Environment. Technology. Resources. Rezekne, Latvia
Proceedings of the 16th International Scientific and Practical Conference. 2025. Volume II, 99-106

The Risk of Personal Smart Devices in the Operational Security for Military Bases, Personnel and Missions

Dimitar S. Dimitrov
IT Department
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
dimitar@nvna.bg

Iliyan Y. Iliev
IT Department
Nikola Vaptsarov Naval Academy
Varna, Bulgaria
i.y.iliev@naval-acad.bg

***Abstract* – The increasing integration of personal smart devices into military operations has significantly expanded the attack surface, introducing critical security vulnerabilities. This paper explores how smart devices can compromise operational security (OPSEC) through unauthorized data leaks, cyber exploitation, and geolocation tracking. It examines real-world incidents, including security breaches during the Russian-Ukrainian conflict and the exposure of military bases via fitness tracking applications. Additionally, the study analyses adversarial tactics that leverage AI-driven OSINT and behavioural analytics to exploit smart device vulnerabilities. Finally, mitigation strategies, including policy recommendations and technical countermeasures, are discussed to enhance the cybersecurity posture of military personnel and operations.**

Keywords – AI, Cyber Threats, Smart Device, OPSEC.

I. INTRODUCTION

The widespread adoption of personal smart devices in the military has reshaped the security landscape, expanding the attack surface and exacerbating OPSEC vulnerabilities in modern warfare. These devices ranging from smartphones and tablets to fitness trackers, smartwatches, and even augmented reality headsets offer unprecedented connectivity, convenience, and mobility. Yet, their presence in both professional and personal military environments has unintentionally created numerous security risks [1]. By relying on these devices for communication, navigation, health monitoring, and data synchronization, military units are exposed to potential adversarial exploitation [2], [3]. The convergence of consumer grade technology with military operations has not only complicated cybersecurity defences but also challenged the reliability of secure communication systems, thereby making these devices prime targets for sophisticated cyber threats.

In modern military operations, smart devices have seamlessly integrated into critical mission activities, serving as tools for navigation, real time communication, health surveillance, and operational coordination. However, their extensive usage has broadened the attack vectors, making them more vulnerable to exploitation by state-sponsored cyber adversaries, organized hacking groups, and even low-level cybercriminals.

Smart devices inherently rely on wireless communication protocols such as Bluetooth, Wi-Fi, and GPS, which remain susceptible to interception, spoofing, and manipulation.

Such vulnerabilities enable adversaries to gather intelligence, conduct cyber espionage, and physically track military personnel, ultimately compromising mission integrity and safety.

Moreover, the continuous synchronization of these devices with cloud servers and social media platforms inadvertently exposes sensitive operational data, increasing the risk of unauthorized access, data exfiltration, and geolocation tracking.

The 2018 Strava heat map incident, for example, revealed secret U.S. and allied military installations, as well as Russian military bases, through aggregated fitness tracking data [4], [5].

The public accessibility of these heat maps provided adversaries with actionable intelligence on troop movements, operational schedules, and even internal base layouts.

In another case, the geolocation data from personal fitness trackers enabled the targeted assassination of Stanislav Rzhitsky, a high-ranking Russian naval commander. By analysing his jogging patterns recorded on a fitness tracking application, adversaries were able to predict his routine and carry out a precision strike with lethal efficiency [6].

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol2.8616

These cases highlight the evolving cyber threat landscape in military operations, demonstrating how adversaries exploit digital footprints left by seemingly harmless personal devices. Addressing these risks requires robust cybersecurity measures, stricter device usage policies, and heightened awareness among military personnel to mitigate potential threats.

The rapid evolution of cyber warfare has further exacerbated these risks, as state sponsored hacking groups and advanced persistent threats increasingly leverage artificial intelligence and machine learning algorithms to automate and optimize their attacks.

AI-driven cyber operations can process vast amounts of data from compromised smart devices to predict military movements, analyse behavioural patterns, and profile personnel vulnerabilities. By correlating this data with open-source intelligence (OSINT), adversaries can create predictive models of troop deployments, mission schedules, and strategic decision-making processes. The integration of AI into cyber espionage tactics enables adversaries to execute highly targeted phishing campaigns, deploy adaptive malware that evolves in real-time, and even generate deepfake communications for social engineering attacks. These capabilities allow adversaries to infiltrate military networks, manipulate operational data, and disrupt critical infrastructure with unprecedented speed and precision.

The growing dependence on personal smart devices has inadvertently created an asymmetric warfare advantage for adversaries, particularly those backed by nation-states with significant cyber capabilities. The lack of standardized regulations governing the use of personal smart devices in military environments further compounds the risk, making them an unintentional weak link in military cybersecurity. Unlike military-grade communication systems, commercial smart devices are not designed to meet stringent security standards, often lacking end-to-end encryption, robust authentication mechanisms, and secure software update protocols. Additionally, the widespread usage of third-party applications many of which request excessive permissions introduces a new layer of vulnerability that adversaries can exploit for surveillance, data exfiltration, and network infiltration. The ease of integrating these applications into personal devices makes it difficult to establish secure perimeters within military bases, thereby compromising OPSEC.

The aim of this research is to assess the vulnerabilities linked to personal smart devices, investigate real-life incidents that demonstrate these risks, and propose actionable solutions at both the policy and operational levels. By gaining a deeper understanding of various attack vectors and their outcomes, military organizations can implement robust cybersecurity protocols to prevent unauthorized access and mitigate the threats these devices present. This study contributes to the ongoing dialogue on cybersecurity within military operations by providing recommendations for securing personal smart devices without compromising the operational capabilities of military personnel. In the subsequent sections, the paper will examine the core vulnerabilities inherent in smart devices, analyse the attack methods adversaries use to exploit these weaknesses, and present case studies that highlight their real-world impact. Additionally, it will explore mitigation strategies aimed at strengthening OPSEC and reinforcing military cybersecurity measures.

II. Materials and Methods

The reliance on interconnected smart devices and technologies creates multiple points of entry for cyber threats, making military personnel and operations more susceptible to intelligence gathering, cyber espionage, and network infiltration.

Since the connection is not completely secured, the primary concerns associated with smart devices is unintentional data leakage. Many applications and built-in functionalities continuously collect and transmit user data, often without explicit consent. Location services, Bluetooth connections, and automatic cloud synchronization expose military personnel to unauthorized tracking. Even when military personnel disable location-sharing settings, metadata embedded in messages, photos, and social media activity can still provide adversaries with crucial intelligence. This kind of passive surveillance allows adversaries to map operational areas, identify personnel movement patterns, and assess the presence of classified facilities [7].

The growing sophistication of state-sponsored cyber operations has further amplified the risks associated with smart devices. APT groups often linked to national intelligence agencies actively exploit smart device vulnerabilities to gather intelligence on foreign military activities. These groups employ a range of tactics, including malware injection, phishing campaigns, and network intrusion techniques, to compromise military networks through personal devices. [8], [9].

Given the widespread usage of consumer-grade smart devices in military settings, adversaries can leverage these vulnerabilities to conduct targeted attacks, gather intelligence, or even manipulate information to disrupt military operations. Beyond cyber threats, supply chain vulnerabilities present another significant risk [10]. Many smart devices are manufactured using global supply chains, making them susceptible to firmware manipulation or pre-installed malware before they even reach the end user. Hardware backdoors embedded in commercially produced devices can enable adversaries to conduct long-term intelligence gathering and system infiltration. Unlike military-grade communication equipment, which undergoes extensive security testing, consumer smart devices do not always meet stringent security standards, leaving them exposed to potential exploitation at multiple stages of production and distribution. The convergence of smart devices with military operations has created a hybrid security challenge, where traditional OPSEC measures are insufficient to counteract the evolving cyber threat landscape.

A. Types of Weakness in Smart Devices

Smart devices contain several inherent weaknesses that make them highly vulnerable to exploitation by

adversaries, presenting significant risks to military operational security. A key issue lies in ***the protocols used*** for data exchange, such as Bluetooth, Wi-Fi, and cellular networks, which are particularly prone to interception, spoofing, and man-in-the-middle attacks. These communication protocols are often poorly secured, allowing adversaries to intercept sensitive military data, manipulate transmissions, and track personnel movements. The absence of robust end-to-end encryption in many commercial smart devices intensifies this vulnerability, enabling unauthorized data extraction and heightening the potential for cyber espionage.

Another critical vulnerability is found in ***the default data-sharing configurations*** embedded in many smart devices and applications. Fitness tracking applications, social media platforms, and cloud-based services frequently collect and store user data without explicit consent. Without careful configuration for privacy, these applications continuously track user activities and locations, creating extensive datasets that can be exploited by adversaries. When aggregated across multiple personnel, this data can unintentionally expose movement patterns, deployment sites, and the positioning of key military assets, posing serious risks to operational security (OPSEC).

Smart devices are particularly vulnerable to cyberattacks due to ***outdated or insecure firmware***. Many consumer-grade devices operate on outdated firmware versions, lacking adequate encryption protocols and essential security patches, making them easy targets for malicious actors. Firmware manipulation, zero-day vulnerabilities, and supply chain attacks provide opportunities for adversaries to compromise devices even before they are deployed in military environments. The military's dependence on off-the-shelf consumer technology amplifies this risk, as these devices do not adhere to the rigorous cybersecurity standards required for military operations.

Supply chain vulnerabilities further compound the cybersecurity risks associated with smart devices [9]. Most smart devices are produced through complex global supply chains, making them susceptible to firmware manipulation or pre-installed malware before they even reach the end user. Embedded hardware backdoors during production allow adversaries to conduct long-term intelligence gathering, data exfiltration, and remote sabotage. In contrast to military-grade communication systems, which undergo extensive security testing, consumer smart devices often fail to meet the stringent cybersecurity standards necessary to safeguard against exploitation throughout production and distribution.

The ***continuous synchronization*** of smart devices with cloud services significantly increases the risk of unauthorized data exposure. Many personal smart devices automatically sync their data with cloud storage platforms, making sensitive military information vulnerable to external breaches. Cyber adversaries can infiltrate these cloud environments, gain access to classified data, and use it to disrupt and compromise military operations.

The ***integration of smart devices with commercial networks***, often lacking military-grade security measures, introduces another layer of risk, allowing adversaries to exploit these unsecured channels for intelligence gathering and system infiltration.

The growing complexity of smart device ecosystems, combined with the absence of standardized security protocols, creates a multi-faceted threat landscape that traditional military OPSEC measures struggle to address. As the military continues to adopt smart devices in its operations, the challenge of protecting sensitive data and communications from cyber threats becomes increasingly daunting.

B. Fitness Tracking Devices

Fitness tracking devices pose a unique security risk due to their continuous monitoring of user activities and locations. These devices, which include brands such as Fitbit, Garmin, and Apple Watch, collect extensive biometric data such as heart rate, sleep patterns, and movement habits. While these features are beneficial for personal health tracking, they also provide adversaries with valuable intelligence on military personnel. In recent years, these devices have been implicated in significant security breaches, where adversaries have exploited publicly available fitness data to track military movements and base locations. One of the most notorious security breaches involving fitness tracking devices was the Strava heat map incident, where aggregated GPS data from users inadvertently exposed sensitive military locations worldwide. The heat map, intended to display global exercise activity, highlighted heavily frequented routes in isolated regions many of which corresponded to secret U.S. military bases and intelligence outposts. The revelation of these locations posed a severe OPSEC threat, as adversaries could analyse movement patterns, shift schedules, and personnel routines. The exposure demonstrated how seemingly harmless fitness applications could compromise national security.

In late 2024, the exposure of Israeli military bases through Strava data further underscored the security risks associated with fitness tracking devices. In this instance, military personnel inadvertently shared their running routes on a publicly accessible platform, enabling adversaries to analyse and map military training facilities, patrol patterns, and operational movements. The intelligence derived from this data allowed hostile actors to estimate troop deployments, operational readiness, and high-value target locations. A report by Haaretz [11], an Israeli newspaper, first revealed a critical security vulnerability within the Strava fitness application that could be exploited by an unidentified actor, potentially a foreign intelligence operative. By creating a fraudulent account, the individual systematically uploaded falsified geolocation data, simulating jogging routes through highly sensitive military installations, including Israeli Air Force bases, intelligence facilities, naval stations, and a U.S. military facility. This deceptive tactic inadvertently exposed the identities of active military personnel, compromising their operational

locations, residential addresses, and movement patterns, thereby posing a significant national security risk.

C. The Importance of Data in the Age of Artificial Intelligence

The advent of artificial intelligence (AI) has profoundly reshaped the realm of cyber warfare and intelligence gathering, intensifying the risks related to personal smart devices in military settings. AI-driven systems possess the capability to analyse massive volumes of data in real time, allowing adversaries to detect and manipulate patterns in military movements, personnel actions, and logistical operations. This convergence of AI with cyber espionage has ushered in a new era where state-sponsored hacker groups can automate and expand their attacks, rendering traditional cybersecurity defences insufficient and inadequate in safeguarding sensitive military assets.

One of the most alarming aspects of AI in cyber warfare is its ability to predict and manipulate human behaviour based on collected data. By analysing geolocation metadata, biometric readings, and device usage patterns, AI-driven systems can generate predictive models of military operations. These models enable adversaries to forecast troop deployments, mission schedules, and logistical weaknesses with a high degree of accuracy. Machine learning algorithms can also aggregate information from publicly available sources, such as social media posts and fitness tracking applications, to refine intelligence assessments and enhance targeting precision. AI enhances the effectiveness of automated phishing and social engineering attacks. Deep learning models can generate highly convincing phishing emails and messages tailored to specific military personnel by mimicking writing styles, tone, and organizational jargon. AI-generated deepfake videos and voice recordings further complicate cybersecurity efforts by making it increasingly difficult to differentiate between legitimate and fraudulent communications. This technology has been used to impersonate senior military officials, tricking personnel into divulging classified information or granting access to secure systems.

AI-driven cyber operations also play a crucial role in automated malware deployment and adaptive cyberattacks. Traditional malware detection systems rely on known attack signatures, but AI-powered malware continuously evolves, modifying its structure and behaviour to evade detection. Self-learning malware can autonomously assess a target's defence, identify vulnerabilities, and optimize its attack strategy in real time. Such adaptive threats pose significant challenges to military cybersecurity teams, requiring continuous monitoring and rapid-response capabilities to mitigate potential breaches.

The ability of AI to conduct real-time data exploitation has further intensified the risks posed by personal smart devices in military settings. AI algorithms can sift through massive datasets collected from compromised smart devices, identifying sensitive information and classifying it for strategic use [12]. This automated intelligence processing allows adversaries to extract mission-critical details with minimal human intervention, significantly reducing the time required to act on intercepted data. The speed and efficiency of AI-driven intelligence gathering enable adversaries to conduct cyber operations at an unprecedented scale, heightening the need for robust cybersecurity frameworks.

D. The Role of Smart Devices in AI-Driven Cyber Espionage

Smart devices play a crucial role in enabling AI-driven cyber espionage. Many military personnel unknowingly carry AI-assisted surveillance tools in the form of fitness trackers, smartphones, and wearable devices that continuously collect and transmit personal data. Adversaries can exploit this data to create detailed behavioural profiles of military personnel, identifying their routines, stress levels, and potential vulnerabilities. These insights can be used to develop targeted cyberattacks that exploit psychological and operational weaknesses.

For example, AI can analyse sleep patterns and biometric data from fitness trackers to determine when personnel are most fatigued or vulnerable to social engineering attacks. If an adversary identifies that a particular soldier regularly experiences sleep deprivation, they can time their cyberattacks to coincide with periods of reduced alertness.

Similarly, AI-driven sentiment analysis of private messages and emails can detect dissatisfaction or stress among military personnel, enabling adversaries to exploit morale issues through psychological manipulation. The growing interconnectivity of smart devices within military environments has also increased the risk of coordinated AI-powered surveillance campaigns. By compromising multiple personal devices, adversaries can establish a network of real-time intelligence sources within military bases and operational zones. AI algorithms can correlate data from different compromised devices to reconstruct tactical movements and strategic planning. This level of intelligence gathering far exceeds traditional reconnaissance methods, making smart device security a top priority for military cybersecurity teams. The risk of AI-assisted malware attacks targeting smart devices has also escalated in recent years. Malicious AI can craft highly personalized phishing messages, manipulate voice recognition systems, and even mimic biometric authentication processes to gain access to classified networks. These attacks can be further enhanced by deepfake technology, which allows adversaries to impersonate military personnel with near-perfect accuracy. The combination of smart devices and AI-driven deception tactics poses a formidable challenge for cybersecurity professionals.

III. RESULTS AMD DISCUSSION

The real-world implications of smart device vulnerabilities in military environments have been demonstrated through several major security breaches. These incidents highlight how adversaries exploit personal technology to compromise military bases, personnel, and operations. The following case studies provide in-depth analyses of how fitness tracking applications, social media

activity, and geolocation data have been used to undermine OPSEC, leading to strategic exposure and, in some instances, lethal consequences.

A. 2018 - Strava's Heat Map Revealing Taiwan's Secrets and Secret US Military Bases

In 2018, Strava, a fitness tracking application, published a global heat map (Fig. 1) that visualized user activity by aggregating GPS data from millions of users worldwide.

While this data was intended for civilian fitness tracking, it inadvertently exposed numerous secret military installations, particularly in Africa (Fig. 2 and Fig. 3), the Middle East, Afghanistan, and Taiwan (Fig. 4). Distinct movement patterns recorded in remote and strategically sensitive areas revealed U.S. and allied military bases.

Fig. 2 shows Camp Lemonnier (top right) and a suspected CIA base (bottom left) in Djibouti, both clearly distinguishable by their illumination. Fig. 3 depicts the U.S. base at Al-Tanf, Syria, near the Iraqi border, appearing as a distinct elongated light signature. Similarly, forward operating bases in Helmand, Afghanistan, are illuminated, indicating significant activity. These examples demonstrate how light emissions and activity patterns can inadvertently reveal the locations of sensitive military installations.

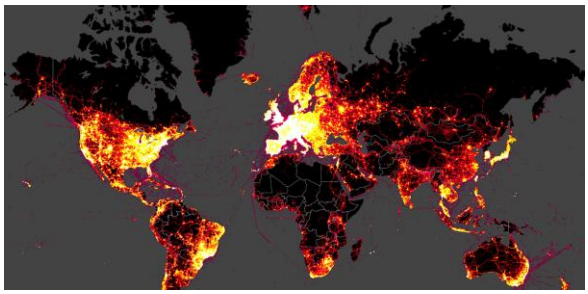

Fig. 1. Stava worldwide heatmap (2018) [13].

The heat map highlighted high-activity exercise routes in isolated regions, which adversaries used alongside satellite imagery and intelligence databases to pinpoint covert military sites. Military analysts noted that the data not only delineated base perimeters but also revealed patrol routes, shift rotations, and internal facility layouts. These insights enabled hostile actors to infer troop deployments, high-value target locations, and logistical vulnerabilities.

Fig. 2. US military and CIA presence in Djibouti [14].

Another significant incident involved the inadvertent disclosure of Taiwan's Missile Command Center (shown in Fig. 4), a facility of high strategic importance. This center oversees Taiwan's long-range missile operations, including cruise missiles capable of reaching mainland China. The exposure occurred when analysts examined Strava's heat map data, which revealed unexpected fitness activity in a restricted area.

OSINT specialists and military analysts detected concentrated movement patterns – primarily from jogging – within a zone off-limits to civilians. These patterns aligned with typical routines of military personnel at secure sites. By cross-referencing the coordinates with satellite imagery and existing maps, analysts pinpointed the activity within a known military installation in Taiwan. Further examination of Taiwan's military infrastructure confirmed that this was not just any base, but the headquarters of Taiwan's missile command.

Fig. 3. US outpost at Al-Tanf, Syria [15].

Reports and prior intelligence assessments indicated the presence of long-range cruise missiles in the area, intended to counter threats from mainland China. Despite efforts to camouflage missile transporter vehicles, analysts observed personnel movements around structures resembling missile launch facilities. The correlation between Strava data and known military logistics strongly suggested a link to Taiwan's missile operations.

Fig. 4. Heatmap of Strava showing activity around and in Taiwan's missile command [16].

OSINT experts and defence analysts corroborated their findings by matching movement patterns with previously leaked information about Taiwan's missile strategy. They

also identified additional concealment measures, such as structures designed to shield vehicles from satellite surveillance. Nonetheless, consistent jogging patterns around the facility provided clear evidence of military activity. The integration of heat map data, satellite imagery, and intelligence reports led to the definitive identification of the site as Taiwan's Missile Command Center, highlighting a significant operational security lapse.

B. The Assassination of Stanislav Rzhitsky through Strava Data Tracking

In 2023, Russian naval officer Stanislav Rzhitsky, a former submarine commander, was assassinated while jogging in Krasnodar. Investigations revealed that his fitness tracking data on Strava had been used by adversaries to monitor and predict his routine (Fig. 5), ultimately facilitating his targeted elimination. Using AI-driven behavioural analytics and OSINT aggregation, adversaries developed a predictive model of Rzhitsky's daily jogging routes. By cross-referencing his social media activity, fitness tracker data, and time-stamped geolocation points, attackers identified the optimal time to strike when security presence was minimal. The precise timing and execution of the assassination suggested the use of AI-enhanced surveillance techniques to anticipate Rzhitsky's movements in real time.

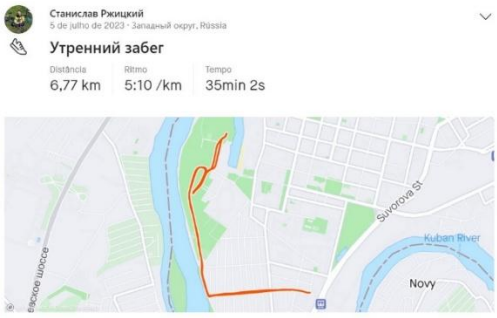

Fig. 5. The route that Stanislav Rzhitsky regularly ran, posted publicly on his Strava account [6].

The assassination served as a stark demonstration of the lethal risks posed by unsecured (unregulated) digital footprints, particularly among high-value military personnel. Following this incident, Russian intelligence agencies imposed strict bans on fitness tracking applications within military ranks, strengthening cybersecurity measures against adversarial intelligence efforts. The case highlighted how AI-driven OSINT can be exploited to execute precision strikes on high-profile targets.

Fig. 6. Russian Airbase in Khmeimim, Syria. [5].

A recurring example of data consolidation from mobile applications and intelligence is the disclosure of the Russian Airbase in Khmeimim, Syria (Fig. 6).

C. 2025 - Military Personnel on a French Nuclear Submarine Reveal Sensitive Information Through Strava

In early 2025, a major security breach within the French Navy's nuclear submarine fleet [17] was exposed when Strava's heat map revealed the operational routes and patrol cycles of ballistic missile submarines (SSBNs). The leak, which was investigated by French intelligence and cybersecurity agencies, showed that crew members stationed at the Ile Longue naval base in Brest had inadvertently shared sensitive operational data through their personal fitness trackers.

This breach allowed adversaries to reconstruct submarine deployment schedules, docking routines, and patrol routes, critically undermining France's nuclear deterrence strategy. More alarmingly, several personnel had used real names on public Strava profiles, making it possible to identify individual crew members and track their activities. The compromised data could potentially enable adversaries to pre-position surveillance assets, track SSBN departures and predict deterrence readiness cycles.

French defence officials implemented emergency countermeasures, including the mandatory deactivation of fitness tracking applications, OPSEC retraining for naval personnel, and real-time cybersecurity monitoring of unauthorized data transmission. However, this incident demonstrated the inherent risks of unsecured digital footprints in the context of strategic military operations, highlighting the urgent need for comprehensive cybersecurity protocols in nuclear deterrence efforts.

IV. CONCLUSION

The findings of this study underscore the significant security risks posed by personal smart devices in military environments. As demonstrated by the documented cases, adversaries have successfully exploited geolocation tracking, metadata exposure, and AI-driven OSINT techniques to compromise operational security. The ability to reconstruct troop movements, predict deployment schedules, and even execute targeted assassinations highlights the severity of the threat landscape.

To mitigate these risks, military organizations must adopt a multi-layered cybersecurity approach. This

includes enforcing strict device usage policies, mandatory OPSEC training, and real-time monitoring of unauthorized data transmissions. Additionally, AI-driven anomaly detection systems should be deployed to identify and neutralize potential cyber threats in real time. The adoption of military-issued, security-hardened devices and strict geofencing of sensitive locations can further reduce vulnerabilities.

The increasing sophistication of cyber adversaries necessitates continuous adaptation in cybersecurity practices. As AI-powered cyber warfare capabilities evolve, military forces must proactively update their defensive strategies to counter emerging threats. Future research should focus on the development of secure-by-design military-grade smart devices and the implementation of AI-assisted counter-surveillance techniques to neutralize adversarial intelligence efforts.

By addressing these challenges, military organizations can strengthen their cybersecurity posture and ensure the integrity of critical missions in an era of digital warfare.

A. Mitigation

To prevent similar security breaches, military organizations must enforce strict digital hygiene policies. Key mitigation strategies include:

- Refining OPSEC Policies**:** Commanders should tailor security measures based on adversary capabilities, balancing operational efficiency with risk mitigation when using smart devices.
- Enhanced Training & Awareness: Utilize subject matter experts to educate personnel on digital footprints, adversarial electronic warfare, and the risks of smart devices, ensuring regular OPSEC training.
- Restricting Location-Based Features**:** Mandatory disabling of fitness tracking apps and location-sharing features to minimize exposure.
- Geofencing & Network Controls**:** Blocking access to social media and tracking apps in sensitive areas to prevent data leaks.
- AI-Driven Security**:** Leveraging AI for real-time anomaly detection and unauthorized data transmission monitoring.
- Strict Device Policies**:** Enforcing the use of military-issued, security-controlled devices to limit risks.
- Tech Industry Collaboration: Partnering with private sector firms to develop secure communication applications for military use.
- Cybersecurity Taxonomy Implementation: Standardizing threat identification and AI-based defenses to strengthen OPSEC policies.
- Specialized Cybersecurity Recruitment**:** Rigorous selection and training of cybersecurity personnel to improve threat response and resilience [18].

ACKNOWLEDGEMENT

This research paper has received funding from Ministry of Education and Science of the Republic of Bulgaria under the National Science Program "SECURITY AND DEFENCE", in implementation of the Decision of the Council of Ministers of the Republic of Bulgaria No: 731/21.10.2021 and according to Agreement No: D01-74/19.05.2022.

REFERENCES

[1] J. K. Kirschbaum et. al., "Internet Of Things: Enhanced Assessments and Guidance Are Needed to Address Security Risks in DOD," United States Government Accountability Office, Washington, USA, Report to Congressional Committees GAO-17-668, 2017.

[2] M. Koller, "Recommendations for Safety-Conscious Smart Device Use by Military Professionals", AARMS., Vol. 21, № 2, pp. 5-14, 2022, https://doi.org/10.32565/aarms.2022.2.1.

[3] K. Dhondt et al., A Run a DayWon't Keep the Hacker Away: Inference Attacks on Endpoint Privacy Zones in Fitness Tracking Social Networks, Conference on Computer and Communication (CCS '22), November 7-11, 2022, Los Angeles, CA, USA. New York, NY, USA, 16 pages, 2022, https://doi.org/10.1145/3548606.3560616.

[4] A. Nocks, The Geointelligence Revolution: Real-Time Reconnaissance and Its Dangers, PIPS, Institute for the Theory and Practice of International Relations, Williamsburg, Virginia, USA, 2018.

[5] Data and Defense: The Case of Strava, Feb. 2, 2018. [Online]. Available: https://medium.com/dfrlab/data-and-defense-the-case-of-strava-6b56ee3b1a2. [Accessed: Feb. 22, 2025].

[6] Russian commander who posted running routine on app is murdered while exercising, July 11, 2023 [Online]. Available: https://g1.globo.com/mundo/noticia/2023/07/11/comandante-russo-que-publicava-rotina-de-corrida-em-aplicativo-e-assassinado-quando-se-exercitava.ghtml [Accessed: Feb. 22, 2025]

[7] S. Szymoniak and K. Foks, "Open Source Intelligence Opportunities and Challenges – A review", Advances in Science and Technology Research Journal, Vol 18, № 3, pp 123-139, 2024, https://doi.org/10.12913/22998624/186036.

[8] S. Grooby, T. Dargahi and A. Dehghantanha. Protecting IoT and ICS platforms against advanced persistent threat actors: Analysis of APT1, in In Handbook of Big Data and IoT Security, Springer, Cham, 2019, pp. 225-255.

[9] D. Dimitrov and D. Nikolov, Current Cybersecurity Issues in the Industrial Control System of Nuclear Power Plants, Vol. 2, Conference on Radiation Safety in the Modern World, November 16-18, 2022, Veliko Tarnovo, Bulgaria, 8 pages, 2022, https://doi.org/10.34660/INF.2023.43.56.040. (In Bulgarian).

[10] N. Takpah and V. Oriakhi, "Cybersecurity Challenges and Technological Intergration in Military Supply Chain 4.0", Journal of Information Security, Vol. 16, № , pp. 131-148, 2025, https://doi.org/10.4236/jis.2025.161007.

[11] Haaretz Investigation: Intelligence Operation Collected Information on Sensitive Israeli Bases, Soldiers, Oct. 29, 2024. [Online]. Available: https://www.haaretz.com/israel-news/security-aviation/2024-10-29/ty-article-magazine/.premium/intelligence-operation-collected-information-on-sensitive-israeli-bases-soldiers/00000192-d7bb-df2b-a5db-d7bf8d440000 [Accessed: Feb. 22, 2025].

[12] V. Atanasov and Y. Sivkov, Evaluating Yolov5 Models on Thermal Imagery for Aerial Drone Applications, Conference 23rd International Symposium on Electrical Apparatus and Technologies (SIELA), June 12-15, 2024, Bourgas, Bulgaria, 4 pages, 2024, https://doi.org/10.1109/SIELA61056.2024.10637871.

[13] Strava oficial site. [Online]. Available: https://www.strava.com/maps/global-heatmap?sport=All&style=dark&terrain=false&labels=true&poi=true&cPhotos=true&gColor=blue&gOpacity=100#1.5/31.1/12.5 [Accessed: Feb. 22, 2025].

[14] Fitness Tracker Data Highlights Sprawling U.S. Military Footprint in Africa, Jan. 29, 2018. [Online]. Available: https://theintercept.com/2018/01/29/strava-heat-map-fitness-tracker-us-military-base/ [Accessed: Feb. 22, 2025].

[15] D. Brown, "Here are some of the biggest reveals from a fitness-tracker data map that may have compromised top-secret US military bases around the world", Jan. 29, 2018. [Online]. Available: https://www.businessinsider.com/strava-heatmap-most-revealing-images-2018-1 [Accessed: Feb. 22, 2025].

[16] An American fitness app leaked global military bases. Do we still dare to publish our running records?, Jan. 30, 2018 [Online]. Available: https://kknews.cc/world/l2ba32g.html#google_vignette [Accessed: Feb. 22, 2025].

[17] French submarine crew accidentally leak sensitive information through Strava app, Jan. 15, 2025. [Online]. Available:https://www.euronews.com/2025/01/15/french-submarine-crew-accidentally-leak-sensitive-information-through-strava-app [Accessed: Feb. 22, 2025].

[18] M. Maroun and A. Ivanova, Ontology-based approach for cybersecurity recruitment, Applications of Mathematics in Engineering and Economics (AMEE '20), June 7-13, 2020, Sofia, Bulgaria, 11 pages, 2021, https://doi.org/10.1063/5.0042320.