ISSN: 2284 – 5224 Vol. 11, No. 2/2021

Journal of Danubian Studies and Research

European Construction between Desideratum and Realities

Current Strategies to Prevent Terrorism in Europe

Nicolae-Florin Prunău[1]

Abstract: One of the main threats to freedom of movement, security and justice is terrorism, a denial of democracy and human rights and, at the same time, a threat that does not recognize borders and affects countries and citizens, regardless of their geographical location. The European Union aims to be a guarantor of these rights, and for European citizens to have confidence that wherever they travel in the EU, their freedom and security are well protected. Individuals and groups should not promote their political goals through terror, challenge the democratic values of societies and jeopardize the rights and freedoms of citizens. Acts of terrorism are criminal and unjustified and must be treated as such in all circumstances. Combating cross-border crime and terrorism is a common European responsibility and EU member states have a primary responsibility for ensuring security, and cooperation is essential for the fight against terrorism.

Keywords: combat; security; strategy; terrorism; threat

1. Introduction

Terrorism continues to be one of the main threats to the security of Europe, the Member States of the European Union and the world[2]. Equally, the *European Security Agenda* identifies terrorism as one of the fundamental threats to European

[1] PhD Student, Business Administration, "*Ştefan cel Mare"* University of Suceava, Romania, Address: University Street 13, Suceava 720229, Romania, Corresponding author: florin.prunau@univ-danubius.ro.

[2] *A New Start for Europe. My Agenda for Jobs, Growth, Fairness and Democratic Change*. Political Guidelines for the next European Commission, European Commission.

security[1]. In this context, as well as in the context of the recent terrorist attacks, the European Parliament adopted the *European Parliament Resolution on counter-terrorism measures* and *Council of Europe Counter-Terrorism Strategy (2018-2022)*. Those were then integrated into the revised form of the *EU Security Union Strategy 2020-2025*[2] and translated into concrete action through the *European Security Agenda* and subsequent sectoral action plans.

The new counter-terrorism measures are based on the premise that the security situation in Europe has changed dramatically over the last decade due to new conflicts in the immediate vicinity of the European Union, the rapid development of new technologies and the worrying rise of radicalization leading to violence and terrorism in European Union and neighboring countries. More precisely, the manifestations of the terrorist phenomenon in Europe required the modification and adaptation of the anti-terrorist measures implemented by the *European Counter-terrorism Strategy*. Terrorist attacks of January 2015 by the editorial staff of the French publication *Charlie Hebdo*, those of Paris on November 13, 2015, the attack in Brussels in 2016, in July 2016 in Nice and Munich, December 2016 in Berlin and May 2017 in Manchester highlighted the urgency of a priority on the internal and external security agenda of the European Union and the Member States: streamlining measures to combat the ever-changing terrorist threat.

2. About Counter-Terrorism Measures

Measures to combat the terrorist threat in Europe have been very diverse, differing from state to state. At a glance, it is easy to see that the new counter-terrorism measures adopted by the European Union are a collection of different but complementary security doctrines and strategies, integrated into a coherent strategy at European level. National counter-terrorism measures in the Member States of the European Union have been based on the following aspects:

a) updating national legislation in the field of counter-terrorism;

b) alignment with international (UN) or European legislation;

[1] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social committee and the Committee of the Regions on the EU Security Union Strategy, 2020.

[2] *Council Conclusions* on the Renewed European Union Internal Security Strategy 2020-2025.

c) the new European anti-terrorism legislative measures and the impact on free movement in Europe.

The package of counter-terrorism measures adopted by the European Union comes as a development of a long process of building European legislation and competences in the field of counter-terrorism and the measures adopted fall within the general directions of the *European Counter-Terrorism Strategy*, and the general trend is to strengthen the tasks and roles of the European institutions/agencies in relation to the Member States. Although Member States still retain the main responsibility for responding to terrorist threats as sovereign actors, the European institutions/agencies act as coordinators or facilitators of pan-European or national operational counter-terrorism cooperation.

The Community dimension, internal to the European Union, includes several distinct dimensions:

a) combating the main source of internal terrorist threat, manifested by the phenomenon of foreign terrorist fighters from the European Union;

b) control of the external borders of the European Union;

c) the issue of monitoring foreign terrorist fighters from the European Union is a complex and difficult one, given the complexity of the transport routes they use to reach conflict areas and return to the European space;

d) prevention of radicalization and violent extremism in the European Union;

e) the package of measures to combat radicalization and violent and nonviolent extremism is the subject of a sectoral strategy of the European Union, in which the emphasis is on rehabilitation, cultural tolerance and education, but also on cooperation with third countries, development and humanitarian aid, etc. to alleviate or eliminate the causes of radicalization.[1] This package of measures includes, but is not limited to:

• rethinking the priorities of the European Union's policies, programs for education, youth and culture in terms of anti-radicalization and extremist political messages;

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response,* 2018.

• streamlining the Center of Excellence and the Radicalization and Awareness Network (RAN);[1]

• expanding and deepening cooperation in the field of combating radicalization and extremism with states such as Turkey, the Western Balkans, the Middle East and North Africa (MENA).[2]

3. EU Counter-Terrorism Strategy

The dramatic events of September 11, 2001 in the USA determined a paradigm shift at the international level, including at the level of the European Union, in addressing the threats to European/global security, materialized in the resizing and configuration of relevant policies/doctrines.

As terrorist attacks continue to hit citizens in Europe and beyond, the fight against terrorism is a top priority for the EU, its member countries and their partners.

Article 83 of the *Treaty on the Functioning of the European Union* (TFEU) gives the European Parliament and the Council the power to adopt minimum rules for the definition of particularly serious crimes with a cross-border dimension, of which terrorism is an example.

To combat terrorism effectively, the EU Counter-Terrorism Strategy focuses on four priorities:

• anticipate;
• prevent;
• protect and
• respond.

Through these pillars, the strategy recognizes the importance of cooperation with non-EU countries and international institutions, given that the security of the Union is closely linked to the situation in other countries, especially neighboring countries.

The counter-terrorism agenda is present in relations between the EU and non-EU countries in various ways, including: high-level political dialogues; adoption of clauses and agreements for specific cooperation or assistance but also capacity building projects with strategic countries. In this regard, the EU is cooperating in the

[1] *EU Security Union Strategy 2020-2025*.
[2] *EU Security Union Strategy 2020-2025*.

field of counter-terrorism with the countries of the Western Balkans; Africa (Sahel, North Africa, Horn of Africa); Middle East and North Africa (MENA) and Asia.

Cooperation with the US is a key component of the EU strategy. In recent years, cooperation agreements have been concluded in areas such as terrorist financing, transport and borders, mutual legal assistance and extradition.

The EU also works closely with other international and regional organizations to build international consensus and promote international counter-terrorism standards.[1]

In order to make the fight against terrorism more efficient, the European Council decided to set up the EU *Counter-Terrorism Coordinator* (CTC), which has a relevant role in monitoring the implementation of strategic documents and action plans for the reference area and regularly reports on their status, which are presented in the specialized working groups of the EU Council - the *Working Party on Terrorism, (Internal Aspects)* (TWP) and the *Working Party on Terrorism (International Aspects)* (COTER).

The *EU Joint Situations Center* (SITCEN), part of the new *European External Action Service* (EEAS), has an important role to play in assessing the level of the terrorist threat to the EU. SITCEN's responsibilities include analyzing trends in terrorism in non-EU countries and developing analytical products to inform EU officials, such as the High Representative for Foreign Affairs and Security Policy.

The entry into force of the Treaty of Lisbon changes the Community's institutional perspective, with implications for the organization and functioning of European bodies, their tasks and, implicitly, the decision-making powers of the national bodies of the Member States in certain areas. The Treaty of Lisbon brings changes in the structure of Community structures, with new structures being set up. Thus, in accordance with the Article 71 of the Treaty on the Functioning of the European Union, the *Operational Committee on Internal Security* (COSI) was set up, bringing together representatives of Member States' capitals responsible for combating organized crime and terrorism. COSI is in charge of evaluating the general direction and the efficiency of the operational cooperation in order to identify possible deficiencies and, implicitly, to formulate recommendations regarding the measures to overcome them.

[1] Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477 / EEC on control of the acquisition and possession of weapons (OJL 137, 24.5.2017, pp. 22-39).

The Lisbon Treaty provides for the creation of a new autonomous structure of the EU[1] - the *European External Action Service* - which, as the title suggests, will play a prominent role in foreign policy and will be under the authority of the High Representative. The new service will support the High Representative in directing the *Common Foreign and Security Policy* and will have the role of ensuring the consistency of the EU's external action. The new structure includes representatives of the European Commission, the General Secretariat of the Council and the diplomatic missions of the Member States (as well as, as mentioned above, SITCEN).

4. Implications of "Cyber Terrorism" for Countries, Organizations and Individuals

In the last 5 years, more connections and more data have been created and distributed than in the entire history of mankind so far. According to specialists, cyberspace is characterized by lack of borders, dynamism and anonymity, generating both opportunities for the development of the information society based on knowledge and risks to its functioning and can be defined from several perspectives, as follows: from the perspective of the national economy; socially; economically and physically.

Mastery of cyberspace in the 21st century is as decisive as mastery of the sea in the 19th century and air in the 20th century. Cyberspace is the battlefield on which the war of the future will go, it is the arena for the New Cold War. An arena in which every nation on Earth, every enterprise and almost every man on the planet has interests and lives.

Cyberspace is now the new platform for political, economic, military and cultural interactions and engagements. This will be the area where the impact on social stability, national security, economic development and cultural communication will take place in the next century (Cunningham, 2020, p. 27).

The new technology will have disproportionate effects, not only on the weapons used in cyberspace, but also on the structure of the field itself. Cyberspace policy dictates the objectives and rules of involvement for cyber capabilities, as well as the organization and execution of operations, but those "rules" apply only to nations and fighters that are willing to subscribe to them. There is no "Geneva Convention" for cyberspace, and setting these limits for defenders in reality only empowers those

[1] Article 27 (3) of the *Treaty on European Union*, as amended by the Treaty of Lisbon.

who do not follow the rules. Cyberspace is the only realm on the planet where the involvement of a nation state can have the same devastating effect as the most powerful nations on Earth. The use of digital space has effectively equalized the playing field.

The digital world is where nations and organizations will continue to fight for the future. Owning that "land" and taking the initiative is nothing new in the annals of espionage and war; it is simply a change of techniques and tactics, adapted to the space in which the confrontation will take place, which will continue to lead the New Cold War.

It is recognized in the literature that the term cyber terrorism was first used by Barry C. Collin in his book *"The future of cyberterrorism: Where the physical and virtual worlds converge"*[1].

Regarding the definitions of cyberterrorism, they are multiple as in the case of the definition of terrorism. Cyberterrorism has been defined as "cyber attacks in cyberspace from both internal and external networks, especially the Internet, which emanate from different terrorist sources, with different sets of motivations and which are aimed at a certain target" (Axelrod, 2002). Like all other forms of war, cyber warfare has its advantages and disadvantages, its possibilities and limitations. To this extent, the spread of war in cyberspace seems inevitable. Cyberwarfare will not always run out of blood, as has been the case so far (van Creveld, 2015, pp. 88-90).

But attacks on computer systems, especially those related to organized crime, have become an increasing threat, both at EU and global level, and there is growing concern about the possibility of attacks. Terrorist or politically motivated information systems that are part of the critical infrastructure of the Member States and the Union.

Various organizations can also use the Internet to transmit the organization's messages, to communicate with network members, sometimes using steganography[2], to raise funds and last but not least to commit traditional forms of crime.

[1] Published in *Crime and Justice International*, vol 13, Issue 2, pp. 14-18.

[2] Steganography (Greek for *„hidden writing"*) is the art of communicating in a way that conceals the existence of communication. The purpose of steganography is to hide messages inside harmless communications so that they are not detected. Steganography differs from cryptography in that messages are not encrypted, but only hidden in a way that makes them almost impossible to detect.

Given that many aspects of modern society are highly dependent on computer systems, especially critical infrastructure, the risks posed by such attacks are considerable, as they can cause destruction, modification or inaccessibility of computer systems and data, thus blocking production processes, systems banking or public administration or, if the computer systems responsible for the administration of nuclear power plants, dams, air, land or naval transport control systems, hospitals or military armament systems, etc. are attacked.

One of the most notorious cyberattacks, also called the first cyber weapon, was the 2009 cyberattack, in which a malware, actually a virus called *Stuxnet*[1], was designed to attack a single, highly accurate target: computers that they controlled Iran's Natanz nuclear facility, where international authorities suspected Iran was working on its secret nuclear weapons program. *Stuxnet* was programmed to make uranium enrichment centrifuges rotate faster than they should, causing them to spiral out of control until they were destroyed.

A similar attack took place in 2012, through a highly sophisticated malware, similar to *Stuxnet*, called *Duqu 2.0*, which exploited a number of vulnerabilities, among its targets being entities related to the negotiations on the Iranian nuclear agreement and security IT companies (Bejtlich, 2018).

Duqu 2.0 has targeted a number of Western organizations and entities operating in Asia and the Middle East. Experts from Kaspersky Lab[2] discovered it while trying a type of phishing attack (*spear phishing*) against them and pointed out that most of the attacks observed in 2014-2015 are related to the P5 + 1 negotiations (United States, United Kingdom, Germany, France, Russia and China, facilitated by the European Union) with Iran. The purpose of the P5+1 events was to achieve a verifiable diplomatic resolution that would prevent Iran from obtaining a nuclear weapon.

A series of cyber attacks were directed against Saudi Aramco, the world's largest oil and gas producer, compromising 30,000 computers, and the code was designed to disrupt and stop oil production (Bronk & Tikk-Ringas, 2019; Haglund, 2017).

Although these attacks were not carried out, being possible to be committed by a state actor (they can be assimilated to acts of war), the consequences cannot be neglected if they were committed by terrorist organizations.

[1] D.E. Denning, *Stuxnet: What Has Changed*; L. Franceschi-Bicchierai, *The History of Stuxnet: The World's First True Cyberweapon.*

[2] *The Mystery of Duqu 2.0 a sophisticated cyberespionage actor returns.*

In addition to the above-mentioned actions, cyber terrorists may also carry out other illegal operations with computer devices or programs, namely: the production, import, distribution or making available in any form of computer devices or programs designed or adapted for the purpose of committing crimes. against the security and integrity of computer systems and data, as well as passwords, access codes or other such computer data that allow full or partial access to a computer system.

5. Conclusions

The EU Council reiterates its unwavering commitment to protecting EU citizens against terrorism and violent extremism in all their forms and irrespective of their origin. In doing so, it remains dedicated to continuing to support enhanced EU external action in the field of counterterrorism and to prevent and counter radicalisation leading to violent extremism and terrorism. In light of the constantly evolving nature of the threats from international terrorism, the Council has decided to update its previous conclusions on EU external action to counter and prevent terrorism and radicalisation leading to violent extremism and terrorism.

At the same time, other key challenges demand further resolute action, such as: bringing foreign terrorist fighters (FTFs) to justice and preventing their movement, especially undetected crossings of the EU's borders; addressing the increase in home-grown radicalisation and anticipating the persistent threat posed by terrorist sleeper cells and lone actors; adequately monitoring individuals released after serving terrorism-related sentences; adapting to the developments in money-laundering and terrorism financing; mitigating the exploitation of rapid technological developments; tackling emerging and hybrid threats to aviation, critical infrastructure and public spaces; and addressing the spread of violent extremist Islamist ideology and the emergence of politically motivated violent extremism and terrorism, especially in view of the growing number of far-right terrorist attacks.

Furthermore, as the impact of the COVID-19 pandemic represents an unprecedented challenge with wide-ranging effects which will only fully unfold in the long term, a specific effort should be made to assess its potential influence on terrorist activities as well as on the prevention and countering of terrorism, and to identify possible targeted EU action.

References

Bejtlich, R. (2018). *Duqu 2.0 The Most Sophisticated Malware Ever Seen*.

Bronk, C. & Tikk-Ringas, E. (2019). *Hack or attack? Shamoon and the Evolution of cyber-conflict*.

Cunningham, Chase (2020). *Cyber Warfare – Truth, Tactics and Strategies*.

Denning, D.E. (2012). *Stuxnet: What Has Changed?*

Franceschi-Bicchierai, L. (2015). *The History of Stuxnet: The World's First True Cyberweapon*.

Haglund, J. (2017). *A Case Study of Four Recent High-Impact Malware Attacks*.

Huntington, Samuel P. (1997). *The Clash of Civilizations and the Remaking of World Order*, Simon & Schuster, Sydney.

van Creveld, Martin (2015). *A History of Strategy from Sun Tzu to William S. Lind*. Castalia House Kouvola, Finland.

Wilson, C. (2003). *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress.*

Official documents

EU Security Union Strategy 2020-2025

Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social committee and the Committee of the Regions on the EU Security Union Strategy, 2020.

Council Conclusions on the Renewed European Union Internal Security Strategy 2015-2020.

The European Agenda on Security, 2019.

SIPRI (*Stockholm International Peace Research Institute*) Yearbook 2019: Armaments, Disarmament and International Security.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Preventing Radicalisation to Terrorism and Violent Extremism: Strengthening the EU's Response, 2018.

UCDP (*Uppsala Conflict Data Program*) –2018 Report.

Directive (EU) 2017/853 of the European Parliament and of the Council of 17 May 2017 amending Council Directive 91/477 / EEC on control of the acquisition and possession of weapons.

Study Group Report on International Law & Cyber Terrorism, 31 July 2016.

Article 27 (3) of the *Treaty on European Union*, as amended by the Treaty of Lisbon.

Pathways for Peace (Inclusive Approaches to Preventing Violent Conflict).

United Nations, Counter-Terrorism Implementation Task Force, Working Group Compendium, *Countering the Use of the Internet for Terrorist Purposes – Legal and Technical Aspects*.

Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation, Adopted by Heads of State and Government in Lisbon. Active Engagement, Modern Defence.

The Millennium Project: Global Futures Studies&Research.

Internet

https://www.visionofhumanity.org/wp-content/uploads/2020/10/GPI_2020_web.pdf.

https://www.economicsandpeace.org/wp-content/uploads/2020/08/GTI-2019web.pdf.

https://www.sipri.org/databases.

Defence Against Terrorism Programme of Work (DAT POW), https://www.nato.int/cps/en/natolive/topics_50313.htm#:~:text=The%20aim%20of%20the%20Alliance%27s,as%20attacks%20on%20critical%20infrastructure.