

Eurocapitales webinar on 5 December 2025 on the theme of “The challenge of cyberattacks and hybrid interference in Europe”

Summary of the speech of Tapio Pyysalo: Countering hybrid attacks

The Role of Cities and Capitals in Countering Hybrid Threats

The speaker, who is the head of international relations at the Hybrid CoE (Centre of Excellence), begins by expressing enthusiasm for discussing hybrid threats and the crucial role that cities and capitals play in countering them. The presentation aims to provide an overview of hybrid threats as a phenomenon, highlight recent examples across Europe, and offer insights into effective countermeasures.

Introduction to Hybrid Threats and the Hybrid CoE

The Hybrid CoE is an international organization with 36 participating states, including all EU and NATO members. Unlike NATO Centres of Excellence, it is exclusively open to EU and NATO countries, not to partner nations. The speaker looks forward to hearing perspectives from representatives of Austria and France, both of which are participating states.

The Growing Challenge of Hybrid Threats

Hybrid threats have become a daily challenge for European countries, with a significant increase in both frequency and severity over the past year. The speaker cites recent statements from German Chancellor Designate Mertz and French President Macron, who both emphasize the heightened seriousness and assertiveness of hybrid threats, particularly from Russia. These threats include cognitive warfare, information warfare, cyberattacks, and sabotage, often targeting key countries like Germany and France. The borderless nature of these threats—whether in cyberspace, online disinformation, or the recruitment of physical saboteurs—makes them especially difficult to counter.

Historical Context and Definition

Hybrid threats are not new; they have existed as long as warfare itself, but their use has become more active and assertive in the current security environment. The term “hybrid threats” emerged in the late 1990s and refers to the coordinated use of multiple distinct elements to undermine stability and security. These threats often exploit systemic vulnerabilities, use proxy actors to evade detection and attribution, and test the boundaries between war and peace. They are designed to challenge democratic values, principles, and institutions.

Key Drivers of Hybrid Threats

Several factors contribute to the rise of hybrid threats:

- **Geopolitical Competition:** Intensifying rivalry, especially with China’s growing economic and political influence, and ideological competition between authoritarian and democratic systems. Both Russia and China seek to reshape the global order using hybrid tactics.
- **Global Instability:** Proliferation of conflicts within and outside Europe, such as the war in Ukraine, which often spill over and affect other countries through hybrid means.
- **Technological Developments:** While technology can help counter hybrid threats, it also creates new vulnerabilities. For example, AI can amplify disinformation, and drones can challenge conventional defenses. Social media, as a primary news source for many, is particularly vulnerable to disinformation campaigns, with up to 80% of false information spread through these platforms.
- **Cost Efficiency:** Malign actors can cause significant harm at minimal cost compared to conventional warfare, especially when unconstrained by democratic or legal boundaries.

Recent Examples and Trends

The speaker highlights several recent trends in hybrid threats:

- **Disinformation:** Used to undermine internal stability and divide populations, both within the EU and NATO and between Europe and its international partners. Artificial intelligence is increasingly used to contaminate large language models with fake news, making media literacy and public awareness crucial.
- **Instrumentalization of Individuals and Organizations:** Hybrid actors use proxies—such as hired agents, sympathizers, politicians, migrants, religious organizations, and research networks—to conduct sabotage, espionage, and influence campaigns.
- **Economic Coercion:** Russia, for example, focuses on circumventing sanctions through shadow fleets and shell companies, and cooperates with other actors on military and dual-use exports.
- **Sabotage of Critical Infrastructure:** Targeted attacks aim to disrupt, intimidate, and hamper support for Ukraine. Cities and capitals are often the first responders in these situations.
- **Assertive Military Activities:** Includes airspace violations by drones and balloons, joint military exercises, and the use of private military companies.
- **Election Interference:** Hybrid actors seek to influence elections to steer countries in new directions, as seen in attempts to interfere with the European Parliament elections and national elections across Europe.

The Role of Cities and Capitals

Cities and capitals are on the front lines of countering hybrid threats. They are responsible for first response (e.g., police, fire departments), building resilience in critical infrastructure, and fostering societal preparedness. The speaker stresses the importance of media and digital literacy, situational awareness, and networks for intelligence sharing among cities and capitals.

Countering Hybrid Threats: Strategies and Recommendations

To effectively respond to hybrid threats, the speaker recommends:

- **Joint Situational Awareness:** Improving detection, identification, and attribution of threats, and deciding on appropriate countermeasures. Cities and capitals should be integrated into national intelligence-sharing networks.
- **Building Resilience:** Through legislation, societal preparedness, and long-term cultural or systemic changes, such as media literacy programs in schools.
- **Deterrence:** Resilience deters attacks by denying benefits to the threat actor (deterrence by denial), while credible countermeasures impose costs (deterrence by punishment).

Conclusion Hybrid threats are becoming more aligned and assertive, requiring coordinated and proactive responses. Cities and capitals have a vital role in building resilience, fostering situational awareness, and implementing effective countermeasures to protect democratic values and institutions.