Future Battlefield: Cybersecurity and AI in National Security Policy

International Relations Insights & Analysis

Future Battlefield: Cybersecurity and Artificial Intelligence in National Security Policy

International Relations Insights & Analysis

Author: Syed Bahadur Abbas

Published on: June 30, 2024

IRIA Defense Review - Use of Advanced Technologies and AI in Shaping Modern Warfare

Future Battlefield: Cybersecurity and AI in National Security Policy

As defense technology advances, nations become increasingly reliant on digital infrastructure, making them vulnerable to cyber threats. The technological advancements in modern warfare techniques have compelled the world powers to develop a strong policy to address these challenges and enhance the overall security posture.

Cybersecurity has become an integral part of any national security policy. The year 2023 witnessed substantial progress on this particular front as several of the world's leading powers, including the U.S., the UK, and NATO, brought forward their respective cybersecurity policies to eliminate threats posed by modern technologies including artificial intelligence (AI).

The advancements in AI and related technologies will completely transform the approach to national defense and war-fighting strategies. Those who fail to induce this perspective into modern security strategy would succumb to a quick death on the future battlefields.

By the end of the year 2023, it became evident that cyberattacks are as effective of a tool to get leverage in conflict as any other modern. It can be used as a deterrence and offense. In November 2023, the United Kingdom hosted an AI safety summit which several world and industry leaders, including representatives from China, attended. The summit gave the world's first-ever AI agreement, signed by the leaders and representatives of 28 different countries.

According to the UK government, the declaration affirms that whilst safety must be considered across the AI lifecycle, actors developing frontier AI capabilities, in particular those AI systems that are unusually powerful and potentially harmful, have a particularly strong responsibility

World leaders attend the AI Safety Summit in Bletchley Park, Britain, on November 2, 2023. (Image Credit: Toby Melville/Reuters)

to ensure the safety of these AI systems, including through systems for safety testing, through evaluations, and by other appropriate measures.[1]

Around the same time, the United States also devised its own set of rules and regulations to ensure the safe and trustworthy development of AI. An executive order from U.S. President Joe Biden in October 2023, stressed the urgency of devising governing legislation for the development and use of AI safely and responsibly.[2]

Role of Cyber in Modern Conflicts

The use of the term cyberwarfare or cyberattacks has become more frequent in the security-related literature of the modern defense doctrine. Russia's territorial invasion of Ukraine in February 2022 was accompanied by significant cyberattacks marking the first modern conflict that was fought simultaneously in the cyber realms as it was fought on the ground.

Similar instances of cyber warfare have been observed in conflicts involving states such as Russia and Georgia, Israel and Iran, as well as ongoing cyberattacks by Russia against Ukraine since 2014. According to a European Union report, the Switzerland-based Cyberpeace Institute recorded more than 1,998 cyberattacks and operations conducted by 98 distinct actors only in the first quarter of 2023.

Russian military personnel of the electronic warfare unit of the Southern Military District during a combat training exercise.
(Image Credit: Russian Ministry of Defense/Global Look Press)

These attacks have targeted 23 different critical infrastructure sectors, impacting not only Ukraine and the Russian Federation but also 49 other countries. The documentation of these incidents contributes to a comprehensive analysis of the use of cyber means in times of war.

Types of Cyberattacks Against Ukraine

Based on the attacks conducted on Ukrainian telecommunication and administrative infrastructure, cyberattack operations can be categorized into the following types.

---

1. IRIA News, US, China, and EU sign first AI safety agreement at global AI summit hosted by UK, International Relations Insights & Analysis, November 4, 2023. https://www.ir-ia.com/news/us-china-and-eu-sign-first-ai-safety-agreement-at-global-ai-summit-hosted-by-uk/

2. The White House, Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, U.S. White House Briefing Room, October 30, 2023. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

- **Destructive Attacks:** These cyberattacks are characterized by their intent to permanently delete data or inflict irreparable damage on systems, rendering them unrecoverable. The consequential impact on organizations can be prolonged, particularly if backup retrieval or system reset proves challenging. Notable instances include the utilization of wiper malware targeting Ukrainian government entities and various sectors. A recent incident involved the resurgence of a destructive wiper malware named 'CaddyWiper,' identified by Ukraine's Computer Emergency Response Team (CERT-UA).[3] In January 2023, Ukraine reported the CaddyWiper attack on its national news agency Ukrinform.[4] Other data-wiping malware deployed against Ukrainian targets include ZeroWipe, DoubleZero, HermeticWiper, WhisperKill, WhisperGate, IsaacWiper, and AcidRain, according to security researchers.

- **Disruptive Attacks:** Cyberattacks designed to disrupt services and operations have been prevalent during the conflict. These attacks targeted Ukrainian organizations in the early stages of the invasion, Russian organizations following a Ukrainian government appeal to civilians, and public institutions in some NATO member countries after security or economic announcements. Distributed Denial of Service (DDoS) attacks, particularly impacting the public and financial sectors, have been predominant. DDoS attacks accounted for more than 99% of all recorded cyberattacks against Ukraine between July and September 2023, according to the CyberPeace Institute.[5] Financial, public administration, and information and communication technology (ICT) sectors were the primary targets A concerning trend is the targeting of vulnerable Ukrainian non-profit organizations, which often lack preparedness and resilience measures.

- **Data Weaponization:** This category includes cyberattacks leading to data theft or exfiltration, primarily for espionage, surveillance, or intelligence purposes. While the latter activities are expected in the context of war and geopolitics, collective actors engaged in the theft of data for activist purposes have been notably active. Data, about both private and public organizations, is exfiltrated and published online at an unprecedented rate. Hack and leak operations involve the weaponization of data, exemplified by a recent incident in March 2023 targeting EU countries. A state-sponsored Russian threat actor used spear-phishing emails containing information about the Polish Ambassador's visit to the United States. This campaign mimicked real information exchange systems used by EU nations, employing malware to infiltrate networks and collect data.

- **Disinformation:** Information operations centered on disinformation and propaganda, although not new, have gained unprecedented speed and scale in the cyber domain. Cyberattacks focused on spreading false information and propaganda are prominent in this armed conflict. Threat actors aim to influence the information space, restricting access to timely, reliable, and official information for the population, or intentionally sowing confusion and undermining information integrity.

---

3. WeLive Security, CaddyWiper: New wiper malware discovered in Ukraine, ESET, Ukraine Crisis - Digital Security Resource Center, March 15, 2022. https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

4. Sergiu Gatlan, Ukraine links data-wiping attack on news agency to Russian hackers, Bleeping Computer, January 18, 2023. https://www.bleepingcomputer.com/news/security/ukraine-links-data-wiping-attack-on-news-agency-to-russian-hackers/

5. CyberPeace Institute Quarterly Analysis Report, Cyber Dimensions of the Armed Conflict in Ukraine, Q3 July to September 2023. https://cyberpeaceinstitute.org/wp-content/uploads/2023/12/Cyber-Dimensions_Ukraine-Q3-2023.pdf

Strengthening Cybersecurity in the Defense Industry

Cybersecurity is crucial within the defense industry to protect sensitive information, critical infrastructure, and military capabilities from cyber threats. This includes employing strong security measures, conducting regular analysis of threats and measures, providing specialized training to personnel, and securing communications. Collaboration with government agencies and cybersecurity experts is also essential to develop effective strategies to address evolving challenges.

A comprehensive national defense policy requires a multi-layered approach to cybersecurity. Below are the key components that contribute to robust cybersecurity measures in national defense policies:

- ***Critical Infrastructure Protection:***

National defense policies emphasize the protection of critical infrastructure, including energy grids, transportation systems, and communication networks, against cyber threats. Disruptions to these systems could have severe consequences for national security.

A Ukrainian sailor uses equipment on board an armored gunboat. (Image Credit: Reuters/Anastasia Vlasova)

- ***Secure Communication:***

For government and defense agencies, ensuring the security of communications within defense networks and among military entities is a top priority. Encryption, secure communication protocols, and intrusion detection systems are implemented to protect the confidentiality and prevent unauthorized access or manipulation. Best practices and tools should be utilized to secure sensitive communications, maintain data privacy, and ensure the complete security of the systems.

- ***Cyber Defense Strategy:***

National defense policies outline comprehensive cyber defense strategies that include proactive measures to detect, prevent, and respond to cyber threats. This may involve the development of cybersecurity frameworks, incident response plans, and collaboration with other agencies and allies.

- ***Intelligence and Surveillance:***

Cybersecurity efforts in national defense policies often involve intelligence gathering and surveillance activities to identify potential cyber threats. This includes monitoring activities in cyberspace, assessing vulnerabilities, and staying informed about emerging threats.

- ***Collaboration and Alliances:***

Engaging in international partnerships and alliances is crucial in the realm of cybersecurity to address global challenges and shared threats. Countries often work together to share threat

intelligence, and best practices, and collaborate on joint cybersecurity initiatives to enhance collective defense capabilities.

- ***Investment in Research and Development:***

National defense policies may allocate resources for research and development in cybersecurity technologies. This includes the development of advanced cybersecurity tools, artificial intelligence applications for threat detection, and other cutting-edge solutions to stay ahead of evolving cyber threats.

- ***Cyber Training and Education:***

Equipping government officials and military personnel with comprehensive cybersecurity training and awareness programs is crucial to enhance their understanding of cyber threats and ensure better preparedness.

- ***Threat Intelligence and Vulnerability Management:***

Collecting and analyzing data on existing and potential cyber threats is crucial to identify the tactics, techniques, and procedures of the adversaries, understand how technology is being weaponized, and deploy proactive defense measures. Identifying and addressing vulnerabilities within the defense systems and networks can help mitigate the risk of exploitation by cyber attackers.

Cyberwarfare specialists of the U.S. Army's 782nd Military Intelligence Battalion (Cyber) supporting the 3rd Brigade Combat Team, 1st Cavalry Division during a training exercise in 2019. (Image Credit: Steven Stover/Wikimedia Commons)

- ***Legislation and Regulations:***

National defense policies may include legislation and regulations that mandate cybersecurity standards for government agencies, military contractors, and critical infrastructure providers. Compliance with these standards helps ensure a baseline level of cybersecurity across the defense ecosystem.

- ***Deterrence and Offensive Cyber Operations:***

Some national defense strategies may include the development of offensive cyber capabilities for deterrence purposes. This involves responding to cyber threats with offensive measures, potentially disrupting or disabling adversary capabilities.

INTERNATIONAL RELATIONS INSIGHTS & ANALYSIS

International Relations Insights & Analysis (IRIA) is a research institute focusing on critical issues that threaten international peace & security. IRIA investigates and offers research and analysis on security, energy, terrorism, foreign affairs as well as global political agendas. We formulate independent, concise, and meaningful research presented in an informative and interactive manner.

IRIA special reports include experts' opinions, special features, cost & benefit analysis. IRIA also examines risk & opportunities, highlight common threats and misconceptions and provide improved set of strategies and countermeasures. The key findings of reports and analysis highlight pragmatic policy options and revise strategies.

IRIA aims to support grassroots democracy, promote peace-building processes and cultural harmony by working with scholars, policymakers, and institutions.

IRIA Publications include Exclusive Reports, Defense Review, and Journal of International Affairs & Politics.

INTERNATIONAL RELATIONS
INSIGHTS & ANALYSIS

US Integrating Advanced Robotic and Autonomous Weapon Systems into Army Units

Syed Bahadur Abbas

International Relations Insights & Analysis

Cover Image:
Artificial Intelligence and Cyber Security.
(AI Generated Image by IRIA)

For more information visit:
www.ir-ia.com