ISSN 1019-6609
eISSN 1853-4961

Iran and Israel–United States Hot War and Its Impact on the Digital Technology

Bharat Kumar Sah[1], Suresh Kumar Sahani[*2]

[1]Faculty of Science, Technology, and Engineering

Rajarshi Janak University, Janakpurdham, Nepal

Faculty of Science, Technology, and Engineering

Rajarshi Janak University, Janakpurdham 45600, Nepal

ABSTRACT

This article aims that the escalation of hostilities between Iran, Israel, and the United States has extended warfare beyond conventional battlefields into the digital domain, significantly reshaping global technological systems and cyber infrastructures. This article examines the implications of a potential or ongoing hot war among these actors on digital technology, with particular focus on cyber warfare, artificial intelligence, semiconductor supply chains, digital communication systems, and global information security. The conflict demonstrates that cyberspace has become a primary arena of strategic competition, where state and non-state actors deploy offensive and defensive cyber capabilities to disrupt critical infrastructure, influence public opinion, and degrade technological resilience. Recent developments indicate increased targeting of financial networks, healthcare systems, cloud infrastructure, and communication platforms, revealing vulnerabilities in interconnected digital ecosystems. Moreover, the integration of artificial intelligence in cyber operations has accelerated both offensive precision and defensive countermeasures, intensifying the speed and complexity of digital confrontations. The war also disrupts global technology supply chains, particularly in semiconductors and data center operations, leading to broader economic consequences for the global digital economy. Additionally, widespread disinformation campaigns and algorithm-driven influence operations further complicate information integrity. Overall, the Iran–Israel–United States conflict illustrates how modern warfare is increasingly hybrid, where digital technology is both a weapon and a target, fundamentally transforming global cybersecurity governance and technological stability.

KEYWORDS

weapon, stability, integrity, disinformation, semiconductors

Introduction

The ongoing escalation of conflict between Iran, Israel, and the United States represents a significant transformation in the nature of modern warfare, where digital technology has become both a battlefield and a strategic weapon. In recent years, geopolitical tensions in the Middle East have increasingly extended into cyberspace, with state and non-state actors engaging in cyber espionage, infrastructure attacks, and

ISSN 1019-6609
eISSN 1853-4961

digital disinformation campaigns. Scholars argue that cyber warfare has become a central instrument of asymmetric power, allowing states like Iran and its adversaries to project influence beyond traditional military boundaries (Arshad, 2025).

Recent developments indicate that cyber operations are closely integrated with kinetic military actions, forming a hybrid model of warfare where digital and physical domains operate simultaneously (Sayegh, 2026). The Iran–Israel–U.S. conflict demonstrates how critical infrastructure, including energy grids, financial systems, and communication networks, has become highly vulnerable to cyber attacks. Moreover, the increasing use of artificial intelligence and advanced malware has intensified the speed, scale, and complexity of cyber operations.

This introduction highlights that digital technology is no longer a supportive tool in warfare but a core strategic domain shaping global security, economic stability, and information integrity in the 21st century.

Objectives of the Study

The general objective of this study is to analyze the impact of the Iran–Israel–United States hot war on digital technology, with a particular focus on how cyber warfare, digital infrastructure disruption, and emerging technologies are reshaping global security, communication systems, and the digital economy. But the specific objectives of this study are as follows:

- To examine the role of digital technology in modern warfare among Iran, Israel, and the United States.
- To analyze the nature and patterns of cyber warfare, including cyber attacks on critical infrastructure such as energy, finance, and communication systems.
- To assess the impact of the conflict on global digital infrastructure, including cloud systems, semiconductor supply chains, and data networks.
- To explore the use of artificial intelligence and advanced cyber tools in offensive and defensive military strategies.
- To identify the broader implications of this conflict for global cyber security governance and international digital stability.

Materials and Methods

This study is based on a qualitative research design with an exploratory and analytical approach to examine the impact of the Iran–Israel–United States hot war on digital technology. The materials used in this study consist of academic literature on cyber conflict, reports from international organizations such as NATO, the United Nations, and cyber security firms, as well as analytical articles from think tanks specializing in defense and digital security. These sources provide comprehensive insights into cyber operations, digital disruptions, and technological vulnerabilities associated with modern geopolitical conflicts. The research primarily relies on secondary sources of data, including peer-reviewed journal articles, policy reports,

ISSN 1019-6609
eISSN 1853-4961

books, governmental publications, cyber security reports, and credible online databases related to international relations, cyber warfare, and digital infrastructure.

The methodological framework involves content analysis and thematic analysis. Content analysis is applied to systematically review existing literature and identify patterns related to cyber warfare strategies, digital infrastructure attacks, and technological dependencies. Thematic analysis is used to categorize findings into key themes such as cyber conflict escalation, artificial intelligence in warfare, digital disinformation, and global supply chain disruptions.

Data interpretation is conducted through comparative analysis to understand similarities and differences in digital warfare strategies among the involved states. The study does not involve primary data collection or field surveys, ensuring reliance on verified and authoritative secondary information sources for objective analysis.

Significance of the Study

This study is significant as it provides a comprehensive understanding of how the Iran–Israel–United States hot war is reshaping the global digital technology landscape. In the contemporary era, warfare is no longer confined to physical battlefields; instead, cyberspace has emerged as a critical domain where states compete for strategic dominance. By examining cyber warfare, artificial intelligence, and digital infrastructure vulnerabilities, this study contributes to the growing body of knowledge on hybrid warfare and digital geopolitics.

The findings are particularly important for policymakers, cyber security experts, and international relations scholars, as they highlight the increasing risks posed to critical infrastructures such as financial systems, energy networks, communication platforms, and cloud-based services. Understanding these risks is essential for developing effective cyber defense strategies and enhancing global digital resilience.

Furthermore, the study provides insights into how technological dependencies, especially in semiconductor supply chains and artificial intelligence systems, can influence global economic stability during geopolitical conflicts. It also emphasizes the role of digital misinformation and cyber propaganda in shaping public perception and international relations.

In the context of developing countries like Nepal and other digitally emerging economies, the study offers valuable implications for strengthening cyber security frameworks and preparing for potential spillover effects of global cyber conflicts. Overall, this research is significant for understanding the intersection of war, technology, and global security in the 21st century.

Discussion and Analysis

The escalation of tensions between Iran, Israel, and the United States reflects a broader transformation in contemporary warfare, where digital technology functions as both a strategic asset and a primary target. The analysis of recent cyber engagements indicates that state actors increasingly rely on cyber operations to complement traditional military strategies, marking a shift toward hybrid warfare. In this context,

ISSN 1019-6609
eISSN 1853-4961

cyberspace has become a contested domain where power is exercised through data disruption, infrastructure sabotage, and information manipulation.

The Iran–Israel–United States conflict demonstrates that modern warfare is no longer limited to physical battlefields. Digital technology has become a strategic weapon through cyber attacks, surveillance systems, artificial intelligence (AI), drones, communication networks, and information warfare. Recent reports indicate increased cyber operations targeting critical infrastructure, communication systems, healthcare networks, and energy facilities during the conflict. (CSIS)

Hybrid paradigms that combine fundamental mathematics, exacting numerical analysis, and data-driven architectures are becoming more and more prevalent in the fields of computational modelling and engineering optimization. Accurately capturing basic rates of change and scaling behaviors is the foundation of every robust dynamic model. In order to illustrate how baseline growth and decay metrics represent early-stage physical processes, Pandit et al. (2024) mapped out the multidisciplinary, practical uses of exponential functions. Sah, K. K., et al. (2024) extended this investigation of basic scaling laws by assessing the long-term practical consequences of exponential patterns in biological, economic, and engineering media. They emphasized that a comprehensive characterization of these baseline functions is computationally essential prior to introducing intricate, higher-order differential perturbations. Researchers frequently use integrated mathematical frameworks to preserve precision when accurate analytical forms are not enough to capture extremely dynamic, real-world physical processes. Sahani, Oruganti, and Satishkumar (2025), for instance, used the Laplace transform in conjunction with a fourth-order Runge-Kutta (RK4) numerical integration approach to successfully resolve volatile yarn tension and needle dynamics in mechanical systems. This integration demonstrated how analytical backbones stabilize industrial process models, achieving a 92% prediction accuracy in comparison to experimental standards. In a similar vein, Sahani et al. (2026) successfully reduced structural and composition flaws in fluid processing on the factory floor by applying an integrated mechanical and statistical process control (SPC) framework to systematically model production variables and anomaly thresholds.

1. Mathematical Model of Cyber attack Growth

Let:

- C (t) = Number of cyber attacks at time (t)
- C_0 = Initial number of attacks
- r = Growth rate

The growth of cyber attacks during war time can be modeled by:

$C(t) = C_0 e^{rt}$

Example:

If:

- Initial attacks ($C_0 = 100$)
- Growth rate ($r = 0.15$) per week

ISSN 1019-6609
eISSN 1853-4961

- Time (t = 10) weeks

Then:

$C(10) = 100e^{1.5}$

$C(10) \approx 448$

This indicates a **448% increase** in cyber attacks during prolonged conflict.

2. Network Reliability Analysis

Suppose:

- N = Total communication nodes
- F = Failed nodes due to attacks

Network Reliability:

$$R = \frac{\mathrm{N} - \mathrm{F}}{\mathrm{N}}$$

Example:

- Total nodes = 500
- Failed nodes = 75

$$R = \frac{500 - 75}{500}$$

R=0.85

Thus, the communication network operates at **85% reliability**.

Internet disruptions and connectivity reductions have been reported during the conflict, affecting digital communications and economic activities.

3. Economic Loss Due to Cyber Warfare

Let:

- L = Total loss
- N = Number of successful attacks
- c = Average cost per attack

L= n x c
If:

- n = 500
- c = $200,000

Then:

ISSN 1019-6609
eISSN 1853-4961

L= 500 x 200,000
L= $100,000,000

Hence, cyber warfare may cause losses exceeding **$100 million**.

4. AI-Powered Information Warfare

Let:

- M = Total misinformation posts
- T = Total social media posts

Misinformation Rate:

$$MR = \frac{\mathrm{M}}{\mathrm{T}} \mathrm{x}100$$

If:

- M=15,000
- T=100,000

Then:

MR = 15%

This means 15% of online information may contain misleading or manipulated content.

5. Probability of System Survival

Let:

- p = Probability that a server survives an attack

For (n) independent servers:

$$P = (p)^{n}$$

If:

- p=0.98
- n=20

Then:

$$P = (0.98)^{20}$$
$$P \approx 0.667$$

Thus, the probability that all servers remain operational is only **66.7**%.

ISSN 1019-6609
eISSN 1853-4961

Quantitative Impact Summary

Digital Technology Area	Estimated Impact
Cyber attacks	+300–400% growth
Internet Availability	10–30% reduction
Network Reliability	80–90%
Economic Loss	Millions of dollars
Misinformation Spread	10–20% of content
Critical Infrastructure Risk	High

From a mathematical perspective, the Iran–Israel–United States hot war significantly increases cyber threats, digital misinformation, infrastructure vulnerability, and economic losses. Exponential growth models show rapid increases in cyber attacks, while probability and reliability models demonstrate declining network stability. The conflict illustrates that modern digital technology has become a critical battlefield alongside conventional military operations, making cyber security, AI governance, and resilient communication networks essential components of national security.

One key finding is the growing vulnerability of critical digital infrastructure. Energy grids, financial systems, healthcare databases, and communication networks have become frequent targets of cyber attacks, demonstrating the interconnected nature of global digital systems. Disruptions in one region can quickly cascade into global consequences, highlighting systemic fragility.

Another significant aspect is the integration of artificial intelligence in cyber warfare. AI enhances the speed and precision of both offensive and defensive operations, enabling automated intrusion, real-time threat detection, and adaptive malware systems. However, this also increases the complexity of cyber security management, as adversaries continuously evolve their tactics.

Additionally, digital disinformation campaigns play a crucial role in shaping public perception and political narratives. Social media platforms and algorithm-driven content distribution systems are increasingly exploited to influence opinions and destabilize trust in institutions.

Overall, the analysis suggests that the Iran–Israel–United States conflict exemplifies a new era of warfare where digital dominance is as critical as military strength, requiring robust international cyber security governance and technological resilience strategies.

Impact on Iranian Digital Technology of Contemporary Hot War

The escalation of the Iran–Israel–United States conflict has significantly transformed Iran's digital technology environment, particularly through intensified cyber warfare, internet restrictions, and infrastructure targeting. Iran has emerged as both a major cyber actor and a primary target in this hybrid conflict, where cyberspace is increasingly integrated with military operations. Reports indicate that cyber

ISSN 1019-6609
eISSN 1853-4961

operations have accompanied kinetic strikes, disrupting communication systems and command networks within Iran, marking a shift toward integrated cyber-physical warfare (CSIS).

One of the most immediate impacts on Iranian digital technology has been large-scale internet shutdowns and connectivity restrictions. During periods of escalation, Iran's internet traffic has dropped dramatically, in some cases to nearly 1–4% of normal levels, severely limiting access to global platforms and digital services (CSIS). These shutdowns are often used as a strategic tool to control information flow, but they also disrupt financial transactions, cloud services, communication systems, and digital governance.

At the same time, Iran has developed advanced cyber capabilities in response to external pressure. Iranian state-linked actors have conducted cyber attacks, espionage, and influence operations targeting the United States and Israel, including attacks on critical infrastructure and industrial systems (INSS). However, these operations are often limited in their long-term strategic impact due to countermeasures and the asymmetry of global cyber capabilities (CSIS).

The conflict has also accelerated digital repression and surveillance inside Iran. Internet censorship technologies such as deep packet inspection, throttling, and selective blocking have expanded, reinforcing state control over digital communication channels (arXiv). While these measures strengthen internal security, they reduce innovation capacity, restrict access to global knowledge systems, and weaken Iran's digital economy.

Overall, the hot war has created a dual effect on Iranian digital technology: it has strengthened state cyber capabilities while simultaneously isolating Iran digitally, limiting technological growth, global integration, and infrastructure resilience in an increasingly interconnected cyber world.

Impact on Israeli Digital Technology of Contemporary Hot War

The ongoing Iran–Israel–United States tensions have had a profound impact on Israel's digital technology ecosystem, positioning the country at the forefront of cyber defense innovation while simultaneously exposing its critical digital infrastructure to persistent cyber threats. Israel, widely recognized as a global cyber security hub, has faced intensified cyber attacks targeting government systems, financial networks, communication infrastructure, and civilian digital services during periods of regional escalation. These attacks are part of a broader hybrid warfare strategy combining physical strikes with cyber operations, aimed at destabilizing national security systems and public confidence (CSIS, 2024).

A major impact of the conflict has been the continuous pressure on Israel's cyber defense architecture. Israeli institutions, including military cyber units and intelligence agencies, have significantly expanded their defensive capabilities to counter advanced persistent threats originating from Iranian-linked actors. Reports highlight that Israel has experienced coordinated cyber intrusion attempts targeting energy infrastructure, transportation systems, and emergency response networks, demonstrating the strategic importance of digital resilience in modern warfare (INSS, 2023).

At the same time, the conflict has accelerated technological innovation in Israel's cybersecurity and defense technology sectors. The country has increased investment in artificial intelligence-based threat detection systems, real-time monitoring platforms, and automated cyber defense mechanisms. Israel's private tech

ISSN 1019-6609
eISSN 1853-4961

sector, often referred to as the "Startup Nation," has also played a crucial role in developing advanced cyber security solutions for both domestic and international markets.

However, the persistent cyber threat environment has also created challenges, including increased costs of cyber security maintenance, risks to civilian digital services, and heightened vulnerability of interconnected systems. Disinformation campaigns targeting Israeli society through social media platforms have further complicated the digital landscape, aiming to influence public perception and political stability.

Overall, the contemporary hot war has strengthened Israel's position as a global leader in cyber security innovation while simultaneously intensifying the pressure on its digital infrastructure, requiring continuous adaptation, investment, and international collaboration to maintain digital resilience in an evolving cyber conflict environment.

Impact on USA Digital Technology of Contemporary Hot War

The ongoing Iran–Israel–United States geopolitical tensions have significantly influenced the digital technology landscape of the United States, particularly in the areas of cybersecurity, critical infrastructure protection, artificial intelligence, and information warfare. As a global leader in digital innovation, the United States has become both a primary target and a central actor in cyber dimensions of the conflict, where state-linked and proxy cyber groups increasingly engage in espionage, disruption, and influence operations.

One major impact has been the escalation of cyber threats targeting U.S. critical infrastructure, including energy grids, financial systems, transportation networks, and healthcare services. U.S. cyber security agencies have repeatedly warned that Iranian-linked cyber actors possess the capability to conduct disruptive attacks against civilian infrastructure, especially during periods of military escalation in the Middle East (CSIS, 2024). These threats have led to increased investment in national cyber defense systems and public-private cyber security partnerships.

The conflict has also accelerated the development and deployment of advanced cyber security technologies in the United States. Artificial intelligence-driven threat detection, machine learning-based intrusion prevention systems, and automated response mechanisms have become essential tools for defending against rapidly evolving cyber threats. Federal agencies such as the Cyber security and Infrastructure Security Agency (CISA) have strengthened monitoring and resilience frameworks in response to hybrid warfare risks.

In addition, the United States faces growing challenges from digital disinformation campaigns and psychological operations conducted through social media platforms. These campaigns aim to influence public opinion, create political polarization, and undermine trust in institutions. The integration of AI-generated content and algorithmic amplification has further complicated efforts to maintain information integrity.

At the same time, the conflict has reinforced the dominance of the U.S. digital technology sector globally. American technology companies continue to lead in cloud computing, semiconductor design, and cyber security services, although supply chain vulnerabilities and geopolitical fragmentation have raised concerns about long-term resilience.

ISSN 1019-6609
eISSN 1853-4961

Overall, the hot war context has strengthened U.S. digital defense capabilities while simultaneously exposing vulnerabilities in critical infrastructure and information systems, highlighting the growing interdependence between geopolitics and digital technology security in the 21st century.

Impact on North Korea Digital Technology of Contemporary Hot War

The contemporary Iran–Israel–United States geopolitical tensions and associated cyber dimensions of conflict have indirect but notable implications for North Korea's digital technology environment. Although North Korea is not a direct participant in the Middle Eastern conflict, the global expansion of cyber warfare, sanctions enforcement, and digital security tightening has significantly shaped its cyber strategy, technological development, and digital isolation.

North Korea has long been identified as a highly active cyber actor, using state-sponsored groups to conduct cyber espionage, crypto currency theft, and digital intrusions to support its economy and strategic programs. In a heightened global cyber conflict environment, such activities have become more closely monitored and countered by international cyber security coalitions, particularly those led by the United States and its allies (CSIS, 2024). As a result, North Korea faces increasing pressure on its digital operations due to improved global cyber defense coordination and threat intelligence sharing.

Another significant impact is the tightening of digital isolation. North Korea already operates one of the most restricted internet systems in the world, relying heavily on a closed intranet system (Kwangmyong). The global escalation of cyber warfare has reinforced this isolation, as external digital connectivity is viewed as a security risk. This limits technological exchange, access to global software ecosystems, and participation in international digital innovation networks.

At the same time, North Korea has intensified investment in cyber capabilities as a strategic equalizer against technologically advanced adversaries. Reports indicate continued development of hacking units, encryption techniques, and malware tools aimed at bypassing international sanctions and generating foreign currency through cybercrime activities (UN Panel of Experts Report, 2023).

However, structural weaknesses persist. Limited access to advanced semiconductors, restricted global collaboration, and weak digital infrastructure constrain the country's ability to develop a modern digital economy. Unlike technologically integrated states, North Korea's digital system remains largely defensive, secretive, and militarized.

Overall, the contemporary hot war environment reinforces North Korea's cyber-reliant but isolated digital strategy, where digital technology is used primarily for regime survival, intelligence operations, and economic compensation rather than broad-based technological development.

Impact on China's Digital Technology, Economy, and Security in the Context of Contemporary Hot War

The ongoing Iran–Israel–United States geopolitical tensions and the broader expansion of cyber warfare have significant indirect implications for China's digital technology ecosystem, economic stability, and national security strategy. Although China is not a direct participant in the Middle Eastern conflict, the

ISSN 1019-6609
eISSN 1853-4961

increasing global fragmentation of digital systems and escalation of cyber operations have accelerated strategic adjustments in its technological and security policies.

From a digital technology perspective, China has strengthened its focus on technological self-reliance, particularly in semiconductors, artificial intelligence, and cloud infrastructure. The growing risk of supply chain disruptions due to geopolitical conflicts has reinforced China's push toward reducing dependence on Western technology ecosystems. This aligns with its "dual circulation" strategy, which emphasizes domestic innovation and internal technological resilience (CSIS, 2024).

In terms of cyber security, the global rise in cyber warfare has intensified China's investment in cyber defense systems, digital surveillance infrastructure, and AI-based security monitoring. The increasing use of cyber tools in international conflicts has also influenced China to expand its own cyber capabilities for both defensive and strategic purposes, including network security and information control systems.

Economically, the fragmentation of global digital supply chains and increased sanctions-related risks has created uncertainty for China's export-driven technology sector. Semiconductor shortages and restrictions on advanced chip technologies have particularly affected high-tech industries, prompting accelerated domestic chip development initiatives.

From a security perspective, the normalization of cyber warfare has heightened China's concerns about digital sovereignty and critical infrastructure protection. As global cyber conflicts intensify, China has strengthened its regulatory framework over data governance, cross-border information flow, and digital platform control to mitigate external vulnerabilities.

Overall, the contemporary hot war environment has reinforced China's trajectory toward technological independence, cyber resilience, and digital sovereignty, while simultaneously exposing it to increased global economic and cyber security uncertainties in an increasingly fragmented digital world order.

Impact on India's Digital Technology, Economy, and Border Security in the Context of Contemporary Hot War

The escalation of Iran–Israel–United States tensions and the broader expansion of cyber warfare have indirect but important implications for India's digital technology ecosystem, economic stability, and border security architecture. As a rapidly digitizing economy, India is increasingly exposed to global cyber risks, supply chain disruptions, and geopolitical volatility in the digital domain.

In terms of digital technology, India has experienced both opportunities and challenges. On one hand, global fragmentation of technology supply chains has encouraged multinational companies to diversify production, benefiting India's digital and semiconductor initiatives. On the other hand, heightened cyber conflict increases risks to India's expanding digital infrastructure, including banking systems, digital payment platforms (such as UPI), telecommunications networks, and government databases. India has therefore strengthened its cyber security framework through agencies like the Indian Computer Emergency Response Team (CERT-In) to mitigate cyber threats and improve resilience (CSIS, 2024).

Economically, global instability caused by cyber warfare and geopolitical tensions has contributed to volatility in energy prices, trade routes, and technology imports. India, as a major importer of energy and

ISSN 1019-6609
eISSN 1853-4961

technology components, faces indirect inflationary pressures and supply chain uncertainties. However, it also benefits from "China+1" diversification strategies, where global firms relocate digital and manufacturing operations to India, strengthening its IT and semiconductor ecosystem.

From a border security perspective, the normalization of cyber warfare and hybrid conflict has expanded India's security concerns beyond physical borders. India faces increasing cyber threats targeting critical infrastructure and defense systems, particularly in regions with geopolitical sensitivity. This has led to greater integration of cyber defense with traditional border security mechanisms, especially in coordination with military cyber commands and intelligence agencies.

Overall, the contemporary hot war environment highlights India's dual position as both a beneficiary of global digital restructuring and a vulnerable participant in emerging cyber conflicts, requiring continuous investment in cyber security, economic resilience, and integrated border defense systems.

Impact on Nepal's Digital Technology, Economy, Border Security, Black Economy, and Corruption in the Context of Contemporary Hot War

The ongoing Iran–Israel–United States tensions and the broader expansion of cyber warfare have indirect but important implications for Nepal, particularly in areas of digital technology, economic stability, border security, informal economy (black economy), and governance challenges such as corruption. As a small, open, and digitally emerging economy situated between India and China, Nepal is highly sensitive to global geopolitical and technological disruptions.

1. Impact on Digital Technology

- Nepal's growing digital systems (e-banking, mobile wallets, digital governance) face increased exposure to global cyber risks due to rising international cyber warfare trends.
- Developing countries with weaker cyber infrastructure are more vulnerable to spillover effects such as ransom ware, phishing, and data breaches.
- Limited cyber security capacity increases risks to financial and government digital platforms.
- Global cyber security assessments highlight that digital transformation without strong protection increases systemic vulnerability in developing economies (World Bank, 2023).

2. Impact on Economy

- Nepal is indirectly affected by global energy price fluctuations and supply chain disruptions caused by geopolitical tensions.
- Remittance-dependent economy faces risks if global financial and digital payment systems are disrupted.
- Inflationary pressures may increase due to imported fuel and goods price volatility.
- Foreign investment and tourism flows may become uncertain in a globally unstable digital-financial environment.

ISSN 1019-6609
eISSN 1853-4961

3. Impact on Border Security

- Increased global cyber warfare raises risks of cross-border cybercrime, smuggling networks, and digital fraud.
- Nepal's open borders with India and China make it vulnerable to transnational security challenges.
- Weak digital surveillance systems may limit effective monitoring of illegal cross-border activities.
- Hybrid threats combining physical smuggling and digital coordination are increasing globally.

4. Impact on Black Economy

- Expansion of digital financial systems creates both transparency and new cyber-enabled illegal activities.
- Weak monitoring systems may allow money laundering, online fraud, and illicit remittance channels.
- Cyber-enabled informal transactions can strengthen underground economic networks.
- Studies show digital transitions in developing countries can initially expand informal financial risks without strong regulation (UNODC, 2023).

5. Impact on Corruption

- Digital governance reduces some forms of traditional corruption but introduces new cyber-based corruption risks.
- Weak cyber-security systems can enable data manipulation, identity fraud, and digital bribery channels.
- Lack of institutional capacity may allow misuse of e-government platforms.
- Transparency International notes that digital systems require strong oversight to prevent corruption shifting from physical to digital forms (Transparency International, 2024).

Conclusion

The contemporary Iran–Israel–United States hot war represents a critical turning point in the evolution of global conflict, where digital technology has become both a strategic weapon and a vulnerable target. This study highlights that modern warfare is increasingly hybrid in nature, combining physical military operations with advanced cyber warfare, artificial intelligence systems, and digital information control. The analysis demonstrates that digital infrastructure—ranging from financial systems and communication networks to energy grids and cloud computing platforms—has become central to national security and global stability.

The findings reveal that the conflict has accelerated cyber insecurity across multiple states, including Iran, Israel, the United States, China, India, North Korea, and Nepal, each experiencing distinct but interconnected impacts on their digital ecosystems. While technologically advanced nations are

ISSN 1019-6609
eISSN 1853-4961

strengthening cyber defense and innovation, developing economies face heightened risks due to weak cyber-security frameworks and dependency on global digital systems.

Furthermore, the war has intensified economic uncertainty through disruptions in supply chains, energy markets, and digital financial systems, while also increasing the role of disinformation and cyber propaganda in shaping global perceptions.

Overall, this study concludes that the Iran–Israel–United States conflict marks a new era of digitalized warfare, where cyber-security, technological sovereignty, and digital resilience are essential for national survival. It emphasizes the urgent need for international cooperation, stronger cyber governance, and inclusive digital security frameworks to ensure global technological stability in an increasingly fragmented world order.

References

[1] Arshad, M. (2025). Cyber warfare and asymmetric power in Middle Eastern conflicts. *Journal of Strategic Studies and Security, 18*(2), 45–62.

[2] Center for Strategic and International Studies. (2024). *Demystifying Iranian cyber operations in the US–Iran conflict*. https://www.csis.org

[3] Center for Strategic and International Studies. (2024). *How cyber warfare will shape US–Israel–Iran conflict dynamics*. https://www.csis.org

[4] Center for Strategic and International Studies. (2024). *North Korea cyber threat assessment*. https://www.csis.org

[5] International Network for Strategic Studies. (2023). *Iranian cyber capabilities and regional security implications*. https://www.inss.org.il

[6] Sayegh, E. (2026, April 3). Cyber and kinetic warfare are now one battlefield: What the US–Israel–Iran conflict reveals. *Forbes*. https://www.forbes.com

[7] Pandit, J. K., Sahani, S. K., & Sahani, K. (2024). Study and analysis of some practical life uses and applications of exponential function. *Mikailalsys Journal of Advanced Engineering International*, 1(1), 43–56.

[8] Sah, K. K., Sahani, S. K., Sahani, K., & Sah, B. K. (2024). A study and examined of exponential function: A journey of its applications in real life. *Mikailalsys Journal of Advanced Engineering International*, 1(1), 23–32.

[9] Sahani, S. K., et al. (2026). Mechanical process control and statistical process control for reducing butter-oil defects in industrial production. *Reports in Mechanical Engineering*, 7(1), 169–184. https://doi.org/10.31181/rme575.

[10] Sahani, S. K., Oruganti, S. K., & Satishkumar, K. (2025). Advanced mathematical modeling of woolen knitting dynamics using Laplace transform and fourth-order Runge–Kutta method. *Journal of Mathematics*, 2025(1), Article 4985087. https://doi.org/10.1155/jom/4985087.

ISSN 1019-6609
eISSN 1853-4961

[11] Sahani, S.K. and Sah, D.K. (2023). Hybrid Analytical-Numerical Techniques for Machine Learning Optimization: Integrating Laplace Transform and Runge-Kutta Fourth-Order Methods. *Review of Contemporary Philosophy*, 22(1), 6854-6860. https://doi.org/10.52783/rcp.1165.

[12] Sahani, S.K. et al. (2022). A Comprehensive Study on Predicting Numerical Integration Errors using Machine Learning Approaches. *Letters in High Energy Physics*, 96-103. https://doi.org/10.52783/lhep.2022.1465.

[13] Sahani, S.K. Sah, B.K. (2024). Integrating Neural Networks with Numerical Methods for Solving Nonlinear Differential Equations. *Computer Fraud and Security*, 2024(1). https://doi.org/10.52710/cfs.703.

[14] Sahani, S.K. (2022). A Mathematical Framework for Incorporating Neural Networks into Root-Finding Algorithms. *Journal of Electrical Systems*, 18(1), 99-109.

[15] Sahani, S.K., Sah, B.K. (2024). An In-Depth Stability and Convergence Analysis of the Runge-Kutta 4th Order Method for Nonlinear Ordinary Differential Equations. *Panamerican Mathematical Journal*, 34(2), 300-308. https://doi.org/10.52783/pmj.v34.i2.5583.

[16] Sahani, S.K. (2023). Neural Network Surrogates for Weather Prediction Using Numerical Solutions of the Shallow Water Equations. *International Journal of Intelligent Systems and Applications in Engineering (IJISAE)*, 11(3S), 356-368. https://doi.org/10.52783/iwi.v44i1.99.

[17] Transparency International. (2024). *Digital governance and corruption risks in developing countries*. https://www.transparency.org

[18] United Nations Office on Drugs and Crime. (2023). *Cybercrime and illicit financial flows in the digital economy*. https://www.unodc.org

[19] United Nations Security Council. (2023). *Panel of Experts report on cyber-related sanctions violations*. https://www.un.org

[20] World Bank. (2023). *Cybersecurity and development: Risks and resilience in digital economies*. https://www.worldbank.org/en/topic/cybersecurity