Social Economic Debates
Volume 9, Issue 2, 2020
ISSN 2360-1973; ISSN-L 2248-3837

EUROPEAN UNION SECURITY - IMPORTANT PREMISES FOR THE PERIOD 2020 – 2025

Mădălina SPERLEA (POPESCU BORDENI)
"Alexandru Ioan Cuza" POLICE ACADEMY, Bucharest, Romania
Email: madisperlea@yahoo.com

Abstract: The European Union, its institutions and its state members have worked to promote and ensure freedom and security. Europe guarantees respect for human rights, the rule of law and solidarity. As Europeans we have the right to live, work and live in other countries than ours. The abolition of internal border controls in the Schengen area was a major step forward for Europe. In addition, technological progresses have revolutionized the ways and speed of communications, which has led to the opening not only of our borders but also of our societies. For the EU members, security is one of the main priorities. The EU's multiannual work programs have provided a solid and concrete basis for strengthening operational cooperation, but there is now a need to build a broader consensus on the vision, values and objectives which stands for EU internal security. The main risks and threats Europe is facing today, such as terrorism, serious and organized crime, drug trafficking, cybercrime, trafficking in human beings, sexual exploitation of children and child pornography, economic crime and corruption, arms trafficking and cross-border crime they are adapting extremely quickly to the evolution of science and technology, in their attempt to illegally exploit and undermine the values and prosperity of our open societies.

Key words: freedom, security, vulnerable groups, crisis, responsibility.

JEL Classification: H56.

1.Introduction

In its political guidelines, the EU Commission stated that nothing should be overlooked to protect citizens. The security it's not important only at personal level, but also protects the fundamental rights and forms the basis of confidence in our economy, society and democracy as well as the foundation of their dynamism. Today, the Europe's security situation continues to change, influenced by evolving threats and other factors, including climate change, demographic change and political instability outside our borders. Globalization, free movement and digital transformation continue to bring prosperity, make our lives easier and stimulate innovation and growth. However, along with these benefits, they also present risks and costs. They can be used improperly for the purposes of terrorism, organized crime, drug traffic and human traffic, which represents as direct threats to citizens and to our European way of life. Cyberattacks and cybercrime continue to rise. Security threats are becoming more and more complex: they feed on the ability to act across borders and interconnectivity, take advantage of the vagueness that now characterizes the boundaries between the real world and the digital world, and exploit vulnerable groups and socio-economic differences.

Attacks can occur at any time and leave very few or no traces; what happens outside the EU can have a critical impact on security inside the EU.

The COVID-19 crisis has also changed our understanding of security threats and related policies. She pointed out the need to ensure security in both the physical and digital environment, she pointed out the importance of open strategic autonomy of supply chains for critical products, services, infrastructure and critical technologies. It has strengthened the need to involve everyone from every sector in a joint effort to ensure that the EU is better prepared and resilient and has better tools to respond when needed.

Individual action alone by Member States it is not enough to protect citizens. The mutual exploitation of strengths to work together has never been more important, and the EU is more able than ever to make a difference. It can be an example by improving its overall crisis management system and working inside and outside its borders to contribute to global stability. While the main responsibility for security lies with the Member States, last few years have brought new perspectives on the understanding that the security of one Member State is the security of all. The EU can provide a multidisciplinary and integrated response, providing Member States' security actors with the tools and information they need.

The EU can also ensure that political security remains based on our common European values, i.e. on respect for the rule of law, equality and fundamental rights, and the guarantee of transparency, responsibility and democratic control, in order to build the necessary trust. It can establish a real and efficient security union, characterized by adequate protection of individual rights and freedoms. Security and respect for fundamental rights are not contradictory goals; these two elements complement each other and form a consistent whole. Our fundamental values and rights must be the base of our security policies, which must respect the principles of necessity, proportionality and legality and be accompanied by adequate guarantees of liability and judicial remediation, while enabling us to react effectively to protect citizens, especially the most vulnerable.

Important legal, practical and supportive tools already exist, but they need to be strengthened on one hand and better implemented on the other. Considerable progress has been made in improving the exchange of information and cooperation with Member States to restrict the scope for action of terrorists and criminals. But efforts remain fragmented.

Also we must act beyond the EU borders. In order to protect the Union and its citizens, it is no longer just a matter of ensuring security within the EU borders, but also handling the external dimension of security. The EU's approach to external security within common foreign and security policy and defense will remain a key component of the EU's efforts to strengthen security within it. In the face of common challenges, it is essential to cooperate with third countries and globally in order to respond efficiently and comprehensively, stability and security in the EU's neighborhood being essential for EU security. This new strategy, which base on the previous activity of the European Parliament, Council and Commission, shows that a real and efficient Security Union must be based on both a solid core of instruments and policies to ensure security in practice and consider that security has implications for all parts of society and for all public policies. The EU must ensure a safe environment for all, regardless of their racial or ethnic origin, religion, beliefs, gender, age and sexual orientation.

This strategy covers the period 2020-2025 and focuses on building the means and capacity to create a resilient security environment for the future. It presents a company-wide approach to security that allows for an effective and coordinated response to rapidly evolving threats. It sets out strategic priorities and adequate actions to deal with digital and physical risks in an integrated manner in the Security Union ecosystem, focusing on areas where the EU can provide support. Its purpose is to achieve tangible security results in order to protect all EU citizens.

2. Research Methodology

The discipline of security sciences now incorporates the liberal arts, social and political sciences, as well as the hard sciences. The amalgamation of so many diverse disciplines requires the adaptation and adoption of research methodologies that can accommodate this evolution.

This work argues on the use of the method of studying laws, provisions and directives based on recent research in security science.

The need of understanding the multiple parameters that may be present when dealing with security issues requires a methodology that can contextualize the issues studied and help to understand the potential present synergies. The use of laws, provisions and directives is one such approach that can provide an accepted alternative academic approach. However, an important step when using them is to first use what is commonly called a pilot study, before starting full data collection.

There is a significant number of reasons why this should be taken; last but not least is the significance of maintaining transparency throughout the process if it’s desired to maintain its validity. The correct realization of the study design is crucial at the beginning, if the effort must not be wasted or does not have the final legitimacy.

The benefits of pursuing such a methodology have been presented, as it provides another way to perform security science research.

3. RESULTS

Evolving security threats in Europe

For the security, prosperity and well-being of citizens, it is essential that they are protected from getting harmed. Threats to their security depend on the degree of vulnerability of their existence and their livelihoods. The greater their vulnerability, the greater the risk that it can be exploited. Vulnerabilities and threats are constantly evolving and the EU needs to adapt.

Our daily lives depend on a variety of services, such as energy, transportation, finance, and health. These services are based on both physical and digital infrastructures, which increases their vulnerability and potential for disruption. During the COVID-19 pandemic, new technologies made it possible for many companies and utilities to continue to operate, whether they provide us with the means to stay connected by teleworking or by maintaining supply chain logistics. However, they have also opened the door to an extraordinary increase in malicious attacks, as their perpetrators try to capitalize on pandemic disruptions and the transition to work at home using digital technologies for criminal purposes. The lack of goods has opened up new opportunities for organized crime. The consequences could have been fatal, disrupting essential health services when they were subjected more than ever.

The unceasing overgrowth use of digital technologies that are useful to us on a daily basis has also made the cyber security of these technologies a matter of strategic importance. Homes, banks, financial services and enterprises (especially small and medium-sized enterprises) are severely affected by cyberattacks. The potential damages are even bigger as the physical and digital systems are interdependent. any physical consequence will imperatively have an impact on digital systems, while cyberattacks targeting information systems and digital infrastructures can lead to the closure of essential services. The internet development and the increased use of artificial intelligence will bring new benefits, but also new risks.

Our world is based on digital infrastructure, technologies and online systems, which allow us to create economic activities, consume products and benefit from services. These infrastructures, technologies and systems are based on communication and interaction. Addiction to online systems has opened the door to a wave of cybercrime. On-demand cybercrime and the underground cybercrime economy provide easy access to online cybercrime products and services. Criminals are rapidly adapting to use new technologies for their own purposes. For example, the counterfeit medicines have entered the legal supply chain. The exponential growth of online child pornography shows the social consequences of the evolution of crime. Most EU citizens were concerned about access to their data by criminals and fraudsters.

The global context also exacerbates these threats. The offensive industrial policies of certain third countries, combined with the constant theft of intellectual property facilitated by the Internet, are changing the strategic paradigm of protecting and promoting European interests. This situation is accentuated by the proliferation of dual-use applications, the robustness of the civil technology sector becoming a solid asset in terms of defense and security capabilities. Industrial espionage has a huge impact on the EU's economy, jobs and growth: the theft of commercial secrets is estimated to cost the EU EUR 60 billion. Therefore, there is a need for further reflection on how dependences and increased exposure to cyber threats affect the EU's ability to protect citizens and businesses. The COVID-19 crisis has also shown that social divisions and uncertainties create security vulnerabilities. They open a wider door to more sophisticated and hybrid attacks by state and non-state actors, with vulnerabilities exploited through a combination of cyberattacks, critical infrastructure damage, disinformation campaigns and action. Radicalization of political speech.

At the same time, older threats continue to evolve. There has been a decrease in terrorist attacks in the EU in 2019. However, EU citizens remain at high risk of jihadist attacks by or inspired by Daesh, Al Qaeda or their affiliated groups. At the same time, the threat of violent right-wing extremism is growing. Racist attacks must raise serious concerns: deadly anti-Semitic terrorist attacks in Halle reiterate the need to step up response in line with the 2018 Council statement. One in five EU citizens is very concerned that a terrorist attack could take place in the next 12 months. The vast majority of recent terrorist attacks were based on low technology and were carried out by isolated actors targeting people in public spaces, while online terrorist propaganda took on new significance with the live broadcast of the Christchurch attacks. The threat posed by radicalized people remains high and is potentially heightened by the return of foreign terrorist fighters and the release of detained extremists. The crisis has also shown that existing threats can change with the circumstances. Organized crime groups have taken advantage of the lack of goods to create new illegal markets. Drug traffic continues to be the largest criminal market in the EU, with illicit drug retail sales estimated at 1 billion EUR per year. International trade in counterfeit pharmaceuticals has also reached billions. At the same time, low confiscation rates allow criminals to continue to expand their criminal activities and infiltrate the legal economy.

The online marketplace and new technologies such as 3D printing make it easier for criminals and terrorists to access weapons. The use of artificial intelligence, new technologies and robotics will further increase the risk of criminals using the benefits of innovation for malicious purposes. These threats cover different categories and affect different parts of society in different ways. All represents a major danger to citizens and businesses and require a comprehensive and coherent response at EU level. At a time when security vulnerabilities can come from even small, interconnected home appliance items, such as an internet-connected refrigerator or coffee maker, we can no longer rely only on traditional state actors to guarantee security. Economic operators must take greater responsibility for the cyber security of the products and services they place on the market, while citizens must also have at least basic cyber security concepts in order to protect themselves.

Conclusion

The EU has shown that it can provide real added value. Since 2015, the Security Union has created new connections in the way security policies are approached at EU level. However, more efforts are needed to mobilize society as a whole, including public authorities at all levels, businesses in all sectors and citizens in all member states. Increasing awareness of the risks of dependence and the need for a strong European industrial strategy requires a European Union with a critical mass of industrial and technological production and a strong supply chain. Strength also requires full respect for fundamental rights and EU values, which is essential for security policies to be legitimate, effective and sustainable. This strategy of the security union sets out concrete lines of work to be followed. It is built around the following common goals:

- strengthening the means and capacities for early screening, prevention and rapid response to crises: Europe needs to be more resilient to prevent future shocks, to protect against these shocks and to withstand them. We need to strengthen our means and capabilities for early detection and rapid response to security-threatening crises, using an integrated and coordinated approach, both globally and through sectoral initiatives (for the finance, energy, justice, law enforcement, healthcare, maritime security and transport sectors, for example) and on the basis of existing instruments and initiatives. the Committee will also present proposals for a comprehensive crisis management system in the EU, which could also be useful in the field of security;

- focus on results: a results-based strategy must be based on a careful assessment of threats and risks so that efforts can be best directed. It must define and use the appropriate rules and tools. It must be ensured that EU security policies are based on reliable strategic information. When the EU needs to legislate, the acts adopted should be monitored, to ensure that they are fully implemented, to prevent fragmentation and to avoid the presence of exploitable gaps. The effective implementation of this strategy will also depend on ensuring adequate funding in the next programming period (2021-2027), including for the relevant EU agencies;
- Involvement of all actors in the public and private sectors in a joint effort: key actors in the public and private sectors are apprehensive to exchange information useful for security, for fear of compromising national security or their competitiveness. However, we are most effective when we are all equipped to support each other. It starts with closer cooperation between Member States, involving law enforcement and judicial services and other public authorities, as well as with the EU institutions and agencies, in order to achieve the understanding and exchange needed for common solutions. Cooperation with the private sector is also essential, especially as the industry has a significant weight on the digital and non-digital infrastructure crucial for the effective fight against crime and terrorism. Citizens themselves can contribute, for example, by developing their skills and knowledge to fight against cybercrime or misinformation. Finally, this joint effort must extend beyond our borders, with the idea of establishing closer connections with partners who share our values.

References

Agence des droits fondamentaux de l’Union européenne (2020), *Your rights matter:Security concerns and experiences*, *Fundamental Rights Survey*, Luxembourg, Office des publications

Décision 2007/845/JAI du Conseil relative à la coopération entre les bureaux de recouvrement des avoirs des États membres en matière de dépistage et d’identification des produits du crime ou des autres biens en rapport avec le crime

Directive 2013/40/UE relative aux attaques contre les systèmes d’information

Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism*, 2019

Europol: *Beyond the pandemic.How COVID-19 will shape the serious and organised crime landscape in the EU* (avril 2020)

https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

OEDT et Europol, *EU Drug Markets Report*, 2019

Rapport d'Europol, *The Trafficking in Human Beings Financial Business Model* (2015)

Rapport intitulé «Recouvrement et confiscation d'avoirs: Garantir que le crime ne paie pas», COM(2020) 217

Stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants, COM(2020) 607

Teijlingen, E., & Hundley, V. (2001). The importance of pilot studies. Social Research Update, 35, 1-4. doi: 20/12/2010