



Why is it necessary to pay attention to hybrid threats?

Background and Rationale of the Micro-Credential Course in Countering Hybrid Threats

Hybrid threats are one of the emerging security challenges with the potential to shape the future of the continent in the worst-case scenario. They are defined by the European Union as actions that use diplomatic, military, economic and technological tactics to destabilize a political opponent. Pressure, disinformation, and criminal use of Communications and Information Systems (CIS) are some examples of hybrid threats. They are designed to be difficult to detect or attribute.

Hybrid threats have not only come to stay, but they are also endlessly evolving: the so-called hybrid toolbox is constantly being updated. Some examples of hybrid attacks affecting the European Union are the referendum on the status of Crimea; the sudden massive influx of illegal migrants from the Russian Federation across the Arctic border into the Kingdom of Norway and the Republic of Finland; the situation in which the Belarusian authorities created an artificial migration crisis, also, the increasing frequency of deliberate disruptions targeting underwater critical infrastructure, attributed to so-called “shadow fleet” activities. These are some of the examples of neighbouring countries demonstrating their ability to use the movement of people to increase their political and economic leverage over the Union, primarily against Lithuania, Latvia, Poland, Finland and Estonia.

Russia's propaganda narratives and conspiracy theories show Russia as a hero in the COVID crisis aiming to show that the West could not cope with the crisis etc. The methods for achieving the hybrid effect are different and are usually used simultaneously. While cyber-attacks, customs restrictions, political pressure or fake news can be considered direct hybrid attacks, there are also more covert methods such as the use of local sanctions, soft films, music videos or books, children's summer camps, etc.

Awareness of hybrid threats and the development of resilience are continuously being developed, both within the European Union institutions and in cooperation with various partners. There is more common language and mutual understanding in this area than ever before. However, it covers a high political level, but does not cover all areas of hybrid threats and needs wider, knowledge-based dissemination. These threats are no longer a problem for just one, neither is the solution. Interoperability evolves in an efficient path only if all actors get involved in the creation of the new tools and solutions, all the players acting in the game. All agents should speak the same language and act as one single strong answer to the citizens.

Hybrid threat research, up-to-date training and public awareness are of key importance to combating hybrid threats. Officials and decision-makers, as well as businesses, senior executives and the public who are aware of and understand the dangers, are our strength and improve our resilience to hybrid threats.

Some specialities related to the handling of hybrid threats are taught in universities of the European Union Member States, as well as in applied law and defence training institutions, but these studies are either military-oriented or closed, with only a small part of the entire

curriculum and open access. Hybrid attacks affect and can paralyze society as a whole or individual parts of it, either at a national or regional level. There is a broad understanding in the European Union of the challenges we face in the form of hybrid threats. Development of a Joint Micro-Credential Programme in Countering Hybrid Threats jointly in different universities in the European Union corresponds to the needs of the current and future security environment. This cooperation created a platform for exchanging experiences and enhancing competence by providing up-to-date knowledge and the critical analytical and administrative capacity at the strategic level, which is essential for making complex management decisions in a changing society, including in countering hybrid threats.