the group in the U.S sector (Simon, 2023).

Cybercriminal syndicates and non-state actors now employ APT-like methods, merging espionage, financial crime, and cyberterrorism tactics, further complicating the distinction between these threats and state-sponsored attacks. Ransomware as a service (RaaS) is a cybercrime model where ransomware creators sell their malware to other hackers, known as "affiliates," who then carry out their own ransomware attacks using the purchased code (IBM, 2024). These actors leverage ransomware-as-a-service (RaaS), botnets, and dark web marketplaces to disrupt national security operations, exploit vulnerabilities, and hold essential infrastructure

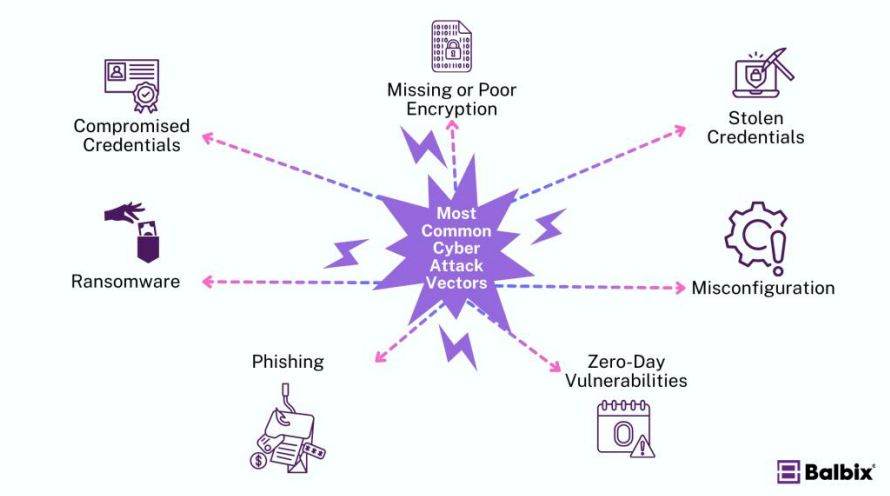
hostage for financial gain. The SamSam ransomware attacks, orchestrated by Iranian nationals without direct ties to the Iranian government, generated at least $6 million in traceable profits, primarily targeting industries with weaker cybersecurity defenses, such as healthcare, academia, and local government entities, causing not only financial losses but also significant reputational damage, as affected organizations often struggle to regain user trust after a cyber incident (Simon, 2022). State actors frequently engage non-state actors for cyber operations to maintain plausible deniability and evade accountability, as cyberspace's inherent anonymity already makes attribution challenging, allowing governments to conduct clandestine or illegal activities without direct repercussions under international law, exemplified by North Korea's use of Bureau 121, a hacking group that primarily targets South Korea while distancing the regime from potential consequences (Aishwarya, 2023).

TACTICS, TECHNIQUES, AND PROCEDURES (TTPS) USED BY APT GROUPS

Initial Attack Vectors

Advanced Persistent Threat (APT) groups employ highly targeted initial attack vectors to gain unauthorized access to networks, often taking advantage of spear-phishing, social engineering, and credential theft as their primary infiltration methods.

Figure 2: Most Common Cyber Attack Vectors



Source: Balbix, 2025

Spear phishing exploits personal details and human emotions, using carefully planned messages to create urgency and fear, which lead victims to act impulsively and fall for the scam (DataGuard, 2024). Spear-phishing remains one of the most effective tactics, as attackers craft personalized emails with malicious attachments or links designed to deceive victims into compromising their credentials or executing malware. APT29 (Cozy Bear), linked to Russian intelligence, utilized spear-phishing to breach the Democratic National Committee (DNC) in 2015, maintaining stealthy access for intelligence gathering, while APT28 (Fancy Bear) launched a separate spear-phishing campaign in 2016, leading to the public release of stolen emails.

Additionally, APT actors frequently exploit zero-day vulnerabilities, taking advantage of unpatched security flaws in widely used software before developers can issue fixes. Zaib (2022) highlighted that Zero-day vulnerabilities allow attackers to bypass defenses, gain network access, and execute data exfiltration, with such exploits increasingly traded in underground markets by nation-state actors, intelligence organizations, and cybercriminals for use in espionage, data theft, or targeted attacks.

The Hafnium group, affiliated with China, leveraged multiple zero-day vulnerabilities in Microsoft Exchange servers in 2021, allowing widespread access to sensitive data across U.S. organizations. Microsoft identified multiple 0-day exploits targeting on-premises Exchange Servers, allowing attackers to access email accounts and install malware for persistent access. This campaign, attributed to the state-sponsored group HAFNIUM operating from China, exploited vulnerabilities CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065 (Microsoft, 2021).

Evasion Techniques and Persistence Mechanisms

Once inside a network, APT groups employ sophisticated evasion techniques to remain undetected while maintaining long-term persistence. One of the most prevalent strategies is Living off the Land (LotL) attacks that

exploit legitimate administrative tools like PowerShell, Windows Management Instrumentation (WMI), and password saving tools like Mimikatz to execute malicious commands without installing external code, making them fileless and harder to detect than traditional malware-based attacks (CrowdStrike, 2023). This technique allows them to blend into normal network activity, making detection significantly harder. A notable example in the United States by the Sandstorm group is the 2017 "NotPetya" cyberattack, which, although primarily affecting organizations in Ukraine, also significantly impacted U.S. companies (Giulia, 2024). In this attack, perpetrators utilized legitimate Windows utilities like PsExec and Windows Management Instrumentation (WMI) to propagate the malware internally, exemplifying the LotL methodology.

In addition, many APTs deploy polymorphic malware and fileless attack techniques that modify their code structure dynamically or operate entirely in memory to evade traditional signature-based detection systems. APT41, a Chinese cyber-espionage group, has been known to use fileless malware and compromised software updates to maintain stealthy persistence across targeted organizations. An example of this is the 2017 CCleaner supply chain attack, in which they infiltrated the software's development environment and injected malicious code into a legitimate update which resulted in the poisoning copies of the popular utility distributed to 2.2 million users by the same group responsible for ShadowPad (Lucian, 2020). This allowed the compromised software to be distributed to millions of users, making detection difficult and exposing the risks of supply chain vulnerabilities.

Lateral Movement and Data Exfiltration

After establishing initial access, APT actors prioritize lateral movement to expand their control within compromised networks, often using privilege escalation, stolen credentials, and misconfigurations to gain deeper access. They exploit Active Directory environments and legitimate administrative tools to navigate sensitive systems undetected, ultimately aiming to exfiltrate data or sabotage critical infrastructure (IBM, 2024). Attackers employ sophisticated data exfiltration techniques, including DNS tunneling, which disguises stolen data as legitimate DNS queries to bypass security defenses, steganography, which embeds malicious data within seemingly harmless files, and covert channels that camouflage exfiltration traffic within normal network activity (Sarika, 2025). The SolarWinds attack in 2020, attributed to APT29, exemplifies these tactics, as the group moved laterally across government and corporate networks for months, siphoning classified information while evading detection (Joseph, 2024). As APT groups continuously refine their tactics to counter evolving cybersecurity defenses, organizations must adopt multi-layered security strategies to manage these persistent threats.

SIEM-HONEYPOT INTEGRATION AS A DEFENSE AGAINST APTS

Security Information and Event Management (SIEM) is a centralized security solution that aggregates and analyzes log data from various sources to provide real-time threat detection and response. In 2023, IBM described security information and event management (SIEM) as a security solution designed to help organizations detect and respond to potential security threats and vulnerabilities proactively, minimizing disruption to business operations (IBM, 2023). SIEM systems help organizations monitor security events, correlate data across networks, and detect potential threats, making them an essential component in defending against Advanced Persistent Threats (APTs). SIEM offers a unified solution to security challenges, combining Security Information Management (SIM) for log management and reporting with Security Event Management (SEM) for real-time monitoring and event handling (Bezas & Filippidou, 2023).

SIEM solutions collect logs from firewalls, endpoints, intrusion detection systems (IDS), and other security devices (Kristian, 2024). Correlating these logs allows SIEM to detect patterns that indicate malicious activities, such as unauthorized access attempts, privilege escalation, or lateral movement within the network. Real-time monitoring allows security teams to quickly identify and respond to threats, reducing the dwell time of attackers within a system.

Advanced SIEM solutions incorporate behavioral analytics to detect anomalies in user and system behavior. Machine learning algorithms establish a baseline of normal activity and flag deviations that could indicate a security incident. For example, if an employee account suddenly accesses large volumes of sensitive data outside of normal working hours, the SIEM system can trigger an alert for further investigation (Qohash, 2025). This proactive approach is particularly useful for tracking APTs, which often operate stealthily over extended periods.

Honeypots and Deception Technology

Honeypots are deceptive security mechanisms designed to lure attackers into controlled environments, allowing organizations to monitor malicious activities and gather intelligence on emerging threats. Morić et al. (2025) described honeypots as being strategically deployed within the LAN segment, integrated into the internal

network, and positioned alongside production servers to detect malicious activities from external sources and internal threats like compromised devices or insider actors. Integrating honeypots with SIEM, organizations can enhance their ability to detect and analyze APTs (Mohd et al., 2022).

Low-Interaction vs. High-Interaction Decoys

Honeypots function by emulating basic services like HTTP, FTP, SSH, or SMTP in environments that appear vulnerable, enabling low-interaction honeypots to gather vital attack data such as scanning attempts and brute-force methods, while high-interaction honeypots simulate fully operational systems to provide comprehensive intelligence on attacker behaviors and methodologies through extensive interaction (Morić et al., 2025). Low-interaction honeypots simulate common vulnerabilities with limited functionality to detect automated attacks, offering basic threat intelligence without risking full system compromise such as botnets and scanning tools. High-interaction honeypots closely mimic real systems for deeper insights into attack methods, but demand more maintenance and security measures to prevent misuse by adversaries, their examples include zero day vulnerabilities, TTPs, behavioral profiling.

Role in Cyber Deception, Threat Intelligence, and Forensic Analysis

Honeypots play a crucial role in cyber deception by diverting attackers from actual critical assets. These decoy systems mimic legitimate targets with subtle vulnerabilities, attracting malicious actors while logging their activities to enhance security (Sage, 2025). A honeynet, which consists of multiple interconnected honeypots, presents various simulated weaknesses to lure attackers, allowing security teams to analyze their methods and strategies in depth. Honeypots contribute to threat intelligence by capturing attack signatures, Tactics, Techniques, and Procedures (TTPs), and malware samples, even in encrypted or IPv6 environments (Moric et al., 2024). Security teams use this intelligence to improve defenses and refine forensic analysis processes, strengthening overall cybersecurity resilience.

How SIEM-Honeypot Integration Strengthens Cyber Defense

SIEM-honeypot integration strengthens cyber defense by enabling early-stage threat detection, real-time correlation of attacker behavior, and automated incident response. Honeypots lure APT attackers into controlled decoy environments, where their actions are logged and analyzed within the SIEM system, providing organizations with critical time to assess threats and deploy countermeasures before real assets are compromised (Morić et al., 2025). Through integrating honeypot data with broader security logs, SIEM systems enhance real-time visibility into attacker behavior, allowing security teams to distinguish between targeted attacks and random scans more effectively (Mohd et al., 2022). This correlation improves the accuracy of threat detection, ensuring that security teams can respond to sophisticated intrusion attempts with greater precision. Additionally, honeypot data enriches SIEM-driven threat intelligence, allowing automated security mechanisms to proactively contain threats. When attack patterns detected in honeypots match known malicious behaviors, SIEM systems can trigger automated responses such as blocking malicious IPs, isolating compromised endpoints, or generating alerts for security teams to investigate further (Morić et al., 2025). Through this integration, organizations can enhance their cyber resilience, improving both threat visibility and response efficiency.

CASE STUDIES

Bank of Hope's Integration of Threat Intelligence with SIEM

Bank of Hope, a prominent Korean-American bank operating across the United States, recognized the need to enhance its cybersecurity posture due to the increasing complexity of threats targeting financial institutions. The bank's existing process for analyzing potential malicious IP addresses was labor-intensive and time-consuming, requiring analysts to consult multiple resources to assess the relevance and threat level of each IP. Bank of Hope faced significant challenges in its cybersecurity operations, particularly in threat analysis. Security analysts spent considerable time researching potential threats manually, leading to inefficiencies and delayed responses (Anomali, 2023). Also, the absence of a centralized threat intelligence system required analysts to consult multiple platforms, increasing the likelihood of oversight and slowing down the detection process. To address these issues, the bank implemented Anomali's ThreatStream, a threat intelligence platform designed to integrate seamlessly with its existing SIEM systems. This integration provided a unified view of threat data, allowing analysts to quickly assess the reputation of IP addresses and other indicators of compromise (IOCs) without the need to switch between multiple tools. The implementation of Anomali's ThreatStream at Bank of Hope led to several notable outcomes. The efficiency of threat analysis improved significantly, reducing the time required to investigate potential threats from up to 30 minutes per incident to just a few minutes. This allowed security analysts to focus on more strategic tasks rather than being burdened by time-consuming manual investigations. Additionally, the automation and enhanced efficiency reduced the need for additional hires, optimizing the existing team's capacity to manage cybersecurity threats effectively. The integration of threat

intelligence into the bank's SIEM system also strengthened its overall security posture, enabling quicker identification and mitigation of potential threats (Anomali, 2023). The successful deployment at Bank of Hope highlights how integrating advanced threat intelligence solutions with SIEM can enhance efficiency, optimize resources, and improve an organization's ability to respond proactively to cyber threats.

Government Agency's Deployment of Honeypots to Study Advanced Persistent Threats (APTs)

Government agencies, such as the FBI, have successfully employed honeypots to counter cyber threats and criminal activities. For instance, the FBI used a fake "secure" messaging app with encryption backdoors to arrest hundreds of criminals (Malcolm, 2023). Recognizing the growing threat of Advanced Persistent Threats (APTs) targeting critical infrastructure, another government agency initiated a pilot project to proactively study and mitigate these threats (Morić et al., 2025). APTs pose a significant challenge due to the sophistication of their actors, who are often well-funded and highly skilled. Their ability to evade detection and persist within networks for extended periods makes mitigation particularly difficult. Traditional security measures frequently lack the depth of insight needed to fully understand the tactics, techniques, and procedures (TTPs) employed by these adversaries. Without comprehensive threat intelligence, organizations struggle to anticipate and counteract evolving cyber threats effectively. To address these challenges, the agency deployed honeypots as part of its pilot project. These honeypots were strategically integrated into the agency's network to attract and monitor APT activities without compromising actual critical infrastructure. By capturing and analyzing attacker TTPs, the honeypots generated actionable intelligence, offering crucial insights into adversarial methodologies. The deployment distinguished between research honeypots—designed for forensic and threat intelligence collection, and production honeypots, which were integrated into security operations for real-time threat mitigation. The evaluation of honeypot solutions revealed significant strengths and limitations, allowing for tailored deployments based on organizational needs. Dionaea and Cowrie demonstrated exceptional versatility and data accuracy, whereas Honeyd and Thug provided valuable insights into scalability and specific attack vectors. Tools such as Nmap and Metasploit were used to assess detection and logging capabilities, revealing that Amun, Dionaea, Cowrie, and Thug effectively captured and analyzed a wide range of threats. However, Glasstopf and Honeyd faced challenges related to configuration and activity tracking. Emerging trends in honeypot technology further enhance their effectiveness. These include integrating machine learning for automated threat detection, adopting cloud-based honeypots to address cloud-native threats, and advancing deception strategies to improve adversary engagement. These innovations position honeypots as dynamic and adaptable tools in modern cybersecurity frameworks. The intelligence collected through this initiative informed the creation of more effective cybersecurity policies and response strategies, strengthening the agency's overall security posture. By integrating honeypots into their cybersecurity strategy, government agencies can gain invaluable insights into adversarial tactics, leading to more adaptive defenses and informed policymaking (Morić et al., 2025).

POLICY RECOMMENDATIONS TO MITIGATE APT THREATS

Strengthening National Cyber Resilience

Advanced Persistent Threats (APTs) pose a growing risk to national security and critical infrastructure. Strengthening national cyber resilience requires a coordinated approach between government agencies and private sector organizations. Public-private collaboration on cyber intelligence sharing significantly enhances threat visibility and response efficiency. Programs such as CISA's Automated Indicator Sharing (AIS) facilitate the real-time exchange of machine-readable threat intelligence, allowing organizations to proactively detect and mitigate cyber threats. The AIS community includes private sector entities, federal agencies, state, local, tribal, and territorial (SLTT) governments, information sharing and analysis centers (ISACs), information sharing and analysis organizations (ISAOs), and foreign government partners and companies (CISA, 2021). Recognizing the need for standardized security practices, leading technology companies have introduced private-sector-driven solutions to mitigate cybersecurity risks. In October 2021, Salesforce, Google, Okta, and Slack launched the Minimum Viable Secure Product (MVSP), a set of baseline security requirements aimed at reducing outsourcing risks while demonstrating how private enterprises can implement robust cybersecurity measures (Eugenia et al., 2022). These voluntary initiatives highlight the importance of industry-driven security standards in supplementing regulatory efforts.

Beyond voluntary frameworks, regulatory compliance plays a crucial role in ensuring organizations adopt stringent cybersecurity practices. The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), enacted in March 2022, mandates that covered entities report cybersecurity incidents within specific timeframes, empowering CISA to enforce disclosure through rulemaking. This legislation aims to unify fragmented reporting requirements and enhance situational awareness across critical infrastructure sectors, ensuring that emerging threats are identified and addressed promptly (Natasha & Hold, 2024). Public-private intelligence sharing enhances private-sector security efforts and regulatory oversight, significantly boosting national cyber resilience to address the dynamic challenges of the advanced persistent threat (APT) environment.

Regulatory and Compliance Measures

Regulatory frameworks are important in mitigating APT risks by enforcing security best practices across industries. Zero Trust Architecture (ZTA) is a fundamental strategy that should be mandated across government networks and high-risk sectors. The Zero Trust Architecture (ZTA) is a cybersecurity model that redefines traditional security by eliminating trust based on network location and enforcing continuous verification and strict authentication for all users and devices, regardless of their location (Ritter et al., 2024). Introducing strict identity verification, continuous monitoring, and least-privilege access controls, ZTA minimizes the risk of unauthorized access and lateral movement within networks. Furthermore, adopting the key recommendations from the National Cybersecurity Strategy 2023 ensures that organizations adhere to a comprehensive security framework that prioritizes resilience, incident response, and risk management (The White House, 2023). Compliance with these measures will help establish a standardized security baseline, reducing vulnerabilities that APT actors often exploit.

Enhancing AI-Powered Cybersecurity Solutions

Artificial intelligence (AI) and machine learning (ML) have become integral to modern cybersecurity defenses. AI-driven Security Information and Event Management (SIEM) systems leverage predictive analytics to enhance the ability to detect anomalies and uncover sophisticated attack patterns (Gavi, 2025). Incorporating AI into cybersecurity strategies allows organizations to proactively identify APT activities before they escalate. Additionally, automated threat hunting and adaptive response mechanisms enable real-time detection and mitigation of malicious activities (Gold et al., 2025). AI-powered defenses enhance response efficiency by dynamically adjusting security controls based on evolving attack tactics, reducing the dwell time of cyber adversaries within a network.

Workforce Development and Cybersecurity Training

A well-trained cybersecurity workforce is essential for defending against APTs. Investing in cybersecurity education and workforce upskilling in collaborative, team-based training, simulating actual cyber incidents and realistic scenarios is important to addressing the talent shortage in the industry (Leidos, 2025). Government initiatives should focus on expanding cybersecurity training programs at academic institutions and offering specialized certifications for cybersecurity professionals. According to Aldaajeh et al. (2022), a web-based virtual platform was specifically designed to perform cybersecurity data analysis and intelligence activities. Training cyber incident response teams in advanced APT mitigation strategies ensures that organizations can effectively detect, analyze, and neutralize sophisticated threats (Ibrahim et al., 2024). Regular exercises, such as red teaming and penetration testing, further enhance the ability of security teams to respond to real-world attack scenarios.

FUTURE TRENDS IN CYBER DEFENSE AGAINST APTS

Next-Generation Cyber Threat Intelligence Platforms

Next-generation Security Information and Event Management (SIEM) systems, combined with deception technologies such as high-interaction honeypots, are becoming essential components of modern cybersecurity strategies. These solutions enable security teams to detect, analyze, and neutralize sophisticated threats by correlating real-time network activity with adversary tactics, techniques, and procedures (TTPs). Rishika (2025) highlights CrowdStrike Falcon Intelligence as a state-of-the-art threat intelligence platform designed to provide real-time visibility, proactive detection, automated analysis, and AI-powered innovations. Leveraging advanced threat intelligence, organizations can enhance their ability to detect, investigate, and mitigate complex cyber threats. Additionally, CrowdStrike (2025), in collaboration with Amazon Web Services (AWS), offers tailored threat intelligence solutions to address both present and future cloud cybersecurity challenges effectively. The integration of artificial intelligence (AI) and machine learning (ML) into SIEM platforms is further revolutionizing cyber defense by automating threat detection and response. AI-driven threat models significantly enhance anomaly detection, reduce false positives, and adapt to evolving attack patterns, offering a proactive approach to mitigating APT risks. As AI-powered analytics continue to advance, organizations can improve their cyber resilience by automating incident response and accelerating threat mitigation efforts.

The Role of Quantum Computing in Cybersecurity

Quantum computing represents both an opportunity and a challenge in the fight against APTs. While quantum technology holds promise for accelerating cryptographic analysis and complex security operations, it also poses a severe risk to current encryption standards (Emmanni, 2023). APT groups, particularly nation-state actors, may exploit quantum capabilities to break traditional cryptographic algorithms, compromising national security and critical infrastructure. To counteract this threat, researchers and government agencies are investing in post-quantum cryptography (PQC), which aims to develop encryption methods resistant to quantum-based

attacks (NCSC, 2024). The U.S. National Institute of Standards and Technology (NIST) has been leading efforts to standardize quantum-resistant algorithms, ensuring long-term data security in an era of quantum advancements.
International Cooperation in Cybersecurity

Given the global nature of APT threats, international cooperation is vital for effective cyber defense. The United States has been at the forefront of cybersecurity coalitions, working closely with allies to strengthen intelligence sharing and coordinated response mechanisms. Initiatives such as the Joint Cyber Defense Collaborative (JCDC) and partnerships with Five Eyes intelligence alliance members have enhanced cross-border collaboration in identifying and mitigating cyber threats (The Record, 2021). Additionally, global cybersecurity agreements, including the Paris Call for Trust and Security in Cyberspace, emphasize the importance of collective defense strategies (Paris Call, 2021). To ensure diplomatic and technological partnerships, the U.S. and its allies can encourage cyber resilience and disrupt adversarial cyber operations more effectively.

II. CONCLUSION AND FINAL RECOMMENDATIONS

Advanced Persistent Threats (APTs) continue to pose significant risks to U.S. critical infrastructure, targeting government agencies, financial institutions, and essential service providers. As cyber adversaries employ increasingly sophisticated techniques, traditional defense mechanisms alone are insufficient. The integration of Security Information and Event Management (SIEM) with honeypot technology has proven to be a valuable approach, enhancing early threat detection, attack attribution, and forensic capabilities. Leveraging real-time analytics and deception strategies allows organizations to proactively identify and manage cyber threats before they escalate into large-scale breaches. However, strengthening national cyber resilience also requires more robust regulatory frameworks and the adoption of AI-driven cybersecurity solutions to stay ahead of evolving attack methodologies.

Federal agencies and important infrastructure operators should prioritize investments in deception-based cyber defense by deploying and refining honeypot-enhanced SIEM systems. These technologies provide valuable insight into attacker behaviors while minimizing risks to actual network assets, enabling proactive threat detection and response. Also, enforcing strict cybersecurity compliance for private sector operators is essential in fortifying national cyber resilience. The federal government should mandate rigorous cybersecurity standards for businesses in critical sectors, ensuring adherence to frameworks such as the Cybersecurity Maturity Model Certification (CMMC) and the NIST Cybersecurity Framework. Strengthening reporting requirements and compliance measures will help mitigate the risks posed by APTs. Furthermore, ensuring collaboration between government agencies, private industry, and cybersecurity experts is crucial in developing a unified defense strategy. Public-private partnerships and real-time threat intelligence sharing, facilitated through initiatives like the Joint Cyber Defense Collaborative (JCDC) and international cybersecurity alliances, will enhance collective efforts to detect, prevent, and respond to emerging cyber threats effectively.

Call to Action

Addressing the growing threat of APTs requires immediate and sustained action from cybersecurity professionals, HR leaders, policymakers, and national security agencies. Organizations must prioritize investments in SIEM-honeypot innovations and AI-driven cybersecurity models to anticipate and neutralize cyber threats effectively. Policymakers must continue refining regulatory measures to hold organizations accountable for maintaining high cybersecurity standards. As cyber warfare tactics evolve, the proactive adoption of advanced defensive strategies will be important in safeguarding national security and important infrastructure. The time to act is now—before the next major cyber incident disrupts essential services and undermines national stability.

REFERENCES

[1]. Aishwarya Ramen. (2023). States' use of non-state actors in cyberspace. Retrieved from Observer Research Foundation. https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace

[2]. Anomali. (2023). Bank of Hope case study: Enhancing threat intelligence with SIEM integration. Retrieved from https://www.anomali.com/resources/case-studies/bank-of-hope-case-study

[3]. Aldaajeh, Saleh & Saleous, Heba & Alrabaee, Saed & Barka, Ezedin & Breitinger, Frank & Choo, Kim-Kwang. (2022). The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. Computers & Security. 119. 10.1016/j.cose.2022.102754.

[4]. Alison Sider, Andrew Tangel and Robert McMillan. (2024). The day Delta's on-time machine broke and the blame game it sparked. Retrieved from Wall Street Journal. https://www.wsj.com/business/airlines/the-day-deltas-on-time-machine-broke-and-the-blame-game-it-sparked-b462fc80

[5]. American Hospital Association (AHA). (2024). A look at 2024's health care cybersecurity challenges. Retrieved from https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges

[6]. Balbix. (2025). Attack vectors and breach methods. Retrieved from https://www.balbix.com/insights/attack-vectors-and-breach-methods/#:~:text=What%20are%20attack%20vectors?,with%20access%20to%20your%20network.

[7]. Benjamin Jensen. (2023). How the Chinese Communist Party uses cyber espionage to undermine the American economy. Retrieved from Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/how-chinese-communist-party-uses-cyber-espionage-undermine-american-economy

[8]. Bezas, Konstantinos & Filippidou, Foteini. (2023). Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs). Indonesian Journal of Computer Science. 12. 443-468. 10.33022/ijcs.v12i2.3182.

[9]. CISA. (2021). Automated Indicator Sharing (AIS). Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/automated-indicator-sharing-ais

[10]. CrowdStrike. (2023). Living off the land (LOTL) attacks. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/living-off-the-land-attack/

[11]. CrowdStrike. (2025). Next-generation threat intelligence with CrowdStrike and AWS. Retrieved from https://www.crowdstrike.com/en-us/resources/white-papers/next-generation-threat-intelligence-with-crowdstrike-and-aws/

[12]. Cybersecurity and Infrastructure Security Agency (CISA). (2021). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a

[13]. Cybersecurity and Infrastructure Security Agency (CISA). (2022). Russian state-sponsored and criminal cyber threats to critical infrastructure. Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a

[14]. Cybersecurity and Infrastructure Security Agency (CISA). (2023). Nation-state cyber actors. Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors#:~:text=Nation%2Dstate%20adversaries%20pose%20an,at%20prolonged%20network/system%20intrusion.

[15]. Cybersecurity and Infrastructure Security Agency (CISA). (2023). The attack on Colonial Pipeline: What we've learned & what we've done over the past two years. Retrieved from https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years#:~:text=On%20May%207%2C%202021%2C%20a,get%20their%20kids%20to%20school.

[16]. Cyware. (2024). Inside Fancy Bear's arsenal: An update on the cyber tactics of APT28. Retrieved from https://www.cyware.com/resources/threat-briefings/research-and-analysis/inside-fancy-bears-arsenal-an-update-on-the-cyber-tactics-of-apt28-5186

[17]. DataGuard. (2024). What is spear phishing in cyber security? Retrieved from https://www.dataguard.com/blog/what-is-spear-phishing-in-cyber-security/#:~:text=Spear%20phishing%20succeeds%20because%20it's,trusted%20entities%20or%20familiar%20contacts.

[18]. Emmanni, Phani Sekhar. (2023). The Impact of Quantum Computing on Cybersecurity. Journal of Mathematical & Computer Applications. 2. 1-4. 10.47363/JMCA/2023(2)140.

[19]. Eugenia Lostri, James Andrew Lewis, and Georgia Wood. (2022). A shared responsibility: Public-private cooperation for cybersecurity. Retrieved from Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/shared-responsibility-public-private-cooperation-cybersecurity

[20]. Financial Times. (2024). [Title of the article]. Retrieved from https://www.ft.com/content/ecfae287-adfe-4f5c-9c7b-7ec1c8b601a7

[21]. Flashpoint. (2024). Evolving tactics: How Russian APT groups are shaping cyber threats. Retrieved from https://flashpoint.io/blog/russian-apt-groups-cyber-threats/

[22]. Gavi, Kounde. (2025). Optimizing Threat Detection and Incident Response through AI-Powered Automation in SIEM Systems.

[23]. Giulia Bellabarba. (2024). NotPetya: Understanding the destructiveness of cyberattacks. Retrieved from https://www.securityoutlines.cz/notpetya-understanding-the-destructiveness-of-cyberattacks/

[24]. Gold, Precious & Moyin, Christianah & Samad, Dolapo & Victoria, Blessing & Falade, Rhoda & Adeola, & Adeola, Falade. (2025). AI-Driven Threat Intelligence: Enhancing SIEM Capabilities for Real-Time Cybersecurity Monitoring.

[25]. IBM. (2023). What is SIEM? Retrieved from https://www.ibm.com/think/topics/siem

[26]. IBM. (2024). Lateral movement in cyberattacks. Retrieved from https://www.ibm.com/think/topics/lateral-movement#:~:text=Hackers%20combine%20and%20repeat%20lateral,infecting%20critical%20systems%20with%20malware.

[27]. IBM. (2024). Ransomware as a service (RaaS). Retrieved from https://www.ibm.com/think/topics/ransomware-as-a-service

[28]. Ibrahim, Nadim & N R, Rajalakshmi & Hammadeh, Karam. (2024). Exploration of Defensive Strategies, Detection Mechanisms, and Response Tactics Against Advanced Persistent Threats APTs. Nanotechnology Perceptions. 20. 439-455. 10.62441/nano-ntp.v20iS4.33.

[29]. Imperva. (2024). Advanced persistent threat (APT) progression. Retrieved from https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/#:~:text=Advanced%20persistent%20threat%20(APT)%20progression,data%E2%80%94all%20without%20being%20detected.

[30]. Jeevaneswaran Muthukumar. (2023). The Silent Intruders: Navigating the Labyrinth of Advanced Persistent Threats (APTs) International Journal of Research Publication and Reviews, Vol 4, no 9, pp 817-836. https://ijrpr.com/uploads/V4ISSUE9/IJRPR17136.pdf

[31]. Joseph Carson. (2024). SolarWinds Sunburst supply chain cyber attack: Impact on the software industry. Retrieved from Delinea. https://delinea.com/blog/solarwinds-sunburst-supply-chain-cyber-attack-software-industry#:~:text=After%20initial%20access%2C%20the%20attackers,DeleteRegistryValue

[32]. Kinza Yasar. (2023). Advanced persistent threat (APT). Retrieved from TechTarget. https://www.techtarget.com/searchsecurity/definition/advanced-persistent-threat-APT

[33]. Kristian McCann. (2024). The seismic shift shaking up SIEM. Retrieved from Cyber Magazine. https://cybermagazine.com/articles/the-seismic-shift-shaking-up-siem

[34]. Kurt Baker. (2025). Advanced persistent threat (APT). Retrieved from CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/

[35]. Lars Ritter, Raphael Röttinger, Sebastian Wenning. (2024).ZERO TRUST ARCHITECTURES IN THE ENERGY SECTOR: APPLICATIONS AND BENEFITS. European Journal of Engineering and Technology Vol. 12 No. 1, 2024 ISSN 2056-5860. https://www.idpublications.org/wp-content/uploads/2024/06/Full-Paper-ZERO-TRUST-ARCHITECTURES-IN-THE-ENERGY-SECTOR-APPLICATIONS-AND-BENEFITS.pdf#:~:text=Energy%20companies%20must%20rely%20on%20ZTA%20to,from%20one%20segment%20to%20another.%20Furthermore%2C%20ZTA.

[36]. Legit Security. (2025). Advanced persistent threat examples. Retrieved from https://www.legitsecurity.com/blog/advanced-persistent-threat-examples

[37]. Leidos. (2025). Cyber talent challenge: Bridging the gap in cybersecurity workforce development. Retrieved from https://www.leidos.com/insights/cyber-talent-challenge-bridging-gap-cybersecurity-workforce-development

[38]. Lucian Constantin. (2020). Chinese hacker group APT41 uses recent exploits to target companies worldwide. Retrieved from CSO Online. https://www.csoonline.com/article/569145/chinese-hacker-group-apt41-uses-recent-exploits-to-target-companies-worldwide.html

[39]. Lucian Constantin. (2020). SolarWinds supply chain attack explained: Why organizations were not prepared. Retrieved from CSO Online. https://www.csoonline.com/article/570191/solarwinds-supply-chain-attack-explained-why-organizations-were-not-prepared.html

[40]. Malcolm Higgins. (2023). FBI honeypot. Retrieved from NordVPN. https://nordvpn.com/blog/fbi-honeypot/

[41]. Microsoft. (2021). HAFNIUM targeting Exchange Servers with 0-day exploits. Retrieved from https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[42]. Mohd Ariffin, Muhammad Azizi & Darus, Mohamed & Haron, Haryani & Kurniawan, Aditya & Muliono, Yohan & Siahaan, Chrisando. (2022). Deployment of Honeypot and SIEM Tools for Cyber Security Education Model In UITM. International Journal of Emerging Technologies in Learning (iJET). 17. 149-172. 10.3991/ijet.v17i20.32901.

[43]. Morić, Z., Dakić, V., & Regvart, D. (2025). Advancing Cybersecurity with Honeypots and Deception Strategies. Informatics, 12(1), 14. https://doi.org/10.3390/informatics12010014

[44]. Natasha G. Kohne, Joseph Hold. (2024). New CISA cybersecurity incident reporting requirements proposed for critical infrastructure companies. Retrieved from Akin Gump Strauss Hauer & Feld LLP. https://www.akingump.com/en/insights/blogs/ag-data-dive/new-cisa-cybersecurity-incident-reporting-requirements-proposed-for-critical-infrastructure-companies#:~:text=Background,setting%20the%20requirements%20via%20rulemaking.&text=CIRCIA%20specifies%20that%20covered%20entities,information%20disclosure%20through%20enforcement%20actions.&text=The%20current%20cyber%20reporting%20landscape,incidents%20in%20critical%20infrastructure%20sectors.&text=The%20NPRM%20attempts%20to%20implement,awareness%20across%20critical%20infrastructure%20sectors.

[45]. National Cyber Security Centre (NCSC). (2024). Next steps in preparing for post-quantum cryptography. Retrieved from https://www.ncsc.gov.uk/whitepaper/next-steps-preparing-for-post-quantum-cryptography

[46]. New York Post. (2024). Seattle-Tacoma International Airport hit with delays after possible cyberattack. Retrieved from https://nypost.com/2024/08/25/us-news/seattle-tacoma-international-airport-hit-with-delays-after-possible-cyberattack/

[47]. Olubudo, Paul. (2024). Advanced Threat Detection Techniques Using Machine Learning: Exploring the Use of AI and ML in Identifying and Mitigating Advanced Persistent Threats (APTs).

[48]. OSL. (2025). Who is the Lazarus Group? The hackers behind billion-dollar heists. Retrieved from https://osl.com/academy/article/who-is-the-lazarus-group-the-hackers-behind-billion-dollar-heists

[49]. Paris Call. (2021). Paris Call for Trust and Security in Cyberspace. Retrieved from https://pariscall.international/en/

[50]. Paudel, Sirish. (2021). A Study on Alleged Russian Interference in the US Elections 2016. SSRN Electronic Journal. 10.2139/ssrn.4707563. https://www.researchgate.net/publication/378497825_A_Study_on_Alleged_Russian_Interference_in_the_US_Elections_2016

[51]. Picus Security. (2024). APT29: Cozy Bear evolution techniques. Retrieved from https://www.picussecurity.com/resource/blog/apt29-cozy-bear-evolution-techniques?hs_amp=true

[52]. Qohash. (2025). Zero-day threat detection. Retrieved from https://qohash.com/zero-day-threat-detection/#:~:text=Behavioral%20Analysis,the%20accuracy%20of%20threat%20detection.

[53]. Rishika Patel (2025). Top threat intelligence platforms to watch in 2025. Retrieved from CIO Influence. https://cioinfluence.com/security/top-threat-intelligence-platforms-to-watch-in-2025/#:~:text=CrowdStrike%20Falcon%20Intelligence%20is%20a,to%20detect%20sophisticated%20cyber%20threats.

[54]. Sage. (2025).. Honeypots and why you need it in your security. Retrieved from A&D Forensics. https://adforensics.com.ng/honeypots-and-why-you-need-it-in-your-security/#:~:text=A%20honeypot%20is%20a%20decoy,How%20Honeypot%20Works

[55]. Sarika Sharma. (2025). DNS tunneling detection. Retrieved from Fidelis Security. https://fidelissecurity.com/threatgeek/learn/dns-tunneling-detection/#:~:text=DNS%20is%20the%20backbone%20of,traffic%20as%20legitimate%20DNS%20queries.

[56]. Sfetcu, Nicolae. (2024). Advanced Persistent Threats in Cybersecurity – Cyber Warfare. 10.58679/mm28378.

[57]. Simon Handler. (2022). The 5×5—Non-state armed groups in cyber conflict. Retrieved from Atlantic Council. https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-non-state-armed-groups-in-cyber-conflict/

[58]. Simon Hendery. (2023). Iranian threat group APT33 targets US defense contractors with novel malware. Retrieved from SC World. https://www.scworld.com/news/iranian-threat-group-apt33-targets-us-defense-contractors-with-novel-malware

[59]. Steven Vaughan-Nichols. (2021). SolarWinds: The more we learn, the worse it looks. Retrieved from ZDNet. https://www.zdnet.com/article/solarwinds-the-more-we-learn-the-worse-it-looks/

[60]. The Record. (2021). Five Eyes issue joint cybersecurity advisory for defending against Log4Shell. Retrieved from https://therecord.media/five-eyes-joint-cybersecurity-advisory-cisa-log4j-log4shell

[61]. The White House. (2023). National Cybersecurity Strategy Implementation Plan. Retrieved from https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf

[62]. Zaib, Raheela. (2022). Zero-Day Vulnerabilities: Unveiling the Threat Landscape in Network Security. Mesopotamian Journal of Cyber Security. 2022. 57-64. 10.58496/MJCS/2022/007.

[63]. Zlatan Moric, Leo Mršić, Zdravko Kunić, Goran Đambić. (2024). Honeypots in Cybersecurity: Their Analysis, Evaluation and Importance. https://www.preprints.org/manuscript/202408.0946/v1