POLICY BRIEF

Emerging Disruptive Technologies & Impacts on National Security

June 2024

Akbar Shaheryar Khan

IPRI Islamabad Policy Research Institute
Research | Innovation | Dialogue | Policy

Executive Summary

Emerging Disruptive Technologies & impacts on National Security

Emerging Disruptive Technologies have a transformative impact on human life in the 21st Century. Technologies, such as artificial intelligence (AI), blockchain, and quantum computing, have profound disruptive and constructive impacts on various sectors. Disruptively, these technologies can render existing industries obsolete, create vulnerabilities in cybersecurity, and exacerbate ethical and privacy concerns. For example, AI's ability to automate tasks can lead to significant job displacement, while quantum computing threatens current encryption methods, potentially compromising sensitive information.

Constructively, these technologies offer unprecedented opportunities for innovation, efficiency, and problem-solving. AI enhances decision-making through advanced data analytics, block chain ensures secure and transparent transactions, and quantum computing promises breakthroughs in fields like medicine and material science.

In the National Security domain, the integration of AI, advanced computing and autonomous systems has led to heightened threat perceptions among state actors. EDTs have become force-multipliers in Military and Intelligence Operations, and thereby transformed traditional notions of Military Strategy and Defense. With traditional paradigms of defense and security becoming obsolete, it becomes clear that technological supremacy in AI and Drones will provide States with a strategic edge against adversaries. Conclusively, National Security of States becomes dependent on States' ability to adapt to the rapid technological innovations taking place.

For a developing country like Pakistan it is a national security requirement to invest its human and monetary resources in catching up with rapid innovations taking place in the field of AI, advanced computing and drone technology. By integrating EDTs into its National Security frameworks, Pakistan can better mitigate its security risks that hinder meaningful economic growth and prosperity.

Policy Recommendations

Skill Development and Capacity-building

To develop a tech-enabled workforce within government ministries, the state should partner with institutions such as NUST and FAST to provide training in artificial intelligence, machine learning, data science, and analytics. This initiative should aim to create a technically proficient rank and file capable of integrating advanced technologies into national defense and governance. Furthermore, training workshops for institutional heads and political leaders are essential to help them formulate policy decisions incorporating technology-based solutions for governance, security, and economic issues.

Implement a "Kill Switch" for Autonomous Weapons

Ensuring human control over autonomous weapons systems is critical. Mandate the inclusion of a "kill switch" in all autonomous weapons to allow human operators to immediately deactivate the system in case of malfunction, unintended actions, or ethical concerns. Regular testing of the kill switch is necessary to ensure its reliability and functionality.

Doctrinal Shift

A holistic, whole-of-nation approach is needed to formulate a National Security Strategy and Security Doctrines that focus on emerging disruptive technologies. This paradigm shift should address how emerging technologies alter traditional notions of strategic stability and deterrence. Restructuring bureaucracies to incorporate technological experts and locally developed computational models into strategic decision-making processes is vital. Additionally, the security and intelligence framework should synergize AI and cyber capabilities to enhance sensing capabilities and incorporate computational and language models into the intelligence analysis process.

Establish Robust Legal Frameworks

Develop and update international and national legal frameworks to address the unique challenges posed by emerging disruptive technologies. This includes clarifying definitions and regulations around cyber warfare, autonomous weapons, and AI in intelligence operations. Revising or creating international treaties and agreements to ensure compliance with the Law of Armed Conflict and human rights laws is essential.

Enhanced Public-Private Partnerships

Encourage enhanced public-private partnerships to foster innovation and ensure the rapid deployment of cutting-edge technologies. Incentivize private sector investment in research and development of security-related technologies through tax breaks, grants, and public recognition.

AI Education

A comprehensive AI education policy is essential to prepare the future workforce for the challenges and opportunities presented by AI technologies. By integrating AI into curricula at all educational levels, fostering public-private partnerships, promoting AI literacy and ethical awareness, and providing adequate support and funding, we can ensure individuals are equipped with necessary skills.

Such measures are critical as the World Economic Forum (2020) highlights the significant job displacement and creation due to AI and automation, while the National Science Foundation (2021) underscores the importance of robust AI educational frameworks. Furthermore, international collaboration to share best practices can help build a global standard for AI education, ensuring students are prepared for the international job market

Emerging Disruptive Technologies and Impacts on National Security

How technologies disrupt National Security

National security refers to the protection and preservation of a nation's people, sovereignty, territorial integrity, and core values from external and internal threats[1]. It encompasses a broad spectrum of areas including, but not limited to, military defense, economic stability, political sovereignty, environmental security, cybersecurity, and the protection of critical infrastructure.

National security aims to ensure a country's survival and well-being by addressing threats that can undermine its stability and ability to function effectively. It involves a combination of proactive measures, such as intelligence gathering and diplomatic efforts, and reactive measures, such as law enforcement and military responses, to safeguard the nation's interests and maintain a stable and secure environment for its citizens.

The rate of technological innovation has rapidly increased in the 21st century and the integration of AI, Advanced Computing and Autonomous systems in private and public sectors have generated new industries and paradigms. Disruptive technology refers to innovations that significantly alter or displace existing technologies, economic structures, and human security paradigms. Such technologies disrupt established ecosystems, creating new opportunities while rendering some professions and technologies obsolete. Historical examples of disruptive technologies include the printing press, which revolutionized information dissemination and significantly impacted literacy and education; the Internet, which transformed global communication, commerce, and access to information; and social media platforms, which have redefined how individuals interact, share information, and influence public opinion. These technologies have not only enhanced efficiencies and created new industries but also disrupted traditional business models and societal norms.

[1] Buzan, B., Wæver, O., & de Wilde, J. (1998). **Security: A New Framework for Analysis**. Lynne Rienner Publishers.

Technological Disruption in the domain of National Security is rapidly altering the threat landscape and compelling state as well as non-state actors to adapt and improvise. [2] Speed and totality are the key components of disruption, this has been true for drone warfare and increasing role of autonomous systems in counter-insurgency and intelligence gathering operations.[3]

The contemporary discourse on national security is not military-centric, but rather it delves into the economic, political and environmental domains. These sub-domains are directly impacted by the disruptive effects of technology. For instance, prior to the advent of social media platforms such as 'X' or YouTube, conducting influence operations on a mass scale required sophisticated, clandestine and costly procedures with a high degree of risk involved.[4]

However, today influence operations are much less costly and can be outsourced to privately owned PR companies and troll farms. This has been made possible with advancements in AI and machine-learning algorithms, coupled with expertise in data analytics and political narratives. These shifts have also compelled States to enact necessary laws to curb disinformation and false narratives, and these prompted the creation of AI-empowered tools and agencies that specifically work to counter fake news and Information operations[5]. Therefore, Technological disruption has also led to constructive measures that are empowered by emerging technologies such as AI.

Shifting Security Landscape

As EDTs become integrated in the security frameworks of nation-states, this has a domino effect which will inevitably lead to strategic competition of technological supremacy. A direct impact of this competition will be felt on the following sub-domains on National Security:

- Military Security
- Political Security
- Economic Security

The disruptions posed by EDTs on these sub-domains will be discussed in this brief with relevant case-studies.

---

[2] Armstrong, P. (2023). **Disruptive Technologies: Develop a Practical Framework to Understand, Evaluate and Respond to Digital Disruption**.

[3] Clarke, R. A., & Knake, R. K. (2010). **Cyber War: The Next Threat to National Security and What to Do about It**. Ecco.

[4] McKinsey. (2021). What's now and next in analytics, AI, and automation.

[5] Meta. (2021). Threat Report: Combating Influence Operations.

Military Security

EDTs such as surveillance drones, swarm and loitering munitions, AI-empowered target detection, and cyber capabilities significantly alter traditional military security concepts by acting as force multipliers for military and intelligence operations. These technologies shorten decision loops, making the contemporary battlefield fast-paced and reducing the fog of war and uncertainty. For instance, during the Battle of Mosul in 2016, the Islamic State used commercial drones to deliver explosives, demonstrating how inexpensive and accessible technology can effectively counter more traditional, costly military equipment[6]. Additionally, AI enhances decision-making and situational awareness, providing real-time intelligence and optimizing logistics, which further increases operational efficiency and effectiveness on the battlefield[7]. These advancements illustrate how emerging technologies disrupt traditional military paradigms, requiring adaptations in strategy and policy to maintain security and operational superiority.

Table 1: List of EDTs and impacts on Military Security

EDTs	Impact
Artificial Intelligence	• Target acquisition • Target detection • Predictive assessments using computational models • Fast decision-making capabilities • Automated logistics
Advanced Computing	• Cyber-attacks on communications and electronic infrastructure • Enhanced signals encryption • Course-correcting missile systems
Automations and Drones	• Surveillance drones for augmented reconnaissance • Loitering drones and automated munitions • Unmanned anti-mine and bomb disposal units

[6] CSIS. (2023). Advanced Technology: Examining Threats to National Security. CSIS
[7] C4ISRNet. (2023). Beyond killer robots: How AI impacts security, military affairs.

Overview of risks and opportunities to Military Security

The risks and opportunities posed by EDTs impact the following elements of military security:

- Defense
- Offense
- Deterrence
- Command & Control
- Force Projection
- Logistics
- Strategic Stability

- **Defense**

  Drone technology and cyber capabilities augmented by advanced computing can bypass conventional defenses used in the battle-field. By adopting AI-guided drones, as seen in Nagorno-Karabakh conflict, traditional air-defenses can be rendered useless, and critical positions can be detected and targeted with precision-munitions[8]. This ultimately poses a significant risk to any military force that is mobilized against a tech-enabled adversary.

  However, AI models can empower air-defenses to target incoming projectiles and drones, and to further augment this, Machine-learning algorithms and data analytics can be utilized in predictive modeling and analyses used in accurate and timely threat assessments.

- **Offense**

  The integration of EDTs in army platoons, brigades and division level can enable military forces to add more precision in ongoing military operations. Offensive capabilities empowered by AI-based models and autonomous systems can significantly impact combat operations against insurgents in both urban and other rugged terrains. The risk of collateral damage is reduced along with troop casualties. Tank systems equipped with AI-based models and data-analysis capabilities can effectively home in on the source of incoming fire from insurgents in a mountainous terrain.

- **Deterrence**

  Cyber-capabilities can be utilized in directing cyber and malware attacks against critical security infrastructures. As a result strategic assets and defense systems can be remotely disabled and neutralized. [9]As a result, conventional notions of deterrence are likely to become obsolete as EDTs are operationalized by States. In 2014 the Stuxnet cyber-attack on Iranian nuclear facilities were a clear demonstration of cyber-capabilities against critical infrastructures.

[8] Schwartz, P. (2021). *The Military Balance 2021*. IISS.

[9] Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

- **Force Projection**
  Long-range autonomous drones such as the MQ-9 reaper drone has displayed how states can target threats over long distances. U.S remote operations against Al-Qaida operatives in the Middle-East region are an example. Similarly Pakistan can target hostile insurgent groups across its border in Afghanistan using long-range drone capabilities.

- **Command & Control**
  Integration of AI in command & control frameworks can significantly improve decision-support and situational awareness of commanders. The integration of AI in the U.S. military's Joint All-Domain Command and Control (JADC2) initiative reflects this shift.

  Advancements in offensive cyber capabilities, supported by advanced computing also has the potential to compromise the cyber-security of command-&-control frameworks, neutralizing the operational security of military operations.

- **Electromagnetic Pulse Weapons (EMP)**
  Electromagnetic Pulse (EMP) weapons represent a significant threat to military security due to their ability to disrupt and disable electronic systems over large areas. EMPs generate intense bursts of electromagnetic energy that can damage or destroy electronic circuits, effectively neutralizing communications, radar, and other critical military infrastructure.

  The use of EMP weapons could cripple a nation's defense capabilities by rendering its electronic equipment inoperable, leading to a severe strategic disadvantage (Center for Strategic and International Studies, 2021). Moreover, the development of high-altitude EMP (HEMP) weapons, which can be detonated in the upper atmosphere to cover vast geographic regions, poses a particularly potent risk.

Case Study: Drone Warfare in Russia-Ukraine conflict

Drones are unmanned automated vehicles which are used for surveillance and warfare. They fall under the category of emerging disruptive technology. Their integration into military operations has impacted traditional military strategy and tactics. There has been a proliferation of drone technology and its use in military operations. The U.S relies on Reaper UAVs to target and surveil threats to U.S security. Al Qaeda Leader Ayman Zahwiri and IRGC commander Qasem Solaimani were targeted by U.S drone strikes. Similarly Turkey, Iran, Russia and China have also operationalized drone technology in Surveillance and Military

operations. As per an article published in November 2020 by a New York based Foreign Affairs article that prior to 2011 only three countries possessed armed drones, but from 2011 to 2020 there are 18 countries that have armed drones of which 11 countries have been supplied drones by China.

Throughout the Russia-Ukraine conflict, Ukraine has adeptly adapted its drone technology usage to meet evolving battlefield conditions. Initially leveraging larger drones like the Turkish TB2 Bayraktar for long-duration missions and heavy target strikes, Ukraine shifted to smaller, commercially available drones as Russia enhanced its air defenses. These off-the-shelf drones, funded through grassroots efforts, have proven critical for battlefield awareness and precision strikes. Modified FPV racing drones equipped with explosives enable high-accuracy, single-use missions while evading Russian defenses. The rapid growth in Ukraine's domestic drone production, from seven to eighty manufacturers within a year, highlights the effectiveness of public-private partnerships in wartime innovation.

Conversely, Russia's drone capabilities have been hindered by Western sanctions, leading to a reliance on Iranian-made Shahed-136 drones. Despite these challenges, drones have demonstrated significant value by shortening the kill chain and enhancing reconnaissance and precision strike capabilities. They provide detailed enemy movement monitoring and support advanced drones in deep strikes.

The integration of drones in modern warfare has profoundly disrupted traditional concepts of tank warfare. [10]In conflicts such as the Ukraine-Russia war, drones have been used extensively to target tanks, showcasing their potential to neutralize heavily armored vehicles at a fraction of the cost. For example, Ukraine has utilized first-person view (FPV) drones equipped with explosives to conduct precision strikes on Russian tanks. These drones are relatively inexpensive, costing around $400, yet they can effectively destroy tanks that cost millions of dollars. The use of drones, forces tanks to operate further from the front lines to avoid being targeted, significantly altering their strategic deployment. [11]

[10] Modern War Institute. (2023). Seven (Initial) Drone Warfare Lessons from Ukraine. mwi.westpoint.edu
[11] Reuters. (2024). How drone combat in Ukraine is changing warfare. Retrieved from Reuters

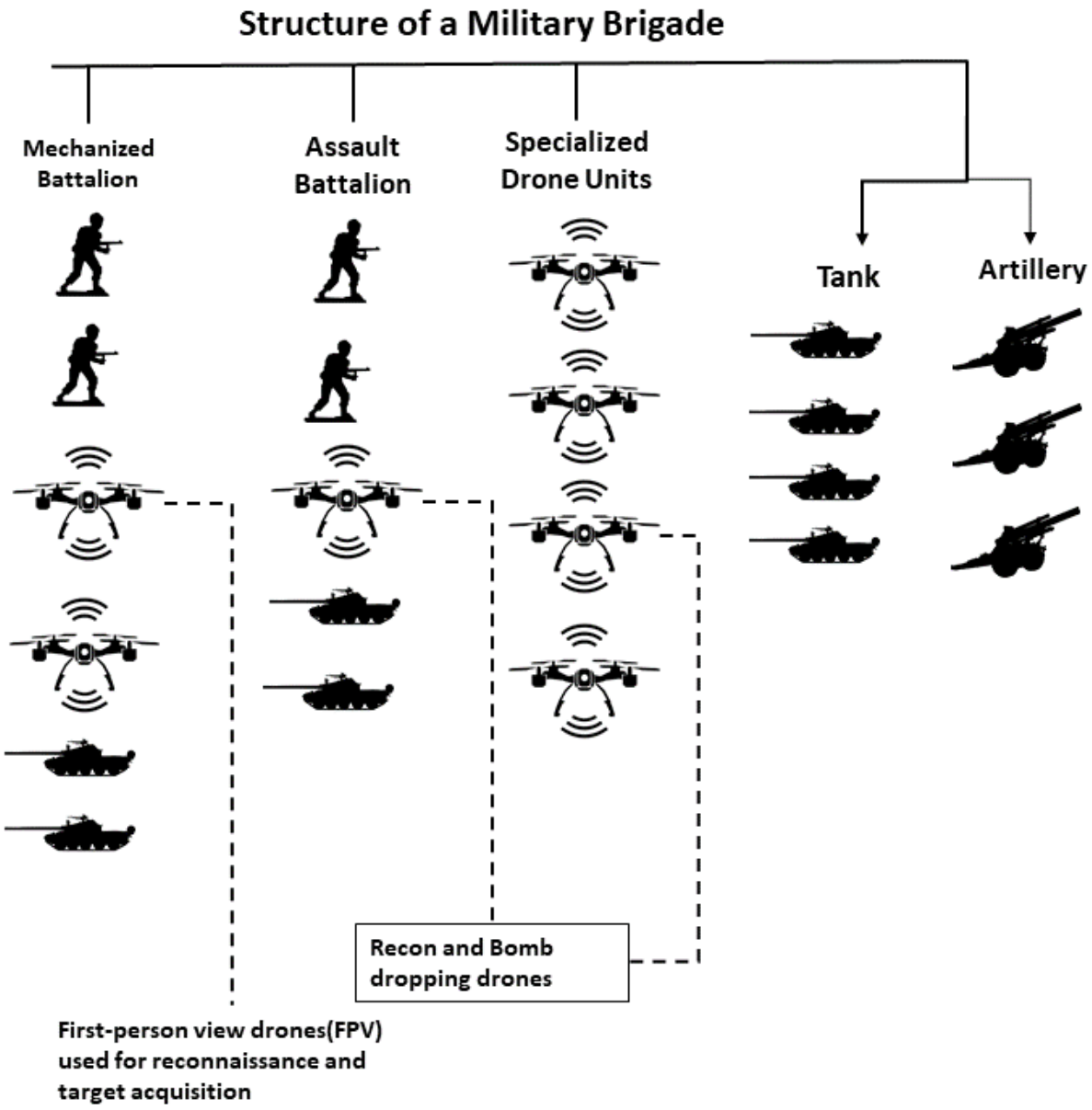


Figure 1: Induction of FPV Drones in Ukrainian Brigades

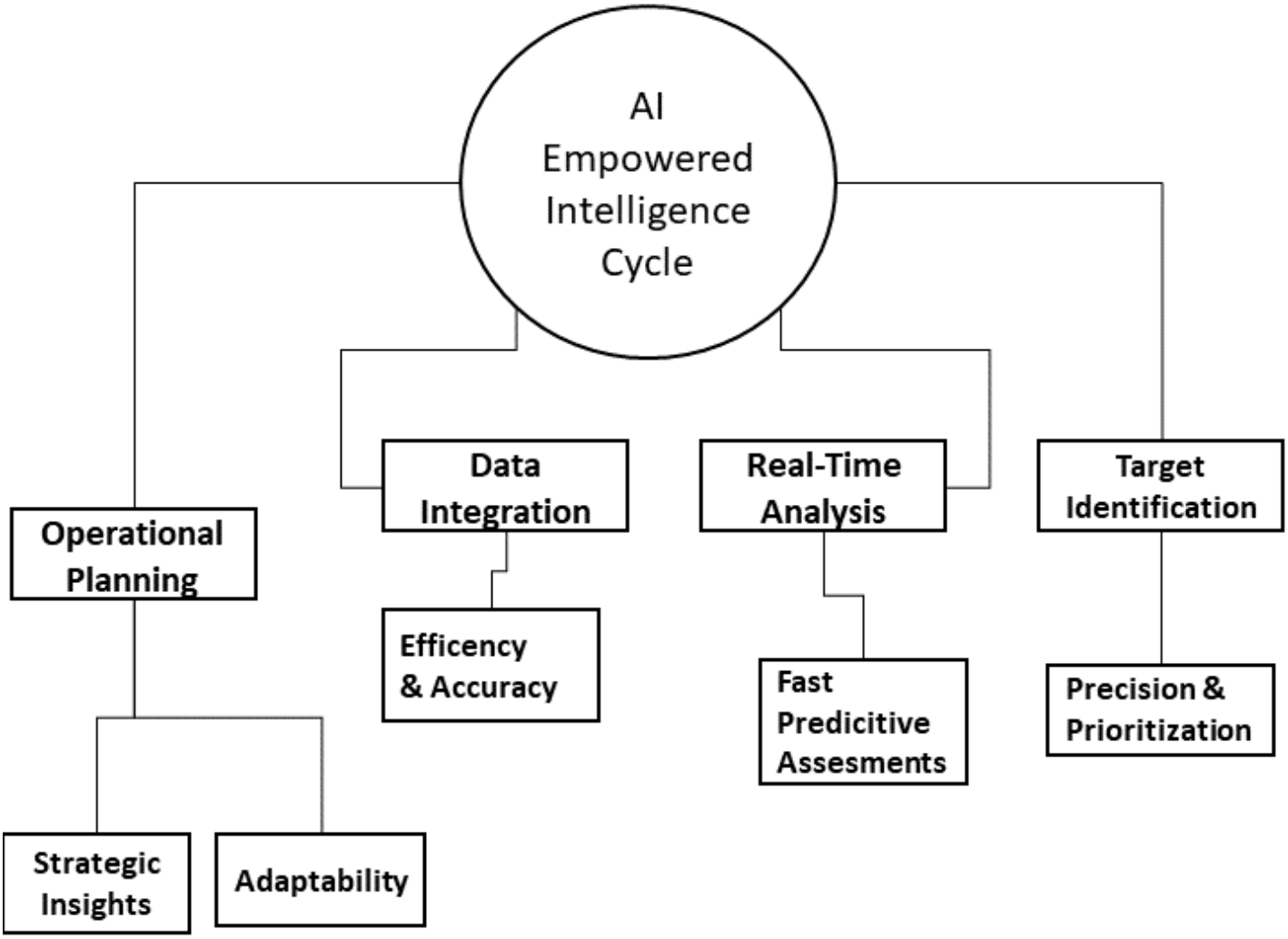
AI Empowered Military Intelligence

Israel's military employs an AI system called Lavender to enhance its operational capabilities, particularly in targeting and intelligence gathering. Lavender leverages advanced machine learning algorithms to analyze vast datasets and identify potential targets with high precision. This system automates the process of selecting bombing targets, which traditionally required manual verification, thereby significantly speeding up decision-making and reducing the operational workload. During operations in Gaza, Lavender has been used to identify and prioritize targets, including individuals and infrastructure linked to Hamas. [12]Despite its efficiency, the use of Lavender has raised ethical and legal concerns due to the minimal human oversight and the potential for collateral damage, highlighting the complexities of integrating AI into military operations.

The Lavender AI system significantly enhances the intelligence analysis process by leveraging advanced machine-learning algorithms to process and analyze vast amounts of data with unprecedented speed and accuracy. By scanning and integrating diverse data sources, Lavender can identify patterns, correlations, and potential targets that might be overlooked by human analysts. Its ability to swiftly analyze and cross-reference data from various intelligence inputs—such as surveillance footage, communications intercepts, and social media activity—allows for a more comprehensive and nuanced understanding of potential threats. This enables intelligence officials to make more informed decisions with greater precision and efficiency. Furthermore, Lavender's continuous learning capabilities ensure that it adapts to new information and evolving threats, maintaining its relevance and effectiveness in dynamic conflict environments. This technological advancement not only accelerates the intelligence cycle but also enhances the overall strategic and tactical planning processes.

AI technologies enable the automatic collection and integration of vast amounts of data from various sources, such as sensors, satellite imagery, and social media, which would be overwhelming for human analysts alone. AI-driven tools like machine learning models can process and categorize this data, identifying patterns and anomalies that might be missed by human operators. For example, AI can automate the identification of specific military assets or behaviors from satellite imagery or intercepted communications, thus speeding up the analysis phase.

[12] Al Jazeera. (2024). 'AI-assisted genocide': Israel reportedly used database for Gaza targets. https://www.aljazeera.com



13 14

Figure 2: Enhancements to Intelligence Process through Lavender AI

[13] Oxford Internet Institute (OII). (2023). Open Source Intelligence (OSINT) and AI: The Informational Pivot of Intelligence Analysis.

[14] Deloitte Insights. (2023). AI's impact on the future of intelligence analysis. https://www2.deloitte.com/

Political Security

Emerging technologies disrupt political security by introducing new tools and methods that can be exploited for malicious purposes, significantly impacting state sovereignty and stability. AI and machine learning algorithms can be used to spread disinformation and propaganda, manipulating public opinion and undermining democratic processes. The use of social media platforms by state and non-state actors to conduct influence operations has become a critical issue, as seen in the exploitation of these platforms to spread terrorist propaganda and recruit members during the COVID-19 pandemic.[15]

As social media penetration has increased over the last decade, there has been a race to obtain data sets of digital users to generate insights about their sentiments and behavior patterns. These data sets, when analyzed through language models, provide valuable insights used in marketing campaigns and influence operations. For instance, AI-driven data analytics can enhance the precision and impact of such campaigns by tailoring messages to specific demographics and behaviors [16]

The use of deep fakes and altered audios on social media has expanded the scope for disinformation and propaganda. Intelligence agencies and insurgent groups have effectively employed AI-generated imagery in influence operations, significantly amplifying their impact. This advancement has led to more sophisticated and subtle forms of online manipulation, making it challenging to discern authentic content from manipulated media.

Cyber capabilities pose significant risks to political security by compromising digital infrastructures, which can lead to political interference and alteration of election results. An example of this is the allegations made by the U.S. against Russia in the 2016 elections, where Russian intelligence reportedly used cyber capabilities to sabotage Hillary Clinton's presidential campaign. This incident underscores the critical need for robust cybersecurity measures and regulatory frameworks to protect the integrity of democratic processes and mitigate the threats posed by emerging technologies.[17]

[15] Centre for International Governance Innovation. (2023). Influence Operations and Disinformation on Social Media. cigionline.org

[16] MIT Technology Review. (2023). How generative AI is boosting the spread of disinformation and propaganda. technologyreview.com

[17] Brookings. (2020). How disinformation evolved in 2020. brookings.edu

Economic Security

Emerging technologies profoundly disrupt economic security by introducing new vulnerabilities and transforming traditional economic structures. Cyber capabilities enable sophisticated attacks on financial institutions, leading to significant financial losses and undermining trust in economic systems, as evidenced by the 2016 Bangladesh Bank heist where hackers stole $81 million via the SWIFT network. Additionally, the widespread adoption of AI and automation can displace jobs and exacerbate economic inequality, as businesses increasingly automate tasks previously performed by humans. [18]

Emerging technologies, particularly in the realm of cyber capabilities, pose significant threats to economic security by compromising digital financial frameworks and banking systems. States that lack robust technological infrastructure and cybersecurity measures are especially vulnerable. For instance, the increased connectivity of energy infrastructures and power grids creates numerous entry points for cyberattacks, which can lead to severe disruptions and economic losses. The 2021 Colonial Pipeline cyberattack in the United States exemplifies the potential impact, causing widespread fuel shortages and highlighting the vulnerabilities within critical infrastructure.[19]

Additionally, the sophistication of state and non-state cyber actors provides them with a competitive edge over less technologically advanced nations. These actors can exploit vulnerabilities to conduct espionage, sabotage, and even influence operations, further destabilizing political and economic security. [20]

Case Study: The NotPetya Cyberattack

In June 2017, the NotPetya cyberattack spread globally, causing extensive damage to various sectors, including banking, shipping, and energy. Initially disguised as ransomware, NotPetya was later identified as wiper malware designed to destroy data. The attack began in Ukraine and quickly affected major corporations worldwide, notably paralyzing Maersk's operations and costing the shipping giant an estimated $300 million. The attack also disrupted healthcare services, impacting patient care and data security. Attributed to Russian military intelligence, NotPetya underscored the vulnerabilities in critical infrastructure and the potential for state-sponsored cyberattacks to disrupt national and economic security, highlighting the need for robust cybersecurity measures and international cooperation.[21]

[18] World Economic Forum. (2020). The Future of Jobs Report 2020. weforum.org

[19] GAO. (2023). Protecting Critical Infrastructure from Cyberattacks. www.gao.gov.

[20] Department of Energy (DOE). (2023). The National Cybersecurity Strategy: A Path Toward a More Secure and Resilient Energy Sector. www.energy.gov.

[21] BBC News. (2018). UK and US blame Russia for 'malicious' NotPetya cyber-attack. BBC News

Legal Domain

The United Nations and NATO have provided several recommendations to address the legal and regulatory challenges posed by Emerging Disruptive Technologies (EDTs) to ensure their safe, secure, and ethical deployment. These recommendations emphasize the need for international cooperation to develop comprehensive legal frameworks that govern the use of EDTs, including AI and autonomous systems, ensuring compliance with international human rights law. NATO's AI Strategy and the establishment of the Data and Artificial Intelligence Review Board aim to operationalize principles of responsible AI use, including a 'Responsible AI' certification standard and practical toolkits to guide ethical AI implementation in military and security operations. Additionally, strengthening cybersecurity to protect critical infrastructure and digital frameworks from cyber threats is crucial, as highlighted by the 2021 Colonial Pipeline attack. Both the UN and NATO advocate for transparency and accountability in the development and deployment of EDTs, requiring regular reporting and oversight mechanisms to ensure alignment with legal and ethical standards. Recognizing the varying levels of technological advancement, the UN urges support for developing countries to help build capacity and close the digital divide, ensuring equitable access to technological benefits

These technologies, including artificial intelligence (AI), autonomous systems, and cyber capabilities, present new challenges that existing legal frameworks often struggle to address. The United Nations emphasizes the need for international cooperation to develop comprehensive legal standards that govern these technologies, ensuring they comply with human rights laws and do not pose undue risks[22]. NATO's initiatives, such as the Data and Artificial Intelligence Review Board, operationalize principles of responsible AI use, aiming to prevent misuse and ensure ethical deployment in military and security contexts. Strengthening cybersecurity to protect critical infrastructure from cyber threats is another critical aspect, as demonstrated by the 2021 Colonial Pipeline attack, which highlighted vulnerabilities in digital frameworks. Furthermore, transparency and accountability are paramount, requiring regular reporting and oversight to ensure alignment with legal and ethical standards. Addressing these legal dimensions is essential for harnessing the benefits of emerging technologies while mitigating their potential risks.[23]

[22] UN General Assembly. (2024). General Assembly adopts landmark resolution on artificial intelligence. Retrieved UN News

[23] NATO ACT. (2023). Digital Transformation and Emerging Disruptive Technologies. from NATO ACT

Policy Recommendations

Skill Development and Capacity-building

To develop a tech-enabled workforce within government ministries, the state should partner with institutions such as NUST and FAST to provide training in artificial intelligence, machine learning, data science, and analytics. This initiative should aim to create a technically proficient rank and file capable of integrating advanced technologies into national defense and governance. Furthermore, training workshops for institutional heads and political leaders are essential to help them formulate policy decisions incorporating technology-based solutions for governance, security, and economic issues.

Implement a "Kill Switch" for Autonomous Weapons

Ensuring human control over autonomous weapons systems is critical. Mandate the inclusion of a "kill switch" in all autonomous weapons to allow human operators to immediately deactivate the system in case of malfunction, unintended actions, or ethical concerns. Regular testing of the kill switch is necessary to ensure its reliability and functionality.

Doctrinal Shift

A holistic, whole-of-nation approach is needed to formulate a National Security Strategy and Security Doctrines that focus on emerging disruptive technologies. This should involvev how emerging technologies alter traditional notions of strategic stability and deterrence. Restructuring bureaucracies to incorporate technological experts and locally developed computational models into strategic decision-making processes is vital. Additionally, the security and intelligence framework should synergize AI and cyber capabilities to enhance sensing capabilities and incorporate computational and language models into the intelligence analysis process.

Establish Robust Legal Frameworks

Develop and update international and national legal frameworks to address the unique challenges posed by emerging disruptive technologies. This includes clarifying definitions and regulations around cyber warfare, autonomous weapons, and AI in intelligence operations. Revising or creating international treaties and agreements to ensure compliance with the Law of Armed Conflict and human rights laws is essential.

Enhanced Public-Private Partnerships

Encourage enhanced public-private partnerships to foster innovation and ensure the rapid deployment of cutting-edge technologies. Incentivize private sector investment in research

and development of security-related technologies through tax breaks, grants, and public recognition.

AI Education

A comprehensive AI education policy is essential to prepare the future workforce for the challenges and opportunities presented by AI technologies. By integrating AI into curricula at all educational levels, fostering public-private partnerships, promoting AI literacy and ethical awareness, and providing adequate support and funding, we can ensure individuals are equipped with necessary skills.

Such measures are critical as the World Economic Forum (2020) highlights the significant job displacement and creation due to AI and automation, while the National Science Foundation (2021) underscores the importance of robust AI educational frameworks. Furthermore, international collaboration to share best practices can help build a global standard for AI education, ensuring students are prepared for the international job market

Action Matrix

Problem/Issue	Pathways to Solution	Actors responsible	Implementation Timelines
Skill Development and training	• Develop partnerships with universities and top institutions dealing with technologies to initiate training programs from Government employees and Key decision-makers in AI and Cyber Domains. • Hold seminars with professionals in AI and Autonomous systems to spread awareness about Emerging technologies. • Reach out to friendly countries such as U.S and China, to share technological expertise with Pakistani experts and decision-makers	• Ministry of Science & Technology • CASS • NASTP • Ministry of Foreign Affairs.	2024 - 2026
Incorporating a 'kill switch' mechanism to restore human control on Autonomous weapons	• Develop and integrate a reliable kill switch mechanism in all AI and autonomous weapon systems. • The kill switch should be easily accessible and operable under all conditions. • To be implemented after inclusion of latest technological development & practices	• Defence Science and Technology Organization (DESTO) • Ministry of Defence • NESCOM • PAC	2024 - 2026
Doctrinal Shift	• Set up research and development cells within think-tanks , with a sole focus of developing strategies related governance and Security using EDTs • Generate debate on EDTs in National Assembly and Senate. • Hold Round-table on EDTs for students and professionals.	• Ministry of Science and Technology • Ministry of Commerce • Ministry of Education and Professional Training	2024 – 2026

Legal Frameworks	• Consult with Legal experts and Tech experts on how to formulate laws specific to the use of AI and autonomous weapons. • Hold seminars on Legal aspects of EDTs	• Ministry of Science and Technology • Ministry of Law • RSIL • ISSI • CASS	2024 - 2025
AI Education	• Review school curriculums and incorporate AI education in school syllabi • Include AI education in CSS exam syllabus	• Ministry of Education • Higher Education Commission	2024 - 2025
Public-Private partnerships	• Partner up with private tech firms and universities to develop AI-based applications to aid in Governance and Security. • Create incubation centers for Technological Firms, where the government can subsidize research and development of EDTs	• Ministry of Science and technology • NUST • FASST • CASS • LUMS • AIR University • Pakistan Armed Forces	2024 - 2026