Background note

Session I: Protection and securing the European Union. Hybrid threats as an external factor destabilising Europe

Introduction

The European Union is a unique supranational organisation, unlike any other contemporary or historical counterpart, founded on the values of democracy, rule of law, tolerance, pluralism, respect for human rights and other principles. The values of the EU also constitute the basis for the principles and institutions including loyalty and cooperation, respect for the political and constitutional structures of individual states, the free market, cooperation, dialogue and consensus. An organisation based on values, principles and ideals, is particularly vulnerable to various forms of destabilisation and threats. That is why, mechanisms to safeguard it from destabilisation, weakening of its axiological attractiveness and internal cohesion, as well as its ability to be proactive and counteract threats are so important.

Building resilience is a key task for the EU. In addition to the full-scale conflict in Ukraine, the EU faces many other, less obvious threats. They jeopardise the unity of the European Union and its ability to act and, in some cases, they also question its fundamentals. What is more, they always erode public trust by removing the equation mark between morality and strength, which is defined as vitality, capability to take effective actions, resilience to threats and challenges.

The possibilities for hybrid activities seem endless. They may target political and diplomatic spheres as well as, disinformation propaganda, as well as economic, cultural, social, military and humanitarian spaces. Hybrid threats are diverse and constantly changing. They can be carried out by special service agents of a foreign state and individuals cooperating with them as well as - knowingly or not - by organisations, associations, institutions, political parties, companies, corporations or celebrities. It should be noted that the characteristic feature of hybrid activities is that they are usually difficult to be clearly categorised and to hold the perpetrators accountable. This causes difficulty in their initial identification and definition.

Latest developments

In 2016, in the Joint Framework on Countering Hybrid Threats, the European Union defined hybrid threats as *"the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be*

used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare.' They can be used to pursue a variety of strategic, operational and tactical objectives, the common denominator of which is to destabilise individual Member States and the Community as a whole and to interfere in their political, social and economic processes.

The Union's flexible approach to this issue stems from the nature of the phenomenon, which is complex, multifaceted and ambiguous, and reflects the different security perspectives and foreign policy priorities of individual Member States. This approach makes it possible to take into account both threats from the East (Russia, Belarus) and South (Iran, terrorist organisations, irregular migration), as well as global ones (China). The catalogue of hybrid methods and tactics includes disinformation and propaganda activities, cyberattacks, interfering with political processes (elections and referenda), economic pressure, orchestrated irregular migration, state support for armed groups and mercenaries, intelligence operations focused on diversion and sabotage, terrorism or the use of chemical, biological, radiological and nuclear (CBRN) weapons. Since 2015, the EU has been experiencing hostile hybrid activities originating mainly from Russia. To a lesser extent - but with a clear upward trend - such methods are also used by Belarus, Iran and North Korea, as well as terrorist organisations and radical groups.

Hybrid methods can be used to varying extents and intensities, and can be freely combined by state or non-state aggressors with different modes of operation. Moreover, the catalogue of hybrid warfare tools is open-ended. In the assessment carried out by EU institutions, its expansion is based on the intensifying political rivalry involving Russia (especially in the aftermath of the invasion of Ukraine) and China, the unstable situation in the EU's neighbourhood and the so-called weaponisation of key sectors (healthcare, climate and environment).

Since 2016, the EU has been developing capabilities to counter hybrid threats in four areas: 1) situational awareness, 2) resilience building, 3) prevention and crisis management, and 4) international cooperation (especially with NATO). The EU Strategic Compass calls for the strengthening of these capabilities as part of the Union's coordinated response to crises caused by hybrid threats and, above all, the creation of new mechanisms and their reliable implementation. The burden of responsibility for combating hybrid threats currently lies with national security institutions(as per Article 4(2) TEU), i.e. special services, police and military, which have the legal authority and enforcement powers to do so. The Strategic Compass makes no changes in this area. In order to foster synergies and achieve a more effective response, the instruments being developed in the EU Hybrid Toolbox are instead intended to provide greater support to national efforts aimed at combating hybrid threats and coordinating joint action by states.

Bolstering the resilience of EU Member States and their societies is aimed at reducing vulnerability to hostile disinformation and propaganda as well as strengthening the protection of critical infrastructure against cyberattacks, terrorism, diversion and sabotage. The Strategic Compass focuses particular attention on strengthening the EU's resilience against foreign information manipulation and interference in political processes.

The approach to combating information manipulation in the EU comprises four elements adopted by the European Commission in December 2018 in *The Action Plan against Disinformation*: 1) enhancing the capacity of EU institutions to detect, analyse and expose disinformation; 2) strengthening coordinated and collaborative responses to disinformation; 3) mobilising the private sector to combat disinformation; and 4) raising awareness and improving public resilience by supporting independent journalism, *fact-checking* initiatives and promoting media education.

In response to Russian disinformation and psychological campaigns, a task force - *East StratCom* - was created in 2015 as part of the European External Action Service to monitor, analyse and respond to Russian propaganda and disinformation. Initially employing only three staff members, now the team consists of 16 full-time employees, which best demonstrates the importance of this unit in the EU. *East StratCom* monitors news published in more than 20 languages. The team identified tens of thousands of cases of Russian disinformation, which were catalogued in the *EUvsDisinfo* database. The team also provides training for personnel of the partner states, works to strengthen independent journalism and promotes the knowledge about the EU and its policies in the Eastern Partnership countries. Similar tasks are carried out by other teams (six full-time staff members each) established in 2017, responsible for the Western Balkans region (Western Balkans Task Force) and the Middle East and North Africa region (South Stratcom Task Force), which focus on countering radicalisation, combating propaganda disseminated by terrorist organisations, and disinformation inter alia from Russia, and Iran. All these teams are part of the Strategic Communication, Task Forces and Information Analysis section of the European External Action Service, which supports the EU institutions with policy planning, strategy and strategic communication tools. It also provides support (including analyses and instructions to combat disinformation) to EU diplomatic missions and operations of the common security and defence policy (CSDP). The section is also developing partnerships with partner states, the G7, NGOs, civil society organisations and the private sector, concerning data collection using modern software and technology. The aim of these activities is to build public awareness and strengthen states' resilience to disinformation in the EU neighbourhood.

Cooperation between the European Union and NATO on strategic communication aims to ensure effective messaging and joint action in response to security challenges. The interaction of the EU's East StratCom unit with the NATO Strategic Communications Centre of

Excellence (NATO StratCom COE) based in Riga is an example of such cooperation. The main objectives of this cooperation include sharing expertise and best practices, enabling complementarity in analysing and countering disinformation. In addition, the coordination of activities in the areas of strategic communication and cyber security fosters synergies. Such cooperation is crucial in a complex and dynamically changing geopolitical landscape.

Building the resilience of EU states also concerns key sectors such as cybersecurity, critical infrastructure, energy, transport, defence, the financial system, maritime security and space. This effort is primarily oriented towards the creation of legal instruments and capabilities to respond to incidents and crises caused by hybrid threats (especially in cyberspace). A breakthrough in the EU's approach to cybersecurity was the adoption of the Directive on security of network and information systems (the so-called NIS Directive) in 2016. It obliges states to ensure a minimum common standard of cybersecurity, including through the adoption of national cybersecurity strategies or the creation of computer incident response teams, which will operate as part of the European CERT network. The EU has also imposed cyber incident reporting requirements on key service providers in the energy, transport, banking and finance, health, water supply and digital infrastructure sectors. Through the European Network and Information Security Agency (ENISA) and the European Cyber Security Organisation (ECSO), the EU also supports research and public-private cooperation in addition to regulation efforts. States' cyberdefence capabilities are developed through four PESCO structural cooperation projects, which address cyber incident information sharing, coordination of operations, support and joint response, as well as research and training. In December 2020, the EU adopted a new cyber security strategy to make states more resilient to cyberattacks and better protect critical infrastructure. An example of sectoral action in this area is the EU Cyber Diplomacy Toolbox adopted in order to deter potential cyber-attackers. In May 2019, the EU established a sanctions regime to respond to cyberattacks perpetrated by third country actors against Member States using infrastructure located outside the Community. Blacklisted entities responsible for or supporting cyberattacks against EU Member States will be banned from entering the EU or have their assets frozen. A similar sanctions regime has been introduced against states that use chemical weapons (the classified list contains 20 substances), which is the EU's direct response to the use of the Novichok paralysing agent on the UK soil by Russian secret services. Between 2019 and 2022, the EU also provided financial support with a total value of €11.6 million to the Organisation for the Prohibition of Chemical Weapons (OPCW) for work against the development and use of chemical weapons.

Challenges

The challenges of building the resilience of the EU and its Member States stem mainly from the hybrid nature of the activities deliberately and intentionally taken by actors who, for various reasons, want to undermine the cohesion of the Union and its efforts. The nature of hybrid threats and the fact that they are multi-directional, conducted covertly using a variety of means and changing over time, is a key challenge for the EU.

A challenge that has been apparent for quite some time now is the complexity of hybrid threats. Despite the fact that the EU has identified a catalogue of hybrid warfare tools, establishing the full taxonomy remains difficult due to their variability and multifaceted nature. The second key challenge is the anticipated increase in the number of sectors susceptible to the so-called weaponisation (including energy security, health, information, climate change, environmental protection or new technologies related to artificial intelligence). This means that there is a growing number of so-called strategic sectors that could become a potential target for hybrid attacks. Moreover, the Baltic Sea region is a good illustration of how hybrid activities are multidirectional and dangerous. It shows that hybrid warfare perpetrated by Russia includes the so-called shadow fleet, sabotaging the telecommunications network, jamming the GPS signal and ecological threats.

The approach to combating hybrid threats adopted by the European Union focuses only on their non-military dimension (i.e. disinformation, propaganda, cyberattacks), and is characterised by insufficient development of a military response capability when the full spectrum of hybrid activities (including military or paramilitary ones) is deployed against it. For this reason, the Union should consider what the role of the *Rapid Deployment Capacity* could be during a hybrid crisis on the territory of its Member States, which would send a clear signal to the aggressor that further escalation of the situation would meet a strong response. These actions should be undertaken in agreement with NATO, based on the principle of complementarity between the two organisations and at the same time they should strengthen the European pillar of the Alliance.

Moreover, deploying instruments that are already in place seems to remain an important challenge for the EU. The EU should clearly define the conditions for the use of solidarity or mutual assistance clauses. This would enhance the security of Member States, which could count on the cohesive action of both the EU and NATO (which is particularly important since the EU explicitly declares close cooperation with NATO in combating hybrid threats). The ambiguous nature of hybrid threats creates the risk of different interpretations of the crisis situation, prolonging decision-making processes at the EU level and thus slowing down the response or making it inadequate. These can be minimised by developing solutions through simulations and exercises both within the EU and in cooperation with NATO, based on

real-life hybrid crisis scenarios. They should also take into account possible future forms of attacks using new methods and tactics.

Discussion points

1. Can the EU effectively prevent hybrid threats instead of being reactive?
2. How to combat disinformation and propaganda, whilst safeguarding freedom of speech and pluralism?
3. How to effectively inform the general public of hybrid threats?
4. Are the existing EU tools sufficient to combat hybrid threats, or are new solutions needed?
5. How can artificial intelligence be used to destabilise the EU and how can we defend against this?
6. How to protect key elements of the democratic system from external interference?
7. How to maintain democracy and the rule of law while strengthening the EU's resilience?