https://ejournal-nawalaedu.com/index.php/SG/index
Volume 3 Nomor 1, 2026
E-ISSN : 3047-9339

https://doi.org/10.62872/ca95a937

Information Warfare in International Relations: The Information War in the Digital Age

Submitted: May 02, 2026; Revised: May 20. 2026; Accepted: May 30, 2026

Fitri Arianti
Universitas Sriwijaya, Indonesia
Fitriarianti400@gmail.com

Abstrak
Artikel ini mengkaji fenomena information warfare (perang informasi) dalam hubungan internasional kontemporer, dengan fokus pada bagaimana aktor-aktor negara dan non-negara memanfaatkan teknologi digital untuk memengaruhi persepsi publik, mendestabilisasi institusi demokratis, dan mencapai tujuan geopolitik. Melalui analisis literatur sistematis terhadap publikasi terkemuka periode 2021–2024, studi ini mengidentifikasi tiga dimensi utama perang informasi modern: disinformasi dan manipulasi media sosial, operasi siber terhadap infrastruktur kritis, dan penggunaan kecerdasan buatan dalam domain kognitif dan keputusan militer. Temuan menunjukkan bahwa kemajuan teknologi, khususnya deepfake, otomatisasi OODA loop, dan komputasi kuantum, secara signifikan memperluas ruang lingkup dan efektivitas operasi informasi, sementara mekanisme pertahanan seperti literasi digital dan diplomasi siber masih menghadapi kesenjangan implementasi yang substansial.
Kata Kunci: *perang informasi, disinformasi, keamanan siber, kecerdasan buatan, hubungan internasional digital.*

Abstract
This article examines the phenomenon of information warfare in contemporary international relations, focusing on how state and non-state actors exploit digital technologies to influence public perceptions, destabilize democratic institutions, and achieve geopolitical objectives. Through a systematic literature review of leading publications from 2021 to 2024, the study identifies three principal dimensions of modern information warfare: disinformation and social media manipulation, cyber operations against critical infrastructure, and the use of artificial intelligence in cognitive and military decision-making domains. Findings indicate that technological advances, particularly deepfakes, OODA loop automation, and quantum computing, significantly expand the scope and effectiveness of information operations,

while defensive mechanisms such as digital literacy and cyber diplomacy continue to face substantial implementation gaps.
Keywords: information warfare, disinformation, cybersecurity, artificial intelligence, digital international relation

INTRODUCTION

The digitalization of global communication has fundamentally transformed the character of interstate competition. Where twentieth-century great power rivalry was primarily conducted through military force, economic coercion, and diplomatic maneuver, contemporary geopolitics increasingly unfolds across digital networks that shape how billions of people perceive reality, form political opinions, and make collective decisions. Information warfare, the deliberate use of information, disinformation, and communication technologies to gain strategic advantage over adversaries, has emerged as one of the defining instruments of twenty-first century statecraft (Luo, 2021).

The salience of information warfare has been dramatically underscored by Russia's comprehensive information operations accompanying its 2022 invasion of Ukraine. Geissler et al. (2022) document the systematic deployment of Russian propaganda across major social media platforms in the weeks surrounding the invasion, illustrating how information operations have become integral to modern military campaigns rather than peripheral adjuncts. Simultaneously, the proliferation of deepfake technologies has introduced new epistemic vulnerabilities: Twomey et al. (2023) demonstrate that synthetic media can undermine the foundational trust in visual evidence that democratic public discourse depends upon.

The scope of information warfare extends well beyond active conflict zones. Chen et al. (2022) examine how social network architectures enable the large-scale manipulation of public opinion through coordinated inauthentic behavior, algorithmic amplification of divisive content, and the exploitation of cognitive biases. Hannah (2021) traces how conspiracy ecosystems, exemplified by the QAnon phenomenon, leverage social media's information visualization affordances to construct alternative epistemic realities that are resilient to fact-checking interventions.

This article seeks to provide a comprehensive analytical account of information warfare in contemporary international relations by: (1) theorizing the mechanisms and modalities of modern information operations; (2) examining the role of emerging technologies, artificial intelligence, quantum computing, and autonomous systems, in transforming information warfare capabilities; (3) assessing defensive strategies and their limitations; and (4) identifying implications for international governance and institutional resilience. The analysis integrates perspectives from security studies, international political economy, computer science, and communications research to capture the genuinely interdisciplinary character of this phenomenon.

METHODOLOGY

This study employs a qualitative systematic literature review methodology, drawing on peer-reviewed publications from 2021 to 2024 across multiple disciplinary domains including international security studies, computer science, communications, and public

health informatics. The literature corpus was assembled through targeted searches of databases including Web of Science, Scopus, and Google Scholar, using keyword combinations including 'information warfare,' 'disinformation,' 'cyber operations,' 'AI military applications,' 'deepfakes,' and 'digital sovereignty.'

The analytical framework organizes the literature along three principal axes. First, the technological dimension examines how specific innovations, social media algorithms, artificial intelligence systems, deepfake generation, quantum computing, and satellite communication infrastructure, create new capabilities and vulnerabilities in the information domain (Krelina, 2021; Goldfarb & Lindsay, 2022; Radanliev, 2024). Second, the strategic dimension analyzes how state and non-state actors operationalize these technologies within broader geopolitical competition frameworks (Geissler et al., 2022; Johnson, 2022). Third, the defensive dimension assesses countermeasures including digital literacy programs, cybersecurity strategies, and diplomatic frameworks (Tınmaz et al., 2022; Abrahams et al., 2024).

Case studies are employed to ground theoretical propositions in empirical evidence, with primary focus on the Russia-Ukraine information environment (2022–2023) and US domestic information ecosystem vulnerabilities. Comparative analysis across cases allows identification of generalizable patterns while preserving context-specific nuances. The study explicitly excludes literature not directly relevant to information warfare's international relations dimensions, including clinical psychology studies on mental health onset (Solmi et al., 2021) and healthcare technology adoption (Stoumpos et al., 2023), except where they illuminate the societal vulnerabilities that information warfare exploits.

RESULTS AND DISCUSSION

A. Social Media as a Theater of Information Warfare

The architecture of contemporary social media platforms creates structural affordances that are deeply amenable to information warfare operations. Chen et al. (2022) conduct a comprehensive analysis of social network behavior and public opinion manipulation, identifying three primary mechanisms through which information operations achieve persuasive effect: algorithmic amplification of emotionally resonant content, coordinated inauthentic behavior by bot networks that manufacture artificial social proof, and the exploitation of filter bubbles that progressively isolate users within self-reinforcing epistemic communities.

Geissler et al. (2022) provide granular empirical documentation of Russian propaganda operations during the 2022 Ukraine invasion, analyzing patterns of content production, dissemination network topology, and audience engagement across Twitter, Telegram, and Facebook. Their analysis reveals a sophisticated multi-platform strategy in which different platforms serve distinct functions: Telegram for encrypted coordination among operational cells, Twitter for international audience targeting, and Facebook for penetrating older demographic segments in European target countries. Importantly, Russian information operations did not merely disseminate false content but strategically amplified genuine divisions within Western societies, exploiting pre-existing fractures in social trust.

Hannah's (2021) analysis of QAnon's growth trajectory illuminates how conspiracy ecosystems can develop self-sustaining informational architectures that are highly resistant

to conventional debunking efforts. By mapping the distinctive information visualization strategies employed in QAnon content, including cryptic textual puzzles, cross-platform trail-following, and community-generated interpretive frameworks, Hannah demonstrates how the participatory structure of social media transforms passive information consumers into active co-producers of disinformation, dramatically multiplying the reach and resilience of information operations at minimal cost to their originators.

Table 1. Typology of Information Warfare Operations in the Digital Age

Operation Type	Primary Vector	Technological Enabler	Key Actor(s)	Reference
Social Manipulation	Social Media Platforms	Bots, Algorithmic Amplification	Russia, China	Chen et al., 2022
Propaganda Warfare	Twitter, Telegram, Facebook	Coordinated Inauthentic Behavior	Russia (Ukraine)	Geissler et al., 2022
Synthetic Media	Video Sharing Platforms	Deepfake AI Generation	Multiple State/Non-State	Twomey et al., 2023
Conspiracy Seeding	Social Media Ecosystems	Info Visualization, Memes	Domestic Networks	Hannah, 2021
Cognitive Hacking	AI Decision Systems	OODA Loop Automation	Military Actors	Johnson, 2022
Infrastructure Attack	Critical Networks	Cyber Intrusion, Jamming	State Actors	Bueger & Liebetrau, 2021

***Note**. Compiled from systematic literature review (2021–2024). Operations are not mutually exclusive.*

B. Deepfakes and the Epistemic Dimensions of Information Warfare

The rise of generative AI–driven synthetic media marks a significant escalation in the tools available for information warfare. Twomey et al. (2023) examine this phenomenon by analyzing social media discourse during the Russia–Ukraine conflict, focusing on multiple deepfake videos that purportedly showed Ukrainian President Zelensky urging surrender. Their thematic analysis shows that even when platforms and fact-checkers rapidly debunk fabricated videos, the initial spread inflicts lasting epistemic harm: audiences retain doubt about the specific incident and, more broadly, grow more skeptical of video evidence as a reliable source.

Weikmann and Lecheler (2022) place deepfakes within the wider field of visual disinformation research, noting that visual media exert a distinctive persuasive force that resists conventional text-based fact-checking. They identify several moderating factors that influence susceptibility to synthetic media: preexisting political beliefs, levels of media and digital literacy, the platform environment (for example, algorithmic amplification and community norms), and whether contextual cues accompany the content. Importantly, their work highlights a "literacy paradox": more technologically sophisticated users do not always become less vulnerable; instead, they may overestimate their detection abilities and thus be misled in different ways. Together, these studies indicate that combating synthetic-media harm requires more than rapid debunking, it calls for platform design

changes, improved contextual signaling, public education that addresses overconfidence, and cross-disciplinary strategies that recognize the durable, system-level effects of deepfake circulation on public trust.

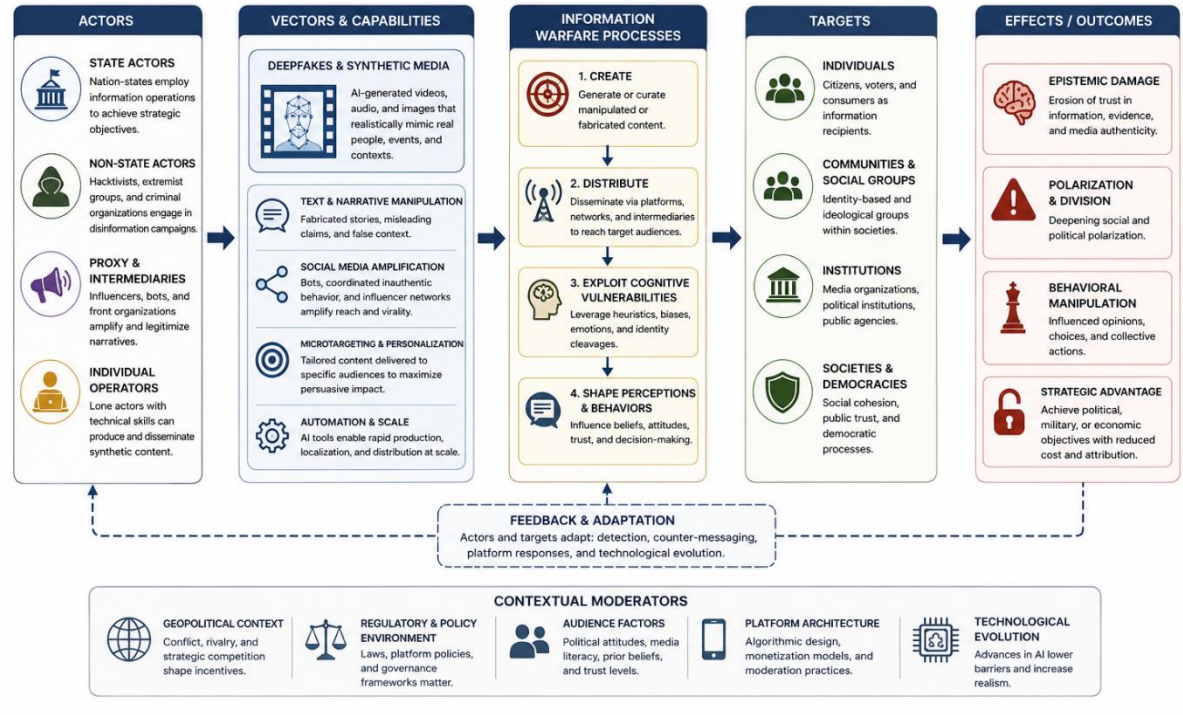

Figure 1. Information Warfare Ecosystem: Actors, Vectors, and Targets
Source: Author's compilation based on reviewed literature (2021–2024).

C. Artificial Intelligence, OODA Loop Automation, and Military Decision-Making

The integration of artificial intelligence into military command-and-control systems represents one of the most consequential and contested developments in contemporary information warfare. Johnson (2022) examines the accelerating automation of the Observe-Orient-Decide-Act (OODA) loop, the cognitive decision cycle that has governed military command doctrine since its formulation by John Boyd. Johnson argues that while AI-driven systems dramatically compress decision timelines and enhance pattern recognition in complex data environments, they also introduce new vulnerability vectors: adversaries who understand the decision logic of an opponent's AI systems can design information operations specifically calibrated to exploit algorithmic blind spots and trigger predetermined responses.

Goldfarb and Lindsay (2022) offer a more nuanced assessment, arguing that AI systems' superiority in prediction tasks is counterbalanced by fundamental limitations in judgment the ability to interpret novel situations, assign context-appropriate weights to competing values, and exercise moral reasoning. Their analysis has direct implications for information warfare: AI systems optimized for prediction will be systematically vulnerable to adversaries who exploit the gap between predictive accuracy in familiar environments and interpretive flexibility in genuinely novel information environments. This suggests that fully automated AI decision-making in military contexts creates exploitable brittleness.

Krelina (2021) provides comprehensive mapping of quantum technology's military applications, with particular relevance to information warfare through quantum

cryptography and quantum sensing. Quantum key distribution offers theoretically unbreakable encrypted communications, potentially neutralizing signals intelligence operations that have been central to information warfare since the Second World War. Conversely, quantum computing's capacity to break current public-key encryption infrastructure creates a race to 'quantum-proof' critical communications before adversaries achieve quantum computational advantage. Radanliev (2024) situates these developments within cyber diplomacy frameworks, arguing that proactive multilateral governance of quantum communication is essential to preventing destabilizing first-mover advantages.

Table 2. Emerging Technologies and Their Information Warfare Implications

Technology	Capability Gain	Information Warfare Application	Reference
Artificial Intelligence	Prediction & Pattern Recognition	Automated disinformation, deepfakes, OODA automation	Goldfarb & Lindsay, 2022; Johnson, 2022
Quantum Computing	Cryptographic Advantage	Breaking adversary encryption, secure military comms	Krelina, 2021; Radanliev, 2024
Satellite Networks	Global ISR Coverage	Surveillance, communications disruption, GPS spoofing	Kang et al., 2024
Game-Theoretic AI	Strategic Optimization	Adversarial modeling, deception strategy design	Ho et al., 2021
Deepfake Synthesis	Synthetic Reality Creation	False-flag videos, fabricated evidence, trust erosion	Twomey et al., 2023; Weikmann & Lecheler, 2022

***Note**. Adapted from reviewed literature. Implications reflect assessed capabilities as of 2021-2024 publications*

D. Critical Infrastructure and the Physical Substrate of Information Warfare

Information warfare extends beyond shaping beliefs; it also targets the physical backbone that sustains global digital communication. Bueger and Liebetrau (2021) draw attention to the acute vulnerability of submarine data cables, which carry roughly 95% of international internet traffic yet remain a largely invisible and underprotected form of critical infrastructure. Their analysis highlights a dangerous asymmetry: because global data flows are funneled through a limited set of cable routes and landing sites, these nodes represent high-value targets whose interdiction could produce widespread disruption with relatively localized attacks.

Complementing this maritime perspective, Kang et al. (2024) investigate the security implications of the rapid expansion of satellite communications, particularly low-Earth orbit constellations. The growing integration of commercial satellite services into both civilian and military networks increases the overall attack surface and creates mixed public–private dependencies. Deployments such as Starlink in Ukraine illustrate the benefits of commercial systems for force-multiplying connectivity, but they also expose risks: commercial operators may not have robust military-grade security controls, and

military reliance on private infrastructure introduces strategic vulnerabilities when corporate incentives, legal constraints, or third-party relationships diverge from national security priorities. Together, these studies show that protecting information sovereignty requires treating undersea cables, satellites, and other physical network elements as core security assets—demanding greater investment, international cooperation on protection norms, and contingency planning that anticipates targeted infrastructure disruption as a central tactic of modern information warfare.

E. Digital Sovereignty, AI Governance, and the European Response

Calderaro and Blumfelde (2022) critically examine the European Union's framing of 'digital sovereignty' as a framework for responding to information warfare threats. Their analysis challenges the premise that regulatory control over digital infrastructure and artificial intelligence provides meaningful protection against information warfare, arguing that the EU's sovereignty discourse misidentifies the source of information security vulnerabilities. Rather than external dependency, they contend that the structural architecture of recommendation systems, platform business models, and algorithmic content curation creates inherent susceptibilities that regulatory sovereignty cannot address without fundamentally restructuring the political economy of digital platforms.

Luo (2021) provides a general framework for understanding digitization risks in international business contexts, identifying four categories of digital risk, data sovereignty, digital disruption, digital espionage, and digital dependence, that collectively constitute the vulnerability landscape that information warfare exploits. His framework highlights the dual-use character of digital infrastructure: the same connectivity that enables economic efficiency and innovation creates attack surfaces that adversaries can leverage for information operations.

F. Defensive Strategies: Digital Literacy, Cybersecurity, and Cyber Diplomacy

Tınmaz et al. (2022) synthesize the digital-literacy literature and find a large gap between the high theoretical expectations placed on literacy as a bulwark against information warfare and the mixed empirical evidence for program effectiveness. Their review highlights substantial conceptual fragmentation: studies define and measure digital literacy in divergent, often incompatible ways, which prevents the field from building cumulative knowledge or identifying best practices. They also show that programs narrowly focused on technical competencies, how to spot bots, use verification tools, or identify manipulation techniques, tend to produce only limited transfer to deeper abilities for critically evaluating information content. This suggests that resilience to information operations requires a broader, more integrated form of media and information literacy that combines technical skills with critical thinking, epistemic humility, and calibrated trust in institutions.

Complementing this individual-level perspective, recent reviews of organizational practice emphasize parallel shifts in cyber defense and digital governance. Abrahams et al. (2024) document the move away from perimeter-based architectures toward zero-trust models that assume compromise and prioritize containment of damage and robust identity and access controls. Saeed et al. (2023) show how rapid digital transformation intensifies vulnerability: integrating legacy systems with cloud services and new platforms often creates brittle seams that attackers can exploit. Both analyses converge on a key point:

technical measures alone are insufficient. Organizational culture, governance processes, and routine practices, incident response readiness, employee awareness, cross-unit coordination, and leadership commitment are critical determinants of cyber and information resilience. Together, these findings argue for multi-level strategies that combine comprehensive literacy education, socio-technical safeguards, and organizational reforms to reduce susceptibility to information warfare and to manage the systemic risks of digital transition.

Table 3. Defensive Countermeasures Against Information Warfare: A Multi-Layer Framework

Defense Layer	Instrument	Implementation Example	Key Reference
Individual	Digital Literacy Education	Media literacy curricula in schools and universities	Tınmaz et al., 2022
Organizational	Cybersecurity Frameworks	NIST / ISO 27001 adoption by public institutions	Abrahams et al., 2024
Organizational	Digital Transformation Resilience	Zero-trust architecture, threat modeling	Saeed et al., 2023
National	Cyber Diplomacy	Bilateral cyber norms treaties, UNGGE processes	Radanliev, 2024
National	AI Governance	EU AI Act, algorithmic transparency mandates	Calderaro & Blumfelde, 2022
Infrastructure	Submarine Cable Protection	NATO maritime monitoring, cable redundancy	Bueger & Liebetrau, 2021
Infrastructure	Satellite Security	Encrypted military SATCOM, anti-jamming protocols	Kang et al., 2024

***Note**. ISR = Intelligence, Surveillance, Reconnaissance. UNGGE = UN Group of Governmental Experts on Cyber Issues*

G. Game Theory and Strategic Dimensions of Information Operations

Ho et al. (2021) review game-theoretic applications in defense contexts, providing a formal analytical foundation for understanding the strategic logic of information warfare. Game-theoretic models illuminate how adversaries make decisions about information operation intensity, timing, and target selection in light of anticipated counteractions. Their review documents growing applications in deception strategy design, where AI-driven game-theoretic systems can identify optimal deceptive strategies by modeling adversary decision processes a development with direct implications for cognitive hacking operations that target military command systems.

Radanliev's (2024) comprehensive analysis of cyber diplomacy connects technological capabilities to the governance frameworks necessary to manage them. His analysis of the intersection between artificial intelligence, IoT, blockchain, and quantum computing in

cyber diplomacy contexts reveals the inadequacy of existing international legal frameworks, which were developed for a world of discrete state actions, to govern information warfare conducted by distributed, automated systems operating across jurisdictional boundaries. The absence of clear attribution standards for AI-conducted operations, the ambiguity surrounding civilian infrastructure targeting, and the lack of agreed norms on deepfake deployment in conflict zones represent critical governance gaps that current diplomatic frameworks are ill-equipped to address.

CONCLUSION

This article has demonstrated that information warfare constitutes a central and structurally transformative dimension of contemporary international relations. The convergence of social media ubiquity, artificial intelligence capabilities, and geopolitical competition has created a qualitatively new information environment in which perceptions, beliefs, and trust structures are themselves strategic assets and targets. Three principal findings emerge from this analysis.

First, modern information warfare operates simultaneously across cognitive, organizational, and physical infrastructure domains, requiring multi-layered analytical and defensive frameworks that transcend traditional boundaries between military, diplomatic, and civil society spheres. The Russia-Ukraine case illustrates how integrated information operations, combining propaganda, deepfakes, cyber infrastructure attacks, and satellite communication disruption, create mutually reinforcing effects that no single defensive instrument can adequately counter.

Second, the accelerating integration of artificial intelligence into information warfare creates both enhanced offensive capabilities and novel defensive vulnerabilities. AI-driven deepfakes, OODA loop automation, and game-theoretic adversarial modeling collectively expand the scope, speed, and sophistication of information operations, while simultaneously creating algorithmic brittleness and epistemic vulnerabilities that skilled adversaries can systematically exploit. The human judgment-prediction gap identified by Goldfarb and Lindsay (2022) represents a persistent structural feature of AI-enabled information warfare that technical solutions alone cannot resolve.

Third, existing defensive mechanisms, digital literacy education, cybersecurity frameworks, and cyber diplomacy, face significant implementation gaps relative to the offensive capabilities they must counter. The literacy paradox identified in the deepfake literature, the organizational culture challenges documented in cybersecurity research, and the governance gaps in cyber diplomacy frameworks collectively suggest that information warfare resilience requires not merely technical countermeasures but fundamental institutional adaptation across educational, regulatory, and diplomatic domains.

Future research should prioritize longitudinal assessment of digital literacy intervention effectiveness, development of attribution frameworks for AI-conducted operations, and comparative institutional analysis of information warfare resilience across democratic systems with varying media ecosystems and regulatory capacities.

LITERATURE

Abrahams, T. O., Ewuga, S. K., Dawodu, S. O., Adegbite, A. O., & Hassan, A. O. (2024). A review of cybersecurity strategies in modern organizations: Examining the evolution and effectiveness of cybersecurity measures for data protection.

Computer Science & IT Research Journal, 5(1). https://doi.org/10.51594/csitrj.v5i1.699

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. Contemporary Security Policy, 42, 391–413. https://doi.org/10.1080/13523260.2021.1907129

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. European Security, 31, 415–434. https://doi.org/10.1080/09662839.2022.2101885

Chen, L., Chen, J., & Xia, C. (2022). Social network behavior and public opinion manipulation. Journal of Information Security and Applications, 64, 103060. https://doi.org/10.1016/j.jisa.2021.103060

Geissler, D., Bar, D., Prollochs, N., & Feuerriegel, S. (2022). Russian propaganda on social media during the 2022 invasion of Ukraine. EPJ Data Science, 12, 1–20. https://doi.org/10.1140/epjds/s13688-023-00414-5

Goldfarb, A., & Lindsay, J. (2022). Prediction and judgment: Why artificial intelligence increases the importance of humans in war. International Security, 46, 7–50. https://doi.org/10.1162/isec_a_00425

Hannah, M. (2021). A conspiracy of data: QAnon, social media, and information visualization. Social Media + Society, 7. https://doi.org/10.1177/20563051211036064

Ho, E., Rajagopalan, A., Skvortsov, A., Arulampalam, S., & Piraveenan, M. (2021). Game theory in defence applications: A review. Sensors, 22. https://doi.org/10.3390/s22031032

Johnson, J. (2022). Automating the OODA loop in the age of intelligent machines: Reaffirming the role of humans in command-and-control decision-making in the digital age. Defence Studies, 23, 43–67. https://doi.org/10.1080/14702436.2022.2102486

Kang, M., Park, S., & Lee, Y. (2024). A survey on satellite communication system security. Sensors, 24. https://doi.org/10.3390/s24092897

Krelina, M. (2021). Quantum technology for military applications. EPJ Quantum Technology, 8, 1–53. https://doi.org/10.1140/epjqt/s40507-021-00113-y

Luo, Y. (2021). A general framework of digitization risks in international business. Journal of International Business Studies, 53, 344–361. https://doi.org/10.1057/s41267-021-00448-9

Radanliev, P. (2024). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. Journal of Cyber Security Technology, 9, 28–78. https://doi.org/10.1080/23742917.2024.2312671

Saeed, S., Altamimi, S., Alkayyal, N., Alshehri, E., & Alabbad, D. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. Sensors, 23. https://doi.org/10.3390/s23156666

Solmi, M., Radua, J., Olivola, M., Croce, E., Soardo, L., De Pablo Salazar, G., ... & Fusar-Poli, P. (2021). Age at onset of mental disorders worldwide: Large-scale meta-analysis of 192 epidemiological studies. Molecular Psychiatry, 27, 281–295. https://doi.org/10.1038/s41380-021-01161-7

Stoumpos, A., Kitsios, F., & Talias, M. (2023). Digital transformation in healthcare: Technology acceptance and its applications. International Journal of Environmental Research and Public Health, 20. https://doi.org/10.3390/ijerph20043407

Tinmaz, H., Lee, Y.-T., Fanea-Ivanovici, M., & Baber, H. (2022). A systematic review on digital literacy. Smart Learning Environments, 9. https://doi.org/10.1186/s40561-022-00204-y

Twomey, J., Ching, D., Aylett, M., Quayle, M., Linehan, C., & Murphy, G. (2023). Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. PLOS ONE, 18. https://doi.org/10.1371/journal.pone.0291668

Wang, C., Chen, X., Yu, T., Liu, Y., & Jing, Y. (2024). Education reform and change driven by digital technology: A bibliometric study from a global perspective. Humanities and Social Sciences Communications, 11, 1–17. https://doi.org/10.1057/s41599-024-02717-y

Weikmann, T., & Lecheler, S. (2022). Visual disinformation in a digital age: A literature synthesis and research agenda. New Media & Society, 25, 3696–3713. https://doi.org/10.1177/14614448221141648