Terrorism – Studies, Analyses, Prevention, 2025, special edition: 249–270

https://doi.org/10.4467/27204383TER.25.022.21525

Article

Results of the survey on the perception of terrorist and sabotage threats among the experts of the EU Protective Security Advisors

KAROLINA WOJTASIK https://orcid.org/0000-0002-1215-5005

Permanent Representation of the Republic of Poland to the European Union in Brussels, Government Centre for Security

DAMIAN SZLACHTER https://orcid.org/0000-0003-2763-9325

Internal Security Agency

Abstract

This article presents the results of a survey on the perception of terrorist and sabotage threats by experts participating in the European Commission's (DG Home) initiative EU Protective Security Advisors (EU PSA). The survey was conducted in February 2025 on a sample of 50 individuals representing EU PSA, EU institutions, and strategic project partners. The questionnaire covered several key aspects of terrorist and sabotage threats, including the types of potential targets, attack methods, and expected developments in hybrid threats. Respondents were also asked to assess which critical infrastructure systems require the highest priority in resilience-building efforts, as well as which counter-terrorism measures should be prioritised at the EU level. Additionally, the survey explored factors that could improve the security of protected facilities and identified the most likely perpetrators of attacks on EU critical infrastructure. The survey results provide valuable insights for shaping counter-terrorism and counter-sabotage policies at

the EU level. The authors emphasise the necessity of standardising physical security measures and developing educational initiatives to build a security culture.

Keywords

critical infrastructure, public space, terrorism, sabotage, resilience, soft targets, hard targets, European Commission, DG HOME, EU PSA, critical infrastructure protection, hybrid threats, hybrid warfare

Introduction

The protection of public spaces and critical infrastructure (CI) is a fundamental duty of the Member States of the European Union. In response to increasing terrorist threats, the EU undertakes initiatives to support Member States in their efforts to protect citizens and CI. One such initiative is the EU Protective Security Advisors (EU PSA)[1], created by the Directorate-General for Migration and Home Affairs (DG HOME) of the European Commission.

The EU PSA initiative has its roots in the EU's work on the protection of public spaces, which began in 2012. The impetus for these efforts was the expert support provided in Poland during the UEFA Euro 2012 European Football Championship. The positive experiences from this event led to further invitations to support security at high-level political events and large public gatherings. A significant milestone in the development of the EU's public space protection policy was the adoption of an action plan in October 2017 dedicated to these issues. As part of its implementation, the EU developed a threat vulnerability assessment tool. This ultimately led to the creation of a group of specialists and the establishment of the EU PSA programme. The EU PSA expert group consists of approx. 130 specialists from the European Commission and EU Member States. These experts have professional experience in public space protection and specialised knowledge in various security fields. Implementation of the EU PSA

[1] *EU Protective Security Advisors (EU PSA)*, https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [accessed: 26.02.2025].

initiative into the official EU anti-terrorism acquis took place in December 2020, with the publication of the EU Counter-Terrorism Agenda.

The EU PSA programme aims to provide support to EU's Member States upon request. The activities carried out under this initiative include:

- raising awareness of vulnerabilities in public spaces and CI by providing a common security assessment system,
- sharing best practices and encouraging knowledge exchange to eliminate identified security weaknesses,
- providing guidance to Member States on organising mass events and protecting high-risk sites,
- building a network of experts by organising international training sessions and initiatives that contribute to developing a shared security culture in the EU.

The EU PSA programme covers the protection of public spaces and CI, including:

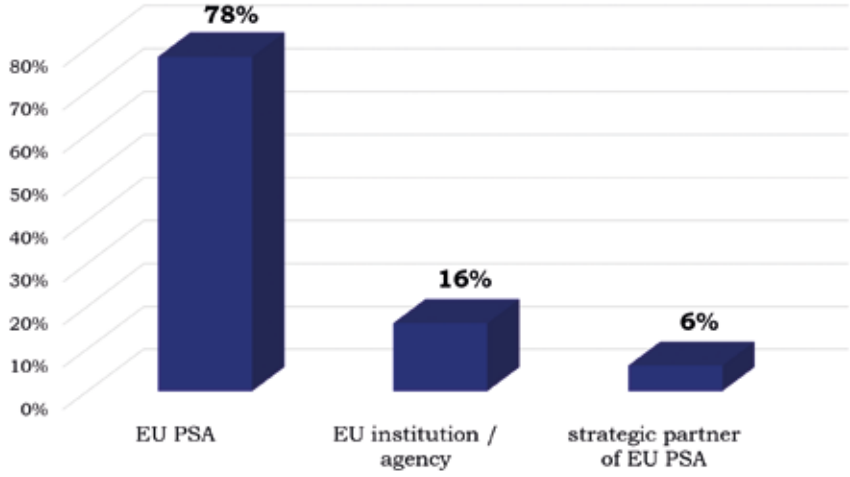
- places of worship and religious institutions,
- cultural events, such as large music festivals,
- VIP events, such as EU summits,
- large infrastructure facilities not included in CI,
- airports, seaports, energy sector facilities and other facilities included in CI.

Given the growing recognition of the EU PSA programme among Member State authorities and the unstable geopolitical situation, interest in its activities is expected to increase. Member States have expressed their intention to invite EU PSA experts to assess national CI facilities, particularly in the context of the EU Directive on the resilience of critical entities. The EU PSA programme is a key EU initiative supporting Member States in protecting public spaces and CI against terrorist threats. By raising awareness, sharing best practices, and providing expert support, EU PSA contributes to improving the security of citizens and infrastructure across the EU. This was the rationale behind the article's authors' decision to conduct a survey on terrorist and sabotage threat perceptions among the EU PSA community. It consists of EU PSA members, representatives of the EU institutions and agencies working with the EU PSA and the initiative's strategic partner.

Results of the survey

The survey was conducted in February 2025, using a standardised questionnaire consisting of 8 questions[2]. It was anonymous in nature. Fifty people took part in the survey[3]. Respondents represented: the EU PSA (78%), the EU institutions and agencies supporting the above-mentioned initiative (16%) and the EU PSA project's strategic partner (6%). The division of respondents is shown in Chart 1.

Chart 1. Division of respondents according to the environment they represent.



Question 1 of the survey was: *What objects are terrorists/saboteurs interested in when planning their activities in the European Union?*

Respondents were asked to rank their answers in order from 1st to 10th place, with 1st place indicating the object in which terrorists/saboteurs are most interested, 10th – the least[4]. Respondents were given the following facilities: buildings of state and EU offices, CI facilities, military bases, symbolic tourist landmarks, sport and entertainment facilities, places

[2] Attachment: template of the research questionnaire.

[3] This represents approx. 40% of the number of EU PSA members.

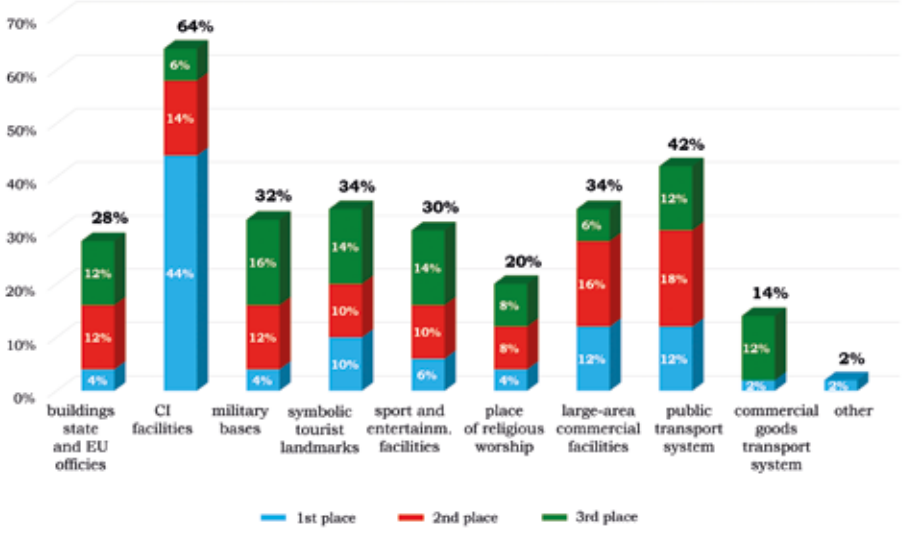
[4] For questions where respondents were asked to rank their answers, the results are presented only for positions 1 to 3. Therefore, the data in the charts displaying these results do not sum up to 100%.

of religious worship, large-area commercial facilities, public transport system, commercial goods transport system and others.

Within the group of facilities that respondents singled out for 1st place, CI facilities (44%), large-area commercial facilities and the public transport system (both 12% each) as well as symbolic tourist landmarks (10%) were most frequently indicated. There is therefore a marked difference in the frequency of indications for CI and subsequent facilities. Among the facilities to which survey participants assigned 2nd place, the public transport system (18%), large-area commercial facilities (16%) and critical infrastructure facilities (14%) were most frequently indicated. Among the facilities that respondents ranked 3, the most common response was military bases (16%). The results for subsequent facilities were the same – symbolic tourist landmarks as well as sport and entertainment facilities were indicated by 14% of the respondents. In the case of the objects that the respondents indicated in 2nd and 3rd place, therefore, no clear predominance of one of them could be established.

The results from places 1st–3rd for the individual responses were added up and it was checked which facilities were most frequently indicated by respondents within the top three. The data obtained shows that these are: CI facilities (64%), public transport system (42%) and ex aequo symbolic tourist landmarks and large-area commercial facilities (34% each). Detailed results are shown in Chart 2.

Chart 2. Facilities of interest to terrorists/saboteurs planning operations in the EU.

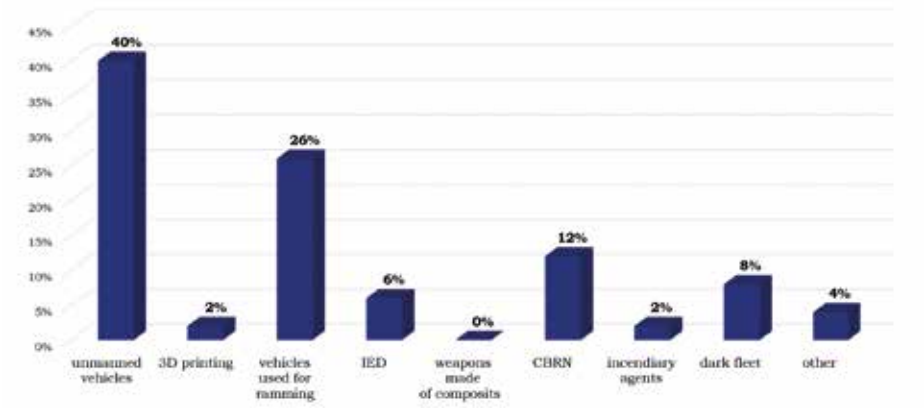


Question 2 of the survey was: *What methods of attack and sabotage can be the greatest challenge for law enforcement authorities and institutions which ensure the security of people and facilities?*

Respondents were able to select one answer from the following categories: unmanned vehicles (air, land, water), 3D printing, vehicles used for ramming the target, improvised explosive devices (IED), weapons made of composites, CBRN, incendiary agents, so called *shadow fleet/dark fleet*, others.

The largest number of respondents (40%) indicated unmanned vehicles (air, land, water). In 2nd place, respondents indicated vehicles used for ramming (26%), followed by CBRN (12%). All results are shown in Chart 3.

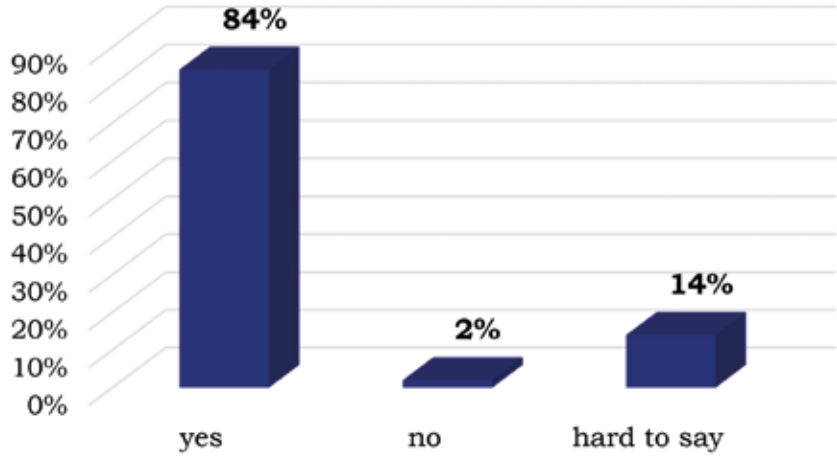
Chart 3. Methods of attack and sabotage that are likely to pose the greatest challenge to law enforcement and institutions providing security for people and facilities.



Question 3 of the survey was: *Should we expect, in a 3-year perspective, the use of terrorist/sabotage activity as part of hybrid threats undertaken on the territory of the EU by a foreign state?*

Respondents could choose one answer from the following options: yes, no, or hard to say. A total of 84% of respondents answered affirmatively, 14% did not take a clear stance, and only 2% provided a negative response. The results are presented in Chart 4.

Chart 4. Could terrorist/sabotage activities be used as a tool of hybrid operations in the EU within the next 3 years?



Question 4 of the survey was: *Which facilities, in a 3-year perspective, will be characterised by the highest level of terrorist/sabotage attack threat in the EU?*

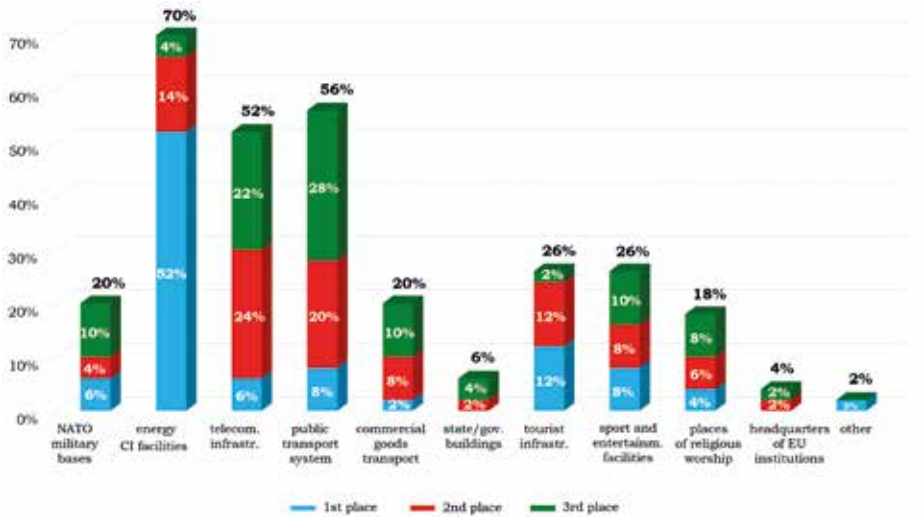
Respondents were asked to rank the provided options from 1st to 11th, with 1st indicating the facility facing the highest level of terrorist/sabotage threat and 11th – the lowest. The following facilities were listed: NATO military bases, energy CI facilities, telecommunications infrastructure, public transport system, commercial goods transport system, government offices, tourist infrastructure, sport and entertainment facilities, places of religious worship, headquarters of EU institutions and agencies, and others.

Among the facilities that respondents ranked in 1st place, the most frequently indicated were energy CI facilities (52%), tourist infrastructure (12%), and sport and entertainment facilities (8%). It is important to highlight the significant dominance of CI, as the next facilities in the ranking received considerably fewer votes. For the facilities ranked in 2nd place, the most commonly selected were: telecommunications infrastructure (24%), public transport system (20%), and energy CI facilities (14%). Among the facilities ranked in 3rd place, the most frequent responses were: public transport system (28%), telecommunications infrastructure (22%), and NATO military bases, commercial goods transport system, and sport and entertainment facilities (each receiving 10%). Therefore, in the case

of 2nd and 3rd place, the phenomenon of dominance of one type of object did not occur.

The results from rankings 1st–3rd were summed for each response to determine which facilities were most frequently placed in the top three by respondents. The data indicate that these are: energy CI facilities (70%), public transport system (56%), and telecommunications infrastructure (52%). Detailed results are presented in Chart 5.

Chart 5. Facilities expected to face the highest level of terrorist/sabotage threats.



Question 5 of the survey was: *Which critical infrastructure systems, in the 3-year perspective, should be treated as a priority in terms of building their resistance to hybrid threats?*

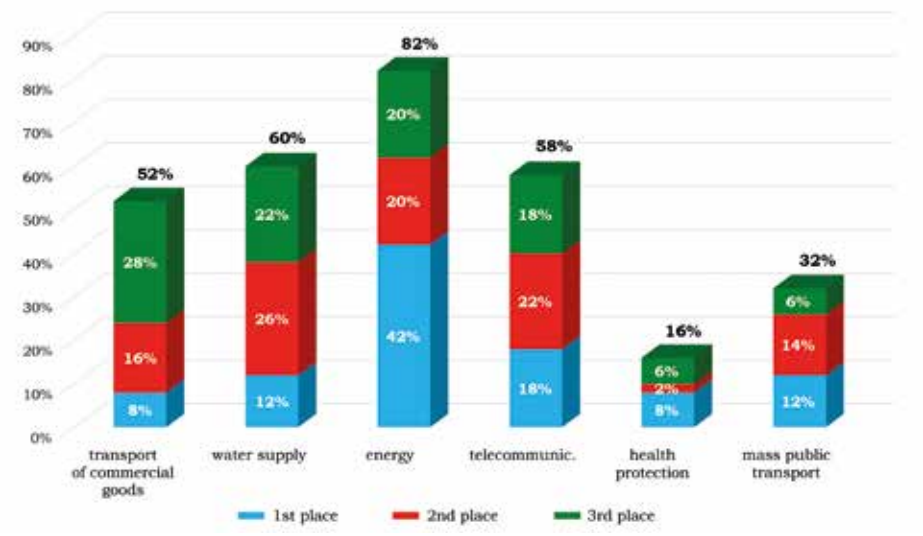
Respondents were tasked with ranking the given systems from 1st to 7th, where 1st place indicated the CI system with highest priority and 7th place. The respondents were provided with the following systems: transport of commercial goods (communication routes and transhipment hubs), water supply, energy, telecommunications, health protection, mass public transport, others.

Among the CI systems ranked 1 by respondents, the energy system was the most frequently selected (42%), followed by telecommunications system (18%) and both the water supply system and mass public transport system (each with 12%). For the 2nd and 3rd places, the responses were more

evenly distributed. The systems most frequently ranked 2 were: water supply system (26%), telecommunications system (22%), and energy (20%). Among the systems ranked 3, the most common choices were: transport of commercial goods (28%), water supply (22%), and energy (20%).

The results from positions 1st–3rd for each response were summed up to determine which CI systems were most frequently ranked in the top three by respondents. The data show that these are the energy system (82%), the water supply system (60%), and the telecommunications system (58%). Detailed results are presented in Chart 6 (the answer "others" was not given).

Chart 6. Priority CI systems in building resistance to hybrid threats.



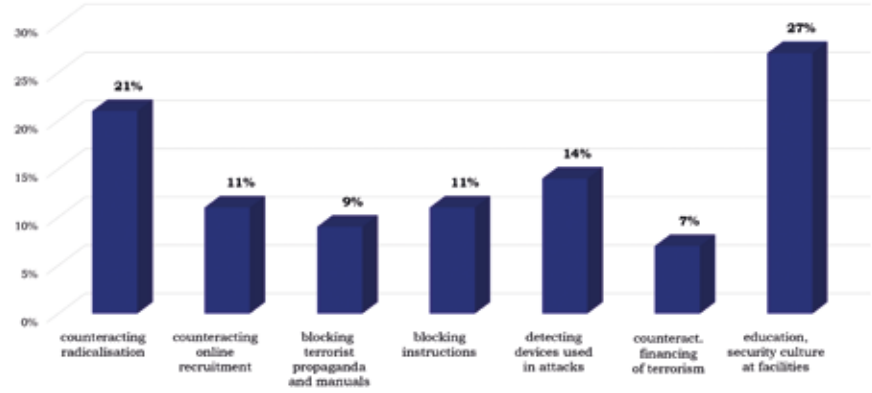
Question 6 of the survey was: *Which of the areas of counteracting terrorist activities require priority treatment on the EU level today?*

Respondents could choose one answer from the following options: counteracting radicalisation leading to terrorist activities, counteracting online recruitment for terrorist/sabotage actions, detecting and blocking terrorist propaganda, detecting and blocking terrorist/sabotage manuals published online, developing technologies for detecting devices used in terrorist attacks, counteracting the financing of terrorism, educational

initiatives concerning security culture for facilities vulnerable to terrorist/sabotage attacks, and other.

Responses to this question were divided. The largest share of respondents indicated educational initiatives and building a security culture in facilities that could be potential targets of terrorist or sabotage activities (27%). The 2nd most selected option was preventing radicalisation leading to terrorist activities (21%), followed by developing technologies for detecting devices used in terrorist attacks (14%). All results are presented in Chart 7.

Chart 7. Priorities in counteracting terrorism.

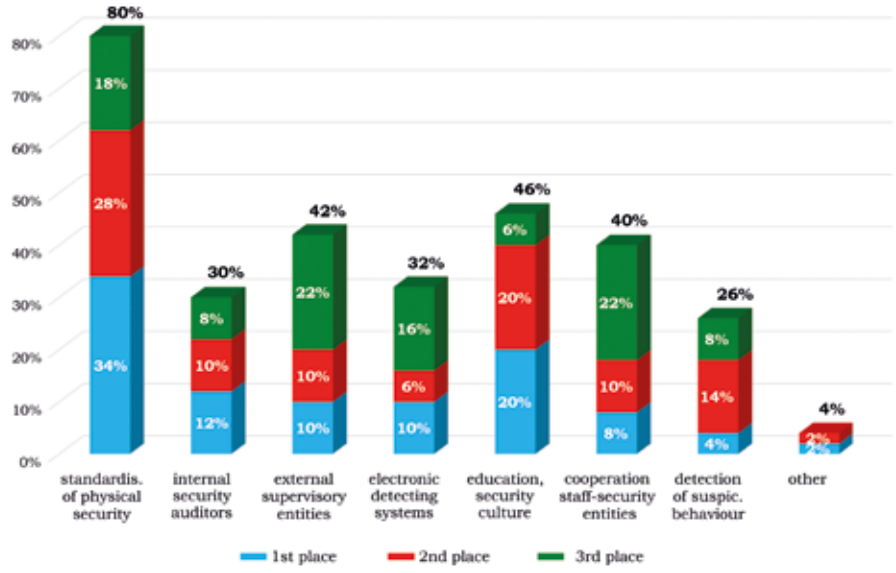


Question 7 of the survey was: *What can increase the level of resistance to terrorist attacks and sabotage activities in protected facilities?*

The respondents were tasked with ranking the given actions from 1st to 8th place, where 1st place represented the most important activities and 8th place – the least important. The provided options were: standardisation of physical security (also security personnel procedures), tasks performed by internal security auditors, external security control tests by external supervisory entities (such as: EU institutions, state control authorities), development of intelligent electronic systems for detecting security incidents, development of anti-terrorist prevention initiatives as part of the security culture of the facility (education for security), improving cooperation between CI entities and entities responsible for security, detection of suspicious behaviour carried out by trained security personnel, and others.

Among the actions ranked 1 by respondents, the most frequently selected were: standardisation of physical security (34%), development of anti-terrorist prevention initiatives (20%), and tasks performed by internal security auditors (12%). The difference between the next-ranked actions – security control tests conducted by external supervisors (such as: EU institutions, state control authorities) and development of intelligent electronic systems for detecting security incidents – was minimal, with both receiving 10% of the respondents. Among the actions ranked 2, the most frequently chosen were: standardisation of physical security (28%), development of initiatives related to terrorism prevention (20%), and detection of suspicious behaviour by trained security personnel (14%). For actions ranked 3, the most common responses were security control tests conducted by external supervisory entities and improving cooperation between CI entities and security organisations (both at 22%). The next most frequently selected action was standardisation of physical security (18%). The results from positions 1st–3rd for each response were summed up to determine which actions were most frequently ranked in the top three by respondents. The data show that these are: standardisation of physical security (80%), development of anti-terrorist prevention initiatives (46%), security control tests conducted by external entities (42%). Detailed results are presented in Chart 8.

Chart 8. Projects aimed at increasing the resilience of protected objects.

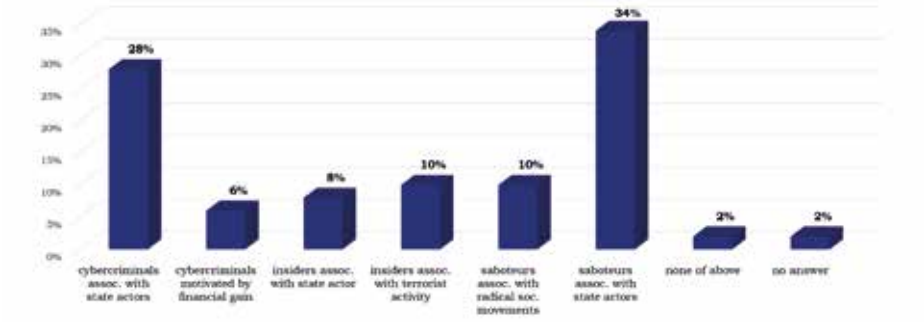


Question 8 of the questionnaire concerned the perpetrators of attacks on CI.

Respondents could choose one answer from the following options: cybercriminals associated with a state actor, cybercriminals who are motivated only by the desire for financial gain, activities of the so-called insiders associated with a state actor, activities of the so-called insiders associated with terrorist activity, saboteurs associated with the activity of radical social movements, saboteurs associated with a state actor, none of the above.

The largest share of respondents (34%) indicated saboteurs affiliated with a state actor. The 2nd most selected option was state-associated cybercriminals (28%), followed by insiders linked to terrorist activities and saboteurs associated with radical social movements (both at 10%). All results are presented in Chart 9.

Chart 9. Potential perpetrators of attacks on CI facilities.



Summary of survey results

Experts involved in the EU PSA indicated CI facilities (64% of all responses), public transport system (42%) and symbolic tourist landmarks as well as large-area commercial facilities (both 34%) as the most potential targets for a terrorist/sabotage attack within the EU. It should be emphasised that when constructing the survey questionnaire, the authors of the article focused primarily on the purpose of the attack rather than the method. The conclusions drawn from the survey research do not differ from other data. The latest TE-SAT report provides data on terrorist attacks that

took place in 2023. In 45 out of 120 cases, more detailed information was provided, which shows that in 1/3 of them the target was CI[5].

As for the methods of attack and sabotage that today pose the greatest challenge for the law enforcement agencies, authorities and institutions responsible for ensuring the physical security, respondents indicated unmanned vehicles (air, land, water) – 40% of responses. Recent years have been a time of intensive development of drones, they are increasingly used to commit crimes. It is worth emphasising that underwater drones may pose a serious threat to maritime CI in the future. In TE-SAT report it was also indicated, that individuals from a variety of ideological backgrounds who may pose a threat are actively seeking online training material and instruction manuals that contain attack tactics and information on how to make weapons, drones, bombs or chemical weapons[6]. In second place, respondents indicated vehicles used for ramming (26%), which is probably related to recent events (attack in Magdeburg in December 2024 and in Mannheim in March 2025)[7]. A total of 84% of respondents believe that in the 3-year perspective, terrorist and sabotage activities will be used as part of hybrid threat scenarios undertaken on EU territory by a foreign country.

As for the types of facilities that in the next 3 years in the EU will be characterised by the highest level of threat of a terrorist/sabotage attack, the respondents most often selected: energy CI facilities (70%), the public transport system (56%) and the telecommunications infrastructure (52%). Attacks, mostly cyberattacks, on energy and telecommunications

[5] *European Union Terrorism Situation and Trend Report* (EU TE-SAT) 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf, p. 12 [accessed: 26.02.2025].

[6] Ibid., p. 7.

[7] Attack in Magdeburg – on 20 December 2024, a driver drove into a crowd at a Christmas market, killing 6 people and injuring over 100. The perpetrator was a 50-year-old doctor of Saudi origin who had been living in Germany since 2006. Attack in Mannheim – on 3 March 2025, a 40-year-old German citizen drove a car into a group of people on a pedestrian street, killing 2 and injuring several others. The perpetrator was arrested by the police shortly after the incident.

infrastructure have been on the rise[8], becoming a staple of hybrid warfare. Attacks on public transport are a common tactic used by jihadist groups[9].

Majority of the respondents indicated that the CI system, that should be treated as a priority in terms of building resistance to hybrid threats in the 3-year perspective, is the energy system (82%). The efficient functioning of the energy infrastructure is a condition for the functioning of modern society. The effects of an attack on the energy system are multi-level. Therefore, the energy system is considered the most vulnerable to attacks.

In the case of the question about the area of counteracting terrorist activity, which today requires priority treatment by the EU, the respondents' opinions were divided, the majority of respondents (27%), however, indicated to educational activities and building a security culture at facilities that could be targeted. This will be a significant challenge for CI operators and the institutions supervising them.

The projects most likely to increase the level of resistance to terrorist attacks in protected facilities are: standardisation of physical security (80%), development of anti-terrorist prevention initiatives as part of the security culture of the facility (46%) and use of security control tests by external entities (42%).

Most respondents believe that the perpetrators of current attacks on CI systems are saboteurs linked to a state actor (34%) or cybercriminals linked to a state actor (28%).

The results of the survey clearly indicate the threat of terrorist and sabotage attacks, targeting in particular CI, mass public transport

---

[8] B. Nieróbca, *Energetyka w sieci cyberzagrożeń* (Eng. Energy sector in the Network of Cyber Threats), EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [accessed: 26.02.2025]; *Raport: cyberbezpieczeństwo w energetyce* (Eng. Report: Cybersecurity in the Energy Sector), https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [accessed: 26.02.2025]; K. Pohoska, *Cyberprzestępczość – prognozy na 2025 rok* (Eng. Cybercrime – Predictions for 2025), Stołeczny Magazyn Policyjny, 3.03.2025, https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html [accessed: 20.03.2025].

[9] *The Tactics and Targets of Domestic Terrorists*, Center for Strategic and International Studies, 30.07.2020, https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists [accessed: 26.02.2025]; B.M. Jenkins, B.R. Butterworth, K.S. Shrum, *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, https://transweb.sjsu.edu/research/Terrorist-Attacks-Public--Bus-Transportation-Preliminary-Empirical-Analysis [accessed: 26.02.2025].

system and telecommunications system. Respondents, representing the community of security experts, stressed the need to prioritise activities aimed at strengthening the resilience of facilities of key importance for the functioning of the state and society.

Based on the analysis of the survey results, it can be noted that in the coming years it will be necessary to further develop measures to prevent attacks, including: standardisation of physical protection, implementation of modern threat detection technologies and educational initiatives in the field of terrorist prevention. In addition, cooperation between CI operators and security authorities will be important to better coordinate actions and respond to incidents more effectively.

The study also confirms that terrorist and sabotage threats are increasingly part of hybrid strategies by state and non-state actors. In the face of rapidly changing security environment, EU Member States should strive to implement comprehensive protection strategies, taking into account both physical and cybersecurity aspects.

Bibliography

EU Protective Security Advisors (EU PSA), https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/eu-protective-security-advisors-eu-psa_en [accessed: 26.02.2025].

Jenkins B.M., Butterworth B.R., Shrum, K.S., *Terrorist Attacks On Public Bus Transportation: A Preliminary Empirical Analysis*, https://transweb.sjsu.edu/research/Terrorist-Attacks-Public-Bus-Transportation-Preliminary-Empirical-Analysis [accessed: 26.02.2025].

Nieróbca B., *Energetyka w sieci cyberzagrożeń* (Eng. Energy sector in the Network of Cyber Threats), EY, 14.08.2024, https://www.ey.com/pl_pl/insights/cybersecurity/energetyka-w-siecicyberzagrozen [accessed: 26.02.2025].

Pohoska K., *Cyberprzestępczość – prognozy na 2025 rok* (Eng. Cybercrime – Predictions for 2025), Stołeczny Magazyn Policyjny, 3.03.2025, https://magazyn-ksp.policja.gov.pl/mag/technologie/137761,Cyberprzestepczosc-prognozy-na-2025-rok.html [accessed: 20.03.2025].

The Tactics and Targets of Domestic Terrorists, Center for Strategic and International Studies, 30.07.2020, https://www.csis.org/analysis/tactics-and-targets-domestic-terrorists [accessed: 26.02.2025].

Other documents

European Union Terrorism Situation and Trend Report (EU TE-SAT) 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [accessed: 26.02.2025].

Raport: cyberbezpieczeństwo w energetyce (Eng. Report: Cybersecurity in the Energy Sector), https://www.inteligentnaenergetyka.pl/enereka/wp-content/uploads/2024/02/Raport_Cyberbezpiecze%C5%84stwo-w-energetyce_ARTSMART_29.02.2024.pdf [accessed: 26.02.2025].

Attachment

Template of the research questionnaire used in February 2025

The EU PSA SURVEY 2025

This survey is conducted among representatives of EU Member States and the European Commission participating in the project of building resistance to terrorist attacks in public spaces – EU PSA (Protective Security Advisors) at DG HOME European Commission. The survey is anonymous, and the survey results will be collected in a way that makes it impossible to identify the person completing it.

The purpose of the survey is to obtain respondents' opinions on the most probable ways of development of terrorist/sabotage threats in the EU.

The results of the survey will be published in a special issue of the scientific journal "Terrorism – Studies, Analyses, Prevention" which will be devoted to terrorist and hybrid threats to critical infrastructure. The special issue will be published in May 2025 and will be distributed at meetings of the EU Council working parties: TWP, PROCIV-CER as part of the Polish Presidency of the EU Council.

In our opinion, the results of this survey could contribute to the discussion about the development of antiterrorist and counter-sabotage initiatives, including risk prevention and awareness-raising at the EU level and in the Member States.

The beginning of the research survey

1. What objects are terrorists/saboteurs interested in when planning their activities in the European Union?

   When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

   When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

   - buildings of state offices and EU institutions,
   - critical infrastructure facilities,
   - military bases,
   - symbolic tourist landmarks,
   - sports and entertainment facilities,
   - places of religious worship,
   - large-area commercial facilities,
   - public transport system,
   - commercial goods transport system,
   - others.

2. What methods of attack and sabotage can be the greatest challenge for law enforcement authorities and institutions which ensure the security of people and facilities?

   Choose one answer:

   - unmanned vehicles (air, land, water),
   - 3D printing,
   - vehicles used for ramming the target,
   - improvised explosive devices,
   - weapons made of composites,
   - CBRN,
   - incendiary agents,
   - so called shadow fleet/dark fleet,
   - others.

3. Should we expect, in a 3-year perspective, the use of terrorist/sabotage activity as part of hybrid threats undertaken on the territory of the EU by a foreign state?

   Choose one answer:

   - yes,
   - no,
   - hard to say.

4. Which facilities, in the 3-year perspective, will be characterised by the highest level of terrorist/sabotage attack threat in the EU?

   When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

   When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

   - NATO military bases,
   - critical energy infrastructure facilities,
   - telecommunications infrastructure,
   - public transport system,
   - commercial goods transport system,
   - government offices,
   - tourist infrastructure,
   - sport and entertainment facilities,
   - places of religious worship,
   - headquarters of EU institutions and agencies,
   - others.

5. Which critical infrastructure systems, in the 3-year perspective, should be treated as a priority in terms of building their resistance to hybrid threats?

   When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

   When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

Terrorism – Studies, Analyses, Prevention
2025, special edition: 249–270

- transport of commercial goods (communication routes and transhipment hubs),
- water supply,
- energy,
- telecommunications,
- health protection,
- mass public transport,
- others.

6. Which of the areas of counteracting terrorist activities require priority treatment on the EU level today?

   Choose one answer:

   - counteracting radicalisation leading to terrorist activities,
   - counteracting online recruitment for terrorist/sabotage activities,
   - detecting and blocking terrorist propaganda,
   - detecting and blocking terrorist/sabotage manuals published on-line,
   - detection technologies for devices used to carry out terrorist attacks,
   - counteracting the financing of terrorism,
   - educational initiatives concerning security culture for facilities vulnerable to terrorist/sabotage attacks,
   - others.

7. What can increase the level of resistance to terrorist attacks and sabotage activities in protected facilities?

   When you use your mobile phone to fill in the questionnaire: drag the option and drop it to arrange the order.

   When you use your computer to fill in the questionnaire: number the options using the button on the left or drag the option and drop it to arrange the order.

   - standardisation of physical security (also security personnel procedures),
   - tasks performed by internal security auditors,
   - the use of security control tests by external supervisory entities (such as: EU institutions, state inspection authorities),

- development of intelligent electronic systems for detecting security incidents,
- development of anti-terrorist prevention initiatives as part of the security culture of the facility (education for security),
- improving cooperation between CI entities and entities responsible for security,
- detection of suspicious behaviour carried out by trained security personnel,
- others.

8. Attacks on critical infrastructure are currently carried out by:

Choose one answer:

- cybercriminals associated with a state actor,
- cybercriminals who are motivated only by the desire for financial gain,
- activities of the so-called insiders associated with a state actor,
- activities of the so-called insiders associated with terrorist activity,
- saboteurs associated with the activity of radical social movements,
- saboteurs associated with a state actor,
- none of the above.

COMPLETE THE INFORMATION

Choose one answer:

- EU Member State representative,
- representative of the EU institution or agency,
- representative of a country that is a strategic partner of the EU PSA.

The end of the research survey

Karolina Wojtasik, PhD, MBA

Security specialist, court expert, academic researcher, vice-president for scientific affairs of the Polish Association for National Security (PTBN), chief expert of the Government Centre for Security (RCB). During Polish presidency of the European Council, she plays the role of the president of PROCIV–CER working party. She deals with the broadly understood security of critical infrastructure, especially in the context of threats to physical and personal security. In addition, she analyses the activities of Salafi terrorist organisations, the modus operandi of the perpetrators of terrorist attacks in the EU and the USA, as well as instructional publications on methods of carrying out attacks on civilians and facilities. Author of books: *Anatomy of a Terrorist Attack. On the Strategy and Tactics of Terrorists, Paths of Jihadi Radicalisation. A textbook for students of sociology, political science and security.* Co-author of the book *The Polish anti-terrorist system and the realities of the attacks of the second decade of the 21st century* and many other publications related to terrorism, as well as security and building the resilience of critical infrastructure. Creator of the popular science channel Anatomia zamachu on YouTube.

Contact: karolina.wojtasik@rcb.gov.pl

Damian Szlachter, PhD

Editor-in-chief of the ISA (ABW) scientific journal "Terrorism – Studies, Analyses, Prevention". Member of the steering committee of the EU Protective Security Advisors group. National expert at the European Commission's Directorate-General for Migration and Home Affairs in the Policy Group on Public Spaces Protection. National auditor for quality control in civil aviation security (of the Civil Aviation Authority). Participant in the work of more than a dozen inter-ministerial teams and state administration working groups tasked with building resilience to terrorist and hybrid threats to strategic facilities for state security and critical infrastructure. Member of the team to investigate the challenges of engineering security of critical infrastructure buildings at the General Office of Construction Supervision. Author of nearly 40 scientific articles and co-author of several books and specialist reports on internal security.

Contact: d.szlachter@abw.gov.pl