ELEKTROTEHNIŠKI VESTNIK 92(5): 229–242, 2025
ORIGINAL SCIENTIFIC PAPER

Hybrid Threats and Mobile Devices: A Systems Perspective on the Use of Smartphones in Hybrid Warfare

Luka Podlesnik, Anže Mihelič, Blaž Markelj

Faculty of Criminal Justice and Security, University of Maribor, Kotnikova ulica 8, 1000 Ljubljana, Slovenia
E-mail: luka.podlesnik@student.um.si

Abstract. The proliferation of civilian mobile technologies in modern conflict zones has significantly transformed the operational, psychological, and cyber aspects of warfare. The paper employs a systems thinking approach to model the use of mobile devices in hybrid warfare, with a particular focus on the Russian-Ukrainian conflict (2014-2024). Using a causal loop diagram (CLD) based on empirical data, the paper shows how mobile devices serve as both tactical tools and systemic vulnerabilities. It identifies the reinforcing feedback loops that accelerate the integration of mobile devices into battlefield operations, such as enhanced communication, crowdsourced intelligence, and deployment of operational apps, while also recognizing the balancing feedback structures that create friction through cyber threats, disinformation, signal exposure, and psychological stress. The model highlights how trust and psychological resilience serve as critical behavioral levers within the system, susceptible to both positive reinforcement and cascading degradation. This systems-based perspective informs strategic planning and underscores the importance of managing both the technological benefits and the emerging vulnerabilities of mobile device use in modern conflicts.

Keywords: hybrid warfare, mobile devices, cyber operations, electronic warfare, digital resilience

Hibridne grožnje in mobilne naprave: sistemski pogled na uporabo pametnih telefonov v hibridnem vojskovanju

Razmah civilnih mobilnih tehnologij v sodobnih konfliktnih območjih je močno preoblikoval operativne, psihološke in kibernetske razsežnosti vojskovanja. Članek s sistemskim pristopom analizira uporabo mobilnih naprav v hibridnem vojskovanju, s posebnim poudarkom na rusko-ukrajinskem konfliktu (2014–2024). S pomočjo diagramov vzročnih zank (CLD) na podlagi empiričnih podatkov pokaže, da mobilne naprave delujejo hkrati kot taktična orodja in kot sistemske ranljivosti. Opiše krepitvene zanke, ki pospešujejo vključevanje mobilnih naprav v bojne operacije – od izboljšane komunikacije in množičnega zbiranja obveščevalnih podatkov do uporabe operativnih aplikacij – ter uravnoteževalne zanke, ki ustvarjajo trenja prek kibernetskih groženj, dezinformacij, razkritja signalov in psiholoških obremenitev. Model poudari, da sta zaupanje in psihološka odpornost ključna vedenjska vzvoda, občutljiva na pozitivne učinke, pa tudi na hitro erozijo. Takšen sistemski pogled podpira strateško načrtovanje in izpostavlja pomen uravnavanja tehnoloških prednosti ter novih ranljivosti, ki jih prinaša uporaba mobilnih naprav v sodobnih konfliktih.

Received 7 June 2025
Accepted 27 October 2025

1 INTRODUCTION

The nature of warfare is evolving in response to deep technological, social, and informational transformations. As modern conflicts increasingly unfold across physical and digital domains, the boundaries between civilian and military spheres are becoming more porous. One of the most notable developments is the increasing integration of everyday digital technologies, particularly mobile devices, into military operations. Once peripheral to state security, smartphones have become central to the way wars are fought, coordinated, and experienced, particularly in hybrid warfare environments where the military, cyber, and psychological domains are deeply intertwined [1, 2]. The ongoing conflict in Ukraine has highlighted how smartphones and mobile applications function not only as tools for coordination and intelligence gathering but also as vectors for surveillance, disinformation, and targeting [3, 4].

Although previous research has highlighted the tactical advantages, psychological effects, and cybersecurity risks of mobile device use in conflict, these dimensions are often analyzed in isolation [4, 5, 6, 7, 8, 9]. What remains underexplored is how these functions and vulnerabilities interact within a dynamic system that evolves in response to operational feedback, adversarial adaptation, and shifts in civilian and military behavior

[1, 10].

This paper addresses this gap by applying a systems thinking approach to model the role of mobile devices in hybrid warfare, with particular attention to the feedback loops that shape their operational, psychological, and cyber dimensions. To guide the analysis, the paper poses the following research question: *How do mobile devices function as enablers and systemic vulnerabilities in hybrid warfare through feedback-driven interactions?* By constructing a causal loop diagram (CLD) based on empirical insights from the Russian-Ukrainian conflict (2014-2024), the paper identifies the key variables, maps their interrelationships, and analyzes the reinforcing and balancing feedback structures that govern the mobile device use in conflict environments. The aim is to move beyond linear assessments and instead reveal the complex, nonlinear dynamics that make mobile technologies both strategic assets and systemic liabilities in modern warfare.

Through this framework, the paper contributes a novel systems-based perspective to the analysis of civilian mobile technologies in war. It models mobile device use in hybrid warfare as a complex adaptive system, mapping interdependencies and emergent behaviors that shape battlefield and information space dynamics. In doing so, the paper offers a conceptual basis for understanding the digital civilian-military interface as an evolving and strategically significant component of modern conflict.

2 Theoretical and Analytical Foundations

Understanding the role of mobile devices in hybrid warfare requires examining their function within broader strategic, technological, and analytical contexts. This section outlines the key conceptual foundations that underpin the analysis. It begins with a discussion of hybrid warfare, the strategic integration of civilian technologies into modern conflict, and the ways mobile devices function as tactical, psychological, and cyber assets. Finally, it introduces a systems thinking perspective to frame how mobile technologies interact with broader operational, informational, and behavioral feedback loops, providing a basis for the causal modeling approach.

2.1 *Hybrid Warfare and Civilian Technology*

Hybrid warfare is an adaptive approach to conflict that combines conventional and nonconventional methods to achieve political objectives under ambiguous conditions. It integrates kinetic force with non-kinetic strategies, such as cyber operations, psychological manipulation, disinformation, and economic coercion. NATO defines hybrid threats as actions by state or non-state actors designed to undermine or harm a target by covertly or overtly combining military and non-military means [11]. This ambiguity is central to the operational logic of hybrid warfare, making attribution difficult and response complex [1, 12].

The 2014 annexation of Crimea and subsequent conflict in eastern Ukraine exemplify hybrid warfare in action. Russia used a combination of regular troops, special forces, local militias, cyber operations, and propaganda to destabilize Ukrainian sovereignty while avoiding full-scale conventional warfare and the associated international consequences. The employment of Battalion Tactical Groups (BTGs), integrated with irregular units, cyber capabilities, and media narratives, allowed Russia to exert control while maintaining plausible deniability [12].

A defining feature of modern hybrid warfare, especially evident in the Russian-Ukrainian conflict, is the strategic appropriation of civilian technologies. The civilian communication infrastructure, particularly the mobile devices and platforms they access, has become integral to both offensive and defensive military operations. Smartphones have blurred the boundary between combatants and noncombatants, serving simultaneously as surveillance tools, propaganda platforms, and intelligence-gathering devices [5].

In Ukraine, smartphones have become critical tools for civilian participation in defense efforts. Civilians have used applications such as ePPO and Diia's e-Enemy feature to report enemy troop movements, share geotagged images of military equipment, and relay real-time targeting information to Ukrainian forces [2, 6]. The massive proliferation of such crowdsourced intelligence demonstrates a significant shift in warfare: from centralized command structures to distributed digital participation. According to Ford and Hoskins [13], this is a form of 'participative warfare' in which civilians equipped with smartphones are not only witnesses of the conflict but also active participants through data production, real-time communication, and operational intelligence support.

This participative dynamic is not without risks. Civilian involvement in military operations can blur the principle of distinction enshrined in international humanitarian law, potentially affecting their protected status under the laws of armed conflict [2]. In addition, the widespread use of smartphones exposes users to electronic warfare, geolocation-based attacks, and surveillance. Russian forces have reportedly used IMSI catchers, malware, and passive RF triangulation to identify and target mobile phone users, sometimes leading to shelling of their locations [14].

The weaponization of civilian technology in hybrid warfare also has a profound psychological and informational dimension. Smartphones mediate the experience of war, enabling users to broadcast real-time images of violence and morale messaging, while simultaneously serving as platforms for strategic influence campaigns.

Social networks and mobile connectivity shape both battlefield perceptions and public opinion, complicating the information environment and contributing to what has been conceptualized as cognitive warfare [5, 11, 15, 16]. The FP Analytics report highlights how multistakeholder partnerships between government, industry, and civil society are central to Ukraine's ability to maintain digital resilience under sustained hybrid threat conditions [17].

Hybrid warfare in the Russian-Ukrainian context reveals how civilian technology has evolved into both a component of military-political strategy and a contested battlespace [1, 11, 18]. The convergence of military objectives with civilian infrastructure demands a reevaluation of traditional distinctions between war and peace, frontlines and home fronts, and combatants and civilians [2, 4]. This new hybridity sets the stage for a deeper exploration of the tactical, psychological, and cyber functions of mobile devices in contemporary conflict, the focus of the following subsection [6, 13].

2.2 Mobile devices as Tactical, Psychological, and Cyber Assets

Throughout the paper, *mobile devices* refer to commercially available, network-enabled civilian technologies, such as smartphones, tablets, and feature phones, used in frontline, near-frontline, or civilian-military interface zones. This includes both smart and non-smart devices, ranging from advanced Android-based tablets used for artillery fire control to basic mobile phones used for making calls and sending SMS messages. These devices typically operate on civilian cellular, Wi-Fi, or satellite networks and are distinct from military-grade radios, unless they are explicitly integrated with mobile platforms. Evidence from the Russian-Ukrainian conflict indicates that mobile devices have been widely used for battlefield coordination, intelligence sharing, and psychological support, but have also introduced risks associated with signal emissions, disinformation, and cyber intrusions [2, 4, 7].

The widespread integration of such devices highlights their evolving status as strategic assets in hybrid warfare. Civilian technologies, once peripheral to military operations, now shape both tactical outcomes and political narratives [2, 4, 5, 19]. This section analyzes mobile devices in three interlinked domains: tactical, psychological, and cyber, highlighting their dual-use character as both operational enablers and systemic vulnerabilities.

2.2.1 Tactical Dimension: The use of mobile devices has significantly improved battlefield intelligence, operational coordination, and overall combat effectiveness. They enable rapid communication, dissemination of intelligence, and coordination between civilians and military personnel [4, 5, 6, 7]. For example, the Ukrainian Ministry of Digital Transformation's e-Vorog application demonstrates how civilian contributions through mobile devices can significantly bolster tactical intelligence capabilities [5, 6].

Applications like Telegram have enabled rapid dissemination of air-raid warnings, logistics updates, and operational intelligence [5, 6, 20]. Various other mobile applications and systems have also played an essential role in providing a tactical advantage. The e-Vorog application has enabled civilians to report enemy locations directly to Ukrainian military intelligence [5, 6], and the ePPO application has allowed civilians to assist air defense units by reporting incoming missiles and drones using GPS-enabled smartphones [2]. The ”Bronya” (”Armour”) software, installed on tablets, has automated ballistic calculations for various artillery systems [7]. These technologies collectively demonstrate how civilian mobile devices and specialized applications have become deeply embedded in tactical battlefield operations.

Despite the tactical advantages, smartphones expose users to vulnerabilities, such as location tracking through electronic warfare systems. Russian military units have exploited this vulnerability with sophisticated technologies, such as Leer-3 drones and Zhitel systems, utilizing signal interception to carry out targeted operations [4, 7, 9, 14, 21]. To mitigate vulnerabilities associated with smartphone use, Ukrainian forces have adopted adaptive countermeasures, such as restricting device use near the frontlines, employing burner phones, and using encrypted communication applications to minimize operational risk [9, 22, 23].

2.2.2 Psychological Dimension: Mobile devices can impact morale and cohesion, pose psychological risks, and facilitate information warfare. They enhance morale by facilitating continuous communication and rapid message dissemination, thereby maintaining crucial interpersonal relationships that foster psychological resilience in combat [3, 4, 5, 6, 7].

They are also tools for information warfare, used to spread information and counter-narratives. For example, pro-Kremlin channels use Telegram and SMS to disseminate disinformation and shape public perceptions [3, 9, 20, 22].

However, constant connectivity has increased exposure to disinformation, potentially worsening stress and psychological trauma, and highlighting the need for media literacy and psychological resilience strategies [5, 6, 24, 25]. The psychological impact of mobile device use has depended heavily on trust in their security and functionality; fluctuations in trust have affected soldiers' willingness to use smartphones for both operational communications and personal connections [2, 3, 5].

2.2.3 Cyber Dimension: The role of mobile devices in hybrid warfare extends beyond tactical and psychological dimensions to the cyber realm. Although not typically used for offensive cyber operations, they play an essential role as tools for situational awareness, real-time intelligence sharing, and decentralized command and control, linking battlefield dynamics with digital decision-making [2, 6, 14].

Despite their utility, mobile devices have become attractive targets for adversaries seeking to disrupt, surveil, or manipulate. Russian and Ukrainian actors have employed various tools and techniques, such as malware, spear-phishing, and DDoS attacks, which have degraded communication platforms and disabled critical infrastructure [8, 23, 26]. In response to persistent cyber threats, external cyber-operational support from actors such as Microsoft, Google, and SpaceX's Starlink has been instrumental in enhancing Ukraine's cyber resilience and protecting mobile communication networks from disruption [3, 8, 17, 26]. More subtly, adversaries have leveraged mobile platforms for cyber-enabled intelligence operations by intercepting data streams, conducting surveillance through compromised apps, and disseminating disinformation through messaging and social media services [3, 8, 22, 23].

In some cases, smartphones have become points of convergence between electronic warfare and cyber activity, where location signals and geolocation data have been harvested for targeting purposes [8, 26], as exemplified by the compromise of the Ukrainian artillery fire coordination application [3]. This was achieved through the deployment of X-Agent malware by the Russian APT28 group, which enabled the retrieval of communications and location data from infected devices [27].

2.3 Systems Thinking as a Modeling Framework

Hybrid warfare is characterized by its complexity, ambiguity, and the co-evolution of the cyber, psychological, and kinetic domains [12]. Traditional linear analysis methods often fail to capture the interconnected dynamic nature of these environments, where effects may be delayed, amplified, or emerge unexpectedly through feedback processes. Systems thinking offers a powerful alternative by framing hybrid warfare as a complex adaptive system, one in which multiple interacting variables produce emergent behaviors, tipping points, and nonlinear outcomes [28, 29]. This approach enables analysts to identify reinforcing and balancing structures, trace unintended consequences, and recognize leverage points that would otherwise remain obscured [29]. Given that hybrid threats often exploit interdependencies across civilian and military domains, systems thinking is particularly well-suited to modeling their strategic and operational dynamics.

To analyze the multidimensional role of mobile devices in hybrid warfare, the paper employs a systems thinking perspective, operationalized through causal loop diagrams (CLDs). Systems thinking enables researchers to move beyond linear cause-effect assumptions and instead understand complex systems as interrelated wholes characterized by feedback, delays, and nonlinearity [30, 31]. The approach is particularly suited to hybrid conflict environments, where mobile technology serves as both an enabler of military effectiveness and a vector for cyber, psychological, and surveillance-related threats.

CLDs are used as the primary modeling method for capturing the dynamic interdependencies of mobile device use during the Russian-Ukrainian conflict. CLDs represent systems as sets of variables linked by causal arrows that indicate positive or negative relationships and feedback loops [29, 32]. They have been shown to improve systemic reasoning, identify leverage points, and foster holistic understanding in complex problem-solving tasks [33].

In practice, the systems thinking approach was used in this paper to trace how variables such as operational effectiveness, cyber threat exposure, troop morale, and disinformation interact over time. Particular emphasis was placed on identifying both reinforcing feedback structures and balancing loops. This approach supports a more nuanced interpretation of hybrid dynamics by revealing counterintuitive behaviors and systemic risks that might not be apparent in static or reductionist analyses [29, 33].

This analytical lens is consistent with earlier applications of system dynamics in the military and cybersecurity domains, where CLDs have been used to model cyber conflict escalation, operational breakdowns, and strategic decision-making [34, 35, 36]. Drawing on qualitative insights from the Ukraine-specific literature, the present paper aligns its model-building with empirical grounding and best practices in system dynamics.

3 Methodology

This paper adopts a qualitative systems thinking methodology to examine the role of mobile devices in the dynamics of hybrid warfare. CLDs are used as the primary modeling technique due to their ability to represent nonlinear interdependencies, feedback structures, and delayed effects in complex adaptive systems [29, 32]. This methodology is particularly suitable for analyzing hybrid conflict environments, where civilian technologies dynamically interact with military operations, psychological effects, and cyber vulnerabilities [12, 28].

3.1 Modeling Framework

CLDs translate a systems thinking perspective into a concrete representation of hybrid warfare as a dynamic system of interrelated variables and feedback loops. In this paper, the CLD models mobile device use both as inputs and outputs of conflict behaviors, capturing how battlefield practices, cyber threats, psychological resilience, and tactical adaptations interact. This method supports the identification of systemic leverage points, reinforcing dynamics, and potential destabilizing feedback loops [29, 33].

3.2 Data Sources and Variable Selection

The model's development is based on an extensive review of the empirical literature on the Russian-Ukrainian conflict (2014-2024), drawing on academic journals, defense policy reports, cybersecurity briefs, military field studies, and credible gray literature. Key documents included case studies of smartphone use, the dynamics of disinformation, intelligence practices, psychological operations, and reports on Russian and Ukrainian cyber tactics. Cross-source triangulation is employed to ensure the empirical validity of each variable, and each causal link is supported by at least two independent sources, thus minimizing speculative or anecdotal inference.

The key variables are selected based on their relevance to mobile device use in hybrid warfare and their role in shaping tactical, psychological, and cyber outcomes. These variables include mobile device use, communication and coordination, exposure to cyber threats, operational effectiveness, trust in mobile technologies, and disinformation dynamics.

3.3 Causal Mapping and Relationship Designation

Once the variable set is established, causal relationships between them are mapped. A positive causal link indicates that an increase in one of the variables leads to an increase in another (or a decrease in one leads to a decrease in the other). Conversely, a negative link signifies an inverse relationship. For example, increased use of mobile devices leads to greater signal exposure (positive link), while increased command restrictions reduce mobile device use (negative link). Each link is coded using conventional systems modeling conventions and is incorporated into the evolving CLD through an iterative mapping process [29].

3.4 Feedback Loop Identification and Classification

The feedback loops, i.e., closed chains of causal relationships, are then identified within the system. Reinforcing loops are defined as self-reinforcing dynamics that amplify change, while balancing loops introduce counteracting mechanisms that moderate behavior. The loops are traced manually and tested through counterfactual reasoning and sensitivity mapping to ensure structural integrity under hypothetical perturbations [29, 32]. Each loop is labeled and classified according to its behavioral function, as described in the Results section.

3.5 Scope and Limitations of the Model

The model focuses on the sociotechnical dynamics of mobile device use in hybrid warfare. It does not explicitly model kinetic force deployment, formal command-and-control hierarchies, or state-level diplomatic strategies. Instead, it focuses on front and near-frontline conditions where civilian and military actors interact through networked mobile platforms. The model is of a qualitative nature, although it identifies relationships and systemic structure; it does not assign quantitative weights, time delays, or probabilities, which would be required for complete simulation modeling [29].

This approach is suitable for the exploratory objectives of this paper and provides a conceptual basis for future research that will use simulation-based techniques. Methods such as system dynamics modeling and agent-based simulation can be used to assess the sensitivity of interdependencies and anticipate potential unintended outcomes of mobile device use in hybrid conflict scenarios. These methodologies offer tools for translating qualitative models into executable simulations that help to visualize how feedback loops and delays shape long-term conflict trajectories [16, 29, 35].

4 Results

This section presents the results of the causal analysis of mobile device use in hybrid warfare. Based on the identified and mapped key variables, a set of core factors and their causal interrelationships was established. The key variables are summarized, along with their definitions and supporting literature, and then the validated causal links between them are presented. Finally, the dynamic feedback structures emerging from the system are analyzed to illustrate the reinforcing and balancing behaviors governing mobile device use in hybrid conflict environments.

4.1 Key Variables

A set of key variables was identified to capture the operational, technological, psychological, and cybersecurity dimensions of mobile device use in hybrid warfare. Table 1, located in (Appendix A), summarizes these variables, provides concise definitions, and links them to their primary supporting literature.

4.2 Causal Relationships

Based on the identified variables, causal relationships were mapped to illustrate how changes in one factor influence others within the system. Table 2, in (Appendix A), presents the validated causal links, while Figure 1 visually depicts these interconnections using the CLD.

4.3 Feedback Structures

The CLD shown in Figure 1 reveals multiple interacting feedback loops that shape system dynamics in hybrid warfare. They fall into two main categories: reinforcing structures, which amplify behaviors and dependencies, and balancing structures, which constrain or correct the system in response to emerging risks, friction, or overload. In the diagram, the reinforcing loops are labeled ”R” and indicate self-reinforcing (amplifying) dynamics,

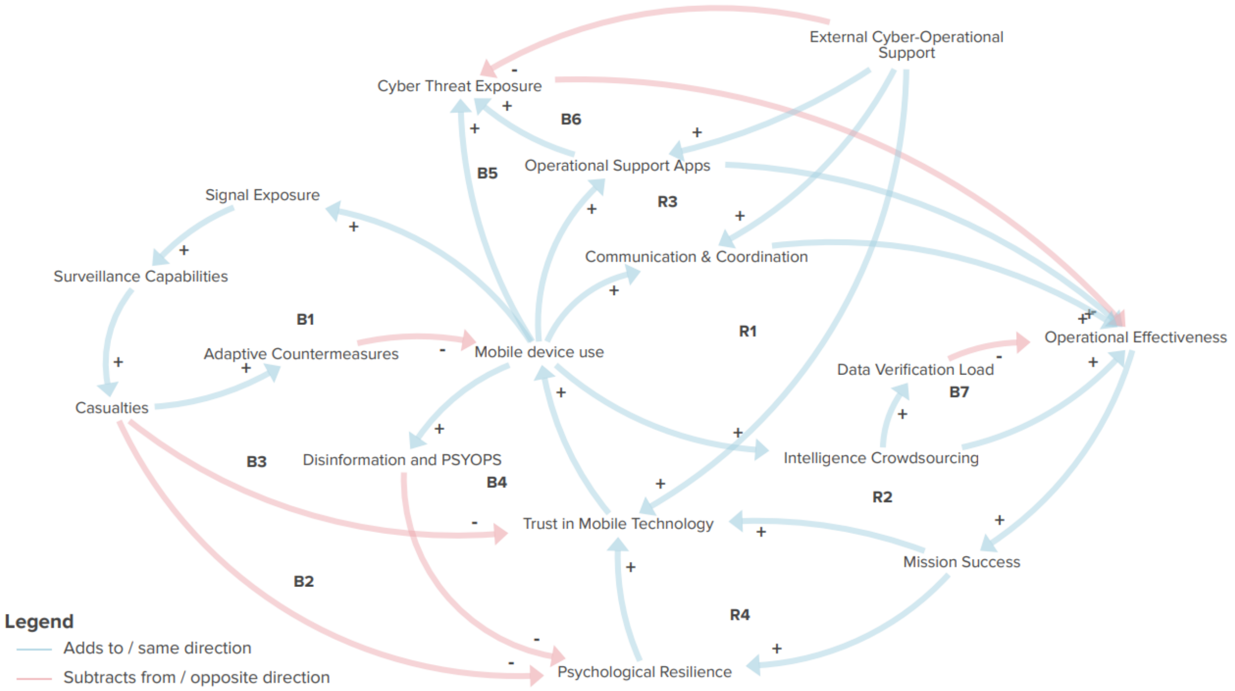
External Cyber-Operational Support
Cyber Threat Exposure
B6
Operational Support Apps
B5
Signal Exposure
R3
Communication & Coordination
Surveillance Capabilities
B1
R1
Adaptive Countermeasures
Mobile device use
Operational Effectiveness
Data Verification Load
B7
Casualties
Intelligence Crowdsourcing
B3
Disinformation and PSYOPS
B4
R2
Trust in Mobile Technology
Mission Success
B2
R4
Legend
Adds to / same direction
Subtracts from / opposite direction
Psychological Resilience

Figure 1. Causal loop diagram showing the key feedback loops governing the use of mobile devices in hybrid warfare. Arrows indicate causal relationships; the (+) sign means the variables change in the same direction, and the (-) sign means they change in opposite directions. The R-labeled loops are reinforcing (amplifying). The B-labeled loops are balancing (stabilizing).

and the balancing loops are labeled ”B” and represent stabilizing or self-correcting processes.

4.3.1 Reinforcing Feedback Loops: Reinforcing (positive) feedback loops reflect the system’s tendency to escalate mobile device use in response to favorable battlefield dynamics and perceived technological effectiveness.

4.3.1-A) R1: Communication-Effectiveness Loop: Mobile device use enhances communication and coordination, thus improving operational effectiveness. This increases trust in mobile technologies and reinforces continued or expanded use.

4.3.1-B) R2: Crowdsourced Intelligence Loop: Mobile device use enables intelligence crowdsourcing, thereby improving battlefield awareness and operational effectiveness. Success reinforces trust in the use of mobile technologies through digital participation, which, in turn, drives greater mobile engagement.

4.3.1-C) R3: Operational Application Performance Loop: Operational support applications, such as fire control and navigation tools, enhance targeting and decision-making, thereby improving mission outcomes. As confidence in these tools grows, mobile device use increases.

4.3.1-D) R4: Psychological Resilience Uplift Loop: R4 is a reinforcing sub-loop that builds on loops R1-R3 by incorporating psychological resilience as a mediating feedback mechanism. Mission success reinforces psychological resilience, which, in turn, strengthens both institutional and user trust in mobile technologies. This loop represents a unified cognitive reinforcement pathway that amplifies the effects of battlefield success within the broader system of mobile engagement.

4.3.2 Balancing Feedback Loops: Balancing (negative) feedback loops highlight risks that suppress or self-regulate mobile device use in the face of systemic strain or adversary response.

4.3.2-A) B1: Signal Exposure and Countermeasures Loop: Mobile device use increases signal exposure, enhancing adversary surveillance capabilities and targeting. Resulting casualties trigger adaptive countermeasures, such as digital discipline or usage restrictions, which reduce mobile activity.

4.3.2-B) B2: Casualties - Mortality Degradation Loop: As casualties increase, psychological resilience erodes. When losses are related to mobile device use, such as through geolocation or signal exposure, morale declines, weakening trust in mobile technologies. This contributes to behavioral disengagement and reduced mobile device use.

4.3.2-C) B3: Casualties - Trust Attrition Loop: Casualties can directly undermine trust in mobile technologies, bypassing psychological resilience as an intermediary. This undermines device use by eroding immediate confidence in the safety of technology.

4.3.2-D) B4: Cognitive Warfare Loop: Mobile devices act as conduits for disinformation and psychological operations (PSYOPS). Exposure to these tactics undermines psychological resilience and trust, thus reducing mobile engagement.

4.3.2-E) B5: Device-Centric Cyber Vulnerability Loop: The increased use of mobile devices expands the overall cyberattack surface, exposing users to various threats, including malware, geolocation tracking, and data interception. These threats degrade operational effectiveness by disrupting communications, compromising data integrity, or revealing troop locations. As operational success declines, trust in mobile technologies weakens, further reducing mobile device use.

4.3.2-F) B6: App-Specific Cyber Risk Loop: Operational support applications, such as those used for artillery targeting or tactical navigation, introduce concentrated cyber vulnerabilities. When compromised, these applications can mislead targets, expose operational plans, or become entry points for malware. Resulting losses in operational effectiveness reduce trust in mobile platforms and discourage further use of these critical digital tools.

4.3.2-G) B7: Data Verification Bottleneck Loop: Crowdsourced intelligence increases the burden of data verification. If not managed effectively, this load reduces operational effectiveness and mission success, weakening trust in mobile technology and limiting further participation through mobile channels.

4.3.3 Stabilizing Influence of External Cyber-Operational Support: Although not a self-contained loop, *External Cyber-Operational Support (ECOS)* functions as an exogenous stabilizing influence. It mitigates cyber threat exposure through secure infrastructure, resilient connectivity, and hardened cloud environments, thus buffering the system against degradation pressures modeled in B5 and B6. In addition, ECOS relies on external software developers, ranging from civilian IT volunteers to private defense technology firms, who produce and maintain operational support applications for targeting, navigation, and mission planning.

By maintaining both the infrastructure and functionality of mobile systems under cyber duress, ECOS amplifies the effectiveness of reinforcing structures and preserves the viability of tactical digital tools. Although not modeled as an endogenous feedback loop, it plays a critical damping role, acting as a force multiplier that enhances the system's resilience during periods of increased cyber and informational threats.

4.3.4 Systemic Interpretation: The causal structure illustrated in the CLD (Fig.1) shows a complex, tightly coupled system in which mobile device use acts as both a catalyst and a consequence of the dynamics of hybrid warfare. The system is characterized by multiple reinforcing feedback loops that accelerate the integration of mobile technologies into battlefield operations, particularly through enhanced communication, the deployment of operational apps, and participatory intelligence gathering. However, these reinforcing dynamics are constrained by interconnected balancing structures that reflect systemic friction and emergent vulnerabilities. In particular, cyber and signal exposures serve as critical balancing mechanisms that limit unchecked growth in mobile device use, especially under conditions of adversary adaptation or tactical degradation [14, 37]. Psychological resilience plays a dual role, serving both as a stabilizing variable within balancing loops (e.g., in response to casualties or disinformation) and as an amplifier in reinforcing loops linked to mission success [22, 37].

The system also exhibits characteristics of path dependence and non-linearity [29]. Small gains in operational effectiveness can initiate reinforcing cycles that increase reliance on mobile platforms. In contrast, discrete shocks (e.g., application compromises, heavy casualties) may trigger a collapse in trust and a cascading disengagement. Additionally, the system depends on exogenous support—such as external cyber-operational contributions—for stability, suggesting that digital resilience is not purely endogenous and requires external scaffolding.

In strategic terms, the model suggests that hybrid warfare involving civilian technologies must be understood not only in terms of tool effectiveness, but also in terms of how those tools shape behavioral patterns, decision-making tempos, and vulnerability surfaces over time. Systemic leverage points, such as improving application security, managing verification bottlenecks, or mitigating cognitive degradation, offer potential intervention pathways that preserve the functional benefits of mobile device use while damping the destabilizing effects of adversary exploitation.

5 Discussion

This section presents the systemic dynamics of the causal loop model, focusing on the behavioral, operational, and strategic implications of mobile device use in hybrid warfare.

5.0.1 Key Systemic Findings: The analysis shows that mobile device use in hybrid warfare is not merely a matter of capability adoption but a systemic phenomenon shaped by dynamic feedback, behavioral reinforcement, and evolving threat landscapes. The integration of mobile devices into communication, targeting, and intelligence processes creates multiple reinforcing loops that increase digital dependence between the military and civilian domains [5, 6]. However, this momentum is counterbalanced by cyber vulnerabilities, cognitive stressors, and adversary adaptation mechanisms that can abruptly alter system trajectories [22, 37].

Several key insights emerge: First, the relationship between trust and performance is recursive. Mobile technologies are embedded not only through demonstrated utility but also through psychological confidence, institutional legitimacy, and user perception. Minor disruptions, such as cyber intrusions into operational applications or the compromise of battlefield communications, can cascade through the system, degrading institutional trust and operational performance [14, 38]. Although the primary impact is on military decision-making and digital confidence, perceived insecurity may also indirectly affect civilian participation, particularly when incidents are amplified through disinformation or widely publicized failures [5, 22].

Second, the system exhibits multiple points of fragility, particularly where exposure to cyber threats overlaps with mission-critical functions. Operational support applications, while enabling tactical agility, introduce concentrated digital risk [1, 14]. This highlights an inherent tension between short-term tactical gain and long-term systemic resilience, particularly in asymmetrical cyber conflict environments [26].

Third, the role of external support is both enabling and revealing. External cyber-operational assistance helps maintain mobile-enabled functionality in contested environments but simultaneously exposes a structural dependency that can undermine sovereign digital autonomy [17, 19]. This suggests that national resilience strategies must carefully balance foreign integration with investments in domestic cyber capabilities.

Fourth, the model underscores the need to govern not only technological systems but also the sociotechnical systems in which they are embedded. Interventions aimed at improving data verification, digital literacy, and disinformation resilience may have system-wide stabilizing effects on key behavioral variables such as trust in mobile technologies and psychological resilience [6, 38]. Thus, a systemic perspective reframes mobile security not as a purely technical problem but as a governance challenge situated within the complexities of behavioral, informational, and infrastructural factors.

5.0.2 Policy and Strategic Implications: This systemic model has several implications for policy, doctrine, and operational planning in hybrid warfare environments.

At the operational level, the analysis highlights the centrality of mobile-enabled communication and coordination as force multipliers. Reinforcing loops such as R1 (Communication-Effectiveness) and R2 (Crowdsourced Intelligence) illustrate how smartphone-based systems can significantly enhance battlefield situational awareness and responsiveness. Secure mobile platforms should be integrated into tactical command workflows, supported by field protocols that limit signal exposure and mitigate the risks associated with electronic warfare.

In the cyber domain, balancing loops B5 (Device-Centric Cyber Vulnerability) and B6 (App-Specific Cyber Risk) highlight the systemic risks introduced by the widespread use of mobile devices. These loops suggest a need for proactive security-by-design practices in battlefield apps, including periodic third-party code audits, threat modeling of user workflows, and strict access control regimes. Importantly, public-private partnerships should be institutionalized, extending beyond ad hoc support, so that civilian tech providers can supply hardened infrastructure, secure cloud services, and zero-trust architectures suited to contested environments [17].

From a psychological and information security perspective, the balancing loop B4 (Cognitive Warfare Loop) reinforces the need to treat disinformation and morale degradation not as peripheral threats, but as core operational risks. Civilian and military training programs should include media literacy, adversarial narrative awareness, and psychological preparedness protocols to mitigate the impact of cognitive warfare [15, 24].

At the governance level, the model suggests that resilience in hybrid conflict environments depends not only on technical safeguards but also on regulatory frameworks and institutional agility. Governments should anticipate that digitally mediated civilian participation, especially in intelligence crowdsourcing, will challenge traditional legal distinctions between combatants and noncombatants. Developing legal doctrines that clarify the rights, responsibilities, and protections of ”participatory civilians” is essential for ethical conduct and operational planning [2, 18, 25].

Ultimately, the model underscores the importance of formally integrating systems thinking into hybrid threat assessment and strategic planning. The application of system dynamics methods enables mapping interdependencies across domains, identifying leverage points within the system, and simulating unintended consequences associated with the deployment of digital tools in conflict environments. This approach bridges the gap between technological adoption and strategic foresight, providing a more comprehensive understanding of how mobile technologies influence conflict dynamics through feedback-driven behaviors.

In summary, the above implications underscore the notion that hybrid warfare is not merely a matter of tactical innovation but also of systemic design. Managing the risks and opportunities of mobile device use requires a multilevel strategy that integrates operational discipline, cyber resilience, psychological safeguarding, and governance innovation into a coherent strategic posture.

5.1 Limitations and Future Research

Although this paper provides a systems-based analysis of mobile device use in hybrid warfare, several limitations restrict the generalizability and operational applicability of its findings.

The CLD is conceptual and qualitative in its nature. While grounded in empirical literature and contemporary conflict data, it does not capture the magnitude, delay, or probability associated with the identified relationships. Without this formal quantification, the model cannot support predictive simulation or scenario testing. Future research should address this by integrating system dynamics modeling (SDM) or agent-based simulations to explore emergent behaviors and nonlinear escalation pathways under varying conditions.

Another limitation comes from the abstraction of the actors. The model treats civilians, soldiers, and institutional stakeholders as interacting nodes within a single system, yet their motivations, technological capabilities, and risk tolerances differ markedly. More granular modeling that disaggregates user groups could yield a more accurate picture of behavior, trust dynamics, and decision-making in frontline and near-frontline settings.

In addition, the model captures the conflict-specific dynamics of the Russian-Ukrainian war from 2014 to 2024. While many insights are transferable, factors such as the telecommunications infrastructure, information control, and cyber doctrine vary significantly across regions. Comparative case studies across other hybrid warfare environments, particularly those involving non-state actors or authoritarian regimes, would help test the model's robustness.

Methodologically, the analysis relies on publicly available sources and open-source literature. Aspects of mobile cyber operations, military doctrine, and information warfare strategy may depend on classified or undisclosed practices, making them only partially observable in the sources used for this model. Supplementing this model with expert interviews, insider accounts, or restricted-access data would enhance empirical depth and facilitate the validation of more nuanced system dynamics.

Finally, while this paper operationalizes systems thinking to explain hybrid dynamics, it does not address its practical integration into strategic planning, training, or decision-support systems. Future work should explore how causal models such as the one proposed here can inform the development of military doctrine, digital risk assessments, and the design of resilience strategies in mobile-centric operational theaters.

The above limitations highlight the need for an interdisciplinary approach that bridges behavioral science, systems engineering, and operational military research. A more comprehensive understanding of mobile technologies in hybrid warfare should depend not only on conceptual advances but also on the development of simulation tools, actor-specific modeling, and comparative frameworks suited to diverse geopolitical and technological environments.

6 Conclusion

The paper explores the systemic role of mobile devices in hybrid warfare through a causal loop model grounded in empirical insights from the Russian-Ukrainian conflict. Rather than treating mobile devices as discrete communication or surveillance tools, the model uses them as embedded components of a broader sociotechnical system shaped by interlocking operational, psychological, and cybernetic dynamics.

The feedback loops identified in the paper demonstrate how mobile device use can become self-reinforcing under favorable conditions, particularly through communication enhancement, intelligence crowdsourcing, and the deployment of operational support applications. However, the reinforcing dynamics are moderated by balancing feedback loops that introduce friction and risk, including cyber vulnerabilities, signal exposure, disinformation campaigns, and the burden of data verification. The model also highlights the central role of trust and psychological resilience as fragile and system-critical variables susceptible to both cascading degradation and strategic reinforcement.

By modeling mobile device use as part of a dynamic, interdependent system, this paper offers a novel systems-based perspective for analyzing digital technologies in hybrid conflict. “It addresses a key gap in the literature by moving beyond isolated assessments of tactical utility or cybersecurity risk to show how mobile technologies function as both strategic enablers and systemic vulnerabilities.

In answering the research question, the analysis shows that mobile devices enable tactical coordination, intelligence crowdsourcing, and digital participation, while simultaneously introducing cyber, psychological, and operational risks. These dynamics are governed by reinforcing and balancing feedback loops, revealing how mobile technologies shape both battlefield effectiveness and strategic fragility within hybrid conflict systems.

The presented framework offers a conceptual basis for future research on civilian-military interaction, digital participation, and sociotechnical resilience in hybrid warfare. As the boundaries between civilians and combatants continue to blur in digitally-saturated operational environments, system-level analysis will be crucial for designing responsible, adaptive, and secure military-civilian integration strategies.

Appendix A
Supplementary Tables

Table 1. Key Variables Related to Smartphone Usage in Hybrid Conflict Environments

Variable	**Definition**	**Sources**
Mobile device use	The general reliance on smartphones for communication, information, intelligence gathering, and logistical coordination during hybrid conflicts.	[5], [18], [22]
Communication & Coordination	Real-time battlefield communication and coordination of military, civilian, and hybrid operations via mobile devices.	[3], [7]
Operational Support Apps	These apps exemplify a new class of mobile-based operational tools that directly augment battlefield effectiveness, such as in precision targeting and fire control.	[1], [18]
Operational Effectiveness	The influence of mobile device-based communication and situational awareness on improving or degrading the operational performance of forces.	[2], [9], [26]
Mission Success	Contribution of mobile device-supported activities to achieving tactical or strategic goals in conflict scenarios.	[3], [6]
Intelligence Crowdsourcing	Mass-scale civilian reporting and open-source intelligence gathering through mobile apps, chats, and platforms.	[2], [6], [20]
Data Verification Load	The cognitive and operational strain placed on military and OSINT analysts responsible for validating crowdsourced mobile intelligence, particularly under conditions of high volume, speed, and adversarial disinformation.	[5], [18], [39]
Surveillance Capabilities	Passive and active monitoring of mobile signals, metadata, and application data to gather intelligence or geolocate targets.	[1], [9], [23]
Disinformation and PSYOPS	The deliberate use of mobile platforms to disseminate false, misleading, or manipulative information aimed at influencing troop morale, civilian perceptions, enemy decision-making, and international opinion during hybrid warfare operations.	[3], [40], [41]
Psychological Resilience	The psychological impact of mobile device communication, information access, and exposure to PSYOPS on soldiers and civilians in conflict zones.	[4], [6]
Signal Exposure	The risk associated with mobile signal emissions leading to detection, targeting, and compromised operational security.	[9], [22]
Casualties	Increased battlefield casualties resulting from adversarial exploitation of mobile device use.	[9], [10]
Cyber Threat Exposure	The vulnerability of mobile devices, communication networks, and associated applications to hacking, malware, disruption, or espionage operations that degrade battlefield coordination, intelligence sharing, and resilience during hybrid conflict.	[8], [17], [23], [26]
Trust in Mobile Technology	Degree of user confidence in mobile device reliability, security, and utility during hybrid conflicts.	[2], [3], [18]
External Cyber-Operational Support	Assistance from allied states, private technology companies, and volunteer organizations in enhancing cybersecurity, communication resilience, intelligence capabilities, and operational effectiveness through mobile platforms during hybrid conflict.	[3], [8], [17], [18], [26]
Adaptive Countermeasures	Tactical behavior modifications (e.g., turning off devices, using encrypted apps, disciplined smartphone usage) to mitigate smartphone-related vulnerabilities during conflict.	[9], [22], [23]

Table 2. Causal Links and Supporting Sources for Mobile Device Use in Hybrid Warfare

Causal Link	**Polarity**	**Supporting Sources**	**Loops**
Mobile Device Use → Communication & Coordination	(+)	[3], [7]	R1
Mobile Device Use → Cyber Threat Exposure	(+)	[3], [22], [23]	B5
Mobile Device Use → Signal Exposure	(+)	[4], [9], [14]	B1, B2, B3
Mobile Device Use → Intelligence Crowdsourcing	(+)	[5], [6], [18]	R2, B6
Mobile Device Use → Disinformation and PSYOPS	(+)	[22], [42]	B4
Signal Exposure → Surveillance Capabilities	(+)	[9], [14]	B1, B2, B3
Surveillance Capabilities → Casualties	(+)	[9], [14]	B1, B2, B3
Casualties → Adaptive Countermeasures	(+)	[1], [4], [14]	B1
Casualties → Psychological Resilience	(-)	[43]	B2
Casualties → Trust in Mobile Technology	(-)	[5], [9]	B3
Adaptive Countermeasures → Mobile Device Use	(-)	[1], [4], [6], [14]	B1
External Cyber-Operational Support → Communication & Coordination	(+)	[3], [19]	/
External Cyber-Operational Support → Trust in Mobile Technology	(+)	[17], [19], [44]	/
External Cyber-Operational Support → Operational Support Apps	(+)	[17], [18]	/
External Cyber-Operational Support → Cyber Threat Exposure	(-)	[17], [19], [38]	/
Communication & Coordination → Operational Effectiveness	(+)	[3], [4], [18]	R1
Operational Support Apps → Operational Effectiveness	(+)	[1], [18]	R3
Operational Support Apps → Cyber Threat Exposure	(+)	[14], [37]	B6
Cyber Threat Exposure → Operational Effectiveness	(-)	[19], [26]	B5, B6
Operational Effectiveness → Mission Success	(+)	[2], [5], [19]	R1, R2, R3
Mission Success → Trust in Mobile Technology	(+)	[3], [6]	R1-R4
Mission Success → Psychological Resilience	(+)	[5], [6]	R4
Trust in Mobile Technology → Mobile Device Use	(+)	[4], [7]	R1-R4
Intelligence Crowdsourcing → Data Verification Load	(+)	[4], [5], [18], [39]	B7
Intelligence Crowdsourcing → Operational Effectiveness	(+)	[18], [39]	R2
Data Verification Load → Operational Effectiveness	(-)	[5], [39]	B7
Disinformation and PSYOPS → Psychological Resilience	(-)	[22], [37]	B4
Psychological Resilience → Trust in Mobile Technology	(+)	[4], [6], [7]	B2, B4

References

[1] Y. Danyk, T. Maliarchuk, and C. Briggs, "Hybrid War: High-tech, Information and Cyber Conflicts," *Connections*, vol. 16, no. 2, pp. 5–24, 2017, Publisher: Partnership for Peace Consortium of Defense Academies and Security Studies Institutes, ISSN: 1812-1098. Accessed: Apr. 15, 2025. [Online]. Available: https://www.jstor.org/stable/26326478.

[2] L. Peperkamp, "Technology and the Civilianization of Warfare," en, *Ethics & International Affairs*, vol. 38, no. 1, pp. 64–74, Jan. 2024, ISSN: 0892-6794, 1747-7093. DOI: 10.1017/S0892679424000121.

[3] C. Bronk, G. Collins, and D. S. Wallach, "The Ukrainian Information and Cyber War," *The Cyber Defense Review*, vol. 8, no. 3, pp. 33–50, 2023, Publisher: Army Cyber Institute, ISSN: 2474-2120. Accessed: Apr. 12, 2025. [Online]. Available: https://www.jstor.org/stable/48755360.

[4] I. Shklovski and V. Wulf, "The Use of Private Mobile Phones at War: Accounts From the Donbas Conflict," en, in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, Montreal QC Canada: ACM, Apr. 2018, pp. 1–13, ISBN: 978-1-4503-5620-6. DOI: 10.1145/3173574.3173960.

[5] M. Ford, "Ukraine, Participation and the Smartphone at War," en, *Political Anthropological Research on International Social Sciences*, pp. 1–29, Nov. 2023, ISSN: 2590-3284, 2590-3276. DOI: 10.1163/25903276-bja10048.

[6] K. Zarembo, M. Knodt, and J. Kachel, "Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion," EN, *Media, War & Conflict*, p. 17 506 352 241 236 449, Mar. 2024, Publisher: SAGE Publications, ISSN: 1750-6352. DOI: 10.1177/17506352241236449.

[7] R. Horbyk, ""The war phone": Mobile communication on the frontline in Eastern Ukraine," en, *Digital War*, vol. 3, no. 1, pp. 9–24, Dec. 2022, Company: Palgrave Distributor: Palgrave Institution: Palgrave Label: Palgrave Number: 1 Publisher: Springer International Publishing, ISSN: 2662-1983. DOI: 10.1057/s42984-022-00049-2.

[8] G. B. Mueller, B. Jensen, B. Valeriano, R. C. Maness, and J. M. Macias, "Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures," Center for Strategic and International Studies (CSIS), Tech. Rep., 2023. Accessed: Apr. 12, 2025. [Online]. Available: https://www.jstor.org/stable/resrep52130.

[9] D. McCrory, "Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States," en, *The RUSI Journal*, vol. 165, no. 7, pp. 34–44, Nov. 2020, ISSN: 0307-1847, 1744-0378. DOI: 10.1080/03071847.2021.1888654.

[10] K. Khoirunnisa and C. Sugiati, "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare," en, *Jurnal Public Policy*, vol. 10, no. 2, p. 138, Apr. 2024, ISSN: 2502-0528. DOI: 10.35308/jpp.v10i2.9026.

[11] M. Galeotti, *The weaponisation of everything: a field guide to the new way of war*, en. New Haven, CT London: Yale University Press, 2022, ISBN: 978-0-300-26513-2.

[12] A. Mumford and P. Carlucci, "Hybrid warfare: The continuation of ambiguity by other means," en, *European Journal of International Security*, vol. 8, no. 2, pp. 192–206, May 2023, ISSN: 2057-5637, 2057-5645. DOI: 10.1017/eis.2022.19.

[13] M. C. Ford and A. Hoskins, *Radical war: data, attention and control in the twenty-first century* (Oxford scholarship online Political Science), eng. New York: Oxford University Press, 2022, ISBN: 978-0-19-768344-6. DOI: 10.1093/oso/9780197656549.001.0001.

[14] C. McDaid, "Location Tracking on The Battlefield," en-GB, Enea, Tech. Rep., Jan. 2024. Accessed: Apr. 9, 2025. [Online]. Available: https://www.enea.com/insights/location-tracking-on-battlefield/.

[15] M. Wasinger, "Then we will fight in the shade," in *Aspects of cognitive warfare*, M. Wasinger, Ed., Vienna, Austria: The Defence Horizon Journal, 2024, pp. 6–13, ISBN: 978-3-200-10166-1. Accessed: May 6, 2025. [Online]. Available: https://tdhj.org/wp-content/uploads/2024/11/2024_TDHJ-Hybrid-CoE-Cgnitive-Warfare-2024_web-v2.pdf.

[16] J. Schröfl and S. Marahrens, "The janus-faced hybrid nature of cyber-related technologies in the cognitive domain," in *Aspects of cognitive warfare*, M. Wasinger, Ed., Vienna, Austria: The Defence Horizon Journal, 2024, pp. 62–69, ISBN: 978-3-200-10166-1. Accessed: May 6, 2025. [Online]. Available: https://tdhj.org/wp-content/uploads/2024/11/2024_TDHJ-Hybrid-CoE-Cgnitive-Warfare-2024_web-v2.pdf.

[17] F. Analytics, "Digital Front Lines: A sharpened focus on the risks of, and responses to, hybrid warfare.," FP Analytics, with support from Microsoft, Tech. Rep., 2023. Accessed: Apr. 25, 2025. [Online]. Available: https://digitalfrontlines.io/wp-content/uploads/sites/8/2023/08/digital-front-lines-report-FP-analytics-microsoft-2023.pdf.

[18] M. Ford, “From innovation to participation: Connectivity and the conduct of contemporary warfare,” en, *International Affairs*, vol. 100, no. 4, pp. 1531–1549, Jul. 2024, ISSN: 0020-5850, 1468-2346. DOI: 10.1093/ia/iiae061.

[19] I. Aviv and U. Ferri, “Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem,” *International Journal of Critical Infrastructure Protection*, vol. 43, p. 100 637, Dec. 2023, ISSN: 1874-5482. DOI: 10.1016/j.ijcip.2023.100637.

[20] A. Bawa, U. Kursuncu, D. Achilov, V. L. Shalin, N. Agarwal, and E. Akbas, *Telegram as a Battlefield: Kremlin-related Communications during the Russia-Ukraine Conflict*, arXiv:2501.01884 [cs], Jan. 2025. DOI: 10.48550/arXiv.2501.01884.

[21] A. C. Fox, “Hybrid Warfare: The 21st Century Russian Way of Warfare,” en, 2017, Publisher: Unpublished. DOI: 10.13140/RG.2.2.35922.38086.

[22] B. van Niekerk, “The Evolution of Information Warfare in Ukraine: 2014 to 2022,” *Journal of Information Warfare*, vol. 22, no. 1, pp. 10–31, 2023, Publisher: ArmisteadTEC LLC, ISSN: 1445-3312. Accessed: Jan. 4, 2025. [Online]. Available: https://www.jstor.org/stable/27240852.

[23] M. Lehto, “Cyber Warfare and War in Ukraine,” *Journal of Information Warfare*, vol. 22, no. 1, pp. 61–75, 2023, Publisher: ArmisteadTEC LLC, ISSN: 1445-3312. Accessed: Jan. 4, 2025. [Online]. Available: https://www.jstor.org/stable/27240855.

[24] M. Papadaki, “Defending free speech with free choice: Towards technology-driven, human-centred, endpoint solutions for society as a whole,” in *Aspects of cognitive warfare*, M. Wasinger, Ed., Vienna, Austria: The Defence Horizon Journal, 2024, pp. 52–61, ISBN: 978-3-200-10166-1. Accessed: May 6, 2025. [Online]. Available: https://tdhj.org/wp-content/uploads/2024/11/2024_TDHJ-Hybrid-CoE-Cgnitive-Warfare-2024_web-v2.pdf.

[25] P. B. Pijpers, “Legislation as an instrument of cognitive warfare,” in *Aspects of cognitive warfare*, M. Wasinger, Ed., Vienna, Austria: The Defence Horizon Journal, 2024, pp. 32–41, ISBN: 978-3-200-10166-1. Accessed: May 6, 2025. [Online]. Available: https://tdhj.org/wp-content/uploads/2024/11/2024_TDHJ-Hybrid-CoE-Cgnitive-Warfare-2024_web-v2.pdf.

[26] H. Lin, “Russian Cyber Operations in the Invasion of Ukraine,” *The Cyber Defense Review*, vol. 7, no. 4, pp. 31–46, 2022, Publisher: Army Cyber Institute, ISSN: 2474-2120. Accessed: Apr. 12, 2025. [Online]. Available: https://www.jstor.org/stable/48703290.

[27] CrowdStrike, “Use of Fancy Bear Android Malware in tracking of Ukrainian field artillery units,” Tech. Rep., 2017. Accessed: Apr. 23, 2025. [Online]. Available: https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf.

[28] M. Nadolski and J. Fairbanks, “Complex systems analysis of hybrid warfare,” en, *Procedia Computer Science*, vol. 153, pp. 210–217, 2019, ISSN: 18770509. DOI: 10.1016/j.procs.2019.05.072.

[29] P. Barbrook-Johnson and A. S. Penn, *Systems Mapping: How to build and use causal models of systems*, en. Cham: Springer International Publishing, 2022, ISBN: 978-3-031-01919-7. DOI: 10.1007/978-3-031-01919-7.

[30] B. Richmond, “Systems thinking: Critical thinking skills for the 1990s and beyond,” en, *System Dynamics Review*, vol. 9, no. 2, pp. 113–133, Jun. 1993, ISSN: 0883-7066, 1099-1727. DOI: 10.1002/sdr.4260090203.

[31] R. D. Arnold and J. P. Wade, “A Definition of Systems Thinking: A Systems Approach,” en, *Procedia Computer Science*, vol. 44, pp. 669–678, 2015, ISSN: 18770509. DOI: 10.1016/j.procs.2015.03.050.

[32] J. D. Sterman, “System Dynamics: System Thinking and Modeling for a Complex World,” en, 2000.

[33] G. Veldhuis et al., “The influence of causal loop diagrams on systems thinking and information utilization in complex problem-solving,” en, *Computers in Human Behavior Reports*, vol. 17, p. 100 613, Mar. 2025, ISSN: 24519588. DOI: 10.1016/j.chbr.2025.100613.

[34] D. Polatin-Reuben, R. Craig, T. Spyridopoulos, and T. Tryfonas, “A System Dynamics Model of Cyber Conflict,” in *2013 IEEE International Conference on Systems, Man, and Cybernetics*, ISSN: 1062-922X, Oct. 2013, pp. 303–308. DOI: 10.1109/SMC.2013.58.

[35] S. Armenia, E. Ferreira Franco, F. Nonino, E. Spagnoli, and C. M. Medaglia, “Towards the Definition of a Dynamic and Systemic Assessment for Cybersecurity Risks,” en, *Systems Research and Behavioral Science*, vol. 36, no. 4, pp. 404–423, Jul. 2019, ISSN: 1092-7026, 1099-1743. DOI: 10.1002/sres.2556.

[36] J. Moffat, “The system dynamics of future warfare,” en, *European Journal of Operational Research*, vol. 90, no. 3, pp. 609–618, May 1996, ISSN: 03772217. DOI: 10.1016/0377-2217(95)00103-4.

[37] Y. Danyk and C. Briggs, “Modern Cognitive Operations and Hybrid Warfare,” en, *Journal of Strategic Security*, vol. 16, no. 1, pp. 35–50, Apr. 2023, ISSN: 1944-0464, 1944-0472. DOI: 10.5038/1944-0472.16.1.2032.

[38] A. Ormrod, D. Ormrod, and J. Slay, “Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian Conflict,” *Journal of Information Warfare*, vol. 22, no. 1, pp. 76–87, 2023, Publisher: ArmisteadTEC LLC, ISSN: 1445-3312. Accessed: Jan. 4, 2025. [Online]. Available: https://www.jstor.org/stable/27240856.

[39] H. V. Beek and S. Rietjens, “Open-Source Intelligence in the Russia-Ukraine War,” en, in *Reflections on the Russia-Ukraine War*, Leiden University Press, Dec. 2024, pp. 57–76, ISBN: 978-94-006-0474-2. DOI: 10.24415/9789400604742-005.

[40] F. Pierri, L. Luceri, N. Jindal, and E. Ferrara, “Propaganda and Misinformation on Facebook and Twitter during the Russian Invasion of Ukraine,” en, in *Proceedings of the 15th ACM Web Science Conference 2023*, Austin TX USA: ACM, Apr. 2023, pp. 65–74, ISBN: 979-8-4007-0089-7. DOI: 10.1145/3578503.3583597.

[41] L. Topor and A. Tabachnik, “Russian Cyber Information Warfare: International Distribution and Domestic Control,” en, *Journal of Advanced Military Studies*, vol. 12, no. 1, pp. 112–127, May 2021, ISSN: 21644209, 21644217. DOI: 10.21140/mcuj.20211201005.

[42] S. J. Lohmann et al., “What Ukraine Taught NATO about Hybrid Warfare,” en, 2022.

[43] L. Zasiekina, T. Duchyminska, A. Bifulco, and G. Bignardi, “War trauma impacts in Ukrainian combat and civilian populations: Moral injury and associated mental health symptoms,” *Military Psychology*, vol. 36, no. 5, pp. 555–566, 2023, ISSN: 0899-5605. DOI: 10.1080/08995605.2023.2235256.

[44] M. Vargas, “Competitive Advantage in the Russo-Ukrainian War: Ukraine’s Technological Potential Against a Kremlin Goliath,” *The Cyber Defense Review*, vol. 8, no. 3, pp. 121–134, 2023, Publisher: Army Cyber Institute, ISSN: 2474-2120. Accessed: Apr. 12, 2025. [Online]. Available: https://www.jstor.org/stable/48755365.

Luka Podlesnik received the B.Sc. degree in Computer Science and Informatics from the University of Maribor, Faculty of Electrical Engineering and Computer Science. He has over ten years of experience in software engineering, team leadership, and systems optimization. He is currently pursuing the Ph.D. degree at the Faculty of Criminal Justice and Security, University of Maribor. His research interests include cyber resilience, cyber threat intelligence, and the role of cyber technologies in contemporary conflict.

Anže Mihelič received the Ph.D. degree in computer and information science from the Faculty of Computer and Information Science, University of Ljubljana. He is currently an Assistant Professor with the Faculty of Criminal Justice and Security and a Researcher with the Faculty of Computer and Information Science at the University of Ljubljana. His research interests include human factors in information and cybersecurity, as well as agile secure software development.

Blaž Markelj received the Ph.D. degree. He is currently an Associate Professor in the field of security studies and the Head of the Department of Information Security at the Faculty of Criminal Justice and Security, University of Maribor. For many years, he has been dedicated to education and research in the field of information security. He is the author of numerous international and domestic scientific and professional articles. As an invited lecturer, he has spoken at various international and domestic events. His expertise lies in the integration of research and practical applications, which he has demonstrated through his involvement as a member or leader of organizational or program committees in numerous information security events over the past few years.