



History:

Collection: 2026

Received: April 12, 2026

Status: Published

Identifiers:

ID: 3-26/DTN

Year: 2026

Volume: 15

First Page: 150

Last Page: 156

Correspondence: Zaighum

Javaid, 935 Ferguson Dr, Milton
ON L9T 6V7, Canada. +1 (647)
285-5959, zjkayani@gmail.com

Funding Statement: The authors
declare that no specific funding was
received for this study.

Ethics Approval Statement:

Ethical approval was not required
for this study, as it did not involve
human participants, animal
subjects, or identifiable personal
data.

Consent for Publication

Statement: The author has
reviewed and approved the final
manuscript and consents to its
publication in accordance with
journal policies.

Additional information is
available at the end of the
article.



Analytical Review Article

**CYBER WARFARE AND INFORMATION OPERATIONS
IN MODERN CONFLICTS**

Taha Nazir¹, Zaighum Javaid^{2,3}

1. Director Advanced Multiple Inc., Canada. Thomson Reuters - ID N-5730-2015 | orcid.org/0000-0002-5308-6798 | <https://tahanazir.com>
2. Chief Executive, Media South Asia Canada Inc., Canada.
3. Host, community radio programs WTOR 770 AM Toronto ON and CFCR FM 90.5 Saskatoon SK Canada.

Abstract

Cyber warfare and information operations have emerged as decisive elements in modern conflicts, complementing traditional military power with digital and psychological tools. These capabilities enable states to disrupt critical infrastructure, influence public perception, and achieve strategic objectives without direct physical confrontation. This article examines the nature of cyber warfare, the role of information operations, and their integration into modern military strategy. A focused case study of the 2026 Iran conflict illustrates how cyber operations function as a parallel battlefield alongside conventional warfare.

Running title: cyber warfare, information operations, digital warfare strategy

Keywords: cyber deterrence, digital battlefield, information warfare tactics, psychological operations online

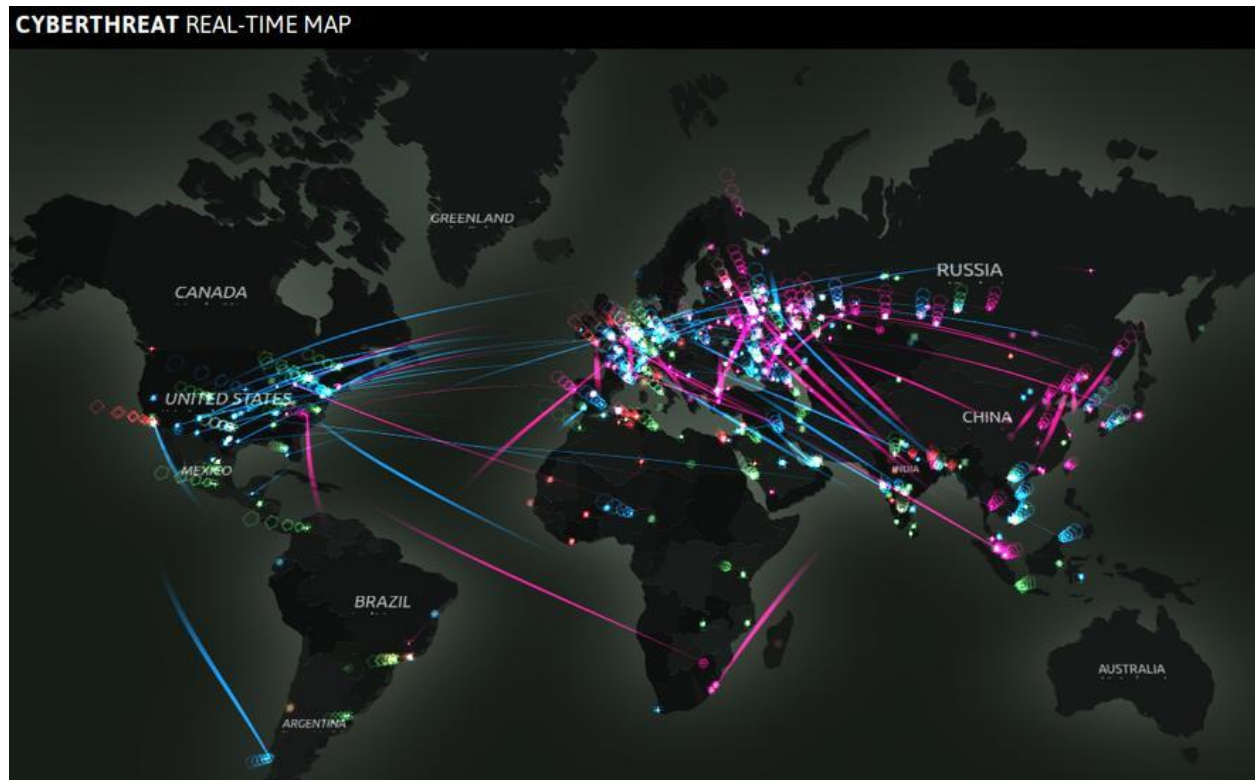
Data Source: Archives, Biographies, Databanks, Encyclopedias, Libraries, Metadata Registries, Reports, Repositories, arXiv, Crossref, OpenAI, Wikipedia, World Health Organization, Zenodo.

Conflict of Interest Statement: The author declares all potential conflicts of interest and affirms that any such interests have been appropriately disclosed in accordance with standard ethical guidelines.

AI Tools and Assistance Statement: Artificial intelligence tools were utilized to support content structuring, data analysis, and evidence synthesis. All outputs were critically reviewed and validated by the author, who assumes full responsibility for the accuracy, interpretation, and conclusions of the work.

Introduction

In the 21st century, warfare has increasingly shifted into the digital domain, where cyber operations and information manipulation play decisive roles in shaping conflict outcomes. States such as United States, China, and Russia have developed advanced cyber capabilities, integrating them into national defense and offensive strategies. Cyber warfare encompasses activities ranging from infrastructure disruption and espionage to psychological operations conducted through digital platforms. This review explores the strategic, legal, and societal implications of cyber warfare and information operations in modern conflicts.



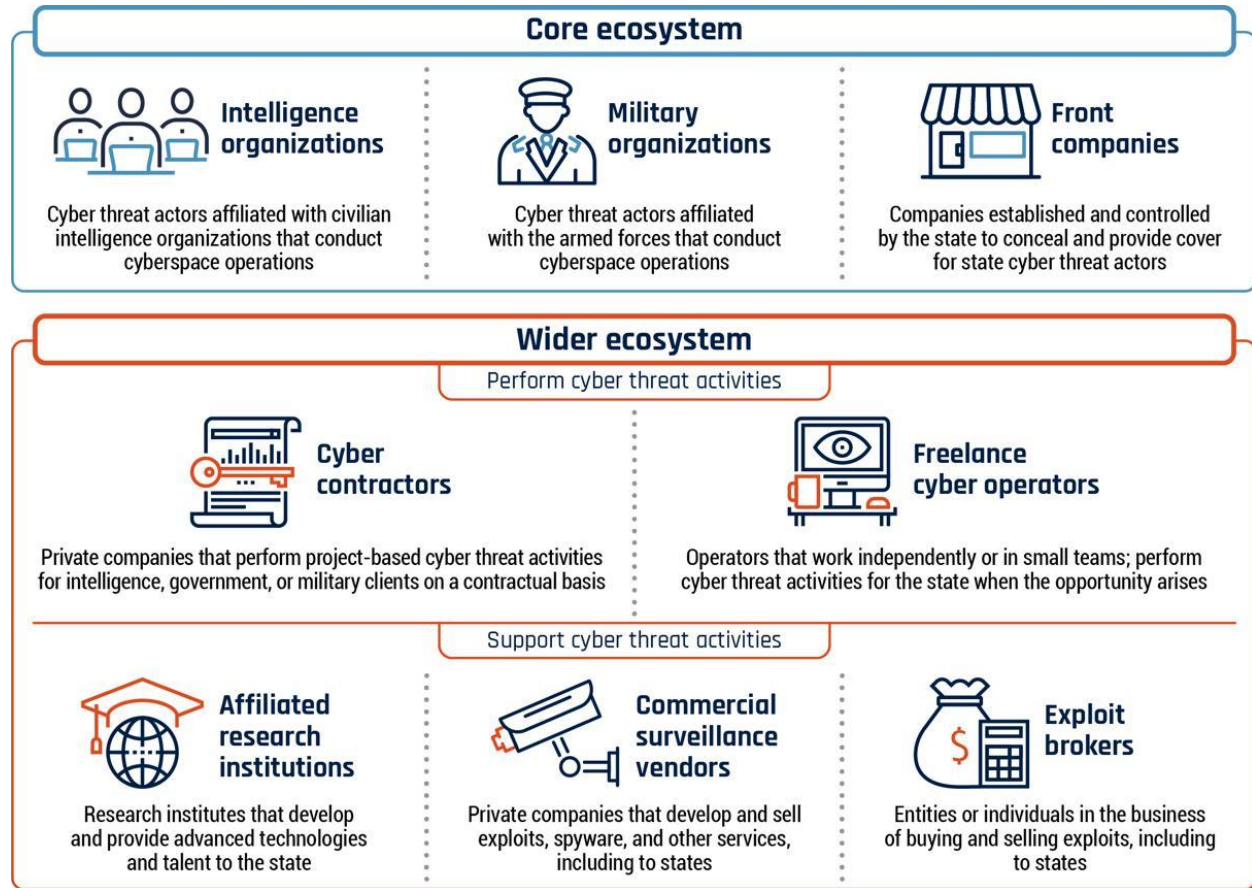
Methodology

This review adopts a qualitative synthesis approach, integrating findings from peer-reviewed journals, cybersecurity reports, defense analyses, and policy papers. Databases such as Scopus, Web of Science, and institutional repositories were consulted. Inclusion criteria focused on studies addressing cyber conflict, information warfare, and digital security frameworks, while exclusion criteria eliminated outdated or non-empirical sources. A thematic analytical framework was applied to identify key patterns and insights.

Main Body / Thematic Analysis

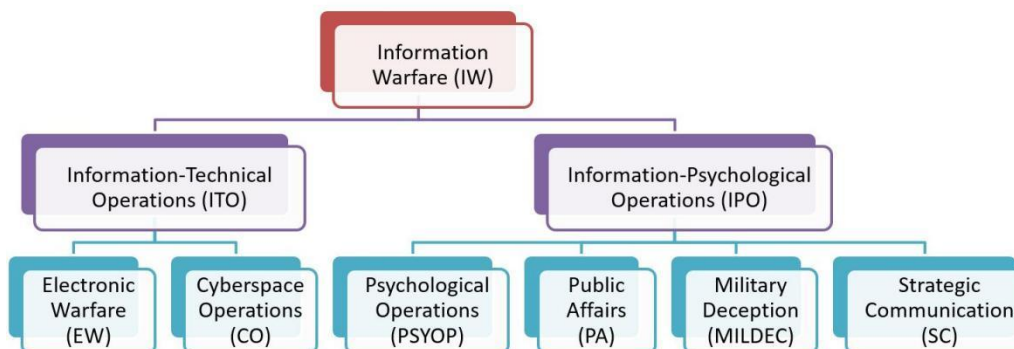
Evolution of Cyber Warfare





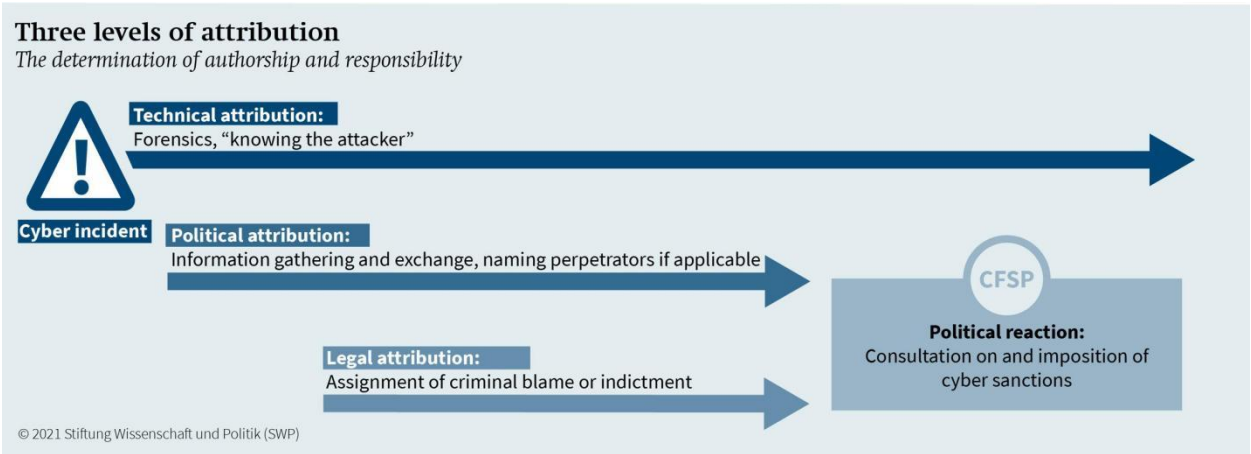
Cyber warfare has evolved from isolated hacking incidents to sophisticated state-sponsored operations targeting critical infrastructure, financial systems, and defense networks. Early examples such as the Stuxnet attack marked a turning point, demonstrating the potential of cyber tools to cause physical damage. Modern cyber conflicts involve coordinated campaigns integrating malware, ransomware, and advanced persistent threats (APTs), often conducted covertly to maintain plausible deniability.

Information Operations and Digital Influence



Information operations involve the strategic use of data, media, and communication technologies to influence public perception and political outcomes. Through social media platforms, actors deploy disinformation, propaganda, and algorithmic manipulation to shape narratives and destabilize societies. These operations exploit cognitive biases and information asymmetries, making them highly effective in modern hybrid warfare environments.

Legal and Ethical Challenges



The legal framework governing cyber warfare remains underdeveloped. While principles of international law—such as sovereignty and non-intervention—apply, their interpretation in cyberspace is contested. Documents like the Tallinn Manual attempt to clarify these issues, yet enforcement remains weak. Attribution challenges complicate accountability, while ethical concerns arise regarding privacy violations, civilian targeting, and the use of autonomous cyber weapons.

Strategic and Global Implications

Cyber warfare significantly alters global power dynamics by enabling smaller states and non-state actors to challenge more powerful adversaries. Economically, cyber attacks can disrupt financial systems, supply chains, and critical infrastructure, leading to substantial losses. Strategically, cyber capabilities are now integrated into military doctrines, enhancing both offensive and defensive operations. The rise of artificial intelligence further amplifies these capabilities, introducing new dimensions of risk and complexity.

Comparative Insight Table

Dimension	Key Observations
Nature of Warfare	Non-kinetic, digital, covert
Key Actors	States, non-state actors, hacktivists
Tools & Methods	Malware, APTs, disinformation campaigns
Legal Status	Ambiguous, evolving frameworks
Global Impact	Economic disruption, political instability

Future Prospects

Future research should explore the integration of artificial intelligence in cyber operations, including autonomous threat detection and offensive capabilities. The development of global cyber norms and treaties is another critical area. Additionally, the impact of quantum computing on cybersecurity and encryption systems requires further investigation.

Recommendations

Governments should invest in robust cybersecurity infrastructure and capacity building to enhance resilience against cyber threats. International cooperation is essential to establish norms and frameworks governing cyber conduct. Public awareness campaigns can help mitigate the impact of disinformation. Furthermore, regulatory oversight of technology platforms is necessary to prevent misuse in information operations.

Conclusion

Cyber warfare and information operations represent a transformative shift in the nature of modern conflict, extending the battlefield into the digital and cognitive domains. Unlike traditional warfare, these forms of conflict operate continuously below the threshold of armed confrontation, making detection and response more complex. The ambiguity surrounding legal frameworks and attribution further complicates efforts to regulate cyber activities and ensure accountability. As cyber capabilities continue to evolve, their integration into military and political strategies will likely intensify, increasing both strategic opportunities and systemic risks. Ultimately, addressing these challenges requires a coordinated global response that combines technological innovation, legal reform, and ethical governance to ensure stability and security in an increasingly digital world.

Review Typology and Reporting

Review designs were classified into standard categories (scoping, umbrella, rapid, qualitative, and mixed-methods), with reporting aligned to established guidelines (PRISMA-ScR, PRIOR, PRISMA-RR, ENTREQ, and PRISMA/MMAT) to ensure methodological rigor and transparency.

Editorial Statement:

This is research-based manuscript, prepared and structured in a scientific manner. Modern AI-assisted tools used to access current and authentic info. The digital archives, bibliographic databanks, online libraries, research articles, academic repositories and encyclopedias employed.

Preprint Notice:

This manuscript is shared as a non-peer-reviewed preprint on platforms such as Zenodo, SSRN, and Research Square to support scholarly discussion. The content is research-based and developed using publicly available and verifiable sources. Readers are encouraged to interpret the material as preliminary and subject to revision.

Legal Disclaimer

This manuscript is provided for academic and informational purposes only and does not constitute professional advice. While based on publicly available data and presented in good

faith, no warranties are made regarding its accuracy or applicability. The author assumes no liability for any outcomes arising from its use, and readers should consult qualified professionals before making decisions.

Peer Review Statement: This manuscript has not undergone external peer review, as it represents a structured synthesis and analysis of existing evidence. The methodological approach adheres to established standards to ensure rigor, transparency, and scientific validity.



References:

- Atlantic Council. (2025, July 29). What the Israel-Iran conflict revealed about wartime cyber operations. <https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/>
- Center for Strategic and International Studies (CSIS). (2026, March 2). How will cyber warfare shape the U.S.-Israel conflict with Iran?. <https://www.csis.org/analysis/how-will-cyber-warfare-shape-us-israel-conflict-iran>
- Center for Strategic and International Studies (CSIS). (2026, March 19). Demystifying Iranian cyber operations in the U.S.-Iran conflict. <https://www.csis.org/analysis/demystifying-iranian-cyber-operations-us-iran-conflict>
- CloudSEK. (2026, March 4). Situation report: Middle East escalation (February 27–1st March 2026). <https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026>
- Cyber Express. (2026, March 11). Cyber warfare escalates amid Iran Israel US tensions. LinkedIn. https://www.linkedin.com/posts/thecyberexpress_the-state-of-cyber-warfare-in-2026-nation-state-activity-7437887429757358080-Gzh8
- Cyble. (2026, March 2). Cyber threat monitor: Iran–Israel–US conflict 2026. <https://cyble.com/resources/research-reports/cyber-threat-monitor-iran-israel-us-conflict-2026/>
- Data Security Council of India (DSCI). (2026). Cyber threat advisory on Middle East conflict [PDF]. https://www.dsci.in/files/content/advisory/2026/cyber_threat_advisory-middle_east_conflict.pdf
- Digital Rulebook. (2026, February 28). The Iran cyberattack is the biggest digital law story of 2026. <https://digitalrulebook.blogspot.com/2026/03/the-iran-cyberattack-is-biggest-digital.html?m=1>
- Falcon Feeds. (2026, April 13). Cyber warfare & information operations in the Iran–Israel conflict. <https://falconfeeds.io/blogs/iran-israel-conflict-cyber-warfare-information-operations-2026>
- Forbes. (2026, April 3). Cyber and kinetic warfare are now one battlefield: What the US-Israel-Iran conflict reveals. <https://www.forbes.com/sites/emilsayegh/2026/04/03/cyber-and-kinetic-warfare-are-now-one-battlefield-what-the-us-israel-iran-con>
- Fortune. (2026, March 29). There are a lot more attacks happening that aren't being disclosed. <https://fortune.com/2026/03/29/iran-cyber-attacks-response-to-war-hacking/>

- Palo Alto Networks Unit 42. (2026, April 16). Threat brief: Escalation of cyber risk related to Iran (updated April 2026). <https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/>
- Politico. (2026, March 2). The cyber war in Iran. <https://www.politico.com/newsletters/weekly-cybersecurity/2026/03/02/the-cyber-war-in-iran-00806706>
- Royal United Services Institute (RUSI). (2026, March 4). Fog, proxies and uncertainty: Cyber in US-Israeli operations in Iran. <https://www.rusi.org/explore-our-research/publications/commentary/fog-proxies-and-uncertainty-cyber-us-israeli-operations-iran>
- Seqrite. (2026, April 5). Iran cyber war 2026: US–Israel strikes, APT attacks & global threats



DownTown

© 2025 DownTown News. This publication is released under the Creative Commons Attribution (CC BY 4.0) license. You are permitted to: Share: Copy and redistribute the material in any medium or format. Adapt: Remix, transform, and build upon the material for any purpose, including commercial use. These freedoms cannot be revoked if the licensing terms are followed. License Terms: Attribution: You must provide appropriate credit to DownTown News, include a link to the CC BY 4.0 license, and indicate if any changes were made. Attribution must be given in a reasonable manner that does not imply endorsement by DownTown News. No Additional Restrictions: You may not apply legal terms or technological measures that restrict others from exercising the permissions granted by this license.

For full license details, please refer to the Creative Commons Attribution 4.0 International License (CC BY 4.0).