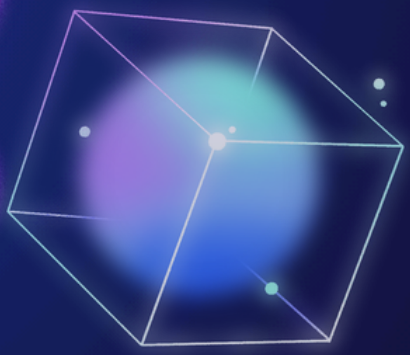
CYBER WORLD INSIGHT

INSIGHTS FROM OUR INTERNS

Cyber World Insight Magazine
Wired into Pakistan's Digital Future



FORTNIGHTLY DIGITAL EDITION
VOLUME 2 | ISSUE XII
JULY 16-31, 2026

CYBERAGE MAGAZINE

FORTNIGHTLY DIGITAL EDITION |
DOWNLOAD PDF AT
WWW.CYBERWORLDINSIGHT.COM/MAGAZINE

CENTER OF CYBER WORLD INSIGHT

Shaping Pakistan's Digital Tomorrow

Volume 2 | Issue XII | July 15-31, 2026

About

CyberWorldInsight is a policy and ideas magazine dedicated to exploring how technology is transforming Pakistan's society, economy, and governance. We bring together voices from academia, industry, and policy to debate the opportunities and risks of the digital age. Our mission is to inform, challenge, and shape the national conversation on Pakistan's technological future.

Publishing Information

Cyber World Insight (CWi) ©2023–2025
The CyberWorld Insight Pakistan
Office #401, Omega Heights, E/11-3,
Islamabad, Pakistan
🌐 Website: www.cyberworldinsight.com
📧 Email:
magazine@cyberworldinsight.com
📱 Phone/WhatsApp: +92 333 5221408

Digital Edition

This is the Fortnightly Digital Edition of Cyber World Insight Magazine.
📲 Available online at:
🌐 www.cyberworldinsight.com/magazine
📥 Downloadable in PDF format for offline reading.

CYBER WORLD INSIGHT

TABLE OF CONTENTS

Executive Editor's Note

As we navigate the complexities of the digital age, the intersection of technology, politics, and society has never been more critical. In this issue, we explore the multifaceted relationships between journalism, power, and the cyber economy, shedding light on the emerging threats and opportunities that shape our world.

Our contributors delve into the growing threat of cyberterrorism and cyberattacks, highlighting the need for robust cybersecurity measures to protect our critical infrastructure, including renewable energy systems. We also examine the profound impact of social media on political agendas and the reshaping of social norms, culture, and daily life in the digital society.

As AI continues to transform the labor market, we must consider the implications for our collective future. Through insightful analysis and thought-provoking commentary, this issue of CyberAge Magazine aims to inform, educate, and inspire our readers to engage with the pressing issues of our time.

Executive Editor, CyberAge Magazine

Jessica Avery

Editor's Note

The Cyber Age continues to redefine the terms on which power, security, and diplomacy are conducted. What once unfolded across borders and battlefields now unfolds, with equal consequence, across networks and code and for Pakistan, charting its own digital trajectory, understanding this shift carries real weight.

This issue of CyberAge Magazine brings together a range of such conversations from the evolving contours of cyber diplomacy, to artificial intelligence's expanding role in modern conflict, to its potential in addressing climate resilience. Each piece approaches its subject with the rigor it deserves, while keeping sight of the real-world stakes involved.

We remain grateful to the researchers and early-career scholars whose work fills these pages, and to our readers, who continue to engage with these questions seriously. We hope this issue informs, challenges, and adds meaningfully to the conversations shaping our digital future

Editor | Cyber Age Magazine

Aqsa Sajid

01

Compression of the Killing chain; Artificial Intelligence Model Modern phase during the Invasion

Author Intro

Maryam Saddique
M.Phil Scholar, Department of Defense and Strategic Studies, Quaid-e-Azam University, Islamabad.

The Iran war (2025-2026) has witnessed the remarkable shift from classical military approaches to plan and sustain strikes towards the use of Artificial Intelligence being utilized to compress the time between "See and Shoot", a process known as the "Killing the compression Chain". Premediative Human controlled processes are being converted into a high paced and a velocity chain of actions, where the major duties a BBC re assigned to algorithms and computers. Political, legal, and ethical oversight finds it difficult to keep up with this gradational speed up of AI. In addition to this, a syntactic restructuring of transformation in military planning and executio of strikes sing technologically advanced weapon against an adversary, is the modern debate

The arrival of technologically advanced weapons, including precision guided weapons, along with networked sensors) has impeller the classic kill chain. A definitive kill chain undergoes several steps from detecting, fixing, tracing, targeting, occupying and analyzing the adversary state, which demands exertion and time. But in the case of Iran, an innovative level of decision compression through the lens of Artificial Intelligence has been propelled. A guaranteed destruction is likely to be drawn when AI systematic channels, recast the targets, in a proritized manner and the pre computed strikes propose the weapons required. Signals intelligence

The AI targeting Load :From Gaza's Laboratories to Iranian Theater of War

Sattelite imagery, drones video and open source data were incorporated bythe US and Israeli AI system in 2026 strike ' opening phase into a continuous and upgraded sequence. The strike causing the killing of the Iranian Supreme Leader Ali Khamenei and the documented annihilation of nearly 900 Iranian targets, would have required several weeks the earlier was to accomplish. As per the reports, around 1250 targets involving the command centers, air defense radars, naval forces and ballistic missile launchers. The possibility of such substantial destruction became a reality because of the AI system's accurate planning and execution capabilities. Where there are human chains that are deliberate, their roles are more likely to get stuck between verification and confirmation of the already created system's proposals" Maneuver testing in Gaza and in U.S. theatre-level commands gave birth to the Iran war's AI targeting stack. It was not created from scratch. "Gospel" and "Lavender" are the AI systems of Israel used in Gaza to gather information and list them into targets. Using these systems, Israel assembled voluminous personal data, including their communications, links to, geo-locations and implemented AI models to assign them with the prospect of targeting

The role of those systems is outstretched from militants to administrative networks of IRGC (Islamic Revolutionary Guard Corps) Cyber Units, missile brigades and air defense crews to explore their connections. AI Systems then demonstrated communications and relationship patterns using graph-style models, hence the complex puzzle of military structures was efficiently solved much swifter than classical human approaches. The American AI tools were turned into an entire seat of war, tested by the 18th Airborne Corps. AI replaced 2000 people with only 20 human analysts in these tests while supporting the intelligence unit. The AI proposed model merged: communication metadata, electronic and radar signals, drone videos, and logistical knowledge, for example, ammunition and fuel sequence. An automatically generated target "tags" were introduced, through the continuous monitoring of night actions at missile bases and blastoff of launch vehicles. Each target tag was presented with military value multitudes, degree of certainty, projected peripheral harm, recommended weapons and objectives, all set to tumble into the fire suppression system.

Operational Outcomes and Novel Fragilities

AI-backed legal inspection serves as an essential but least reviewed layer. AI generated outlines are the summarized intelligence, which also involves a six law of war analysis ie;(LOAC) (The Law of Armed Conflict), delivered to the military lawyers. The proportionate probability of strike is calculated by the AI system by suggesting the target type(ie civilians or military). The final callconsistently offered by the authorities over the already AI-shaped illustration, depends on the availability of time and capacity to sustain hassle, for example, against mobile missile launchers.Reliance of authorities on AI systems is a possibility in a short time. The main operational payoffs of AI systems are speed and coordination. AI compressed kill chains permitted neat and orderly campaigns, including (suppression of air defenses, naval assaults, SEAD, leadership strikes against cyber and electronic attacks on persuasive communication) in the Iran War. AI helped to achieve these targets in surging waves. Iranian control and command structures were exploited, jammed, clogged and bombarded quicker than their revival.

But fresh fragilities come in modern waves, side by side. AI systems require and depend on constant high-volume data, turning into an equal target to deception or data tricking. To confuse AI models, Iran learnt its lessons through Gaza and Ukraine, and used bogus communication traffic, strictly controlled electronic signals, decoy missile launchers and synthetic signals and dummy radars.Secondly, technology turns a rare choice into easy and normal targets, causing an uncontrolled escalation. AI models prioritize the most essential and critical targets such as political leaders, strategic missile bases, control and command centers and sensitive nuclear facilities. Ali Khamenei's striking demise is an example of AI early detection of essential targets, which compels military planners to strike in the early hours of war. The AI models present such targets as "no-brainers," and the conflict turns out to be an irrevocably heightened event

The computerization of Risk Threshold and the Civilian Harm

A liable political response is absent and raises tough questions over AI-motivated targeted casualties of civilians. Lavender, along with its systematic models, revealed the capacity of the anticipated death toll of civilians in strikes in Gaza. Military commanders relied upon AI-model proposed levels under the AI-estimated numbers. In the case of Iran, a similar pattern was used with more rigorous limitations where artificially produced numbers by s has two profound ramifications,

First, killings become easier to approve when AI models transform sophisticated moral questions into color-marked threat levels and numbers, for example, "(Target worth: high, Anticipated Death Toll: 20-35 persons, Regulatory Risk: low>blue)". These kinds of coded displays make it easier for politicians to step in for escalatory decisions without accountability for civilian harm.[17]

Second, the political accountability and responsibility become blurred, a single mistake can deceive AI, and a complete chain turn into a vulnerable devastation, starting from (Military personnel> Commander> Military lawyer> Engineers> to Government). Who shall be held answerable over the hazy line between traditional law expectations over human response and AI-compressed killing chains

The Iran war serves as a learning lesson to other states.becomes appealing for Middle Eastern powers in order to utilize it as an amplifier. AI can perform the job of 50000 people with the replacement of 50 people. Instead of stockpiling of aircrafts, jets, planes, missiles, or tanks, authorities can invest in AI Algorithms.[19]

Secondly, in the future, adversary states will aim to corrupt or disrupt AI systems themselves instead of intercepting or shooting down jets, planes, and missiles. The chief target shall shift from traditional assets towards the kill chain. For that, altering or stealing machine learning models, blocking the systems, seizing the cloud and communication networks and corrupting the data, will be the preceding steps.[20]

Thirdly, non-preparation of concurrent international rules and regulations regarding arms control is the concerned dilemma. Most treaties and laws are man-made, with pocket-sized or no room for discussing the role of highly progressed AI algorithms in warfare.[21]

They stay ignorant about;

1. The limitation regarding the participation of AI tools in selecting targets.
2. Where should be the real human control implied in case of uncontrolled and swift warfare?
3. Processes concerning the check and balance of corporate-retained warfare technology
4. How AI-proposed verdicts can be recorded to advance future investigations.
5. AI-endorsed patterns of escalation should be unmistakably distinguished.[22]

Pressure for new rules will likely be more in the future because of the similar use of AI system in the Iranian war, Ukraine and Gaza as,

1. (a).The ability of human-control in the Kill Chain to say ‘STOP’ undoubtedly.
2. Neutralization of specific targets must be banned completely.
3. Human-settled and AI-endorsed patterns of escalation should be unmistakably distinguished.

Conclusion.

Iran war, , thus, for states serves as a learning realization which comes with a propelling warning to rethink modern AI advancements. On one side, AI-motivated escalation has successfully transitioned the regional conflict into hastened and more turbulent phenomena. On the other side, this high advancement of AI can risk the accelerated technological dependency of a state to rely on AI systematic models. Defensive and balancing use of AI models is the crucial field to be explored where early warning systems must be improved, battle devastation analysis must be turned with greater accuracy, and firmly managed fires without slipping into a prototype where political supervision and ethical self-control can’t function in the overly accelerated and automated war.

02

Network-Centric Warfare and Pakistan

Author Intro

M. Talha Zubair

An Alumnus of Quaid -i- Azam university, who's a researcher and a poet ; working to bridge the realms of military , computing, and morality through strategic analysis.

Understanding the Term: Digital Blip Rewriting Battlefield

Today, we live in a world where a single command can compress decades of intellectual labor into a fraction of a second. A digital blip, and in exactly thirty seconds or so, one can access, understand, and imply concepts that once took years to master. This radical compression of time and information has fundamentally rewritten the rules of modern warfare; sheer speed and availability of information have become the ultimate weapon, fundamentally changing how militaries fight.

This exact compression of time and data has reshaped the calculus of war and brought us a new doctrine/mechanism that aims to enhance combat power through the use of information technology and computer networking, known as Network Centric Warfare.

It is defined as "A military doctrinal concept that uses communication technology to enhance/upgrade the battlefield awareness, coordination, and effectiveness of the military operation/campaign." It creates a thread of awareness from sensors detecting threats to military decision-makers and the fighting soldiers on the battlefield.

The United States of America used this technique in Operation Enduring Freedom in Afghanistan, where the war was against terrorism, and the aim was to target Al-Qaeda and the Taliban. The USA used different network-centric techniques, such as satellite imaging of Al-Qaeda camps.

Key elements of network-centric warfare

The true power of Network-Centric Warfare lies in its ability to fuse sensors, commanders, and shooters into a single, real-time nervous system. At its core, the effectiveness relies on seamless battlefield information sharing and a decentralized command and control (C2) system, architectured in such a way that initiates unprecedented battlespace awareness by linking remote sensors, strategic decision-makers, and frontline shooters; connecting entities across the operational theater and ensuring a higher probability of successful strikes because shared intelligence dramatically accelerates decision-making and multiplies force lethality. Instead of relying on the casualty-heavy massing of troops, connected units can “self-synchronize” to execute precise, undetected strikes from safe standoff distances, forming an interconnected web that accelerates the speed of command and the overall tempo of military campaigns. All this synchronized harmony ultimately guarantees greater operational survivability by trading physical mass for information superiority, allowing forces to ensure maximum lethality, dominant operational tempo, and overall a safe strike without being detected.

Origin and future of NCW; The Digital Genesis: Tracing the Origins of Network-Centric Warfare

Warfare reflects the age it belongs to; as times change, military tools naturally evolve to outpace and neutralize new adversaries. The NCW was a myth in the past, with the development of technology in the early 2000s, when the USA’s computers were attacked in 2003, namely by Titan Rain it was a APT Likewise in 2007 a cyber attack struck Estonia which is also known as Estonian denial of services, and the cyber-attack on the Iranian nuclear program served as the spark that ignited a whole new era of digital warfare.

The origin of NCW is rooted in this series of digital warfare. With fundamental changes in society, business, and technology. The development in these areas has increased competition, and so a new era of warfare has turned into a reality, and now, as time flies by, it will become more lethal. Technology has developed further with the advent of artificial intelligence and information technology; with all these powers, combined with the intellect and capability of the modern human brain, humans can even come up with more genres of warfare, which may be very similar to NCW or even overlap with it.

In the book "Network-Centric Warfare: Its Origin and Future", Vice Admiral Arthur K. Cebrowski and John J. Garstka explain that the idea of NCW is based upon tools and tactics of warfare that have evolved with military technologies, and now, fundamental changes are affecting the very character of war. The paradigm shift from platform-centric warfare to network-centric warfare is the most important and significant revolution in military affairs (RMA) in the past decades, and now it is up to the states to utilize this technology-centric warfare approach. Either for the betterment of the world or being lustful for power and resources, they may use all these technologies against humanity.

Caption:

A visual representation of the Network-Centric Warfare operational architecture, highlighting the continuous integration of the Sensor Grid, Command and Control (C2) Grid, and Shooter Grid across the land, air, sea, and space domains.

Strategic Impacts of NCW

The fundamental impact of Network-Centric Warfare lies in its sweeping overhaul of modern operational architecture because its principles are borrowed heavily from the rapid evolution of global business models and economic networks to force a reevaluation of the broader geopolitical landscape. In this highly interconnected era, non-state actors can no longer be viewed as isolated, independent anomalies; Instead, they must be recognized as active participants within a simultaneously adapting, global ecosystem.

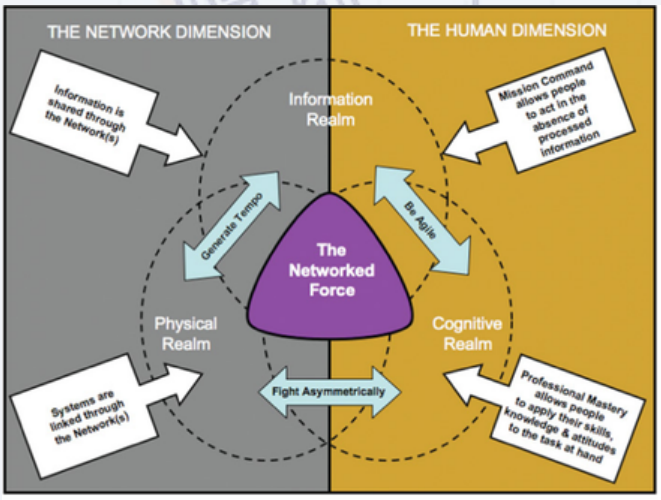
To survive in this volatile political environment, states are to make agile strategic choices, recognizing that modern conflicts are fought not just on physical battlefields, but across complex, integrated networks, and so States are no longer needed just to update their physical arsenals; they are to execute strategic shifts in their military objectives and operational methods. Foundational theorist Vice Admiral Arthur K. Cebrowski outlined that this era is defined by a decisive shift from platform-centric capabilities, which measured power by individual tanks, ships, or aircraft, to network-centric integration, which depends more on information intelligence and swift attacks. This paradigm shift represents a true Revolution in Military Affairs (RMA). At the tactical level, this transformation is driven by commercial information technology that yields unprecedented battlespace awareness. Military top brass can now observe, evaluate, and execute real-time decisions faster than the adversary can react. Besides mere tactical superiority, this networked approach is heavily favored because it is economically preferable, replacing the sheer physical mass of traditional armies with precision data, interconnected sensors, and shared intelligence. Modern militaries can project power and achieve strategic goals with leaner, highly cost-effective forces

.

Economic viability:

Modern Network-Centric Warfare (NCW) systems offer a highly cost-effective and overwhelmingly lethal alternative to Traditional military operations, which inherently suffer from massive financial and operational overhead. Hiked costs are primarily driven by an over-reliance on redundant manpower, rigid and time-consuming weapon deployment cycles, and critical delays in manual threat evaluation and weapon assignments.

By seamlessly fusing human cognition and advanced automated technology, NCW generates superior situational awareness and accelerates the speed of command and control (C2); where this interoperability makes way for precise, real-time coordination among decentralized military units. Ultimately, trading some physical mass for information superiority and significantly reducing the financial burden, frontline casualties, and the exorbitant costs associated with re-planning of operations if needed.



Caption:

A conceptual framework detailing the intersection of the Network Dimension (physical and information realms) and the Human Dimension (cognitive realm), which is required to generate an agile, self-synchronizing military force.

A paradigm shift in warfare: From Stones to cyberspace

In the past years, warfare has evolved and developed; humans have covered a long distance, from fighting with stones and rocks to swords and arrows, and then to muskets, rifles, and finally modern killing machines such as auto/ semi-auto guns, tanks, missiles, modern

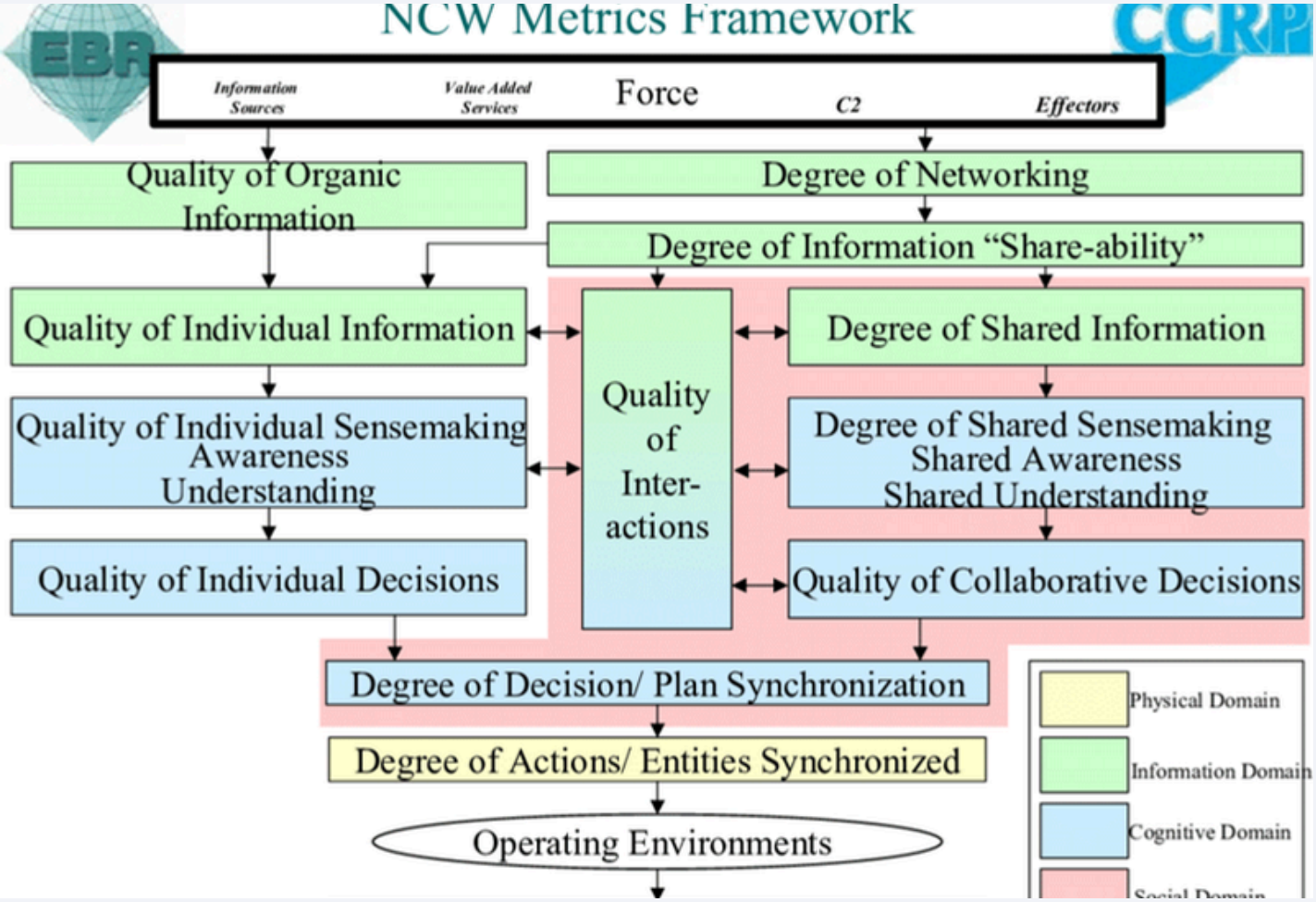
frigates, destroyers, and aircraft carriers. Indulging all three areas, Earth, Water, and Air, and even now, moving to outer space and weaponizing other celestial bodies.

Network-centric warfare is more than just a technology; it is an advancement in how wars are fought; an upgradation of warfare, which will ultimately develop in the future, even making nuclear weapons more destructive and obnoxious. NCW is an organizational innovation to make way ahead of adversaries and deter other states. It is the beginning of a period of paradigm shift from traditional warfare to pushing military decision or strategy making out to the edge of the battlefield. The shift is characterized by focus on speed, information flow, and shared awareness among entities in the battlespace, resulting in more effective and efficient decision-making and successful execution of military operations.

Network-centric warfare is delivering powerful dynamics at the strategic level, and the advent of NCW strategies and methodologies of warfare has changed. In the past, one needed a regiment, a company, a traditional tactic to confront the enemy; however, in the current scenarios, a state only needs malicious software, malware to disrupt the functioning of the enemy's statecraft. Elements of battlespace and the realm of decision making are changed, where both play a crucial role in NCW,

Metrics Framework:

A structured framework system designed to measure the effectiveness and performance of the technique's concepts and technologies. It involves defining specific metrics by assessing various elements of NCW, for say Battlespace awareness, Battlespace knowledge and Military utility.



Caption:
The structured Metrics Framework system is designed to measure the effectiveness and interoperability of forces across the physical, information, cognitive, and social domains.

This ultimately aims to provide a quantitative hypothesis regarding investment strategies and other complexities. Metrics within this framework cover aspects like speed of command, force agility, shared situational awareness, and interoperability.

All these aspects are aimed at evaluating the network-centric capabilities of the force, and so the metrics framework is crucial for understanding and optimizing the benefits of NCW in military operations and military campaigns.

Pakistan on the Roads of Network Centric Warfare:

The doctrinal developments and evolving dynamics of South Asia, particularly India's investments and developments in technology and network-centric warfare, carry implications for Pakistan. Indian Military's heterogeneous nature, demonstrated quite vividly in the recent May 2025 skirmishes, where many **"firsts"** were characterised, namely 1). use of ballistic and cruise missiles by both sides; India being the first. 2). use of armed UAVs. It was not merely an attack rather an arrogant and over confident India trying to set a new normal in the domain of South-Asian Warfare. Pakistan following its Quid-pro-Quo-Plus strategy, vigorously responded to the unprovoked Indian aggression through air and ground retaliation; in fact, it was the 'pinnacle' of Pakistan's military retaliation.

However, maintaining this level of deterrence in the future dictates and demands that Pakistan must urgently accelerate the development of indigenous NCW tools and techniques.

Increasing the efficiency in NCW is not a singular milestone; it is a complex combination of intelligence gathering, communication, and situational awareness for timely decision-making. Pakistan must navigate through challenges, such as;

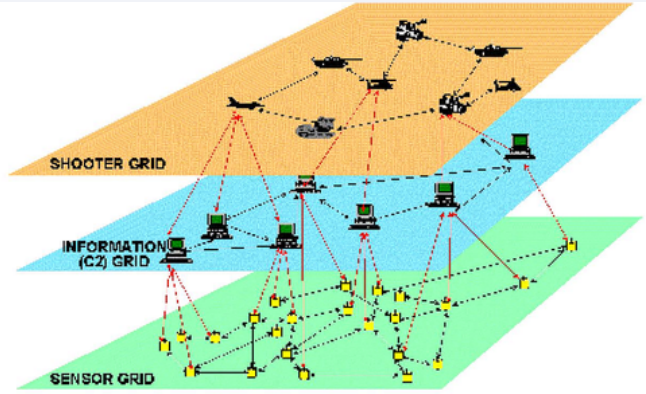
- Costly arms race.
- Conventional imbalance.
- Lagging in the field of technology/ technology deficit.

Addressing these challenges is the only viable way to rapidly develop NCW. Merely inaugurating technology parks does not equate to genuine network warfare readiness.

As "execution outweighs rhetoric", the operational reality remains that when genuine threats materialize, the defense network neutralizes them in time. Pakistan's continued, quiet mastery of this domain remains its most effective, proven deterrent against the immediate and evolving threat from India.

Analysis and Conclusions:

In the name of technological developments, we are not only focusing on infrastructure but also on the actual defense systems, which are coming in handy when the need arises! Though there is still space for improvement, Pakistan does not lag at the very back in the field of NCW. For instance, developing a mechanism that may look something like the image below;



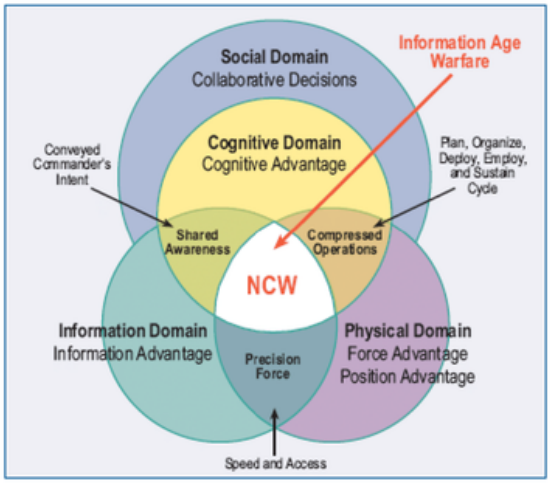
Caption:

The fundamental topology of a network-centric battlefield, demonstrating how raw data flows horizontally from the Sensor Grid to the Information (C2) Grid, before transmitting execution commands to the connected Shooter Grid

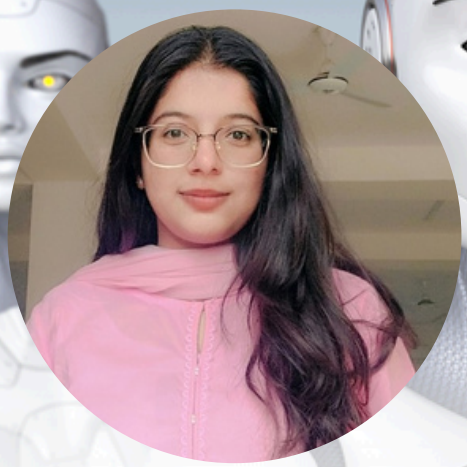
Today wars highly depend upon reconnaissance and intelligence information which we term as information superiority, that plays a crucial role in the NCW or any other warfare technique as the maneuvers are to be taken by keeping in view the intelligence reports, they serve as a light for the soldiers to move ahead, by the development of NCW Pakistan can overcome any intelligence relating problem, yet we own the world's best intelligence system we should still develop in technology and modern warfare techniques rather the very old school ones.

Demands of commercialization and business people playing the role of non-state actors in statecraft are the reasons for major advances in Information and Technology, which are now imperative for any state's survival. Globalization not only impacts Pakistan but also impacts warfare. "It is not about the network only, it is about how we develop the network". **It is more like an art of Networking!** To reach its full potential and limits, Network Centric Warfare should be deeply rooted in the operational systems of the state and military. It will be a steady simultaneous process for a state like Pakistan to fully empower the art of NCW, We cannot achieve it overnight, but with consistency and sincerity towards the techniques, we can secure a better and more efficient system , leading us to be in a better position if any network- centric war occurs with our immediate threats in the future.

To conclude, "Warfare in the Information Age will inevitably show some unique characteristics that will distinguish NCW from the previous ages," affecting the capabilities and warfare techniques that are brought to battle, battlespace and battle time management, balancing all these ensures a successful operation and achievement of the objectives.



Caption:
The interacting domains of Information Age Warfare demonstrate how the synthesis of an information advantage, cognitive advantage, and collaborative social decisions generates a highly lethal precision force.



03

DIGITAL ARMIES: INSIDE THE NEXT CYBER FRONT OF NATION-STATE WARFARE

Author Bio

Zarmeen Imran

She is a recent graduate of Kinnaird College for Women, Lahore, where she completed her Bachelor's degree in International relation. Her research and writing focus on contemporary global affairs, migration governance, regional security dynamics and international relations.

Introduction:

Cyberspace has become a major player in international security and a new era of conflict in cyberspace has emerged in the 21st century. Modern warfare is played in code, algorithms, malware and data breaches, unlike conventional warfare, which is played with weapons and infantry. Cyberwars are developing in the world where states can wage covert, but potentially devastating operations to disrupt critical infrastructure, compromise government systems and undermine entire economies (RAND Corporation, 2025). Digital hostilities are a type of fighting in which the belligerents assert their power without entering a country's borders, making it difficult to differentiate between peace and conflict.

Cyber warfare provides states with the strategic benefit of operating in anonymity, deniability and scalability when carrying out espionage, sabotage and disruption. In Russia, for instance there have been recent incursions into European power grids, while in China there have been cyber espionage operations targeting Taiwan and persistent conflicts between Israeli and Iranian forces in cyberspace (Financial Times, 2025; CSIS, 2025; Financial Times, 2025). This is made more complicated by the presence of non-state actors and hacktivists who also want to achieve their . goals These changes pose important questions

- What are the states doing to integrate into their warfare cyber operations? What technologies and tactics are they using?

- What does this changing battle space imply for the future of global security in a world that relies on and is becoming more vulnerable because of digital networks for critical systems and societies?

The Emergence of Cyber Warfare Nation-State:

The development of nation-state cyber warfare is one of the biggest changes in worldwide security in the last 20 years. While some early hackers were driven by personal finance or fame, the most impactful digital operations are modernly conducted by state actors that want to gain economic, political and military benefits (RAND Corporation, 2025). Cyber capabilities allow states to avoid the traditional battlefield, and to attack adversaries regardless of their line of business power generation, finance, communications infrastructure etc. The United States, for example, has created US Cyber Command to cultivate offensive and defensive digital capabilities, and cyber superiority is as vital as dominance in air, land or sea (War on the Rocks, 2025). Russia on the other hand uses cyber weapons for espionage, election manipulation, and infrastructure sabotage in Europe and North America China is focused on large scale IP theft and cyber espionage to gain faster economic and technological growth.

EXISTING CYBERSPACE COMBAT VENUES

a**. Israel vs. Iran: The Same Cyber War:**
Israel and Iran have been at war in the digital realm since the 12-day kinetic war. Before the physical confrontation, Israeli cyber espionage allegedly helped to sabotage Iranian air defense systems and aid with the high value intelligence operations. In response Iran launched a hack-and-leak attack on Israeli supply chain companies. At the same time, pro-Israeli hackers are said to have stolen $90 million from Iranian financial systems, and temporarily disrupted the operation of a banking data center (Financial Times 2025).

b. In Norway, the Dam Breach of Russia:
Hackers connected to the Russian government recently accessed the control system of a Norwegian dam and temporarily opened it up in April 2025. The physical damage was relatively insignificant, but it highlighted important weaknesses in European infrastructure. In fact, they found that the problem was a weak password, a reminder that hacking can sometimes be done with simple, not sophisticated, means (The Times, 2025).

c**. Chinese Cyber Theft of Intellectual** Property vs. Taiwan/ Europe:
The number of cyber attacks launched against Taiwan's government and telecommunications networks has increased by over 200%, from 1.1 million to 2.4 million per day, in an effort to steal data and disrupt operations carried out by Chinese cyber groups (CSIS, 2025). APT31 is a group linked to China's Ministry of State Security that targeted the Czech Republic in Europe. In a public statement, the Czech president has stated that the Chinese cyber threat is as great as it is from Russia (Financial Times, 2025)

d. Hybrid War in Europe by Russia:
Russia has, since the invasion of Ukraine in 2022, engaged in a hidden and unacknowledged warfare known as a shadow war involving cyber warfare, disinformation, and sabotage in most European nations. Those cases of Russian hybrid warfare increased by six times between 2022 and 2024, directed at internal unity of action and eroding the position to support Ukraine.

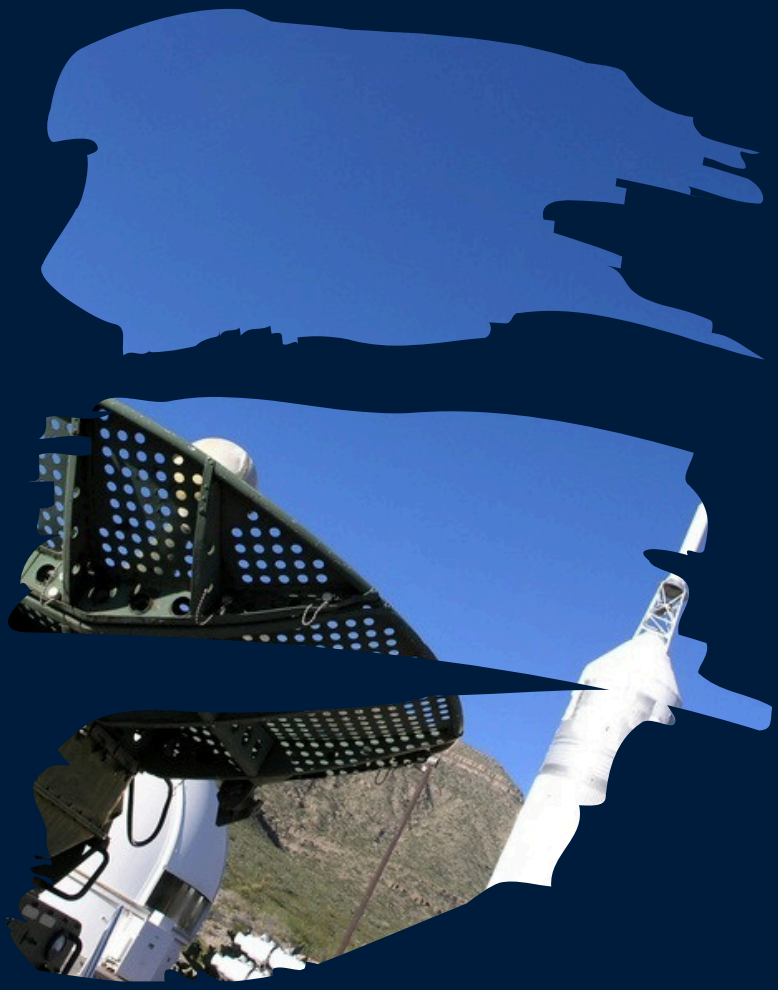
e. Cyber Threat Iran Produces to Allies:
After a series of military operations by the United States, the Australian government and other allies have cautioned against expected increases in Iranian-backed cyberattacks. Iranian bad guys have been using brute-force, bypassing multi-factor authentication and other means of intrusion to access allied networks. The risks are further compounded by the use of proxy actors, which would allow for plausible deniability and expand Iran's cyber reach (The Australian, 2025).

National Cyber Defense Stands

A**.United Kingdom: Cyber EM Command & National Cyber Force:**
The Strategic Defence Review in the UK has created a new Cyber and Electromagnetic (Cyber EM) Command, which is set to be established in 2025 with a £1bn budget. It's a single point that brings together the military, civilian, and private sector expertise, and incorporates the newest technologies in the field of artificial intelligence and quantum technology. The National Cyber Force (NCF), a joint unit of the Ministry of Defence and GCHQ for offensive cyber operations, is also active in the UK (IT Pro, 2025).

B. India: Defence Cyber Agency (DCyA)
In early 2021, India formed its tri-service Defence Cyber Agency to coordinate cyber defence between the Army, Navy and Air Force. But experts in the field seem to have identified the lack of skills and infrastructure to tackle the threats being faced by India, especially with the looming tension between India and China and Pakistan

C. NATO
The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia provides member states with research, training and intelligence. The IMPACT alliance, a UN-affiliated alliance of 152 Member States, and the world's largest cybersecurity partnership,



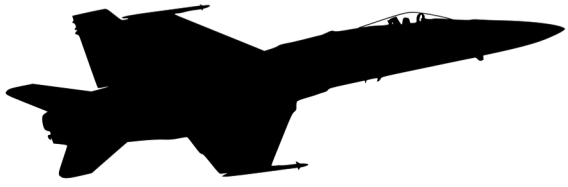
The U.S. and its partners are also rolling out artificial intelligence and methods to create digital replicas of critical infrastructure systems, which can simulate potential attacks and countermeasures before they happen (War on the Rocks, 2025). China is also a major proponent of using AI-generated disinformation, such as deepfakes and synthetic media, to manipulate political processes, including in Taiwan . A parallel development is the growth of so-called “turnkey” hacking tools pre-packaged offensive capabilities which enable less technically advanced actors to carry out meaningful cyberattacks with little technical expertise. Ransomware tools that were originally designed to attack US and allied infrastructure have shown that they can be adapted in various ways to support state goals. There's a troubling ambiguity with these technologies: An AI-powered attack can be carried out quickly, with a high level of deniability, and it's increasingly hard to attribute the attack as well (and hence, deter it). AI has broadened the arsenal of both state and non-state actors, but it has also added to the uncertainty of modern cyber warfare (Axios, 2025; RAND Corporation, 2025).

D. The policy and institutional initiatives in the United States.

In June 2025, the US released an Executive Order that demanded enhancements to various areas of software supply chain security, quantum-resistant cryptography, AI vulnerability management, patch management practices, and security framework modernization (The White House, 2025). In parallel, the CISA International Strategic Plan (2025-2026) is focused on enhancing the security of the domestic infrastructure and building joint cyber defence with international partners (CISA, 2025).

Advancements and the challenges in the field of innovation with AI and Offensive Technology.

AI is changing the nature of cyber conflict and creating new types of security threats in the process.AI is revolutionizing the way states engage in cyber conflict and is introducing new forms of security threats. AI systems can search for vulnerabilities in seconds, create complex malware and automate attacks that would have been impossible to execute manually before (Axios, 2025). Russian actors have reportedly tried AI-powered phishing attacks that are reportedly able to evolve



04

Artificial Intelligence and the Future of Climate Resilience”

Author Bio

Fatima Batool
An internt working in Content Writers Section at CCWI. She is undergrad Student at Kinnarid College for Women University, Lahore. Her area of interest is geopolitics, diplomacy and histroy.

Abstract;
Natural disasters have been on the rise and have been severe with climate change posing a threat to human security, infrastructure, and economic stability. Conventional systems of climate monitoring tend to have difficulties when it comes to handling bulk and intricate environmental data to provide sufficient timely response and decision-making. The concept of Artificial Intelligence (AI) has become an effective climate control and disaster prediction tool through the ability to analyze data in real-time, detect patterns, and make predictions. The paper will explain how AI is used in climate monitoring and early warning, discuss the use of AI in disaster prediction, and address the issues of data quality, governance, and equity. It contends that with the assistance of inclusive policies and institutional capacity, AI-based systems can contribute to disaster preparedness to a substantial extent.

Introduction
Climate change is increasing disasters related to climate, including floods, drought, cyclones, heatwave and wild fires. The Global South is especially exposed to the impacts of extreme weather, which is especially prevalent in vulnerable areas.
Human security and sustainable development therefore require effective monitoring of climate and disaster prediction.
The traditional climate surveillance is based on historical data, observations, and slow models of forecasting. Conversely, Artificial Intelligence allows processing vast quantities of satellite, sensor, and climate model data in a short period of time. AI helps to predict disasters more accurately and responds sooner because it creates complex environmental patterns.

The Role of AI in Climate Monitoring
Climate monitoring can be enhanced with the help of Artificial Intelligence that can process landscapes of environmental data which can be hard to handle manually. The machine learning methods can be used to analyze satellite images, ocean temperature data, atmospheric patterns, and land-use changes and identify the initial signs of climate variability.
AI usage at remote sensing enables the monitoring of glaciers, forests, coastlines, and weather systems in real-time.

The AI-powered models have the potential to detect trends of deforestation, increase in the sea level, or unusual shifts in the temperatures in real-time and assist policymakers in developing specific climate mitigation policies. Also, AI can improve climate modelling by providing better simulation accuracy and less uncertainty in the long-term climate predictions.
Amine dangerous areas.

AI IN DISASTER PREDICTION AND EARLY WARNING SYSTEMS

AI in Disaster Prediction and Early Warning Systems

AI can also be incredibly important in disaster prediction because it is able to analyze historical and real-time environmental data to predict the likelihood and severity of extreme events. AI models in flood forecasting are utilized to produce early warning signals using rainfall, river flow, soil moisture, and terrain data. In the case of wildfires, AI systems will be used to check the dryness of vegetation, temperature, and wind speed to determine dangerous areas.

Cyclone tracking and prediction of intensity, which are enhanced by AI, are also useful in evacuation planning and emergency preparedness. Even though the process of predicting earthquakes is still a technical issue, AI has demonstrated the ability to identify seismic signal patterns and the occurrence of early tremors. The events show that AI can shorten the response time and enhance disaster management measures.

Case Applications and Global Examples

A number of international programs also indicate the increase in the application of AI in disaster management. Meteorological and space organizations use AI to analyze satellite information to monitor the weather constantly. Intense floods have been monitored by installing AI-based systems on the river basin areas to notify the locals ahead of the floods.

The AI-powered drone imagery utilized by humanitarian bodies is used to map the damages of a disaster and quickly assess the damage. Mobile-based AI warning systems have increased delivery of communication with remote and vulnerable populations in developing countries. These applications point out how AI can be used to enhance coordination, accuracy, and efficiency of responding to emergencies.

AI and Weather Perdictions

"Embrace the future of AI and cybersecurity, innovate boldly, and let your impact resonate in every corner of the digital world."

Challenges and Limitations

Although AI-based climate monitoring has its merits, it has a number of challenges. The availability and quality of data are also of significant issues; in particular, in the developing world, climate data are either dispersed or no longer current. Machine learning models which are trained on biased or unrepresentative data might produce incorrect forecasts.The digital gap between developed and developing nations restricts the equal access to AI technology. The high implementation costs and infrastructure demands also limit the large scale adoption in the resource restricted regions. Strong governing aspects are needed in issues of ethical concern like privacy of data, transparency and accountability. Over-reliance on automated systems without human oversight can lead to more risks in operations during the emergencies.

Future Outlook and Policy Relevance

AI will continue to have a larger role to play in climate governance and disaster risk reduction. Resilience can be increased by applying AI in national climate plans, disaster management systems and urban planning. The governments are supposed to invest in climate data infrastructure, training efforts, and cooperation at the international level.The partnerships between the government and the companies can serve to close the financial and technological gaps, whereas the international organizations can facilitate the transfer of technology to the disadvantaged areas. It is also necessary to develop ethical and regulatory frameworks in order to be responsible about AI deployment. The implementation of AI must not be a substitute of human decision-making processes during disaster response operations.

05

The Algorithmic Blade: Israel's Cyber-Intelligence Enabled Decapitation Strategy

Author Bio

Aqsa Sajid is an M.Phil Scholar and her research interest lies in Defence Studies, South Asia, and International Law

Introduction

The nature of modern warfare is experiencing a fundamental change, moving away from the attrition-focused models of warfare characteristic of the industrial era towards precision warfare integrated with cutting-edge technology. With states today adopting cyber and artificial intelligence technologies as key weapons in their arsenals to implement a force multiplier approach, it can be argued that decapitation warfare, the centuries-old practice of taking out enemy leaders in order to disrupt the command and control structure, is enjoying a resurgence in the twenty-first century

This paper examines the application of the "cyberintel enabled decapitationby Israel against both state and non-state adversaries from 2024 onwards. Although decapitation warfare has long been a practice associated with counterterrorism operations, its revival and technologically advanced nature require further scholarly attention. It marks the move of the state into an "advanced cyber age" characterized by the use of information dissemination and digital intelligence for coercive purposes. Three distinct methods will be employed in this research: a quantitative historical analysis of the longstanding decapitation doctrine of Israel; an assessment of recent case studies of Hamas, Hezbollah, and Iranian decapitation efforts; and a quantitative discourse analysis of Israel's X reports on these cases.

Decapitation Strategy: A conceptual History

A fundamental shift in the nature of the modern conflict is taking place from the conventional, attritional styles of warfare typical of the industrial era to one characterized by readiness and technological sophistication. The modern state has become proficient at using cyberspace and artificial intelligence (AI) in combat to revitalize the ancient strategy of decapitation, or the strategic elimination of an opponent's leadership.

"Striking the head of the snake" involves the decapitation, or elimination of the leadership of an institution. As British military theorist J.F.C Fuller stated, the objective was to destroy the adversary's command system by striking at the brain and rendering the body incapable of functioning. This is supported by John Warden's "Five Rings" theory, which holds that destruction of the inner ring, consisting of the leadership, is the key strategic to point; the one that offers the best results with the least collateral damage.

Nevertheless academic opinion about the viability of decapitation is sharply divided. Although supporters such as Bryan C. Price said that this technique may be quite effective against value-based and charismatic organizations, opponents like Jenna Jordan claim that the approach is likely to fail when applied to bureaucratic organizations with solid succession policies. With the advent of modern times and development in cyber technology and AI, the use of this approach has become even more possible and has also changed the entire risk versus reward equation associates ted with the choice of the target and engagement process. Josh Luckenbaugh, and C.J. Moses are among the researchers analyzing this trend.

Israeli History of Decapitation and AI Integration

Israel's decapitation strategy has been deeply embedded in its historical threat perception since its establishment in 1948, operating under an "official state of emergency" most of the time. As pointed out by Nachman Ben-Yehuda, political assassinations have been used by Jewish paramilitary organizations, such as Haganah, Lehi, and Irgun, during the British Mandate era, and this has become institutionalized in the Israeli intelligence and defense services.

Historically, this strategy involved the assassination of Palestinian militant figures, for example, those executed in the 1956 campaign against Palestinian resistance fedayeen leaders or the killing of Palestinian militant leader and secretary of the PLO in Tunis, Khalil el-Wazir, in 1988. In the 1990s, there was a move toward the institutionalization of mista'arvim (special undercover units), used to carry out targeted killings against key individuals, including Fathi Shikaki Yahya Ayyash. Nevertheless, in the post-2024 era, we can witness a revolution; the Israeli decapitation strategy has moved from the use of traditional kinetic tactics to the Cyber-Intel Enabled Decapitation Strategy, using information provided by CCTV cameras, mobile and signal stations to identify key target figures.

Analysis of Twitter Discourse

The tendency towards decapitation in Israel's approach stems from its long history of perceived threats to its security. Since its founding in 1948, Israel has often been operating under a declared "official state of emergency." According to Nachman Ben-Yehuda, political assassinations have been carried out by Jewish paramilitary organizations, including the Haganah, Lehi, and Irgun during the British Mandate,

To explore the manner in which advanced operations are articulated, we undertook a quantitative discourse analysis of confirmed Israeli social media accounts using Python in order to facilitate data visualization.

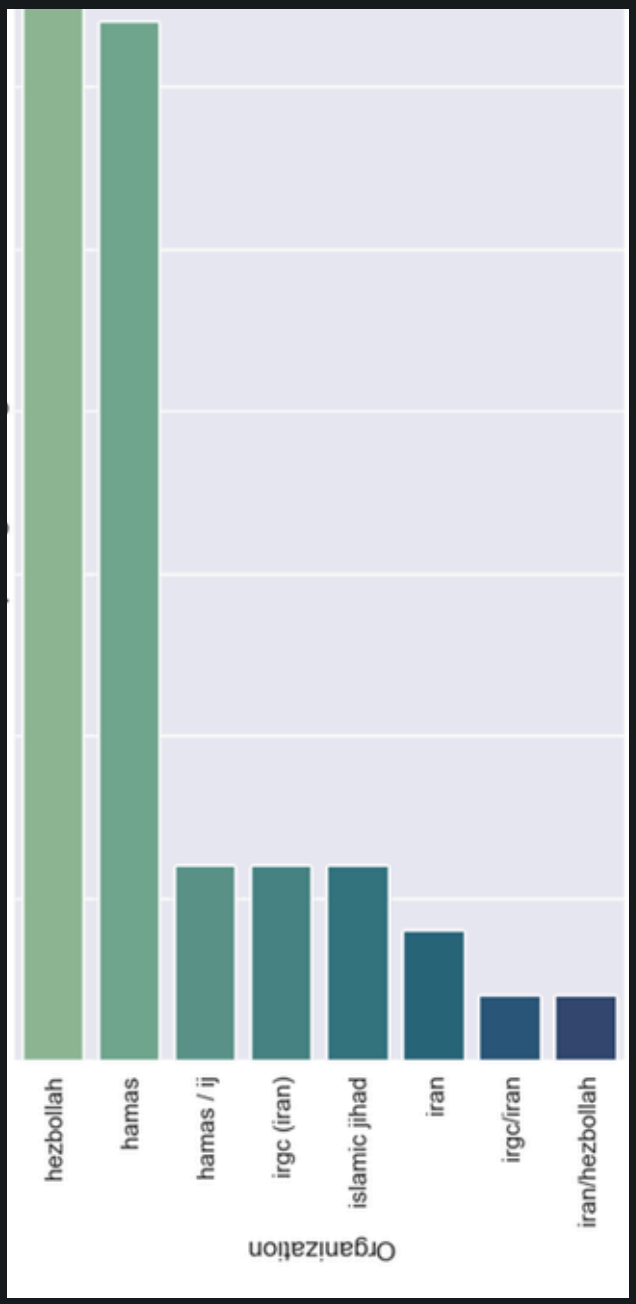
Frequency of Intelligence

Discussion

In our analysis, we uncovered a distinctive trend in the frequency of discussions related to intelligence. The discourse is marked by significant variations that reflect operational dynamics and appear to indicate a reactive communications strategy rather than a stable oneThe frequency data reveal a clear hierarchy of organizations targeted. These include Hezbollah and Hamas, demonstrating that this particular operation reflects the strategic importance of these two organizations within the context of the conflict at hand General" Intelligence Discussion vs. "Cyber"/"AI" Mention

It emerges from this discourse analysis of Israeli state communication that there is an intentional distinction made between the language of "intelligence" and the technology behind the "cyber" and/or "AI-enabled" process. While terminology related to intelligence is often used to denote precision and power, technical language referring to "AI," "cyber-espionage," or "algorithmic surveillance" is extremely rare.

.

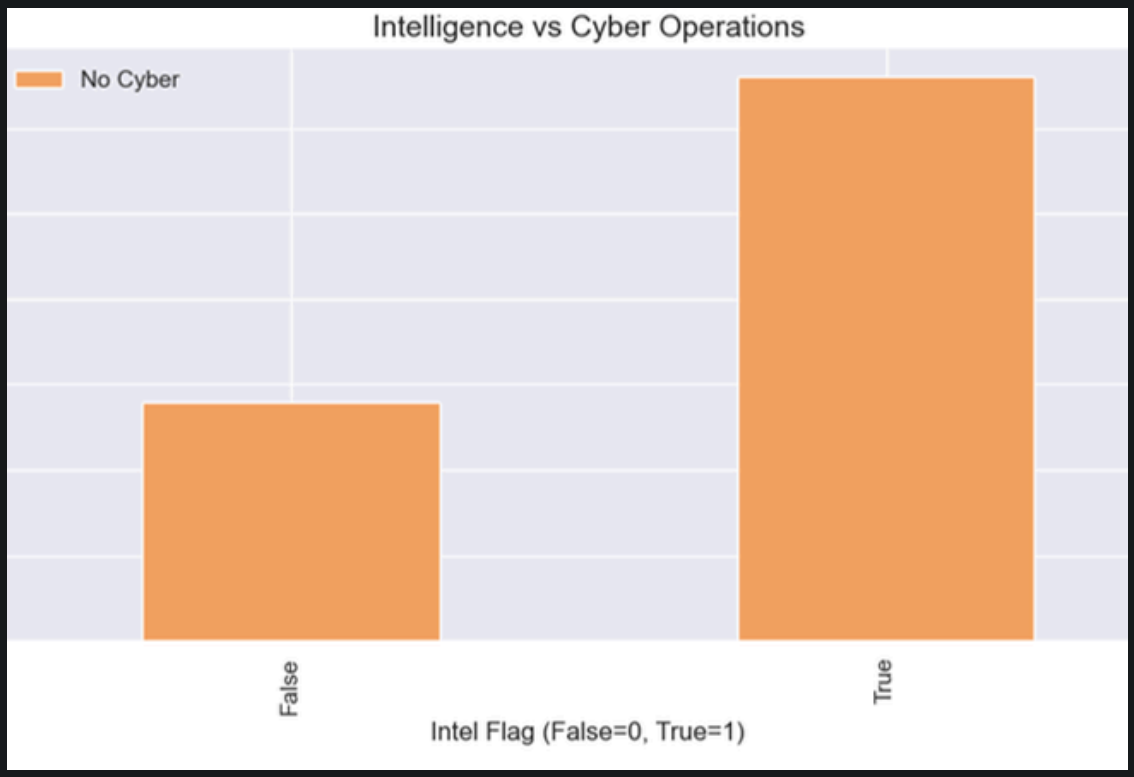


Communication Strategy

From the keyword frequency analysis, one can conclude that there is a deliberate strategy to use vocabulary such as "target," "command," and "control" instead of more explicitly technical terms, like "AI" and "cyber." In other words, Israel is emphasizing the end result of the operations, namely the neutralization of institutional enemies and the success of their strategy, while the technologies used to achieve this goal remain undisclosed.

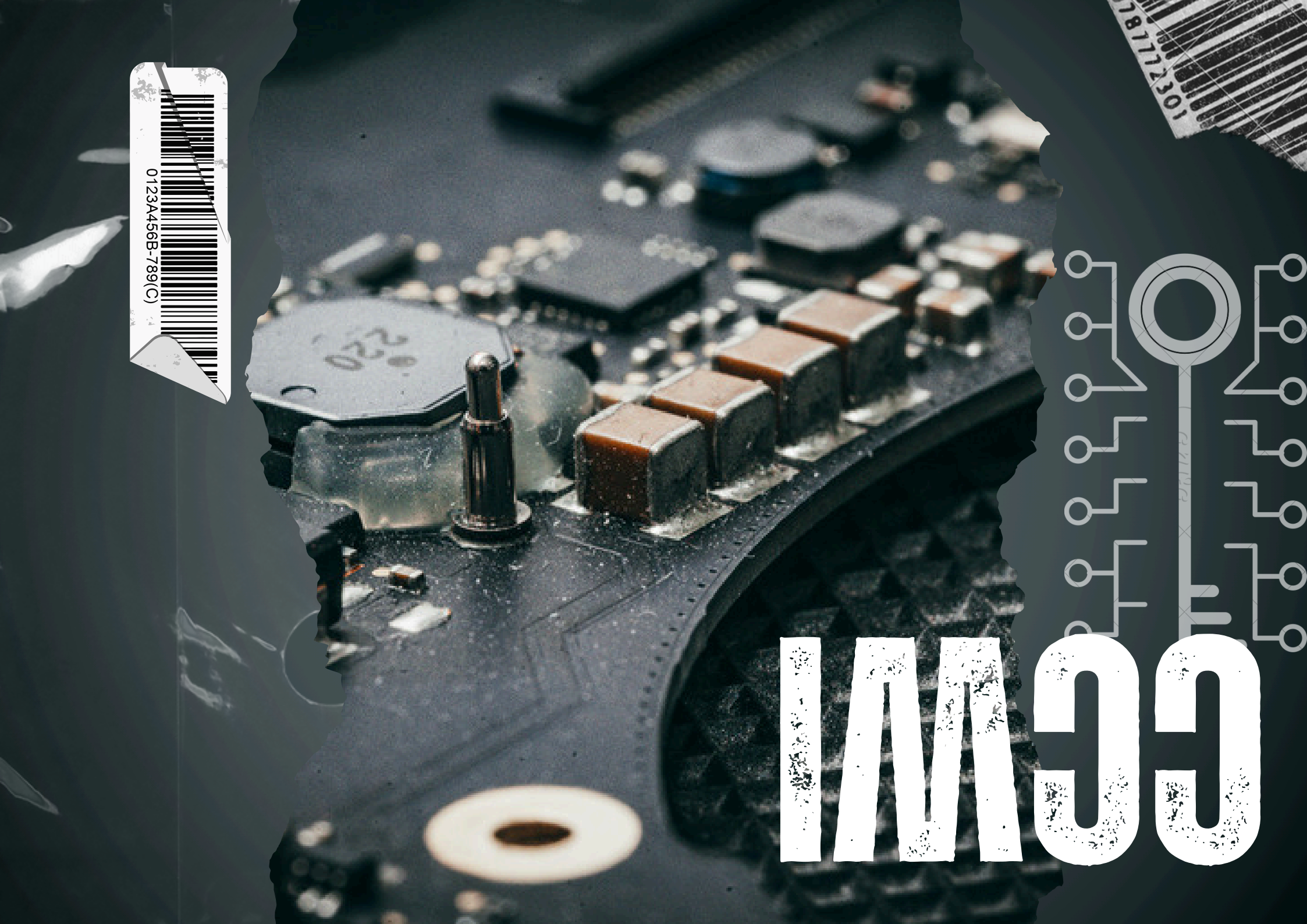
Limitations

There are several notable limitations associated with this research. First of all, the data set has been compiled through AI technology (Grok). Therefore, it may contain some discrepancies or be missing something in its content. Furthermore, it is important to keep in mind that the study is necessarily restricted to the realm of public discourse, meaning that it reflects the chosen communication strategy.



Conclusion

The rise of the "Cyber-Intel Enabled Decapitation Strategy" constitutes a revolutionary trend in modern international military action. Through the utilization of artificial intelligence and cyber intelligence in real time, Israel has elevated the concept of decapitation to become a legitimate form of statecraft. As can be seen from our analysis of the discourse, the way in which Israel conducts itself is meticulously crafted to demonstrate control, precision, and intent, while at the same time keeping hidden those technologies that enable its actions. For future research, one should go further than the narrative presented here and examine how such cyber warfare is changing international relations


0123A456B-789(C)
IMAGE


LIVE
online
LEARNING