PUBLIC

Security of Explosives pan-European Specialists Network

D9.2

Updated threat and attack strategies

KEMEA

D9.2

Updated threat and attack strategies

Main Author(s)	
Name	*Organisation*
Ioannis Daniilidis	KEMEA
Georgios Antonopoulos	KEMEA

Document information	
Version no.	*Date*
1.0	2023-03-31

Summary

Deliverable D9.2 is an updated follow-up report to the D9.1 deliverable. The subject of study is the review and analysis of the evolution of the threats and attack strategies, the motives and vulnerabilities that are the root cause. In the frame of EXERTER WP9 a structure has been developed with the pillars that comprise the sequence for the identification of a threat, the vulnerabilities and the potential attack strategies. The definition of the aforementioned pillars enables the projection to the trends, patterns and future threats and attack strategies using explosives; these are reported in more detail in the EU-RE D9.4, Updated threats and attack strategies – Annex 1, connected to this report, and in the upcoming EXERTER D6.18 (EU-C).

The report investigates the motives and enablers that induce radicalization, confidence and knowledge to materialize attacks, both in the frame of the terrorism but also of general use of explosives by other actors such as organised crime groups. Furthermore, the case study of dangers emanating from conflict zones has been analysed. While thorough review of past events has been deployed as lessons learnt, an attempt is made to identify and report the evolution of trends on targets, vulnerabilities, threats, attack strategies and mode operandi.

The invaluable pool of resources through the interaction and feedback with the practitioners in the course of the EXERTER workshops, provided another channel of input to this study. The deployment of explosives through different channels of acquisition, preparation and attack planning is a very challenging and multi-faceted issue to tackle, that will enable interference and effective counter measures to the time-line of an attack.

TABLE OF CONTENTS

1. Introduction

1.1. Background

Throughout human history, there have been many threats to the security of nations. These threats have brought about large-scale losses of life, the destruction of property, widespread illness and injury, the displacement of large numbers of people, and devastating economic loss. Recent technological advances and ongoing international political unrest are components of the increased risk to national security. One major component of threat is the engagement of explosives to cause terror and destruction.

In the course of the last decades numerous attempts and attacks using explosives to various targets have been recorded. The motives and radicalisation channels, especially enhanced during the COVID-19 period, have influenced a wide group of people of different social background. A continuously evolving landscape of terrorist and organised crime group threats and attack strategies has been enabled through technological advancements and available knowledge, constituting a major global security challenge for governments, but also a regional concern for decision-makers and the general public.

Attacks have been carried out in recent years and many attempts have been foiled according to Europol's statistics report[1]. An increasing trend of lone actors associated with jihadist and right-wing violent extremism form the greatest threat associated with potential terrorist and violent extremist attacks in the EU. The online environment plays a key role in this as it facilitates (self-) radicalisation and the spread of terrorist propaganda. Worldwide efforts from agencies associated with security issues (for example Europol, Interpol and national agencies) have increased their capabilities in identifying terrorist and violent extremist content, collaborating with online providers to remove it. The EU Internet Referral Unit (EU IRU), based at Europol's European Counter Terrorism Centre (ECTC), has been actively engaging in this domain, promoting new and innovative approaches to technological challenges.

The impact of the COVID-19 pandemic on terrorism was particularly visible in terms of shaping extremist narratives. This has made some individuals more vulnerable to radicalisation and recruitment into terrorism and extremism. Social isolation and more time spent online have exacerbated the risks posed by violent extremist propaganda and terrorist content, particularly among younger people and minors. The societal impact of the COVID-19 pandemic remains to be evaluated in the forthcoming years, but society must remain vigilant about some of the long-term challenges that follow on from this unprecedented crisis.

Undoubtedly, the geopolitical shifts and the fallout from Russia's war of aggression against Ukraine will have a lasting impact on the EU's security for years to come. This war has already attracted several radicalised individuals from Member States who have joined the fight on both sides. Moreover, the ongoing war is likely to spark violent extremist reactions and mobilisation, particularly in the online domain. Furthermore, influences that emanate from such conflict zones including transfer of explosives and weapons, pose another threat to civil society. It is imperative that close monitor of the developments and the lessons learnt in the past in dealing with foreign fighters returning from battlefields in the Middle East, must be active.

Close collaboration amongst Member States and beyond, with international agencies (such as Interpol, Europol etc) is crucial to understand and mitigate terrorist threats to EU communities.

Based on the aforementioned considerations and with guide the trends and patterns in past attacks, this report presents an overview of the situation in the European frame, the current and emerging threats as well as potential attack strategies, based on publicly available information and expert knowledge.

---

[1] EU Terrorism Situation and Trend Report 2022

1.2. Objectives and scope

The overall purpose of this report is through the examination of past events and analysis of the current global evolving situations, to project and identify potential threats and attack strategies concentrating on deployment of explosives.

To this end, the report will provide an overview of the terrorist and organised crime threats, adopting a historical and legal perspective, exposing vulnerabilities that become enablers for terrorist attack strategies.

In addition, the last chapter will draw upon the main findings of the previous parts, so as to reach conclusions on emerging trends and patterns, which could further be the basis of plausible scenarios and predictions of future incidents.

This report is connected to the EU-RE classified report D9.4, Updated threats and attack strategies – Annex 1, and the EU-C D6.18, where more details can be found.

2. Review of Terrorist Threats

Commencing this report, the definition of terrorism will provide the frame of action for actors involved in the attacks. Furthermore, the general landscape of security and its vulnerabilities exposes the motives and trends for evolved strategies and exploitation of resources. A number of current developments in modern terrorism, encompassing the technological enablers that enhance and modify the targets, threats, vulnerabilities and attack strategies in the European territory, is presented.

2.1. Defining Terrorism

Terrorism is the use of force or violence against persons or property in violation of the criminal laws of a state for purposes of intimidation, coercion, or ransom. Terrorists often use threats to:

• Create fear among the public.

• Try to convince citizens that their government is powerless to prevent terrorism.

• Get immediate publicity for their causes.

Acts of terrorism include threats of terrorism; assassinations; kidnappings; hijackings; bomb scares and bombings; cyber attacks (computer-based); and the use of chemical, biological, nuclear and radiological weapons.

High-risk targets for acts of terrorism include military and civilian government facilities, international airports, large cities, and high-profile landmarks. Terrorists might also target large public gatherings, water and food supplies, utilities, and corporate centers. Further, terrorists are capable of spreading fear by sending explosives or chemical and biological agents through the mail.

Terrorism remains a key threat to the EU's internal security. More than 20 completed, foiled and failed terrorist attacks were recorded in the EU. The attacks were carried out from different actors with different motive; religious and political motives are the main incentives for carrying out terrorist attacks.

Lone actors remain the primary perpetrators of terrorist and violent extremist attacks in Europe. However, attack plots involving several actors were also disrupted. Individuals carrying out attacks alone have been associated mainly with jihadist terrorism and right-wing terrorism and violent extremism. This does not necessarily mean that these individuals act in complete isolation. Online community building often plays a key role, as it connects peers virtually on a global scale. This drives radicalisation and provides access to terrorist propaganda, instructional material and opportunities for procurement of weapons and explosives precursors.

Weaponry was used in the completed terrorist attacks that is relatively easy to source and does not require extensive skills for assemblage or use; a recent example is the attack at Hamburg to a Jehovah witness church. Weapons used in attacks in the EU included bladed weapons, vehicles (in ramming attacks) and improvised incendiary devices (IIDs). Disrupted plots showed the intent and efforts to produce improvised explosive devices (IEDs).

Terrorist propaganda disseminated online has continued to reflect themes related to COVID-19. The increased amount of time spent online due to COVID-19 restrictions, amongst other reasons, constitutes a risk factor in vulnerable individuals' potential pathway to extremism. The combination of social isolation and more time spent online during the pandemic has exacerbated the risks posed by violent extremist propaganda and terrorist content online, particularly among younger people and minors. Gaming platforms and services are increasingly used by right-wing terrorists to channel terrorist propaganda targeting a younger generation of users. Pandemic-linked restrictions also have the potential to exacerbate pre-existing mental health issues potentially prompting violent acts that resemble terrorist or violent extremist attacks.

Violent anti-COVID-19 and anti-government extremism, which is not affiliated with traditional violent extremist and terrorist activities, emerged in some Member States and non-EU countries. Such forms of violent extremism materialised in open threats, hateful messages spread online and, in some cases,

the use of violence. Targets included politicians, government representatives, police, health authorities involved in the management of the crisis, or personnel from test and vaccination centers.

Geopolitical developments in key regions outside of the EU influence terrorist narratives and propaganda spread in Member States. The current terrorist threat for Member States appears not to have been directly affected by the Taliban's takeover of power in Afghanistan. However, it increased global attention on religiously motivated insurgencies and, thereby, provided jihadists affiliated with both al-Qaeda and the self-proclaimed Islamic State (IS) terrorist group opportunities to promote their own narratives.

2.2 Defining Conflict Zones

2.2.1 Conflict Zones

Recent developments with the conflict between Russia and Ukraine over the last year have emerged another pool of potential threat, outside the terrorist frame: the concern is of the influences emanating from conflict zones. Such zones have been on the fringe of the European borders over the last decades such as Syria, Armenia, Kosovo. The traditional issues derived from conflict zones are enhanced with the technological advancements. Points of concern are about how likely is a transfer to a European setting (such as the phenomenon returning Foreign Terrorist Fighter (FTF) that was analysed in EXERTER D9.1) and which factors could impede or limit this transfer? Or, which repercussions will have this development for the European security environment in terms of technology policy and research?

The definition of the term Conflict has evolved over the last decades and has become more "hybrid" and gained much broader influence on scale, time and space. This change was a result of the technological developments, the globalization, the wars of previous decades, the economic failures, as well as the terrorist and general organized crime group (OCG) networks created.

Defined after the 2006 summer war between Israel and Hezbollah and currently used for explaining the tactics used by the Taliban, the Syrian opposition, the Islamic State in Iraq or the Ukrainian forces against the Russian invasion on Ukraine, the concept of hybrid conflict has acquired a significant degree of popularity for defining the new wars of the 21st century.

This model causes a great confusion and difficulty to take new emerging dynamics. Conflicts characteristic of the globalized world are innovative in terms of actors involved (states, group of guerrillas and terrorists, criminal and private militaries under contract) and by the means used (simple and affordable weaponry used in novel ways, highly sophisticated weapon systems or dual-use technologies), the tactics employed (limited conventional actions, terrorist acts, insurgency, guerrillas or information operations), the chosen scenarios (from urban and densely populated areas to remote or hard-to-reach places), the multipliers used (positioning and geolocation systems, open source intelligence (OSINT) and social networks (SOCMINT), information networks, advanced communications and the Internet) or the sources of financing managed (from legal activities to criminal acts with close collaboration with organized crime). All aforementioned characteristics make the "new wars" very different from the most representative conflicts of the past, where regular armies belonging to a nation-state tended to fight conventionally and symmetrically on clearly defined fronts, with technologically advanced means for the time and subject to the customs of war commonly accepted by the contenders. Consequently, it is not unexpected that any adversary – both conventional and irregular – will try to take advantage of the current opportunities offered to exploit, as has happened in Afghanistan or Iraq and is happening in the Islamic State. The vast gaps and enormous limitations of the Westernized style of combat, based on technological supremacy, doctrinal, organizational, logistical and tactics of its armed forces and in strict compliance with the laws and customs of war in order to achieve quick, decisive, forceful victories with hardly any collateral damage that, as the War on Terror and the disorders brought about by the Arab Spring have confirmed that this is more the exception than the norm.

Although both state and non-state actors engage in hybrid warfare they vary widely in their means and actions; all exhibit the capability to synchronize various instruments of power against specific vulnerabilities to create linear and non-linear effects. By focusing on these characteristics of a hybrid warfare actors' capabilities, together with the target's vulnerabilities in these areas and then overlaying these with the means and effects, a generic description of hybrid warfare is drawn. A hybrid warfare is described as: *the synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects*. The hybrid warfare is asymmetric and uses multiple instruments of power along a horizontal and vertical axis, and to varying degrees shares an increased emphasis on creativity, ambiguity, and the cognitive elements of war. This sets hybrid warfare apart from an attrition-based approach to warfare where one matches the strength of the other, either qualitatively or quantitatively, to degrade the opponent's capabilities.

2.2.2 Influences of conflict to the broader security environment and specially to Europe

In the current war in Ukraine vast information, photos, videos via the TV and the various social media applications is generated and distributed. Along with these many different perspectives of the battles taking place are disseminated, the missiles deployed, the loaded with explosives UAVs, the VBIEDs, the tactics to attack and ambush the enemy. All the above become more evident when the immigration flows of people crossing the borders of Europe, becoming the live testimony of the atrocities. The societal impact of the conflict zone of Ukraine affects psychologically the everyday life and mind of the European citizens in an indirect way in a broader zone than this of the conflict itself. Recently two cases with postal IEDs took place to Ukrainian Embassy in Madrid Spain transfer the conflict setting to Europe.

A novelty introduced clearly in this conflict is that the engaging parties in the war are not only states but also various non-state actors (mercenaries, minority or religious groups) who fight for profit or their own causes. Although both state and non-state actors engage in hybrid warfare the means and actions vary widely. The common denominator though is that all exhibit the capability to synchronize various instruments of power against specific vulnerabilities to create linear and non-linear effects.

The use of multiple instruments of power (soft and hard) as a leverage tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects, along with propaganda and fake news influences the below indicative list of the domains:

1. political domain where creates obstacles and problems in the government s decision making
2. economic impact where the leverages of energy, water, raw materials or recently seen food supply disrupt the operation of trade networks, factories etc.
3. civil domain in which is cultivated fear, public disappointment, frustration
4. information domain –cyberattacks or spread of disinformation via social media and through other possible means that the perpetrator exerts influence or controls
5. terrorism and organized crime

Criminals exploit the plethora of channels available for gaining access to new sophisticated weapons and explosives, or from terrorists to transfer the expertise of the battlefield. Immigration is one of the tools to achieve the goal and one of the first implicit problems to be encountered from the states in the vicinity of a conflict. Fears that terrorists deliberately infiltrating refugees are a reminder of the November 2015 terrorist attacks in Paris; at least two of the attackers were believed to have entered the European Union via Greece, posing as asylum seekers. The landscape induced due to the conflicts and the states in the perimeter of the zone becomes very complex with multiple actors involved; an enmeshed situation is developed by the media and the minds of politicians, security professionals and the public, making it the more imperative to assess the threat of terrorism objectively as it relates to mass migration. All the aforementioned domains are not independent and every disorder in one or more of them, disturbs the social function as a whole.

Given that domestic jihadi terrorists have been responsible for many of recent plots in the West, an arguably more likely scenario is that refugees from Syria and elsewhere will be targeted for recruitment

by Western extremists upon arrival, rather than traveling with the pre-existing intention of committing acts of terrorism. It is well known that recruitment of extremists takes place in refugee camps.

2.2.3 General measures to face the European security challenges

The spread of a conflict to a neighboring country besides the above-mentioned factors could merely serve political or military estimations, so Europe would be ready for the worst case scenario and elaborate its policies, contingency plans, create an atmosphere of cooperation between the public and private sector, educate on relative issues and strengthen the will of its citizens and update through research the technological "hard power" needed in the case of such a scenario.

3. Conclusion

A detailed review and analysis of past events, in combination with partners of EXERTER as well as expert invitees to workshops in the course of the annual scenarios addressed for the EXERTER project, have assisted the report of highlights of the multiple facets of the complex and evolving frame formed by the targets, vulnerabilities, threats and attack strategies. Knowledge and technological enablers available and accessible to everyone, as well as identified vulnerabilities (legal etc) create a challenging task for development of counter measures in the time-line of a planned attack. The actors involved in acquiring and deploying explosives (HMEs or from conflict zones etc) with different motive are increasing and close monitoring is required.

The analysis has shown the global scale of the issue of deployment of explosives as rapid exchange of information and network forming is possible; hence, efforts and collaborations must be at international level amongst agencies and organisations (both state and non-state) to counter act to the evolution of the multiparameter landscape through a systematic evaluation and gap analysis.

Reference List

- Council of Europe on Strengthening Chemical, Biological, Radiological and Nuclear Security in the
- European Union – an EU CBRN Action Plan, Brussels, 29 June 2009
- Explosive Threats – The Challenges They Present and Approaches to Counter Them, Peter Hotchkiss, Ph.D. Sandia National Laboratories
- The CBRN threat: Past, present and future, Andrew Prosser and Sergio Bonin, Research gate
- Algorithms and terrorism, UNCRI
- CBRN terrorism: threats and the EU response, European parliament, briefing January 2015
- Terrorist Groups, Artificial Intelligence and Killer Drones
- Jacob Ware, September 2019, WARONTHEROCKS.COM
- Terrorists 'certain' to get killer robots, says defense giant, Published 30 November 2017 BBC
- Artificial Intelligence, The Visible Path, Atul Pant
- Evolving Security Threats and Advanced Security Technologies, Special Report, v3, World Institute for Nuclear Security, April 2018
- Homeland Threat Assessment, October 2020
- Improvised Explosive Device (IED) Guidelines for Crowded Places, Australia – New Zealand Counter Terrorism Committee
- The Tactics and Targets of Domestic Terrorists, S.G. Jones, C. Doxsee, N. Harrington, Center for Strategic & International Studies, July 2020
- Malicious use of artificial intelligence, February 2018
- Syria's War and the Descent Into Horror." 2022. **https://www.cfr.org/article/syrias-civil-war**.
- Global Terrorism Index GTI-2022 – Measuring the Impact of Terrorism, Institute of Economics and Peace
- How ISIS Is Transforming | RAND." 2022. https://www.rand.org/blog/2017/09/how-isis-is-transforming.html.
- Uppsala/ Peace Research Institute Oslo (PRIO) Armed Conflict Database /Armed Conflict Location Events Database (ACLED)
- "Counterterrorism and youth radicalization in Jordan: Social and political dimensions." CTC Sentinel 10.4 (2017): 25-30.
- Izzi, Valeria. "Promoting Decent Employment for African Youth as a Peace-Building Strategy" n.d., 64.
- "Analysing Terrorism from a Systems Thinking Perspective." https://www.researchgate.net/publication/262826171_Analysing_Terrorism_from_a_Systems_Thinking_Perspective.
- "Political Socialization and Terrorist Radicalization Among Individuals Who Joined Al-Shabaab in Kenya: Studies in Conflict & Terrorism: Vol 37, No 11." https://www.tandfonline.com/doi/abs/10.1080/1057610X.2014.952511.
- 'ISIS in Their Own Words' by Anne Speckhard and Molly D. Ellenberg." https://digitalcommons.usf.edu/jss/vol13/iss1/5/.
- 'ISIS in Their Own Words' by Anne Speckhard and Molly D. Ellenberg." https://digitalcommons.usf.edu/jss/vol13/iss1/5/.
- "How Terrorist Groups End: Lessons for Countering al Qa'ida | RAND." https://www.rand.org/pubs/monographs/MG741-1.html.
- "How Terrorist Groups End: Lessons for Countering al Qa'ida | RAND." **https://www.rand.org/pubs/monographs/MG741-1.html**.
- Wood, Alex Stephen. "Dangerous Allies: States, Paramilitary Violence, and Civil War," n.d., 86.
- "FARC | History & Peace Deal | Britannica." https://www.britannica.com/topic/FARC.

- "Colombia Reaches New Peace Deal with FARC Rebels | News | Al Jazeera." https://www.aljazeera.com/news/2016/11/13/colombia-reaches-new-peace-deal-with-farc-rebels.
- "US Removes Colombia's FARC from Terrorism Blacklist - CNNPolitics." https://edition.cnn.com/2021/11/30/politics/farc-delisting/index.html.
- "US Could Drop Colombia's FARC from 'Terror' List by End of Month | Conflict News | Al Jazeera." https://www.aljazeera.com/news/2021/11/24/us-to-drop-colombia-farc-rebels-terror-list-end-of-month.
- Bauman, Z. (2002). Reconnaissance wars of the planetary frontierland. *Theory, Culture & Society*, *19*(4), 81-90. doi: 10.1177/0263276402019004006
- Bloom, M. (2012). *Bombshell: women and terrorism*. Pennsylvania: University of Pennsylvania Press.
- Bruce, G. (2013). Definition of terrorism social and political effects. *Journal of Military and Veterans Health*, *21*(2), 26-30.
- Cronin, A. K. (2003). Behind the curve: Globalization and international terrorism. *International security, 27*(3), 30-58.
- Das, R. (2016). The burden of insecurity: Using theories of International Relations to make-sense of the state of post-9/11 politics. Relationsinternational.com.
- Ellis C., Pantucci R., van Zuijdewijn J. R., Bakker E., Gomis B., Palombi S. & Smith M. (2016). Countering Lone-Actor Terrorism Series No. 4. Lone-Actor Terrorism Analysis Paper. *Royal United Services Institute for Defence and Security Studies*.
- European Commission. (2020). *A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond*. 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 COM(2020) 795 final.
- European Parliament. (2018). *The return of foreign fighters to EU soil: Ex-post evaluation*. European Parliamentary Research Service
- Europol. (2016). Changes in modus operandi of Islamic State terrorist attacks. Review held by experts from Member States and Europol on 29 November and 1 December 2015. Europol Public Information.
- Europol. (2019). *TE-SAT 2018: EU Terrorism Situation and Trend Report*. Publications Office of the European Union.
- Europol. (2020). *TE-SAT 2019: EU Terrorism Situation and Trend Report*. Publications Office of the European Union.
- Europol. (2021). *TE-SAT 2020: EU Terrorism Situation and Trend Report*. Publications Office of the European Union.
- Europol. (2022). *TE-SAT 2021: EU Terrorism Situation and Trend Report*. Publications Office of the European Union.
- Ganor, B. (2015). Global alert: The rationality of modern Islamist terrorism and the challenge to the liberal democratic world. New York: Columbia University Press.
- Gilsinan, K. (2015). ISIS: An Organization – and an Idea. *The Atlantic*.
- Hoffman, B. (2006). *Inside terrorism*. New York: Columbia University Press.
- Jones, S. G., Toucas, B., & Markusen, M. B. (2018). *From the IRA to the Islamic State: The evolving terrorism threat in Europe*. Center for Strategic & International Studies.
- Joosse, P. (2007). Leaderless resistance and ideological inclusion: The case of the Earth Liberation Front. *Terrorism and Political Violence*, *19*(3), 351-368. doi: 10.1080/09546550701424042.
- Mockaitis, T. R. (2007). *The" new" terrorism: myths and reality*. London: Greenwood Publishing Group.
- Neumann, P. R. (2016). Radicalized: new jihadists and the threat to the West. Bloomsbury Publishing.
- Pantucci, R. (2011). A typology of lone wolves: Preliminary analysis of lone Islamist terrorists. *International Centre for the Study of Radicalisation and Political Violence.*

- Pillar, P. R. (2011). Jihadi Terrorism: A Global Assessment of the Threat. Στο Coolsaet, R. (Ed.), *Jihadi terrorism and the radicalisation challenge: European and American experiences*. London: Routledge.
- Rapoport, D. C. (2002). The four waves of rebel terror and September 11. *Anthropoetics*, *8*(1), 1-17.
- Schmid, A. P., & Jongman, A. J. (1988). Political terrorism: A new guide to actors, authors, concepts, data bases, theories and literature. New Brunswick, NJ: Transaction Books.
- Schmid, A. P. (1992). The response problem as a definition problem. *Terrorism and Political Violence*, *4*(4), 7-13. doi: 10.1080/09546559208427172
- Seib, P. and Janbek, D. 2011. Global Terrorism and New Media: The post-Al Qaeda generation. London: Routledge.
- Simon, S. & Benjamin, D. (2000). America and the New Terrorism. *Survival*, 42(1). 59-75.
- START (National Consortium for the Study of Terrorism and Responses to Terrorism). (2018). Global Terrorism Database (GTD)
- START (National Consortium for the Study of Terrorism and Responses to Terrorism). (2018). *Terrorist Attacks Involving Package Bombs, 1970 – 2017*. Factsheet.
- Teichman, J. (1996), "How to define terrorism", in Gearty, C.A. (Ed.), *Terrorism*, Dartmouth, Aldershot.
- Tucker, D. (2001). What is new about the new terrorism and how dangerous is it?. *Terrorism and Political Violence*, *13*(3). doi: 10.1080/09546550109609688.
- United Nations Office for Counter-Terrorism (UNOCT). (2018). United Nations Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism.
- Van Ginkel, B., & Entenmann, E. (2016). The Foreign Fighters Phenomenon in the European Union. Profiles, Threats & Policies. *The International Centre for Counter-Terrorism – The Hague (ICCT)*, *7*.

Disclaimer:
The content of this report reflects only the author's views and the European Union is not liable for any use that may be made of the information contained herein.