Dr. Franjo Tuđman Defense and Security University
Royal Norwegian Embassy in Zagreb
UTSYN – Center for Security and Resilience
with the support of
KONGSBERG DEFENCE & AEROSPACE

***Conclusions and Recommendations***

**HYBRID THREATS AND CYBERSECURITY**

Roundtable on Protecting Populations and States from Hybrid Threats in the Domain of Information Influence Operations and Critical Infrastructure Protection

***Summary***

The roundtable on protecting populations and states from hybrid threats in the domain of information influence operations and critical infrastructure protection highlighted the need for cooperation within NATO and, in particular, institutional collaboration between Croatia and Norway Strengthening economic ties with allied nations contributes to securing and enhancing the reliability of supply chains. Trade, industrial cooperation and R&D cooperation between Norway and Croatia offers significant mutual benefits for both states. By advancing collaborations between Croatia(n) and Norwegian entities such as Kongsberg in this initiative, the groundwork is laid for broader and more enduring partnerships between the two allied nations.

Special emphasis was placed on the collaboration of academia and non-governmental organizations to address the increasingly pronounced threats posed by hybrid threats and disinformation. Results of analyzed strategies that have proven effective, as well as those that have not made the desired outcomes, offer an opportunity to draw meaningful lessons. There is no universal approach to fostering resilience, and as each country explores and tests various practices, the insights gained from these efforts can be mutually beneficial.

A particular focus was placed on critical infrastructure protection (CIP), primarily maritime and underwater infrastructure, digital systems, and critical points. To effectively implement CIP, alignment of protective systems at the national and NATO levels is necessary, along with the adoption of the Total Defense concept, which entails a high level of readiness of the state and all stakeholders in the national and homeland security systems to effectively respond in situations of war, crises, and disasters.

When discussing specific examples of hybrid threats, cognitive warfare, sabotage, and information-communication manipulation, Russia was identified as primary sources of Europe’s security challenges. In Southeastern Europe and the WB6 countries regional actors facilitating Russian malign actions represent an additional risk.

Actively identifying and addressing societal anomalies resulting from hybrid actions - especially disinformation and targeted manipulation of individuals as fundamental societal elements - must be an imperative. Strategic education, regulation, and the coordination of defensive activities are crucial in this regard.

Security challenges in the digital sphere, such as GPS signal interference in countries bordering the Russian Federation, underscore the need for increased investment and the development of new, advanced innovations in protective mechanisms. Strategic action at all levels is realized through active communication and knowledge transfer, making strategic communication and information exchange vital for an effective response to all challenges. Credible, truthful, and cooperative communication, strategic information sharing, and interoperability across all societal sectors are fundamental needs.

The protection of underwater critical infrastructure requires intensive bilateral cooperation between Croatia and Norway across all fields (military, intelligence, scientific, and technological), which would result in the development and implementation of automated systems for early threat detection. Conducting joint military exercises is essential in this context.

Finally, given the overall expansion of digital space, social networks, and media that enable the rapid dissemination of news and significantly influence younger generations - future policymakers - it is necessary to strengthen trust in national, European and transatlantic institutions to safeguard democracy and maintain a healthy approach to socio-political processes.

Conclusions:

1. **Increasing investment in CIP at the national level** – with joint measures and active exchange of experiences at the NATO alliance level – through the establishment of a special joint body for CIP. This body, through the coordinated efforts of all sectors (military, intelligence, etc.), and particularly through joint financial and material initiatives, would develop new and harmonized systems for CIP.
2. **Enhancing societal resilience against hybrid threats** – in addition to existing fact-checking systems, new approaches should be developed (e.g., TV programs, radio shows, educational initiatives in schools, fostering critical thinking, etc.) to penetrate all segments of society, particularly the most vulnerable groups significantly affected by disinformation efforts. An outstanding example is *The Anatomy of Disinformation*, a Polish TV program that highlights cases of disinformation and their harmful impacts. Furthermore, consideration should be given to introducing new regulations in the digital space to prevent data misuse and manipulation within the information environment. Coordination between allies on messaging and choice of platforms will increase the effectiveness of our efforts.
3. **Strategic communication, knowledge creation, exchange, and information management**

Knowledge Creation – Encompasses scientific and research activities focused on hybrid threats and the development of both reactive and proactive responses to them.

Knowledge Exchange – Refers to the dissemination of knowledge through scientific and research platforms, as well as among direct and indirect stakeholders.

Knowledge Communication – Involves delivering key findings and guidelines to external stakeholders (e.g., the public, institutions, media, etc.).

1. **Strengthening trust in institutions** – revising strategies and complementary approaches at national, European and transatlanticlevels to enhance transparency in communication with citizens.
2. **Incorporating the total defense concept into curricula** - introducing elements of defense, security, and resilience into existing and new study programs, with an emphasis on the synergy between the public, private, civil, and military sectors.