edam
Ekonomi ve Dış Politika Araştırmalar Merkezi

GCSP
Geneva Centre for Security Policy

ADVANCED RESEARCH WORKSHOP (ARW)

EMERGING DISRUPTIVE TECHNOLOGIES (EDT) IN DEFENSE: LESSONS FROM UKRAINE

27 - 28 OCTOBER,
2023 ISTANBUL,
TURKIYE

NATO OTAN
This workshop is supported by:
The NATO Science for Peace and Security Programme

SPEAKERS:

Ambassador (Ret) Tacan Ildem

Chairman, EDAM & Former NATO Assistant Secretary General for Public Diplomacy

H.E. Ambassador Vasyl Bodnar

Ambassador of Türkiye to the Republic of Türkiye

Mr. James Apparthurai

Deputy Assistant Secretary General for Emerging Security Challenges, NATO

Dr. Eyup Turmus

Advisor and Program Manager, NATO Science for Peace and Security (SPS) Programme
(Presentation on the NATO SPS Programme)

OPENING REMARKS

Succeeding in the era of digitalized warfare will necessitate two critical requirements and defense technology strategies: investing in cyber capabilities and fostering the development of dual-use technologies. The development and adoption of emerging and disruptive technologies (EDTs) is a race against time. Therefore, integrating these groundbreaking capabilities in the Allied military decision-making more rapidly than our strategic rivals.

Innovation transforms warfighting, rendering it much more advanced. The fusion of information and data-centric warfare leads to higher efficiency, more effective C4ISR and a decisive victory on the battlefield. AI-driven technologies also help us decipher the adversary's tactics. The use of natural language processing algorithms to translate Russian troops' communication is one prominent example from the ongoing Russo – Ukrainian War.

Opening Remarks

The development and military application of EDTs should be an ‘all-society’ approach. Moving forward, building better relationships with the start up industry and fostering the trust between NATO and private stakeholders will be key. The Defense Innovation Accelerator for the North Atlantic (DIANA) is a promising opportunity to involve the business sector in EDT-related projects. In essence, the initiative should not be a horizontal effort that merely involves militaries and governments. Instead, it needs to adopt an across-the-spectrum approach, based on public-private scientific and strategic community cooperation.

Assuming the EDT capacity to be a lone wolf warfighter, or a panacea, would be a flawed consideration: it is about the merger. Conventional trends such as artillery and trench warfare are still prominent. Nevertheless today, such capabilities are augmented by drones. In modern conflicts, even the most remote points in the battlefield are connected by space-based satellite technologies and robotic systems.

In the future operating environment (FOE), the successful integration of AI and robotics-driven technologies to support our existing capabilities will require smart governance and effective oversight.

SPEAKERS:

Dr. Can Kasapoğlu

Director of Defense Research, EDAM & Non-Resident Senior Fellow, Hudson Institute

Major General (Ret) Paul Hurmuz

Senior Associate Expert, New Strategy Center Romania

Dr. Jean-Marc Rickli

Head of Global and Emerging Risks, GCSP

MODERATOR

Sine Ozkarasahin

Defense Analyst, EDAM

PANEL I:

Digitalization of the Battlefield & the Future Operating Environment (FOE)

The future operating environment (FOE) will likely be a unique battlefield with the merger of old and new technologies. Conventional assets such as Cold War remnant artillery systems will co-exist with dronized warfare assets. Satellite internet connection provided by private firms such as Starlink, will become the new norm in wartime communications.

This new battlefield will necessitate new, innovative concepts of operations (CONOPS). Modern conflicts already present us with some interesting examples. For instance, in contemporary wars, drones take on critical artillery spotting roles and facilitate satellite internet access across the battlefield. In the ongoing Russo – Ukrainian War, robotic warfare assets generate an asymmetrical naval impact.

Battlefields are becoming increasingly transparent and digitalized. Thus, in the FOE, information superiority and dominance in the electromagnetic spectrum will be the two keys to victory.

PANEL I:
Digitalization of the Battlefield & the Future Operating Environment (FOE)

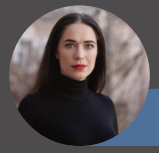
Emerging disruptive technologies (EDTs) will not simply delete the past and introduce a completely new future. Instead, these novel capabilities will serve as a booster for existing military concepts and systems.

In parallel, artificial intelligence (AI) will be both an analytical enabler (targeting, situational awareness, OSINT purposes) and a force multiplier. Nevertheless, EDTs also come with dangerous consequences. These AI-driven risks mainly pertain to information warfare, and include techniques - tactics - procedures (TTPs) such as espionage, hacking, manipulation, subversion and deepfakes. In the future, increasing our societies' resilience by introducing strong verification tools against the malicious use of AI will be a strategic necessity.

SPEAKERS:

H.E. Ambassador Vasyl Bodnar

Ambassador of Türkiye to the Republic of Türkiye



Dr. Hanna Shelest

Security Studies Program Director, Ukrainian Prism

Federico Mantellassi

Research and Project Officer, GCSP

Federico Borsari

Leonardo Fellow, CEPA

MODERATOR

Francis Farrell

Reporter, The Kyiv Independent

PANEL II:

Emerging Disruptive Technologies (EDTs) in Ukraine

The ongoing Russo – Ukrainian War is heavily dronized. Ukraine is losing approximately 10,000 drones a month. In the future, the development and procurement of strategic, medium / high altitude long endurance (MALE / HALE) drones will surely be important. However, the mass production of mini commercial UAVs will also be crucial.

During its strikes against the Russian Black Sea deterrent, Ukraine successfully used UAVs and USVs in joint campaigns to attack naval bases in the occupied Crimea. In such missions, USVs assumed kamikaze attack roles, where the UAVs provided assistance in critical tasks such as target acquisition and reconnaissance.

However, drones are no silver bullets, meaning they come with certain limitations. Putin's ongoing invasion in Ukraine showed that UAVs still remain vulnerable in contested airspaces. Moreover, prioritizing R&D efforts in counter-drone systems (C-UAS) as much as the investments in the UAS industry will be paramount. Future efforts should also focus on establishing an uninterrupted and high-end C4ISR capability for successful drone operations in hostile environments.

PANEL II:
Emerging Disruptive Technologies (EDTs) in Ukraine

In the FOE, civilian entities and private sector organizations are also playing a critical role. Some prominent examples from the Ukrainian battlefield include mobile apps such as ePPO. The app is designed to allow citizens to report any sightings of Russian cruise missiles or Shahed-136/131 kamikaze drones to Ukrainian authorities using their smartphones, bolstering early detection and interception efforts. Another critical initiative is Delta, a crowdsourced, advanced software-augmented database, which generates outputs that can be translated into targeting data.

The West is already using the lessons from Ukraine's experience to feed its own EDT efforts. One important example is the US' Replicator initiative. The project relies on the mass production to outnumber competitors like China, which will be crucial in highly contested environments.

SPEAKERS:

Samuel Bendett

Senior Associate (Non-resident), Europe, Russia, and Eurasia Program

Sam Bresnick

Research Fellow, CSET

Dr. Can Kasapoglu

Director of Defense Research, EDAM & Non-Resident Senior Fellow, Hudson Institute

MODERATOR

Sine Ozkarasahin

Defense Analyst, EDAM

PANEL III:

Red Team Tracker: EDT Trends in Russia, Iran and China

Despite Western sanctions, the Kremlin still has numerous trade routes that are open and lucrative. Russia can still freely trade with China and Iran, as well as most countries in Southeast Asia and Latin America. Blocking or limiting these routes will not be an easy fix, and needs a collective, Allied effort. Especially for Shahed kamikaze drone transactions, a significant share of the trade in question goes through the Caspian region. This hostile route is menacing and detrimental to both NATO and Ukraine.

In Russia, crowdfunding and volunteer efforts form an important part of indigenous UAS efforts, especially for the production of first-person-view (FPV) UAVs. At the time of writing, Russian civilian enterprises supply the Ministry of Defense with around 30,000 FPV drones per month. In an increasingly dronized battlefield, building a similar, counterbalancing capacity will be crucial for the West.

PANEL III:
Red Team Tracker: EDT Trends in Russia, Iran and China

Iran is benefiting from an extensive, international smuggling network to bolster its military prowess. This supply web serves both Tehran's disruptive military capability generation effort, as well as Iran's proxies such as the Lebanese Hezbollah and Hamas. Open-source intelligence suggests that Iranian drones crashed in Ukraine feature critical foreign equipment, even American components. Using Western technologies, the Islamic Revolutionary Guard Corps (IRGC) is projecting its military prowess across various theaters ranging from the Ukrainian battlefield to the ongoing war in Israel.

The West needs a new outlook on Iran. Rather than appeasement, this new understanding should be centered on defeating Tehran's offense-dominant regime. It should bolster intelligence efforts to counter Iran's global supply chain network and persecute the European / NATO suppliers involved in this malicious web.

While China is currently undertaking a significant military modernization effort, Beijing's EDT roadmap still has some overlooked vulnerabilities. These are mostly in areas such as building combat experience for its UAS, establishing strong subsea communications over long distances, interoperability and China's perceived weakness against spoofing. The West should capitalize on these loopholes, and prioritize these areas in its own EDT efforts to widen the technological gap at its advantage.

SPEAKERS:

Gurkan Cetin

Group Leader, Autonomous Systems and Robotics, HAVELSAN

Osman Okyay

CEO, Kale Group

Rear Admiral (Ret) Hasan Ozturk

Consultant, METEKSAN

Ugur Coskun

CEO, AATG (Former CEO of BITES)

MODERATOR

Dr. Can Kasapoglu

Director of Defense Research, EDAM & Non-Resident Senior Fellow, Hudson Institute

PANEL IV:

Turkiye's Way: Turkish Unmanned Systems Portfolio and AI Strategy

Besides the systems themselves, the concepts of operation (CONOPS) these technologies are used in is equally significant. Apart from exporting UAVs, Ankara also already transferred the 'Turkish way of drone warfare' to Azerbaijan, as well as friends of NATO including Ukraine.

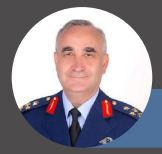
Amongst the Allied efforts on unmanned systems and network-centric warfare, the 'digital troops' concept is an important initiative that stands out within the Turkish defense technological industrial base (DTIB). Based on the joint use of UAVs, USVs and UGVs, the principle is built on the idea of creating a networked 'orchestra of unmanned systems'. Moving forward, the initiative in question can provide an important foundation for the Alliance's multi-domain unmanned combat operations.

PANEL IV:
Turkiye’s Way: Turkish Unmanned Systems Portfolio and AI Strategy

Turkish USV solutions such as MARLIN have proved themselves in NATO exercises. Building on the lessons learned from Ukraine, Türkiye’s burgeoning success in the naval domain can bolster the Black Sea littoral member states’ offensive capabilities against Russian aggression in the region.

Another area necessitating an intra-Alliance cooperation is the establishment of a legal / regulatory framework governing the proliferation and use of unmanned technologies. Any future effort should be built on a human-in the-loop structure, as the human element continues to be a crucial element of unmanned combat operations.

SPEAKERS:

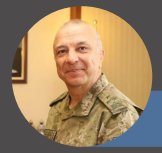


Lt. Gen. (Ret) Nihat Kokmen

Former Military Representative of Türkiye to NATO

Ambassador (Ret) Fatih Ceylan

Chairman of Ankara Policy Center



Lt. Gen. (Ret) Yavuz Turkgenci

Former Turkish Third Army Commander

MODERATOR

Sinan Ulgen

Director, EDAM & Non-Resident Senior Fellow, Carnegie Europe

PANEL V:

Lessons Learned for NATO and the Way Forward

Cyberattacks and hacking incidents are climbing fast. Therefore, shielding our defense production supply lines, R&D initiatives and sensitive communications against such threats becomes a strategic priority. Potential areas to focus on include quantum-resistant or post-quantum cryptography and the protection of critical national infrastructure such as underwater and underground structures.

AirLand battles and dogfights are rapidly fading away from the battlefield. In the coming years, the main arenas of contestation will be the information domain and space (exo-atmospheric technologies).

Tomorrow's wars will be mostly sensor-driven. In the FOE, multi-domain sensor fusion will be key in various domains including early threat detection, monitoring and process control.

PANEL V:
Lessons Learned for NATO and the Way Forward

Opening PESCO projects to NATO member countries' participation will be paramount in building a strong and collective Western EDT capability. Such a policy decision will also pave the way for deepened EU – NATO cooperation.

Military-technological partnerships should not be one-sided, centered on a top-down approach where one country develops a system and sells it to another. Instead, the Alliance should prioritize interoperability and encourage collaborative projects. Next, it should provide an oversight for the efficient and swift implementation of the chosen initiatives.

Moreover, investment in strategic communication (StratCom) and defense intelligence will be key to adapting NATO's key elements and resources to enhance predictive intelligence capabilities, particularly in the area of defense technologies and the military application of AI.

Ekonomi ve Dış Politika Araştırmalar Merkezi

edam

GCSP
Geneva Centre for Security Policy

NATO OTAN

This workshop is supported by:

The NATO Science for Peace and Security Programme