Introduction: Objectives and Major Themes

The Atlantic Council's *Forward* Defense program is pleased to provide an abridged version of the fourth installment of our bi-monthly Defense Technology Monitor reports.

These reports are designed to **track** selected developments in global defense technology and adoption advancement; **provide a high-level analysis** of key trends, drivers, uncertainties, and challenges associated with key technologies and capabilities and their implications for defense, international security, and geopolitics; **highlight notable innovations and acquisitions** in the global defense and commercial high-tech industry; and **identify** non-technical trends and broader competitions that are shaping technology adoption and the future fight.

Each Defense Technology Monitor will be divided into sections examining categories of technology or capability, such as:

- Artificial intelligence and data
- Autonomous systems
- Platforms and weapons systems
- Information domain, cyber and electronic warfare
- Manufacturing and industry

This month's report delves into the critical trends shaping modern defense technology. It begins with the pivotal role of drone warfare, showcasing how drones are revolutionizing battlefields through enhanced reconnaissance and offensive capabilities. This issue explores their extensive use in conflicts like Ukraine and Gaza and highlights advancements in counter-drone technologies such as laser and radio frequency weapons. Shifting focus to artificial intelligence (AI), the report examines its growing applications in defense. It underscores the significant impact of AI in military operations, particularly in targeting and data analysis. The discussion also addresses the broader implications of AI, including its exploitation by criminals for cyber-attacks and phishing, which present serious security challenges. Additionally, the ethical and operational complexities of integrating AI into defense strategies are explored. The report further investigates advancements in cyber and electronic warfare. It covers calls for robust security in the information domain and the electromagnetic spectrum to counter sophisticated threats. Highlights include new quantum navigation technologies that offer protection against jamming and a strategic emphasis on safeguarding critical infrastructure from cyber threats, particularly from malicious actors like Chinese hackers.

Artificial Intelligence (AI) and Data

AI and Data – Operational Challenges in Gaza

The utilization of AI in targeting operations by the Israeli Defense Forces in Gaza has ignited intense scrutiny over its ethical ramifications and operational validity. These AI systems, tasked with identifying and striking military targets amidst dense civilian populations, pose significant risks of collateral damage. Critics argue that the systems lack the nuanced judgment required to distinguish between combatants and non-combatants effectively. This scenario also raises larger geopolitical concerns, as the reliance on automated decision-making in such sensitive contexts could escalate conflicts unintentionally and affect global perceptions of AI in warfare. As AI continues to play a pivotal role in military strategies, there is an increasing call from the international community for stringent oversight, transparent engagement rules, and ethical constraints to govern its use.

Autonomous Systems

Criminals are employing generative AI tools

Criminals are increasingly harnessing generative AI to enhance their operations, creating more sophisticated threats to digital security. From crafting undetectable phishing emails to generating convincing deepfake audios and videos, these tools allow for a range of deceptive practices previously unattainable with traditional methods. This trend poses new challenges for cybersecurity defenses, necessitating advancements in digital verification techniques and the development of countermeasures to detect and mitigate the effects of AI-generated content. The implications are broad, affecting everything from individual identity security to national security, as these technologies can be used to influence public opinion, manipulate stock markets, or even sway political elections.

Platforms and Weapons Systems

The status of laser system developments

The development of laser weapon systems by the US military highlights significant advancements in directed energy applications for defense. These laser systems, designed for precision targeting and minimal collateral damage, are tested under various operational scenarios to determine their efficacy against threats like drones, missiles, and other aerial targets. While promising, the deployment of these systems faces hurdles such as the need for substantial power sources, environmental limitations affecting beam propagation, and integration challenges with existing military platforms. Ongoing research aims to overcome these obstacles, with the goal of fully operationalizing laser weapons to provide a cost-effective, reliable, and scalable defense solution.

The Information Domain, Cyber, and Electronic Warfare

Growing concern about Chinese threats to US infrastructure

Emerging concerns over cyber threats to US infrastructure have been amplified by revelations of covert operations by Chinese hackers. These operations involve embedding malicious software in critical systems that could be activated remotely to cause significant disruption during geopolitical tensions. This strategy represents a shift towards more aggressive postures in cyber warfare, where the potential for damage extends beyond espionage to actual physical and economic harm. The United States is responding by bolstering its cybersecurity defenses, with an emphasis on enhancing resilience, detecting pre-emptive breach attempts, and mitigating potential impacts through rapid response and recovery strategies.

Manufacturing and Industry

AUKAUS and prospect of Pillar II expansion

The Defense Minister of the Republic of Korea announced the country's intention to pursue collaboration on emerging technologies with the United States, United Kingdom, and Australia as part of Pillar II of AUKUS. The potential expansion of the AUKUS alliance into advanced technology sectors under Pillar II reflects a strategic initiative to deepen military cooperation beyond traditional domains. This collaboration aims to leverage cutting-edge technologies, including AI, quantum computing, and advanced cyber defenses, to maintain a competitive edge in the Indo-Pacific region. While this expansion requires careful management of technology transfers, alignment of regulatory standards, and protection of intellectual property rights, the initiative could set a precedent for future international defense and security collaborations, fostering a more integrated approach to global security challenges.

If you are interested in learning more about emerging defense technologies and capabilities and would like to read this month's *full* issue of the Defense Technology Monitor, please contact *Forward* Defense program assistant, Abigail Rudolph.