Formosa Journal of Multidisciplinary Research (FJMR)
Vol. 4, No. 4, 2025: 1975-1990

Operational Security in Modern Warfare: Lessons from the Ukraine-Russia Conflict

Dwi Erita Millynia[1]*, Agung Risdhianto[2], Editha Praditya Duarte[3], Hikmat Zakky Almubaroq[4]
Universitas Pertahanan Indonesia
Corresponding Author: Dwi Erita Millynia dwierita01@gmail.com

A R T I C L E I N F O
Keywords: Defense Management, Intelligence Gathering, Operational Security, Risk Management

Received : 15, March
Revised : 29, March
Accepted: 28, April

A B S T R A C T
The evolution of modern warfare, particularly in the Ukraine-Russia War, highlights the crucial role of Operations Security (OPSEC) in addressing vulnerabilities from the growing reliance on cyber technologies, portable devices, and social media. While these tools enhance efficiency and situational awareness, they also introduce risks through Signals Intelligence (SIGINT) and Open Source Intelligence (OSINT). This study identifies key vulnerabilities in smartphones, commercial radios, platforms like Discord, social media apps like Strava, and drones like DJI. It emphasizes the need for OPSEC measures, including military-standard equipment, secure communication, and proper training. Examples from the Ukraine-Russia War, such as the use of modified drones for kamikaze missions and unencrypted communication, demonstrate the importance of robust risk management. Additionally, proprietary networks like NIPRNet, SIPRNet, and JWICS offer effective mitigation. This journal stresses that while modern technology is vital in Fifth Generation Warfare (5GW), its vulnerabilities must be managed through OPSEC frameworks to ensure security, maintain information superiority, and achieve mission success.

DOI: https://doi.org/10.55927/fjmr.v4i4.133
ISSN-E: 2829-8896
https://npaformosapublisher.org/index.php/fjmr

INTRODUCTION

In modern military operations, the use of cyber domain, portable electronic devices (PEDs), and social media has revolutionized the way armed forces communicate, strategize, and engage with their environments. These tools offer significant advantages, such as enhanced situational awareness, real-time information sharing, and increased operational efficiency. Portable electronic devices allow rapid access to mission-critical data, while social media provides a platform for psychological operations and narrative shaping in information warfare. However, these technologies also introduce substantial risks, including vulnerabilities to cyberattacks, data leaks, and the unintentional exposure of sensitive operational details, undermining mission objectives through information breach by adversary intelligence gathering effort. The pervasive influence of cyber domain, portable electronic device and social media in military related issues aligns closely with the principles of Fifth Generation Warfare (5GW), which emphasizes on non-kinetic, perception-driven strategies. In 5GW, the manipulation of information through cyber domain and its mediums can become both a powerful asset and a critical liability, highlighting the delicate balance military organizations must maintain in leveraging modern technology.

Defense management studies play a pivotal role in guiding the effective and secure integration of cyber technologies, portable electronic devices (PEDs), and social media into military operations. Defense management is the process of translating national security strategies into trained, equipped, and ready forces while managing resources, capabilities, and risks management (Hari Burcu-Marcu et al., 2009). This field equips senior leaders with the tools to assess and mitigate risks associated with these technologies, ensuring they are leveraged to enhance operational effectiveness without compromising security. Defense management emphasizes the importance of risk management, which is defined as balancing current capabilities against future needs while addressing vulnerabilities that may emerge in rapidly evolving technological environments (Galvin et al., 2019). By applying rigorous risk management frameworks, defense management studies provide a structured approach to identifying the potential threats and developing strategies to minimize their negative impacts (D. van der Waal & V. Versluis, 2017). Operation Security (OPSEC) is a critical component for minimizing risk by classifying information into classified and undisclosed categories, safeguarding classified and highly classified information by employing secured or encrypted devices, and creating protocols regarding the use of commercial portable electronic device (PED) and social media by military and supporting personnels (M. Kubilay Akman, 2018). The implementation of OPSEC ensures that the use of cyber domain, PEDs, and social media aligns with broader defense objectives while safeguarding operational integrity in the complex landscape of modern warfare.

The Ukraine - Russia conflict highlighted the critical importance of Operational Security (OPSEC) in modern warfare and has demonstrated how vulnerabilities in cyber domain, the use of portable electronic devices (PEDs), and social media can be exploited by adversaries as intelligence gathering sources (Paul Schwartz et al., 2023). Cyberattacks on critical infrastructure,

intercepted communication line, and the unintended exposure of military positions through geotagged social media posts have all highlighted the necessity of robust OPSEC measures. This journal focused on how both Ukraine and Russian forces practices their operational security in this conflict and lesson learned from real-world examples.

LITERATURE REVIEW

In the context of modern military operations, the increasing reliance on the cyber domain has become a crucial factor in both operational effectiveness and threat mitigation. The manipulation of cyberspace as a strategic warfare tool is particularly evident in hybrid and fifth-generation conflicts. Jakobsson and Nielsen (2023) highlight how cyber operations amplify effects across multiple domains, including disrupting command structures, falsifying intelligence, and bypassing force protection measures.

In the context of Russia's cyber campaigns, its operations in Ukraine provide a practical case study of cyber warfare integration within military strategies. These campaigns, as part of broader hybrid warfare tactics, exploit vulnerabilities in cyberspace to disrupt both military and civilian infrastructure (Stoddart, 2024). Additionally, Russia's advanced cyber capabilities underscore the necessity for improved cybersecurity measures, particularly in countering information operations and electronic warfare (McCrory, 2020).

In the context of operational security (OPSEC) in modern warfare, safeguarding sensitive information is vital to preventing cyberattacks and data leaks that could compromise mission integrity. Lessons from the Ukraine conflict demonstrate the importance of robust OPSEC measures, including protecting military positions from geotagging and social media exposure, as well as securing communication channels against cyber threats (Schwartz et al., 2023).

In the context of cybersecurity policies and risk management, hybrid warfare has had a profound impact on global cybersecurity strategies. In response to cyber threats stemming from the Russia-Ukraine conflict, NATO and the European Union have reinforced their cyber resilience efforts, prioritizing network security and mitigation strategies to protect critical infrastructure (Kelemen, 2023). Countries facing similar threats must develop comprehensive cybersecurity policies to counteract evolving cyber warfare tactics and ensure national security.

METHODOLOGY

This journal uses literature review method by examine various research, credible analysis reports, books, news articles, and government documents from open sources relevant to the subject focusing on the use of cyber domain, portable electronic devices (PEDs), and social media in Ukraine – Russia War by both sides in the conflict. Each lesson learned obtained than discussed by defense management perspective especially on why the use of cyber domain, portable electronic devices (PEDs), and social media in modern warfare can be leverage as intelligence gathering tools by adversary. Furthermore this journal also highlight how operation security (OPSEC) procedure can be leverage as risk

management and mitigation tool to minimize negative effects of cyber domain, portable electronic devices (PEDs), and social media in modern warfare.

RESULT AND DISCUSSION

5th Generation Warfare and Multi Domain Battle Concept

The evolution of warfare through history is reflected in the generational framework, which categorizes warfare based on the timeline and characteristics of wars fought from the Napoleonic era to the present day. The 1st Generation Warfare emerged in 1648 with the Napoleonic Wars, relied on strict discipline, line-and-column tactics, and massed infantry formations. The Industrial Revolution introduced 2nd Generation Warfare, where massed firepower such as artillery, machine guns, trench warfare and attritional strategies seen in World War I. The 3rd Generational Warfare introduced in the early 20th century brought maneuver warfare, blitzkrieg tactics, and more technological advance weapons exemplified in World War II. The 4th generation warfare emerged during and post the Cold War era and characterized by asymmetric warfare, non-state actors, and blurred distinctions between civilians and combatants, with psychological operations aimed at undermining state cohesion, as seen in the Vietnam War and various insurgencies. The profound impact of technological and societal advancements shifted the framework into the 5th generation warfare (5GW) which leverage cyber domain and electronic devices to gather intelligence and conducting information war.

Table 1 Generation Warfare

Generation	Timeframe	Key Characteristics	Examples
1st GW	Post-1648 (Modern State Emergence)	Line and column tactics, regimental structure, strict discipline, focus on massed infantry.	Napoleonic Wars
2nd GW	Industrial Revolution	Massed firepower (artillery, machine guns), trench warfare, attritional strategies.	World War I
3rd GW	Early 20th Century	Maneuver warfare, focusing on speed, surprise, and bypassing enemy defenses; often referred to as "blitzkrieg tactics."	World War II, German Blitzkrieg
4th GW	Post-Cold War Era	Asymmetric warfare, non-state actors vs. states, blurred lines between civilians and combatants, focus on moral superiority, and weakening state cohesion through psychological operations.	Vietnam War, Insurgencies in Iraq and Afghanistan
5th GW	Current and Emerging	Intelligence gathering, manipulation of context and narratives, often through non-kinetic means like cyber domain and electronic signals vulnerability.	Ukraine-Russia Conflict

Source: (Daniel H Abbott, 2010)

The 5th Generation Warfare uses multiple domains including cyber domain and electromagnetic signals to disrupt adversaries through cyberattacks

on critical infrastructure, intelligence gathering networks, and information war. 5th Generation Warfare also characterized by increasing use of Portable Electronic Devices (PEDs) to enhance communication, operational efficiency and situational awareness. While the increasing use of PEDs brought many advantages it also become vectors for cyber vulnerabilities, potentially exposing sensitive data or geolocational information critical to military operations. Social media used also has emerged as a double-edged sword in 5th Generation Warfare, serving both as a platform for narrative control and psychological operations, and as a risk for inadvertent information leaks or adversary manipulation. These technologies discussed above are not merely tools but also theaters of conflict, where risk management and information dominance can decisively shape outcomes of the conflict or skirmishes. The transition between 4th Generation Warfare and 5th Generation Warfare underscores the increasing use of cyber domain and electromagnetic signals, and also the need for robust operational security (OPSEC) measures as a risk management effort to harness the advantages of these tools while mitigating their inherent risks, solidifying their role as central components in the warfare of the information age (Szymoniak & Foks, 2024).

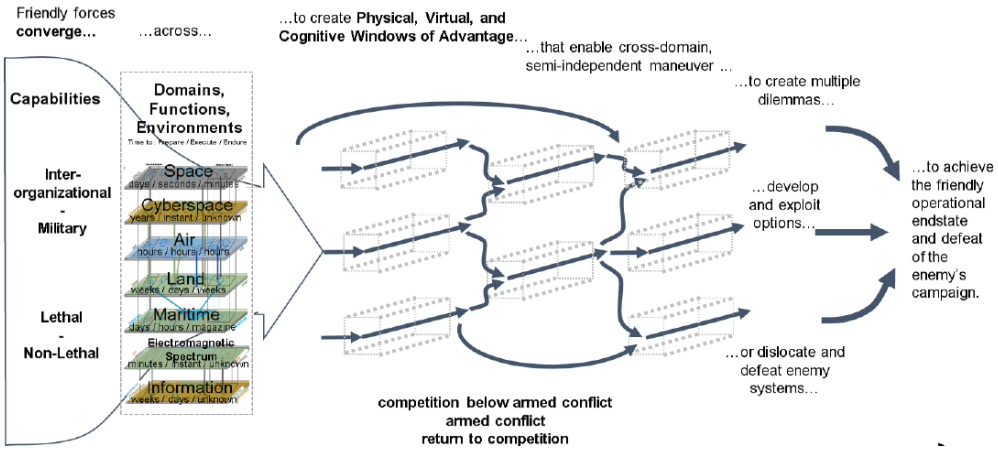

Figure 1 Multi Domain Battle Concept (Operation Headquarters Department of The Army, 2022)

Technological advances in both civilian and military use today which are reflected in 5th Generation Warfare (5th GW) are also addressed by armed forces in the world, one of which is the U.S. Army Training and Doctrine Command (TRADOC) along with other armed forces in the United States that created the Multi Domain Battle concept. MDB serves as a military response to the challenges posed by 5GW, providing a structured approach to counter the complexity, ambiguity, and non-kinetic threats characteristic of Fifth Generation Warfare. Together, they reflect the changing nature of conflict in the 21st century, where achieving dominance requires not just physical force but also cognitive, informational, and cross-domain superiority. Multi Domain Battle concept converge multiple domains such as Space, Cyber, Air, Land, Maritime, Electronic Spectrum and Information to create advantages for friendly forces, dilemmas for adversary and finally disrupt or defeat adversary. Multi Domain Warfare is one of the many concepts of operations or doctrines applied by armed forces in the

world that focuses on the utilization of various domains that were previously not given much attention by previous warfare generations such as the cyber domain, electromagnetic spectrum and information war (Miranda Priebe et al., 2021). The Ukraine – Russia Conflict demonstrates how modern warfare is increasingly multidomain, requiring forces to operate seamlessly across virtual, physical, and cognitive spaces. As such, the Ukraine War serves as a real-time example of the challenges and strategies outlined in the 5th Generation Warfare and Multiple Domain Battle concept, which emphasizing the necessity of multi-domain integration and resilience to achieve success in the face of rapidly evolving threats especially in cyber and electromagnetic spectrum (US Army Training and Doctrine Command (TRADOC), 2017).

Intelligence Gathering Methods in Modern Warfare

Intelligence gathering is a critical component of Fifth Generation Warfare (5th GW), where the focus shifts combine multi domain approach with both kinetic and non-kinetic strategies to achieve objectives. Intelligence gathering refers to the systematic process of collecting, analyzing, and disseminating information to support decision-making in military, political, and security operations. There are five disciplines of intelligence gathering—Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Open-Source Intelligence (OSINT), Geospatial Intelligence (GEOINT), and Measurement and Signature Intelligence (MASINT), each offer distinct methods to collect data from various sources. HUMINT relies on interpersonal interactions, such as informants or espionage, while SIGINT involves intercepting electronic communications. OSINT leverages publicly available data like social media and news, GEOINT uses satellite Imagery and mapping, and MASINT analyzes technical measurements, such as radar or radiation signatures (Lowenthal & Clark, 2016). In 5th GW, the increasing use of the cyber domain, portable electronic devices (PEDs), and social media presents significant opportunities for intelligence gathering. Cyber technologies enable access to adversary systems and networks, PEDs can inadvertently reveal geolocational and operational data, and social media offers a wealth of information for monitoring sentiment, identifying key actors, and detecting vulnerabilities. While these tools enhance intelligence capabilities, they also highlight the need for robust counterintelligence measures to prevent exploitation by adversaries, underscoring the dual-edged nature of technological advancements in modern warfare (Dorel Danciu, 2024).

Table 2 Five Disciplines of Intelligence Gathering

Discipline	Description	Sources/Methods	Primary Uses
Human Intelligence (HUMINT)	Intelligence gathered through interpersonal interactions.	Informants, interviews, debriefings, espionage activities.	Accessing sensitive or classified information unavailable through other means.
Signals Intelligence (SIGINT)	Intelligence obtained from intercepting electronic communications.	Phone calls, emails, radio transmissions, encrypted messages.	Monitoring adversary communications, detecting threats, and conducting cyber surveillance.

Open Source Intelligence (OSINT)	Intelligence derived from publicly available information.	News reports, social media, academic studies, government publications, public databases.	Establishing broad situational awareness, identifying trends, and gathering contextual data.
Geospatial Intelligence (GEOINT)	Intelligence derived from imagery and geospatial data.	Satellite imagery, aerial photography, mapping data, LiDAR.	Analyzing terrain, monitoring military movements, and supporting operational planning.
Measurement and Signature Intelligence (MASINT)	Intelligence based on the analysis of technical measurements and physical phenomena.	Radar signals, nuclear radiation, chemical composition, acoustic signatures.	Detecting and analyzing missile launches, nuclear tests, and environmental threats.

Source: (Lowenthal & Clark, 2016)

The increased reliance on the cyber domain, portable electronic devices (PEDs), and social media in the modern era has significantly enhanced the potential of Signals Intelligence (SIGINT) and Open Source Intelligence (OSINT) as tools for intelligence collection. SIGINT capitalizes on the vulnerabilities of unsecured or poorly encrypted devices by intercepting communications, including phone calls, emails, and messages transmitted over inadequately protected networks. Commercially available PEDs, which are primarily designed for civilian use, often lack the robust encryption and advanced security protocols required for military operations. These devices are particularly susceptible to interception and exploitation by adversaries, enabling them to extract critical information or track geolocational data. Similarly, OSINT benefits from the widespread use of social media and the digital footprints left by users. Adversaries can analyze publicly shared content, such as social media posts, photographs, or geotagged images, to derive actionable intelligence, including military positions, troop movements, and operational timelines. These points of vulnerability are common in modern warfare such as in the Ukraine - Russia War where the use of cyber domains, PEDs and social media is carried out at strategic, operational and tactical levels (Leonhardi et al., 2015).

Operational Vulnerability Lessons in Ukraine – Russia War

During the Ukraine - Russia War there were several examples of exploits of vulnerabilities from the use of cyber domains, PEDs and social media by both sides. An example of such exploitation is the use of smartphones in active battlefields and rear areas, which has significant implications for intelligence collection through Signals Intelligence (SIGINT) and Open Source Intelligence (OSINT) methods (Freese, 2023). The use of smartphones enables adversaries to monitor troop movements and identify potential targets by intercepting cellular signals and Global Positioning System (GPS) emissions from these devices (Melkozerova, 2024). A notable instance of this occurred on January 2, 2023 when Ukrainian armed forces launched a long-range attack on Russian troop positions in the Makiivka Russian-occupied city. This strike, facilitated by the detection of cellular and GPS signals emitted by smartphones used by Russian personnel,

resulted in the destruction of a Russian base and caused 89 casualties (Kwan, 2023).

The use of unencrypted communication tools represents a significant vulnerability that has been observed in the ongoing Russia-Ukraine conflict. According to an analysis report by the Royal United Services Institute for Defense and Security Studies (RUSI), Russian forces have frequently relied on Baofeng-brand commercial radio communication devices, manufactured in China, due to the inadequate performance of their standard-issue R-187P1 Azart and R-168-5UN-2 tactical military radio communication systems (Cranny-Evans & Withington, 2022). This reliance on commercial devices highlights critical operational security risks, as such equipment lacks the encryption systems necessary to protect communications from interception. In contrast, Personal Electronic Devices (PEDs) designed to military standards incorporate specialized features and specifications that are essential for secure operations. For instance, military-grade radios are equipped with advanced encryption systems, making their transmissions resistant to interception by commercial radio scanners. This example underscores the strategic importance of employing military-standard communication tools to safeguard operational integrity and prevent exploitation by adversaries. Radios such as the BaoFeng UV-82HP, observed in use by Russian forces in Ukraine, present significant vulnerabilities that can be readily exploited by Electronic Warfare (EW) practitioners (Office of The Director of National Intelligence (ODNI), 2023). First, the absence of discernible military-grade encryption renders these devices highly susceptible to straightforward jamming techniques. Second, the open frequencies utilized by these radios are easily exploited to disseminate false or misleading information, impersonating friendly forces in the vicinity (Seth G Jones, 2022). These vulnerabilities have been effectively leveraged by Ukrainian forces, enabling them to achieve tactical advantages. By exploiting these weaknesses, Ukrainian forces have successfully sown disorganization, doubt, and demoralization within Russian units, demonstrating the critical importance of secure communication systems in modern warfare.

The use of cyber-based information and communication platforms to coordinate troop movements and fire support represents a significant vulnerability in modern warfare. This issue has been notably observed in the Ukraine-Russia conflict, where Russian forces utilized the U.S.-based platform Discord for operational coordination. According to Russian state media outlet TASS, the Russian Ministry of Defense (MOD) has since banned Discord due to its inherent security risks (Matthew Loh, 2024). Originally designed for live streaming and group communication among gaming communities and online streamers, Discord was employed by Russian troops to monitor enemy movements through livestreamed frontline drone feeds and to coordinate fire support using artillery, mortars, and kamikaze drones. However, using an open and commercially available platform for such critical military operations introduces severe vulnerabilities. Discord's lack of robust encryption and open access nature makes it susceptible to intelligence gathering efforts, allowing adversaries to intercept communications, determine troop positions, and

anticipate imminent attacks. This example underscores the importance of utilizing secure, military-grade communication platforms to safeguard sensitive operational information in high-stakes environments. The ban on the Discord platform by the Russian Ministry of Defense (MOD), implemented to mitigate vulnerabilities within the cyber domain, has elicited varied responses. This decision has been met with particular concern due to the absence of any viable alternative communication platform offered by the MOD. The lack of a substitute has disrupted frontline troops who had relied on Discord for combat operational purposes, including monitoring enemy movements and coordinating fire support. This disruption highlights the critical need for secure and reliable communication solutions that balance operational effectiveness with cybersecurity imperatives in modern warfare.

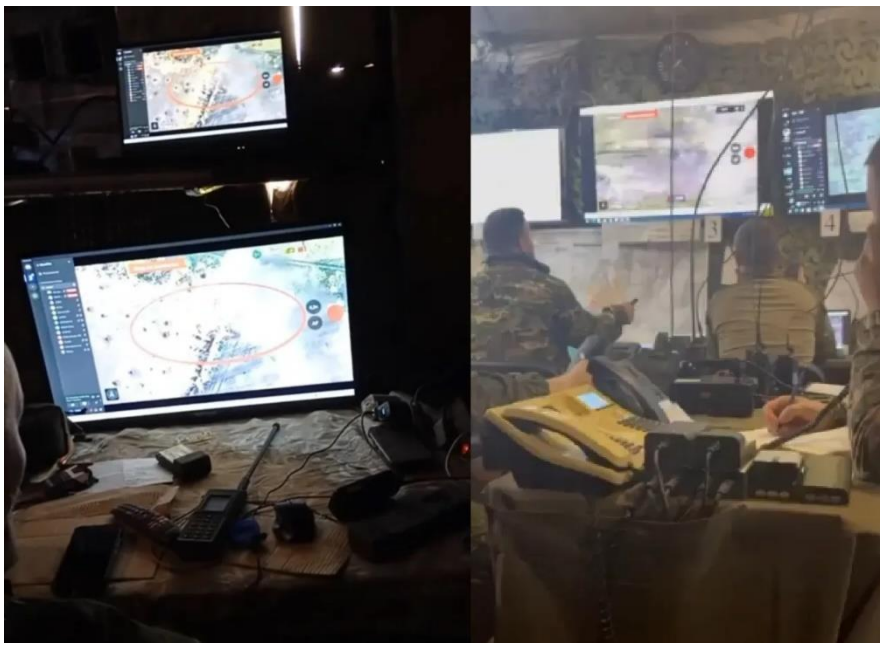

Figure 2 Russian troops using Discord platform in Ukraine (Matthew Loh, 2024)

The use of social media in modern warfare as a tool for propaganda and public relations offers significant strategic advantages. It can help garner public support on the home front while also fostering goodwill and winning the hearts and minds of the local population in areas where operations are conducted (Bejar, 2010). However, the use of social media also introduces significant vulnerabilities if not carefully managed. For instance, in January 2023, a Russian volunteer posted videos and pictures revealing the activities of the 10th Spetsnaz Brigade during operations in Kherson-Ukraine and potentially compromising operational security. Another example occurred in July 2023, when a Russian submarine commander was assassinated while jogging. According to Russian state media outlet TASS, the assassination was linked to the use of the Strava exercise application, which collects and streams jogging and cycling routes (Knight, 2023). These incidents underscore the dual-edged nature of social media in warfare—while it serves as a powerful communication and influence tool, its improper use can lead to critical security breaches, exposing personnel and operations to significant risks.

The Ukraine-Russia War has witnessed the widespread utilization of commercial drones, such as those manufactured by DJI, which have been improvised for military missions. These drones have been employed for reconnaissance and further modified, often using 3D printing, to function as kamikaze drones or to deploy munitions. This innovation has demonstrated remarkable cost-effectiveness, exemplified by widely circulated footage of a $500 DJI drone successfully neutralizing a multi-million-dollar tank. Despite their success, the use of commercial drones presents significant vulnerabilities. These drones often operate on unsecured frequencies, making them highly susceptible to signal jamming. Additionally, DJI drones are equipped with an embedded safety feature known as Aeroscope, which provides access to critical data such as the drone's location, speed, bearing, and the operator's position (Hollister, 2022). These vulnerabilities underscore the dual-edged nature of commercial drone technology in modern warfare, highlighting its potential for both tactical success and operational risk.

Operational Security (OPSEC) as Risk Mitigation Tool

Operations Security (OPSEC) is a systematic process designed to identify and safeguard critical information and indicators of friendly activities, thereby preventing adversaries from exploiting vulnerabilities that could compromise operational effectiveness. In the context of Fifth Generation Warfare (5th GW), the significance of OPSEC is greatly amplified, as 5th GW emphasizes information manipulation, perception management, and the exploitation of technological and human vulnerabilities. By protecting critical information, OPSEC ensures that adversaries are unable to aggregate seemingly trivial or unclassified details into actionable intelligence. The primary purpose of OPSEC is to safeguard mission integrity by reducing adversarial awareness, preventing the aggregation of sensitive data, and supporting other security disciplines such as cyber and physical security. Ultimately, OPSEC plays a crucial role in ensuring the success of operations, particularly in an era where non-kinetic and psychological strategies are pivotal. By maintaining information superiority, OPSEC enables military forces to deny adversaries the insights necessary to disrupt or degrade operational effectiveness.

Operations Security (OPSEC) as a formalized concept was developed by the United States during the Vietnam War. It emerged from the efforts of a group called the Purple Dragon Team, a multidisciplinary task force formed in 1966 under the direction of the U.S. military and intelligence community. The team was tasked with analyzing how adversaries were able to predict and counter U.S. military operations. The team discovered that adversaries were effectively piecing together seemingly unclassified or trivial information from U.S. communications and behaviors to anticipate actions. This realization led to the formalization of OPSEC as a systematic approach to identifying critical information, assessing risks, and implementing measures to protect operational integrity. The principles and practices of OPSEC were later codified and institutionalized with the signing of National Security Decision Directive (NSDD) 298 by President Ronald Reagan in 1988, which established a national-

level OPSEC program and required federal agencies involved in national security to implement OPSEC processes.

Table 3 Opsec Approach to Osint and Sigint Issues in Ukraine – Russia War

Technology	Vulnerability	OPSEC Mitigation Effort
Smartphone	- Emission of GPS and cellular signals that reveal troop locations. - Risk of cyberattacks and malware. - Data leaks via unregulated apps.	- Prohibit personal smartphone use in sensitive areas. - Use military-grade devices with secure communication protocols.
Commercial Radio	- Lack of encryption makes communications vulnerable to interception and jamming. - Susceptible to adversary exploitation through misinformation.	- Mandate the use of military-standard encrypted radios. - Conduct regular training on secure communication protocols.
Open Source Streaming and Communication Platform (Discord)	- Open platform prone to cyber infiltration. - Adversaries can intercept or disrupt operational coordination.	- Prohibit the use of commercial platforms for military operations. - Transition to secure, military-approved platforms.
Social Media Apps (Strava, Instagram)	- Geotagging reveals sensitive information, including troop movements and base locations. - Posts can inadvertently disclose operational details.	- Restrict social media use in operational areas. - Provide training on personal digital hygiene and OPSEC awareness.
Commercial Drone	- Unsecured frequencies vulnerable to jamming. - Embedded safety features (e.g., DJI Aeroscope) expose drone and operator locations.	- Transition to secure, military-standard drones. - Implement frequency encryption and anti-jamming technologies.

Source: (Operation Security (OPSEC) NTTP 3-13.3M, 2017),

Employing risk mitigation efforts, such as Operations Security (OPSEC), is of paramount importance in modern warfare, as evidenced in the ongoing Ukraine-Russia War. Military personnel increasingly rely on the cyber domain, Portable Electronic Devices (PEDs), and social media, all of which introduce significant vulnerabilities. To address these challenges, OPSEC, as outlined in various Department of Defense (DoD) directives, instructions, field manuals, and other service-specific regulations, provides a comprehensive framework to mitigate risks associated with these technologies. The first critical issue is the use of smartphones during combat operations. According to Department of Defense Instruction, all electronic assets procured by the DoD, including smartphones, must adhere to strict security standards, such as incorporating Trusted Platform Module (TPM) version 1.2 or higher, as required by Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) (US Department of Defense (DOD), 2014). Cryptographic products must then be utilized to protect sensitive information stored and transmitted on these devices. Following the DoD's approach, individual military branches have also established prohibitions and guidelines to mitigate risks associated with PEDs. For instance, the U.S. Air Force explicitly prohibit the use of PEDs, including

smartphones in sensitive operations. Moreover, US Air Force regulations mandate that personnel refrain from publicly disseminating or publishing information or imagery that displays critical operational details (Air Force Instruction 10-701, 2019). This includes information such as improvised explosive device (IED) strikes, battle scenes, casualties, destroyed or damaged equipment, personnel killed in action (both friendly and adversary), and protective measures of military facilities. These prohibitions also extend to posting sensitive information on social media or other internet-based platforms without proper oversight and approval. These OPSEC measures underscore the necessity of strict controls over electronic devices and digital content to safeguard critical information, maintain operational security, and mitigate risks in the modern battlefield.

The second critical issue in modern combat operations is the use of commercial radios in active combat zones. According to Department of Defense Directive (DoDD) guidelines, non-secured or non-encrypted wireless devices are strictly prohibited in areas where classified information is discussed or processed unless written approval is obtained from the Designated Approval Authority (DAA) in consultation with the Cognizant Security Authority (CSA) and Certified TEMPEST Technical Authority (CTTA). The CTTA, a U.S. Government official, is responsible for overseeing the security of an organization's physical, technical, personnel, and information infrastructure. Additionally, Operations Security (OPSEC) protocols across all military branches emphasize the mandatory use of proprietary military-standard radios that meet rigorous specifications, including encryption capabilities (Operation Headquarters Department of The Army, 2021). These military-grade communication devices undergo extensive testing to ensure they provide secure, reliable communication, protecting sensitive operational details from interception or exploitation by adversaries. This requirement underscores the critical need to avoid vulnerabilities inherent in commercial radio systems, which lack the necessary encryption and security features to withstand adversarial threats in high-stakes operational environments.

Table 4 Us Dod Networks

Feature	NIPRNet	SIPRNet	JWICS
Classification	Unclassified	Secret	Top Secret
Primary Use	Administrative and routine tasks	Tactical/operational classified info	High-level intelligence sharing
Encryption	Secured	Encrypted	Fully encrypted
Users	DoD Personnel, Contractors	Military, DoD, Allies	Intelligence Agencies

Source:(US Department of Defense (DOD) Directive 8100.02 Regarding Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), 2004)

Third issue is the use of open-source streaming and communication platforms such as Discord for coordinating troop movements, executing fire support missions, and relaying information to headquarters presents substantial vulnerabilities. These platforms designed for commercial applications lack the

security measures necessary to safeguard sensitive operational data, leaving them susceptible to exploitation through Open Source Intelligence (OSINT) and Signals Intelligence (SIGINT) methods by adversaries (Ward, 2018). To address these vulnerabilities, defense organizations should implement a structured framework for network systems categorized by classification levels, such as Unclassified, Secret, and Top Secret. For instance the U.S. Department of Defense (DoD) operates distinct networks tailored to these classifications: the Non-Classified Internet Protocol Router Network (NIPRNet) for unclassified but sensitive information, the Secret Internet Protocol Router Network (SIPRNet) for classified information up to Secret, and the Joint Worldwide Intelligence Communications System (JWICS) for information classified at the Top Secret level and above. Utilizing proprietary and secure networks specifically designed for military operations would significantly mitigate vulnerabilities, ensuring that critical functions, such as troop coordination, fire support missions, and information relay, are protected from adversarial exploitation.

The fourth issue concerns the use of social media, which poses significant vulnerabilities due to posts or uploads that may inadvertently disclose sensitive information or geolocation data. Such actions can compromise operational security by revealing deployment timelines, locations, or other critical information (Linder, 2024). To mitigate these risks, comprehensive Operations Security (OPSEC) training is essential for Department of Defense (DoD) personnel and military branch members. This training aims to enhance awareness and discipline, ensuring that individuals refrain from sharing details about ongoing or upcoming deployments or other sensitive activities on social platforms. Despite its risks, social media can also serve as a powerful tool when used strategically. It can be leveraged to create positive narratives, bolster public support, and foster goodwill by winning the hearts and minds of target audiences. By striking a balance between cautious use and strategic messaging, social media can contribute positively to operational objectives while minimizing vulnerabilities through disciplined adherence to OPSEC principles.

The last issue is the use of commercial drone like DJI drone for reconnaissance and improvised using 3D printer technology becoming effector as kamikaze drone or drone dropped munition, which utilized greatly in Ukraine – Russia War. However due to commercial nature of the drone, the drone come with vulnerability points from the nonencrypted frequency used that prone to signal jamming and the safety feature embedded in the drone like Aeroscope in DJI drone which able to show the flight data and drone operator location openly. To mitigate this, OPSEC emphasized on using military standard equipment which more secured from enemy signal jammer and tracking capability. Another indigenous effort is showed by Ukraine 68th Jager Brigade which successfully modify software program to disable the tracking feature like Aeroscope in DJI drone (Skove, 2022).

CONCLUSIONS AND RECOMMENDATIONS

Conclusion

The increasing reliance on technology in modern warfare, as demonstrated in the Ukraine-Russia War, underscores the critical importance of

Operations Security (OPSEC). The vulnerabilities associated with smartphones, commercial radios, open-source communication platforms, social media, and commercial drones highlight the challenges posed by the cyber domain and modern electronic devices. Each of these technologies, while offering operational advantages, also creates significant risks of exploitation through Signals Intelligence (SIGINT) and Open Source Intelligence (OSINT) methods. To mitigate these risks, OPSEC emphasizes the use of military-standard equipment, secure communication protocols, and rigorous training to enhance awareness among personnel. Innovative approaches, such as disabling tracking features in drones and implementing secure networks like NIPRNet, SIPRNet, and JWICS, demonstrate effective solutions to these vulnerabilities. Additionally, social media, while a double-edged sword, can be strategically leveraged for positive narratives if managed within OPSEC guidelines. By adopting comprehensive risk mitigation measures, military organizations can harness the benefits of modern technology while safeguarding operational integrity, maintaining information superiority, and ensuring mission success in the complex landscape of Fifth Generation Warfare (5GW).

Recommendations

To enhance operational security (OPSEC) in modern warfare, the military must regularly train personnel on cybersecurity, secure communication, and the risks of using personal electronic devices (PEDs). The use of commercial communication platforms like public radios and open-source apps should be restricted to prevent exploitation by adversaries. Additionally, all communication tools, drones, and networks must meet military standards with strong encryption to prevent interception and cyber threats.

Governments should also strengthen cybersecurity policies by collaborating with allied nations to protect critical infrastructure. Military personnel's social media use must be strictly monitored to avoid unintentional leaks of operational information. Counter-intelligence measures should be implemented to prevent surveillance and espionage. Lastly, military drone technology should be developed with encrypted frequencies and anti-jamming features to prevent tracking and interference by adversaries.

ADVANCED RESEARCH

Advanced research in the domain of Operations Security (OPSEC) amid modern warfare should focus on the integration of artificial intelligence (AI) and machine learning (ML) to proactively detect, analyze, and neutralize emerging cyber threats and intelligence vulnerabilities. This includes developing AI-driven systems capable of real-time monitoring of communication networks, identifying anomalous data patterns indicative of SIGINT or OSINT intrusions, and automatically enforcing security protocols. Research should also explore the enhancement of quantum-resistant encryption technologies to future-proof military communications against evolving computational threats. Furthermore, interdisciplinary studies combining behavioral science and cybersecurity can improve understanding of how human factors, such as social media behavior or inadvertent data disclosures, impact OPSEC, leading to more effective training

programs and user-centric security designs. These advancements, supported by robust international collaboration and continuous policy evolution, will be pivotal in maintaining a technological edge and safeguarding operational integrity in the era of Fifth Generation Warfare (5GW).

REFERENCES

Air Force Instruction 10-701 (2019).

Bejar, A. (2010). OPSEC and Social Media. *US Naval War College*.

Cranny-Evans, S., & Withington, T. (2022). Russian Comms in Ukraine: A World of Hertz. In *https://rusi.org/explore-our-research/publications/commentary/russian-comms-ukraine-world-hertz*.

D. van der Waal, & V. Versluis. (2017). *Introduction to risk management*. Erasmus+.

Daniel H Abbott. (2010). *The Handbook of 5GW Book Jacket None*. Nimble Books LLC.

Dorel Danciu. (2024). *SOCIAL MEDIA AND THE SECURITY OF MILITARY OPERATIONS*. https://www.ceeol.com/search/article-detail?id=1205990

Freese, K. (2023). Smart Phones Playing Prominent Role in Russia-Ukraine War. In *US Army Training and Doctrine Directorate (TRADOC)*.

Galvin, Tom., Waters, D. E.., Yuengert, Lou., Meinhart, R. M.., Gellert, F. J.., & Work, R. O. (2019). *Defense Management: Primer for Senior Leaders*. Department of Command, Leadership, and Management, School of Strategic Landpower, U.S. Army War College.

Hari Burcu-Marcu, Philipp Fluri, & Todor Tagarev. (2009). *Defence Management an Introduction*. Geneva Center for Democratic Controlled of Armed Forces.

Hollister, S. (2022). DJI drones, Ukraine, and Russia — what we know about AeroScope. In *https://www.theverge.com/22985101/dji-aeroscope-ukraine-russia-drone-tracking*.

Knight, M. (2023). Russian commander killed while jogging may have been tracked on Strava app. In *https://edition.cnn.com/2023/07/11/europe/russian-submarine-commander-killed-krasnador-intl/index.html*.

Kwan, R. (2023). Russia blames its soldiers' cellphone use for missile strike that killed dozens. In *https://www.nbcnews.com/news/world/russia-blames-soldiers-phone-use-ukraine-missile-strike-rcna64187*.

Leonhardi, E. V.; Murphy, M.; & Kim, H. (2015). Social Media Policy and its Impact on Operational Security. *Calhoun: The NPS Institutional Archive DSpace Repository Analysis of Department of Defense*. http://hdl.handle.net/10945/45890

Linder, E. (2024). Russian government warns soldiers and residents of Ukrainian-threatened regions to avoid dating apps and social media. In *https://www.abc.net.au/news/2024-08-22/russian-government-tells-kursk-region-stay-off-dating- apps/104256114*.

Lowenthal, M. M.., & Clark, R. M. (2016). *The Five Disciplines of Intelligence Collection*. CQ Press, an imprint of Sage Publications, Inc.

M. Kubilay Akman. (2018). OPSEC Model and Applications. *The Central and Eastern European Online Library*. https://doi.org/10.24356/SD/25/3

Matthew Loh. (2024, October 9). *Russia cut off its troops from Discord, the video gaming comms tool they use to coordinate attacks in Ukraine*.

Https://Www.Businessinsider.Com/Russian-Troops-Discord-Drone-Attacks-Shut-down-Ukraine-War- 2024-10.

Melkozerova, V. (2024). Russia cracks down on personal phones on the frontline. In *https://www.politico.eu/article/russian- duma-adopts-law-on-punishment-for-soldiers-using-gadgets-on-the-frontline/*.

Miranda Priebe, Douglas C. Ligor, Bruce Mcclintock, Michael Spirtas, Karen Schwindt, Caitlin Lee, Ashley L. Rhoades, Derek Eaton, Quentin E. Hodgson, & Bryan Rooney. (2021). *Multiple Dilemmas: challenges and options for all domain command and*. RAND CORPORATION.

Office of The Director of National Intelligence (ODNI). (2023). *Support Provided by the People's Republic of China to Rusia*. Operation Headquarters Department of The Army. (2021). *US Army Field Manual FM 3-12 Cyberspace Operations and Electromagnetic Warfare*. https://armypubs.army.mil

Operation Headquarters Department of The Army. (2022). *US Army Field Manual FM 3-0 Multidomain Operations*.

Operation Security (OPSEC) NTTP 3-13.3M (2017).

Paul Schwartz, Dmitry Gorenburg, & Olga Thomas. (2023). Russian Military Mobilization During the Ukraine War. *Center for Naval Analyses (CNA)*.

Seth G Jones. (2022). Russia's Ill-Fated Invasion of Ukraine Lessons in Modern Warfare. *Center for Strategic and International Studies*.

Skove, S. (2022). How Ukraine learned to cloak its drones from Russian surveillance. In *https://www.c4isrnet.com/battlefield- tech/2022/10/17/how-ukraine-learned-to-cloak-its-drones-from-russian-surveillance/*.

Szymoniak, S., & Foks, K. (2024). Open Source Intelligence Opportunities and Challenges – A Review. *Advances in Science and Technology Research Journal*, *18*(3), 123–139. https://doi.org/10.12913/22998624/186036

US Army Training and Doctrine Command (TRADOC). (2017). *Multi-Domain Battle: Evolution of Combined Arms for the 21st Century 2025-2040*.

US Department of Defense (DOD). (2014). *US Department of Defense (DOD) Instruction 8500.01 regarding Cybersecurity*. US Department of Defense (DOD) Directive 8100.02 Regarding Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) (2004).

Ward, D. (2018). Fit to Be Spied: Fitness Trackers and OPSEC Risks. *NCO Journal*. http://www.armyupress.army.mil/Journals/NCO-