



CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM



EMERGING THREATS in TERRORISM

Research Report by the
NATO Centre of Excellence Defence Against Terrorism



EMERGING THREATS

in

TERRORISM

Haldun Yalçınkaya
Elif Merve Dumankaya

COE-DAT
Centre of Excellence Defence Against Terrorism

EMERGING THREATS in TERRORISM

Contributing Authors: Haldun YALÇINKAYA, Ph.D. (TOBB ETU, Türkiye)
Elif Merve DUMANKAYA (Bilkent University, Türkiye)

NATO COE DAT Project Team Leaders: Lt.Col. Uwe BERGER
Maj. Ali MAVUŞ

First Edition, Ankara, Dec 2022

Published by

Centre of Excellence Defence Against Terrorism (COE-DAT)

Publisher Certificate Number: 51450



Address : Devlet Mahallesi İnönü Bulvarı Kirazlıdere Caddesi No:65 Çankaya 06582

Ankara - TÜRKİYE

P.O. Box Address : P.K.-57 06582

Bakanlıklar-ANKARA TÜRKİYE

PHONE : +90 312 425 82 15

FAX : +90 312 425 64 89

E-MAIL : info@coedat.nato.int

Printed by Başkent Klişe Matbaacılık

Bayındır 2. Sk. No: 30/1 06420 Çankaya/Ankara (0312) 431 54 90

© All rights reserved by the Centre of Excellence Defence Against Terrorism.

No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of COEDAT.

Disclaimer

This project report is a product of the Centre of Excellence Defence Against Terrorism (COE-DAT), and is produced for NATO, NATO member countries, NATO partners and related private and public institutions. The information and views expressed in this report are solely those of the authors and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the authors are affiliated.

43 pages;

ISBN: 978-605-74376-3-1

1. Terrorism 2. Counter Terrorism 3. Security 4. Emerging Threats.

To cite this book: Haldun Yalçinkaya and Elif Merve Dumankaya, *Emerging Threats in Terrorism*, (Centre of Excellence Defence Against Terrorism, 2022)

CONTENTS

List of Figures	4
List of Tables	4
1. Executive Summary	5
2. Introduction and Methodology	6
a. Introduction	6
b. Methodology	6
3. Researching the Emerging Threats in the Future in terms of Terrorism	12
a. Main Security Challenges in the Current International Environment	12
b. Security Challenges in Different Regions	14
c. Emerging Terrorist Threats	17
d. Comparison of the Emerging and the Traditional Threats	20
e. A New Wave of Terrorism in the Future?	22
f. The Relationship Between the Rise of Emerging Threats and the Trends in Terrorism	24
g. Non-Aggressive Terrorist Activities	26
h. Emerging Threats and Terrorist Groups	28
i. Capacity of States in Countering Emerging Terrorist Threats	29
j. Vulnerabilities of States for Countering Emerging Threats	32
k. International Security Environment’s Agenda for the Following Years	35
4. Key Results & Recommendations	38
5. References	43

LIST OF FIGURES

Figure 1 – The Stages of the Delphi Method for the Research.....	9
Figure 2 – Fields of Security Challenges.....	15
Figure 3 – Can Non-Aggressive Terrorist Activities be possible?.....	32
Figure 4 – “Emerging Threats Empower Terrorist Groups in their Asymmetrical Struggle against the States.” What is your take on this Statement?.....	34
Figure 5 – Strengths of States in Countering Emerging Terrorist Threats.....	36
Figure 6 – Vulnerabilities for States in Detecting and Responding to Emerging Threats	39
Figure 7 – Vulnerabilities of Regions	42
Figure 8 – How do you think these Threats will evolve in the next Ten Years and in which Sectors of Security will they pose the Greatest Challenges?.....	46
Figure 9 – Security Challenges in the Current International Environment (Preparatory Survey).....	49

LIST OF TABLES

Table 1 – Distribution of Experts’ Fields	10
Table 2 – Areas of Students who Participated in the Preparatory Survey.....	12

1. Executive Summary

Terrorism has emerged as one of the greatest challenges to international security in the 21st Century. This situation compelled us to reconsider to what extent organizations could exploit the means that the current advancements provide us with, and how they could trigger ongoing instabilities. Therefore, this report intends to shed light on **Emerging Threats in Terrorism** by answering the following question:

“What are the emerging threats in terms of terrorism in the future?”

The project team implemented the Delphi Technique that enables researchers to explore what experts foresee concerning the emerging threats in terrorism. In order to conduct this research, the project team identified 30 different experts from Africa, Asia, Europe, and the Middle East who are specialized in various disciplines in order to benefit from their experience and knowledge. The areas of expertise of the respondents cover Biosecurity and Health Security, Changing World Order, Critical Infrastructure, Cyber Security, Economic Security and Development, Emerging Technologies, Energy Security, Environmental Security, Hybrid Warfare, Intelligence, Maritime Security, Migration, National Security, Nuclear Threats (Chemical Biological Radiological Nuclear (CBRN)), Social Media, Terrorism, Radicalization and Terrorist Financing.

Even though our main focus is on the responses of the experts participating in the Delphi Technique Survey, we benefited from the younger people’s evaluation of current and future threats. It was quite fruitful to compare the priorities and perceptions of the younger generation. We can conclude that their concerns are more about what they have been experiencing, instead of what they expect to be witnessing. For instance, they included epidemics and pandemics, online radicalization, societal problems, terrorist organizations’ occupation of legitimate authorities, and transportation, as being among both current and future terrorist threats.

The threats are highly uncertain, as we observe baby steps in the evolution of the international order. Among others, the first signals of mass migration attempts, demographics, increasing population, and climate change are exponentially growing issues. We are fast approaching a time when these potential problems will become more volatile, and the first half of this century might be the time humankind will not be able to avoid tackling them. Given the intertwined and cyclical nature of these problems, we should start dealing with each without further delay. We gathered our experts’ forecasts about which sectors of security will pose the greatest challenges. In this sense, we can categorize the emerging terrorist threats identified by our experts as:

- New and Emerging Technology-Related Threats
- Innovative New Threats Against Conventional Sectors
- Accumulation of Classical Terrorist Threats
- Innovative New Threats against Non-Conventional Sectors

As can be comprehended from these categorizations, emerging threats push legitimate authorities and traditional counter-terrorism approaches to evolve in order to respond to these threats. Despite this, the threats are not new, but transformative. Therefore, there is no doubt that the scope, perspective, and implementation of countering these threats should also be transformative.

2. Introduction and Methodology

a. Introduction

Not only the changing international environment but also the spread of technological advancements have been challenging every single party to reconsider their security structures. In this sense, terrorism has emerged as one of the greatest challenges to international security in the 21st Century. Terrorist organizations can easily adapt themselves to this changing environment and have become “learning organizations” by altering their patterns of behaviour in an environment in which they hold an asymmetric position compared to states that are the legitimate actors that possess larger human resources as well as wider inventories¹. This situation compelled us to reconsider to what extent these organizations could exploit the means that the current advancements provide us with and how they could trigger ongoing instabilities. Therefore, this report intends to shed light on the Emerging Threats in Terrorism.

Drawing on a multidisciplinary approach, this report garnered the knowledge of a wide variety of experts to develop a future forecast. In order to conduct this research, the project team identified 30 different experts from Africa, Asia, Europe and the Middle East who specialize in various disciplines, to benefit from their experience and knowledge. Since a parallel project with the same research question has been conducted for the American continent, this project deliberately excludes experts from that region.

The principal research question in this report addresses the following question:

“What are the emerging threats in terms of terrorism in the future?”

To provide comprehensive answers to this question, the project team implemented the Delphi Technique² that enables researchers to explore what experts foresee about the emerging threats in terrorism. The Delphi Technique surveys were disseminated in two rounds. The first round of the survey is structured with open-ended questions requiring short essay-style answers. Following the analysis of the first round, the research team developed follow-up supportive questions and distributed them to the first-round respondents based on the answers given during the previous round.

b. Methodology

To grasp a framework of how emerging threats in terrorism are likely to evolve in the future, the research team implemented the Delphi Technique which helps researchers undertake a form of brainstorming about the current issues and the possible scenarios that these issues could lead to. The Delphi Method was introduced by Olaf Helmer, Nicholas Rescher, Norman Delkoy and others in 1959³, and the first work that used this technique was titled “*Report on a Long-range Forecast*”, published in 1964.⁴ Depending on a high level of accountability and reliability, the Delphi Technique allows researchers to come up with an analysis including future forecasting about the topic under investigation.

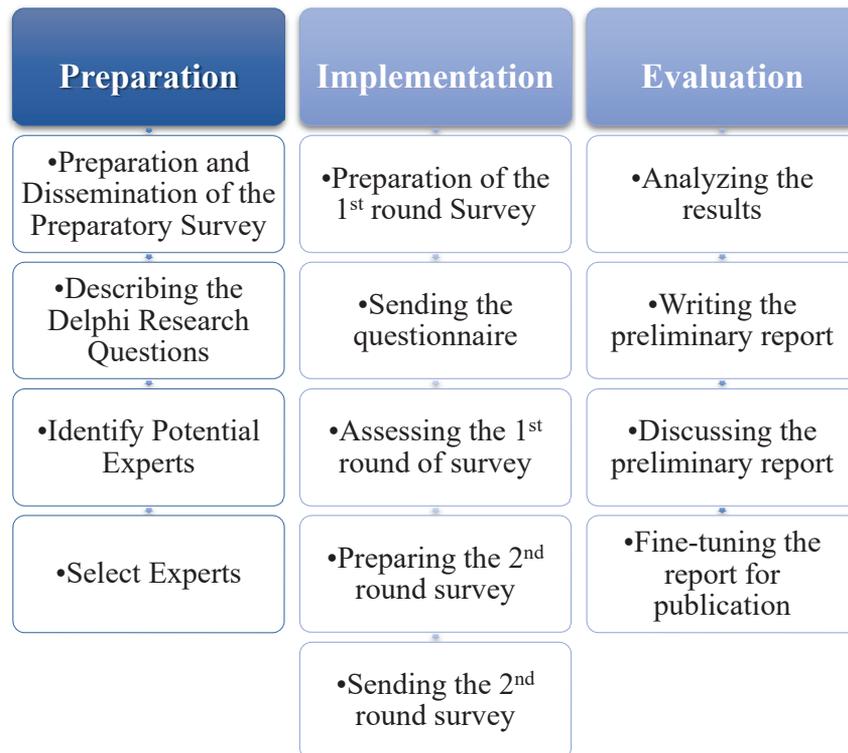
¹ Cenker Korhan Demir, “Öğrenen Örgütler ve Terör Örgütleri Bağlamında PKK”, *Uluslararası İlişkiler*, Vol. 5, No. 19, 2008, p. 58.

² The technique is explained in detail within the Methodology section that falls under this chapter.

³ Olaf Helmer and Nicholas Rescher, “On the Epistemology of the Inexact Sciences,” *Management Sciences*, Vol. 6, No.1, 1959.

⁴ Theodore J. Gordon and Olaf Helmer, “Report on a Long-Range Forecasting Study”, RAND Corp., R-2982, 1964.

Figure 1 – The Stages of the Delphi Method for the Research



The Delphi Technique consists of three different stages (Figure 1). During the Preparation Stage, researchers must first identify the potential experts that could be best suited for the research. At this stage, the research team contacted 57 experts from various disciplines in order to invite them to take part in the Delphi Survey. The distribution of experts we reached may be found below (Table 1):

Table 1—Distribution of Experts' Fields

Field	Participated	Not Responded	Rejected	TOTAL
Biosecurity and Health Security	1			57
Changing World Order	1		2	
Critical Infrastructure	1	1		
Cyber Security	1	2	1	
Economical Security and Development	1	2	1	
Emerging Technologies	3	2		
Energy Security	2	1	1	
Environmental Security	1	3	1	
Hybrid Warfare	1			
Intelligence	0	1	1	
Maritime Security	2	1		
Migration	1	2		
National Security	2			
Nuclear Threats (CBRN)	4		1	
Social Media	3	2		
Terrorism, Radicalization	5		1	
Terrorist Financing	1	1		
TOTAL	30	18	9	57

8

The research team specified seventeen different areas that would help to organize a comprehensive forecasting about the Emerging Threats in Terrorism. Since we aimed at including 30 experts, we invited many academics to take part in the research. Next, the research team prepared twelve supporting questions in line with the main research question and shared open-ended questions with the experts. The first-round of the survey was completed at the beginning of July 2022.

Supporting Follow-up Questions

Q1: What are the main security challenges in the current international environment?

Q2: What are the security challenges in your specific region?

Q3: What are the emerging terrorist threats concerning your area of expertise? Please discuss them.

Q4: How would you compare the emerging threats to the traditional ones in terms of the severity of the challenge?

Q5: In your professionally educated opinion, will we witness a new wave of terrorism in the future? If yes, please discuss.

Q6: How does the rise of emerging threats relate to trends in terrorism?

Q7: Considering that the objective of terrorism is to spread fear to the public, can non-aggressive terrorist activities be possible? What are the possible non-aggressive terrorist activities that may rely on non-traditional terrorist tactics?

Q8: Do emerging threats empower terrorist groups in their asymmetrical struggle against the states?

Q9: What are the strengths of states in countering emerging terrorist threats?

Q10: What are the possible vulnerabilities for states in detecting and responding to these threats?

Q11: How do you think these threats will evolve in the next ten years and in which sectors of security they will pose the greatest challenges?

Q12: Would you provide your foresight about the international security environment's agenda for the following years?

These first-round, open-ended questions were distributed to the selected 30 experts⁵. They were meant to invite the experts to reflect on their concerns and observations in their area of expertise. After collecting the answers, the research team analyzed the commonly-shared concerns and the issues highlighted across different responses, with regard to the Emerging Threats in Terrorism. Then, the team created a multiple-choice questionnaire for the second round and shared it with the experts participating in the first round. Both surveys concluded with the compilation of the answers of 30 experts.

These surveys were distributed and administered through online channels and the experts did not know others participating in the survey. The logic behind this was to avoid any possible biases. That is, the founders of the Delphi Technique were concerned with an asserted belief that if open discussion takes place between experts included in the Technique, the researcher could lose his or her control over the process resulting in a potential vicious cycle in terms of the variety of answers.

Moreover, the success of the method lies in the initial selection of experts. Since this technique neither aims to produce a universal, fully representative sample nor a data set that could be used for statistical analysis, it heavily depends on the ideas of a limited number of respondents. In addition, expert selection, their degree of expertise for this research, and the number of respondents participating in the survey are crucial to the Delphi Technique. In general, 30 out of 57 experts agreeing to be involved in the research, with a 52 percent rate is considered satisfactory for the prerequisites of the Delphi Technique.⁶

As an additional step at the Preparation Stage, the research team prepared an online survey for undergraduate and post-graduate students. This Preparatory Survey included the supportive follow-up questions of the Delphi Technique. One hundred and twenty Turkish students ranging from undergraduate, MA, and Ph.D.-level studies took part in the survey. The majority of the students have an educational background in International Relations, Political Science, and Public Administration⁷.

⁵ Responder experts' countries included Germany, India, Israel, Italy, Japan, Macedonia, Pakistan, Romania, Saudi Arabia, Singapore, Türkiye, Ukraine, and the United Kingdom.

⁶ Gordon, T.J., "The Delphi Method," *Futures Research Methodology*, Vol. 2, Issue 3, 1994, p. 7 (pp.1-30).

⁷ Other majors were Civil Engineering, Cyber Security, Economics, Electronical Engineering, Energy Policies, English Language and Literature, European Studies, History, Human Rights, International Law, IPE, Law, Management, Medicine, Military History, Security Studies, Sociology, Sports Sciences, and Terrorism Studies.

Table 2 – Areas of Students who Participated in the Preparatory Survey

International Relations, Political Science, and Public Administration	Other
81	39
67,50%	32,50%

Contrary to the experts later arguments, students expected *migration* to be the most serious challenge possessing high risk in the current security environment. Considering the growing societal tensions and economic burdens on states stemming from uncontrolled and irregular migration, it is no surprise that students found migration to hold high risk. This is followed by Cyber Security and Social Media, Economic Security in general, Terrorist Financing in particular, Emerging Technologies, and lastly, Pandemics, Natural and Human-made Disasters, and Bio-terrorism.

When they were asked, “*What innovative tools and methods terrorism can resort to in the next 10 years?*”, the students’ answers revolved around the following themes: Cyber Security, Emerging Technologies, Artificial Intelligence (AI), Autonomous Weapons Systems, Armed Unmanned Aerial Vehicles (UAVs), Migration, Weapons of Mass Destruction (WMDs), Robots, Biological Weapons and Bio-terrorism, Food Security, and, Threats to the Ecological Order and Metaverse.

In addition to these fields, students also specified certain areas to which terrorism will pose the greatest threats. Apart from the items given in the previous answers, they included epidemics and pandemics, online radicalization, societal problems, terrorist organizations’ occupation of legitimate authorities, as in the case of the Taliban, and transportation.

Even though our main focus was on the answers of the experts participating in the Delphi Technique Survey, it was quite fruitful to compare the priorities and perceptions of the younger generation. We can conclude that their concerns are more about what they have been experiencing, instead of what they expect to be witnessing.

3. Researching the Emerging Threats in the Future in terms of Terrorism

a. Main Security Challenges in the Current International Environment

The second decade of the 21st Century coincides with an era that signifies the character of the international system as *uncertain*. Following World War II, even though the nuclear armament race created some kind of stability and balance in the international system in terms of preventing wars to some extent, this seems to have changed over time⁸. Nowadays, the outbreak of war between states has become, to some extent, more likely than it was before. In addition, the involvement of new actors in the system could be regarded as a challenge⁹. Therefore, uncertainty and unexpected elements in the current system diversified the agenda of *international security*¹⁰.

⁸ John J. Mearsheimer, “Back to the Future: Instability in Europe After the Cold War”, *International Security*, Vol. 15, No. 1, 1990, pp. 5-56.

⁹ Şaban Kardaş, “The Transformation of the Regional Order and Non-state Armed Actors: Pathways to the Empowerment”, pp. 21-39 in Murat Yeşiltaş and Tuncay Kardaş (eds.), *Non-State Armed Actors in the Middle East: Geopolitics, Ideology and Strategy*, (London: Palgrave MacMillan, 2008).

¹⁰ Arnold Wolfers, “National Security as an Ambiguous Symbol”, *Political Science Quarterly*, Vol. 67, No. 4, December 1952, pp. 481-502.

Ongoing challenges are so compelling that neither prevention of wars and the proliferation of destructive weapons, nor easing the impacts of climate change and pandemics, seem to be easily achieved by the *international community*. Experts underlined that there is a growing lack of trust of international agreements and conventions in the sense that neither these regulations nor the international community will be able to prevent turmoil. On the other hand, this could further lead to proliferation of nuclear weapons as the most important tool to defend territorial integrity and non-interference in internal affairs.

Contrary to what happened right after WWII, for states, nuclear arsenals could be the most important tools to defend territorial integrity and non-interference in internal affairs resulting in turmoil in the international system. In addition, according to the experts, the new era can also lead to further challenges that do not recognize borders such as *terrorism, disruptive technologies, and emerging rogue states*.

In this sense, *terrorism* occupies a huge place in the international agenda following the destruction of the 9/11 attacks. Terrorist organizations are quite flexible and adjustable to contemporary conditions. Bearing in mind that these are “*learning organizations*”, evolving in time depending on their needs to survive in such an asymmetric environment, they can make use of societies’ vulnerabilities and internal divisions stemming from political and ideological polarization. In recent years, rising hostilities and violence among religious extremists, and far-right and far-left extremists, have become a tangible security risk. Religiously-motivated terror attacks in the West have reached historically high levels in the period between 2014-2016. Being radicalized in similar ways, and provoking hatred of each other, a triangular reinforcing cycle of violence among religious extremists, and far-right and far-left extremists, is leading to an increase in the number of attacks from each side. In this sense, social media has allowed extremist groups to increase their effectiveness by supporting political fault lines in terms of race, gender, culture, religion, and ideology. According to some of our experts, states are more focused on increasing their capacities as part of renewed *great power competition*, and are paying less attention to terrorists, because of the recent developments in Ukraine. Expectedly, these organizations are also observing some states and are willing to make use of state distractions. The terrorist organizations, from our experts’ viewpoints, consider this misfocus a perfect time for *vengeance* to pay back for the two long decades of the War on Terror.

Furthermore, *disruptive technologies* can be used as a vicious tool to overcome this asymmetric position by terrorists, rogue states, and other actors to weaken societies, economies, and most importantly the trust in democracy. Sophisticated software for using social networks will influence the cognition of populations, politicians, or any other target groups to change their perceptions, attitudes, and beliefs to undermine the trust in governments.

In the current international environment, *rough states* are direct threats to international security. In this context, our experts refer to the Russian aggression toward Ukrainian soil and share the idea that “The Russian re-invasion of Ukraine clearly is teaching that any state which does not respect the international system can create security challenges in their regions.” The threat of rouge states is largely related to rivalries between great powers, provoking short- and medium-term security challenges with more-than-regional implications. In terms of this rivalry, the US, China, and Russia take the lead. The Russo-Ukrainian conflict could be best described as a manifestation of the rivalry between Russia and the US/NATO, for some. Another example is the Chinese *Belt and Road Initiative*

which the US (and Western) policy-makers widely consider to be a thinly veiled attempt to gain strategic influence throughout various countries in the Indo-Pacific region.

Apart from these wide-ranging global security challenges, the experts underlined several topics with a regional impact and stressed that they are rarely based on a single issue. For instance, the *Middle East* is a perfect example of how political, religious, and economic rivalries overlap, leading to various conflicts in different countries. In the long term, the shifting balance of power in geopolitics remains a concern as China’s influence in particular is growing, while US power and influence are decreasing over time.

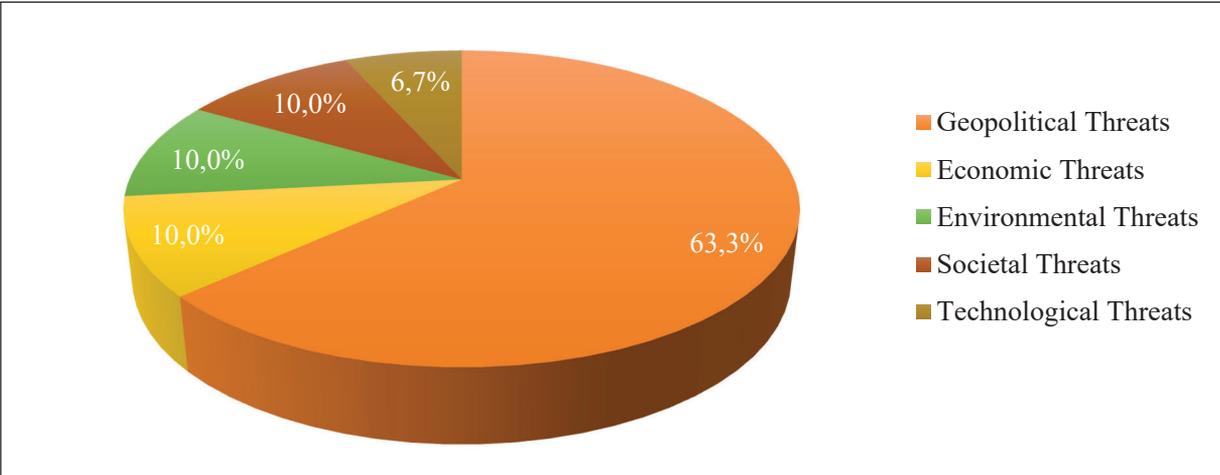
In addition, with a forward-looking perspective, there is an expectation for the main security challenges to be *non-traditional security challenges* such as climate change, changing demographics, ecological extinction, and population growth in many countries, as well as technical developments such as increasing automation and the accompanying lack of economic opportunities for a growing number of people around the world.

The literature on security has subdivided threats essentially into five fields¹¹:

- i. Economic Threats
- ii. Environmental Threats
- iii. Geopolitical Threats
- iv. Societal Threats
- v. Technological threats

12

Figure 2 – Fields of Security Challenges



We asked our experts to identify, in their view, the most urgent threats. Among these, the experts defined *Geopolitical Threats* as the most prominent ones in the current international environment and the rest are considered equal threats to society. As follow-up questions, we also asked them to identify the most challenging threats for each five sub-fields.

¹¹ World Economic Forum, “The Global Risks Report 2022”, 17th Edition, January 11, 2022, <https://www.weforum.org/reports/global-risks-report-2022/>. (Accessed November 15, 2022)

Geopolitical Threats

According to the experts, great power rivalry over existing resources and competition revolving around global value chains, constitute the greatest challenges in terms of geopolitics. In parallel with this, populist and personality-centred leaders are also found to be problematic. This is because they could prioritize their pursuit of self-interest and survival in their domestic political environment and they might be threatening the established international norms and rules-based international political order, when their domestic survival is under threat. The evolution of global militant-religious, ideologically and politically-motivated terrorism, is another area for growing challenges directed at international security. Surprisingly, experts indicated that present and possible *varieties of inter-state warfare* are of great importance. Admittedly, the current war in Ukraine as well as the confrontations in the South China Sea have been occupying a major place in geopolitical analyses. Lastly, uncontrolled proliferation of chemical, biological, and nuclear weapons of both state and non-state actors is among the geopolitical threats that we are going to be dealing with in the near future.

Economic Threats

Globalized market disruptions and possible supply chain problems are found to be the main economic threats in the current era. Especially, the Russian aggression towards Ukraine and the discourse that Russian political elites have been using in the same direction increased the concerns over functioning global market efficiency and the flow of goods. In addition, experts stated that lack of economic opportunities is another aspect that we should consider if we are to maintain the sustainability of the system. These threats are followed by the movement of illicit goods (drugs, contraband, and oil) and money laundering.

Societal Threats

The most challenging threat that needs attention concerns identity politics. As one respondent argued, the “domination of identity politics within countries challenges the pillars of nation-states, hence resulting in transnational intrastate conflicts and civil wars”. Another dimension of the societal threat is that around the globe, racism and xenophobia are increasing exponentially. The flow of irregular migrants and lack of social integration deepen the societal threat levels in many countries. In this sense other facets of security, such as food security, can disrupt social cohesion, and therefore, have to be taken into consideration when we discuss societal threats.

Environmental Threats

Within the context of environmental threats, climate change has been seen as the most dangerous threat. The lack of a clear explanation of what the possible effects will be, increases the concerns in this direction. The ranking of other threats according to the votes of the experts is as follows: rapid population growth culminating in food and water shortages; environmental terrorism; and ecological extinction.

Technological Threats

As a considerably new domain, cyber-attacks are found to be the most serious technological threat. In parallel with cyber-attacks, the use of disruptive technologies holds second place. What is quite intriguing here is that the spread of fake information holds third place, leaving behind the proliferation of AI, the increasing pace of digitalization, and automation.

b. Security Challenges in Different Regions

The geographical scope of this research covers Africa, Asia, Europe, and the Middle East, while excluding the rest of the world. Regarding its security challenges and their effect on the rest of the world, the Middle East is exclusively taken into account. Hence, in this report, Europe, Asia, Africa as well as the Middle East were examined in terms of regional security challenges. Since some of the challenges are directly threatening every part of the world, we are listing the common points that the experts pointed out.

The majority of the experts believe great power politics and states' flagrant violation of the rule-based order are likely to dominate the international agenda. In this sense, the decline in the power of the US and increasing Chinese power in this system will lead to uncertainty. The challenge to international order would automatically add up to new crises in alliances and rivalries. Furthermore, the uncontrolled flow of people, namely irregular migration, changes in regional demographics, ideological disunity as a result of faltering economies, and finally, access to water and food security, are recognized as challenges that are going to be affecting all regions in the world. In addition to these issues, the return of foreign terrorist fighters to their homelands who lead the recruitment cycles of terrorist organizations that they are affiliated with, will require serious attention. This may also result in an increased risk of cross-border conflict forcing the governments to take different measures to meet the current threat. As considerably emerging areas of challenge, nuclear threats, cyber security, and maritime risks pertaining to intentional or unintentional environmental consequences are going to be an item on the international security agenda. Lastly, the impact of the COVID-19 pandemic on different sectors is still not certain and will require a multidimensional perspective.

Regional Security Challenges in Africa

Different from the other regions covered in this report, Africa's regional challenges revolve around social, developmental, and economic dimensions. Experts stated that the most severe threat which will directly challenge the continent is *Food Security*. Difficulty in accessing potable water and adequate nourishment make food security a priority in the region. Economic scarcities and underdevelopment in most parts of the continent worsen concerns over achieving food security. Experts stressed that these consequences can be further triggered by the increasing devastating effects of climate change. From another point of view, African societies' fragmentation, and composition of various cultures, transform the continent into a vulnerable place, leading to conflicts between ethnic and tribal groups.

In addition to these general threats concerning Africa, our experts conveyed their further hesitations on different security challenges that sub-Saharan Africa may be dealing with in the near future. In

this sense, Sub-Saharan Africa's security challenges are related to weak-state formation. Many areas are not under the control of central governments. A few countries have succeeded in representing different ethnic or tribal factions in politics, often leading to a situation where disenfranchised groups resort to violence. Population growth coupled with a lack of economic growth and development has been an increasing concern for many governments, and is unlikely to be solved in the near future.

The terrorist incidents that have increased in the Sub-Saharan African region in recent years indicate a weakness in this sense. The most active and capable religiously-motivated terror organizations, DAESH and al-Qaeda have shifted their focus of efforts to the Sahel region and Sub-Saharan Africa. In 2021, almost half of terrorism-related deaths all over the world occurred in Sub-Saharan Africa.

In short, Africa's security challenges will likely be revolving around mostly non-traditional security sectors; however, according to the experts, fragility and instability in different parts of the continent will force decision-makers to take precautions against the traditional security challenges.

Regional Security Challenges in Asia

The experts have expressed opinions that the biggest security challenge in Asia is great power politics. Along with rising Chinese power in the current international system, especially the South China Sea, has been one of the disputed areas of great power politics. As a second challenge, experts stated that climate change is of great importance in the region. Since this is going to have an impact on not only the environment but also on refugees (*climate refugees*), and nutrition supply chains, climate change should be observed carefully. Another problem in the region covers population growth and changes to demography. According to our experts, an imbalance created by these issues might trigger instability, economic grievances, and transformation in the ethnic and tribal composition of countries. From an energy security perspective, a growing number of citizens could force countries to meet the energy demand which may create room for vulnerability.

Putting specific importance on South Asia, experts shared their expectations on possible inter-state political disputes, strategic competition, terrorism, sub-nationalism, identity politics, and increasing far-right movements in the region. Some experts' answers were quite hesitant about the role of social media and the internet in the sense that these might create turmoil that anti-authoritarian ideas from far-right movements could benefit from. In addition to these increasing far-right movements in the region, sectarianism seems to have a negative impact on these strengthening divisions in South Asian societies.

From a traditional security perspective, experts stated that porous border control in "hot spots" within Southeast Asia, growing normalization of radical content in mainstream discourse, lack of a concerted reintegration of detainees back into society in certain countries, drug trafficking and small arms proliferation will probably become the main security challenges. In addition, given the geopolitics of the region, religiously-motivated terrorism remains the main form of extremism and the experts underlined the fact that insurgencies in the region could aim to imitate the Taliban's approach in Afghanistan, turning the region into a chaotic place.

Regional Security Challenges in Europe

Security concerns within Europe expressed by the experts were generally defined within the framework of the problems that may arise as a result of the ongoing Russo-Ukrainian war. In this sense, experts stated that the greatest security challenge to Europe is *Energy Security*. The external dependency of most countries in Europe and the fact that this need is largely met by Russia, leave countries in a difficult situation in meeting their energy demands.

From a different perspective, the invasion of Ukraine could also transform Europe into a place where great power politics take centre stage. From another point of view, the unforeseen consequences caused by the effects of climate change in Europe, as in most regions, forces this issue to be examined regarding security concerns.

In terms of the domestic politics of European countries, intensifying far-right and far-left movements are found to constitute a great problem in European security. The last couple of years witnessed the rise of these movements, resulting in an unexpected series of incidents, forcing not only decision-makers but also our experts to define these factors as the most challenging threats directed at European security.

Contrary to comments on the other regions, *cyber security* is listed among the top challenges that should, and will, occupy Europe's agenda. In their comments, experts expressed their concerns about possible cyber-attacks directed at critical infrastructure elements. They also mentioned that the use of cyberspace by the state as a means of conflict may create a new area of vulnerability.

16 In line with tensions in the Black Sea region, experts stressed that the region has faced the most difficult times; the real threat of nuclear war is higher than ever. The Russian invasion of Ukraine is the largest attack on one state by another. According to them, rebuilding peace and trust is almost impossible in the upcoming decades. The Black Sea region is an area with numerous frozen conflicts that could break down any minute and Russia's behaviour destabilizes the region's environment and requires a closer look.

From a Balkans perspective, experts brought up two main challenges in the region. First, European Union (EU) ignorance is fuelling political instability. Failing to find a solution to integrate the Western Balkans into the EU in the past two decades and encouraging the Ukraine and Georgia to start EU negotiations is considered a sign of ignorance on the part of the EU.

In a nutshell, Russian aggression is considered to be the main security challenge for Europe. Depending on countries' priorities, geographical concerns and structures, security challenges differ from each other.

Regional Security Challenges in the Middle East

For a long time, the greatest challenge to Middle Eastern security and societies has been *ethnic-religious clashes, radicalization, and religiously-motivated terrorism* which also leads to *instability* by triggering cross-border conflicts. According to the experts, these are the results of authoritarian regimes that have made the region the most unequal, both politically and economically, and made the area a laboratory for great power rivalry. Here, a small group wields both economic and political

power. Furthermore, the COVID-19 pandemic exacerbated the situation by causing 8.8 million people to lose their jobs. This could fuel some people's radicalization tendencies.

As a region that has been struggling with the dimensions of terrorism for many years, the Kurdistan Workers' Party (PKK) and its associates, DAESH and their foreign terrorist fighters, as well as anti-ISIS Western foreign fighters' level of radicalization and use of violence, have significantly increased in Syrian-Iraqi battlefields. Undoubtedly, the traditional forms of terrorism will remain as a threat in the region.

The Gulf region's main and foremost security challenge is Yemen's civil war, and the negative security externalities this civil war brings out. From a larger perspective, Iran's interference in the region reflects in civil unrest (Lebanon, Yemen), international tensions (Yemen-UAE; Syria-Israel) and regional governance issues. The integration of renewable energy to the region may also bring about a number of novel challenges. The economics of production of such energy necessitates regional integration of the grid. To be more precise, the grid is integrated, with Iraq to be added next year. However, countries borrow from each other only in emergency times - a truly rationalized grid does not yet exist. While economics may dictate such an integration, the individual countries may not be willing to cede sovereignty to regional formations - indicating various diplomatic tensions. Also, the region is investing a lot in the export of renewable energy, especially via alternative energy vectors such as hydrogen and ammonia (using seaborne tankers). The introduction of these new energy vectors will put a fresh emphasis on the Red Sea as well as the Arabian Sea, as emerging loci of energy exports. The regions being close to piracy – areas of Somalia – may result in the relapsing of maritime security challenges in the area.

Finally, climate change is a real security challenge. Rising temperatures have rendered certain places in the Gulf area literally uninhabitable – as temperatures over 50 degrees Celsius make living conditions extremely difficult. This risk is something that needs closer attention in the security agenda.

c. Emerging Terrorist Threats

The changing composition of actors in international relations requires an assessment of current threats by taking every party into account. Our experts reiterated this by putting emphasis on three different sources of main security threats:

- i. Conventional actors
- ii. Non-conventional actors which employ asymmetric tactic
- iii. Revisionist state actors that are trying to change the status quo through a combination of conventional and non-conventional means

The interplay between these actors in the current international system also triggers a change in the definition of security and calls for a rethinking of responses to new threats. The traditional means to respond to threats have been formed by taking the state as the referent object of security; however,

the elements of traditional statehood are transforming as well. The human element with its social needs and also its new “powers” of communication and disruption are making borders fluid and law enforcement insufficient.

State and non-state actors are taking advantage of these gaps, whereby a state’s pace of adaptation is playing into their hands. In this sense, the main security challenges of the current international environment are threats and risks that can come from a combination of different sources, such as non-state actors or the collaboration of hostile states with non-state actors or individuals targeting critical infrastructures, to disrupt production and transportation. Indirect disruption of an “enemy’s” economic and/or political power has the advantage of avoiding detection, and saves the initiator from retaliation. Thus, many states may also be using non-state proxies and such tactics to gain the upper hand in undeclared “wars.”

Undoubtedly, the threats have been changing throughout history depending on technological and sociological developments. Therefore, a steady change in new emerging threats is inevitable. The issue is to give an answer to the question “*What are the approaching emerging threats?*” For example, the pandemic and its possible threats to humanity was known. However, this threat had been neglected for decades. Hence, not only being aware of the emerging threats but also taking them into account and prioritizing them as part of security policy is another issue that we need to consider.

In this sense, the experts listed eleven different emerging terrorist threats that we should seriously approach by understanding their diversification and their relationship with the evolving nature of international security. They are as follows:

1. Cyber threats directed at critical infrastructure systems
2. The growing rate of radicalization due to falling living standards
3. Online radicalization
4. The proliferation of emerging technologies to malicious groups
5. Far-right/ far-left/ anti-globalization violence
6. Armed ethnic sub-nationalism
7. Economic instability
8. Marginalized and segregated migrant groups
9. Use of social media as a means of violence
10. Nuclear security and nuclear terrorism
11. Agricultural policies regarding the future of food security
12. Biotechnology and genetic modification and manipulation

Even though it has been a growing area for many years, there is no considerable legal framework regarding cyber security that could strengthen states’ efforts to deal with these non-traditional threats. Furthermore, it is difficult to attribute the source of cyber-attacks in many cases and it is hard to

respond. Negative impacts or possible devastation that cyber threats may cause could also change the course of what states make of “violence”. That is, despite the fact that these threats seem to be tangible, they can lead to severe consequences, reifying cyber threats. From another point of view, there is different reality pertaining to the unconventional world or new dimensions of society, the cyber world. In this new dimension of human beings, there are many security challenges and related concerns arising from unknowns.

And still, radicalization, which constitutes the initial step for climbing the staircase to terrorism as Fathali M. Moghaddam puts it¹², is a great concern. The growing rate of radicalization due to falling living standards reflects the increasing involvement and role of non-state actors, like terrorist groups, or individuals with social needs, such as grudges against a former employer or general dissatisfaction. From the viewpoint of our experts, these people are prone to collaborate with terrorist groups to organize physical attacks or cyber-attacks on critical facilities. In addition, extensive use of information and communication technologies, online radicalization and its relationship with offline actions are major areas of concern. The internet is a “library” where radical ideas are propagated and an alternative medium for like-minded radicals to congregate. It is important to identify ways to detect them early and develop response mechanisms.

Undoubtedly, the latest breakthrough in security-related technological improvement is the proliferation of drones and associated technologies on the battlefield. Unmanned Aerial Vehicles even with mounted arms or land and navy vehicles would be game-changers for state militaries on the one hand. On the other hand, their capacity for being used by malicious groups should be considered as an emerging threat to societies. Proliferation of advanced weaponry, notably anti-tank guided weapons, and MANPADS, is another parallel area we should take into account in terms of the evaluation of emerging terrorist threats. The looting of army ammunition depots in Libya and Syria provided terrorist groups with large numbers of lightweight, sophisticated weapons such as ATGMs and MANPADS.

Besides the aforementioned threats, experts pointed out the declining trust in democracies which could lead to ideological and political polarization within societies in the long run. Terrorists can take advantage of such divided societies by triggering ethnic sub-national, violent extremist movements and interests. This could be followed by worsening far-right/ far-left/ anti-globalization violence.

Meanwhile, economic instability can be considered a multi-faceted threat. That is to say, on the one hand, terrorist organizations may attract individuals who are economically deprived. On the other hand, considering that states do not have unlimited resources, a possible instability in the economy may risk states’ ability to allocate resources efficiently to security problems.

Marginalized and segregated migrant groups (unintegrated) are potentially likely to attach themselves to some terrorist organizations. People’s transborder mobility in the name of asylum-seeking could be a source of vulnerability for states, if those people are affiliated with a terrorist organization. This needs to be tracked more carefully. However, it creates a new challenge for security concerns in the coming years.

¹² Fathali M. Moghaddam, “The Staircase to Terrorism: A Psychological Explanation”, *American Psychological Association*, Volume 60, No. 2, 2005, pp. 161-169.

The terrorist threat in the realm of nuclear security has been at the top of the agenda of both policy-makers and academics for the past three decades. Nuclear terrorism is traditionally thought to involve non-state actors. The Russian invasion of Ukraine and the shelling of the nuclear power plant in Zaporizhzhia showed that state actors can also engage in attacks on nuclear facilities with the purpose of terrorizing their adversary.

Terrorist organizations could damage the sustainability of agricultural processes and threaten the demand-supply chain of agricultural products. They may even harm this cycle by reducing the social security of the workers.

Lastly, biotechnology and genetic modification and manipulation need to be closely watched. The fact that terrorist organizations are learning organizations with human elements, make it easier for them to adapt to changing technology. In this sense, even though genetic modification and manipulation seems to be a low probability, the outcomes and devastation it may cause could have terrible consequences.

In addition to these elements, experts also mentioned their concerns about the ongoing war in Ukraine. They stated that just as Afghanistan served as a sanctuary for jihadist organizations in the 1980s, for many right-wing violent extremist groups, Ukrainian battlefields have become places to congregate, radicalize, fight, and acquire military capabilities. And similar to the path of jihadist groups, the goal of many of these members is to return to their countries of origin (or third-party countries), use their know-how to commit terrorist acts, radicalize others, and recruit new members to their cause.

20

d. Comparison of the Emerging and the Traditional Threats

Although technological innovations ease various aspects of human life, the abuse of developed technologies has been paving the way for new challenges. Most of these new threats are different and more importantly unexpected than the traditional ones. Some of the experts found these threats to be more challenging than ever, whereas others believe that they were not different at all.

Those agreeing that there are emerging challenges which are very different from their predecessors stated that the new security threats are more diverse, more severe, difficult to identify, and unpredictable. These challenges do not work in a hierarchical structure and easily operate globally with low communication costs, creating difficulty in tracing the flow of information and also money. They are also not long-lived, act ad-hoc but then quickly turn into another type of structure with different actors leaving and joining. This is not due to the fact that the challenge is materially more substantial. But rather, the terrorists may target “concepts” such as blackouts that sever access to the net. These concepts increasingly lie at the centre of the “new social contract” between the state and society, but for which new security concepts have not yet been sufficiently developed.

In contrast to those arguing that the nature of threats is changing, several experts believe that the basis of threats have not changed, such as political motivation and the search for the means to cause harm. In the traditional approach to threats, analysts used to differentiate between civilian and military targets, discussed certain weapons systems that are allowed to be used by states, and the

declarations of war to use these means in order to reach victory. In traditional understanding, it is perceived that destruction, and loss of life and resources, during war, are vast.

Our experts agreed that the impact and the emerging threats themselves are comparatively more severe than the traditional ones. As a follow-up question, we asked them to score the five most severe emerging threats which seem to be greater than the other. In this sense, *cyber-attacks* took the lead. On the one hand, experts shared their concerns over the misuse of cyberspace by malicious groups and criminal and terrorist organizations targeting critical infrastructure systems and nuclear facilities. On the other hand, they drew attention to *state-sponsored cyber-attacks*. It is their expectation that cyber-attacks, launched both by states and illegitimate groups, are likely to increase in the following years. However, the damage they may pose is still unclear. Another possible scenario includes a cyber-attack on financial sectors. Experts stated that cyber-warfare will probably take place between states, becoming a part of a larger traditional confrontation.

The second most severe emerging threat is *the proliferation of emerging technologies to malicious groups*. Terrorists could benefit from these technologies and conduct even more lethal attacks on states. All states should increase their level of readiness and preparedness to deal with these threats and allocate sufficient resources. In this sense, the rate of diffusion of Emerging Destructive Technologies (EDTs) is also worrisome and even faster. Experts concluded that it usually takes several years, if not months, for a system, product or technique incorporating advanced technologies to find widespread use. States, armed forces and security institutions often cannot keep pace with this speed, i.e., they are not efficient in adopting and using EDTs, whereas terrorist groups and non-state actors can act much more flexibly and show a high degree of adaptability.

Moving away from these security-orientated threats, *the lack of global cooperation in addressing threats including climate change, migration, and the global health crisis* comes as the third most challenging source of threat. Global cooperation to address these threats is highly essential. Solutions should be problem-solving, according to the experts, because their fundamental reasoning is deeply rooted in the existing socio-political structure. This exacerbates the threats because their resolution necessitates a complete transformation of the political-economic system. However, it also exacerbates societal polarization, both intra-state and trans-nationally. As a result, it invokes the traditional understanding of threats; however, we should move beyond this understanding and seriously consider the upcoming non-traditional threats and take required precautions.

These are followed by the challenges posed by *infectious diseases to health and livestock*. The risk is that biotechnology can be used to accelerate such threats. Furthermore, we can categorize infectious diseases in this sense. They are still a big challenge for human health and livestock. Although it is possible for new pathogenic agents to emerge with the natural rate of evolution and directed natural selection mechanisms, it is possible to accelerate these processes by designing them biotechnologically. In this context, the experts touch upon the fact that many conspiracy theories have been discussed in the popular press regarding the COVID-19 pandemic, although there is no scientific data that this pandemic was caused by human intervention.

Turning back to threats that challenge national security structures, the experts drew attention to *the spread of far-right, far-left, and anti-globalization extremist movements*. These groups may misuse intercommunication via encrypted messaging services to plan and execute terrorist attacks and post

content on social media to encourage like-minded individuals. Furthermore, this content may attract teenagers to follow the ideas of these malicious groups. Countering these threats requires special attention for the youth dimension.

In the last instance, experts recalled *nuclear terrorism*. However, some of the experts made a distinction and stated that nuclear challenges can be either from terrorist groups or states, stressing that state-nuclear terrorism can be much more severe than traditional nuclear terrorism because a state like Russia has more military means at its disposal than non-state actors. The emerging threat of nuclear terrorism could cause a chain reaction of chaos worldwide, the consequences of which are unpredictable but definitely disastrous. The cyber-attacks, as mainly mentioned above, are surely another possible scenario, especially attacks on nuclear facilities which could cause severe consequences.

e. A New Wave of Terrorism in Future?

22 Long before terrorism's internationalization and globalization, a considerable part of the Terrorism Studies literature paid great attention to the evolution of terrorism and tried to detect the patterns in the history of terrorism. In this sense, David C. Rapoport led the efforts to categorize and exhibit the trends of terrorist actions, groups, and tactics. Rapoport (2004) coins these patterns as, like-minded terrorist organizations acting in the same time period as, "*Four Waves of Modern Terrorism*"¹³. These waves reflect similarities of ideology, tactics and mindsets of terrorist organizations. Starting from the third wave, Rapoport examines terrorist organizations' mobilization out of the provinces they were born in, and states that "*Terrorism is internationalized*". As we have seen in the 9/11 attacks, it is indeed internationalized and globalized. At this point, Bruce Hoffman, one of the prominent scholars in Terrorism Studies, further argued that the new acts and new organizations are far more different than the others and admits we are witnessing a *new terrorism*. As a response to what has been debated in this literature, we asked the experts whether or not we will witness a new wave of terrorism¹⁴.

The main academic propositions forwarded by our experts which may indicate a "*fifth wave*" of terrorism refer to some elements of such a wave as follows: a) hyper-local tribalism; b) social media-inspired lone actor terrorism; or c) the creation of terrorist "semi-states". Some of these have already been manifested: type [a] has been seen across Africa; type [b] manifests itself in Europe, and type [c] with DAESH. Experts indicated that we should not necessarily seek to separate the current terrorism wave from the fourth one. However, we need to keep an eye on two related phenomena - firstly, the relationships between terrorist groups and potential state sponsors, and secondly, the use of cyber capabilities by terrorist groups.

In addition, even though there will not be a new wave on the global scale, according to the experts, it is likely that there will be ebbs and flows when it comes to terrorist attacks on the regional level. They were cautious about the fact that whether this qualifies as a "new wave" depends on the timeframe of the analysis. In the Sahel region, for example, there has been a significant increase in attacks that

¹³ David C. Rapoport, "The Four Waves of Modern Terrorism" in Audrey Kurt Cronin and James M. Ludes (eds.), *Attacking Terrorism: Elements of a Grand Strategy*. (Washington: Georgetown University Press, 2004), pp. 46-73.

¹⁴ Bruce Hoffman, *Inside Terrorism*, (New York: Columbia University Press, 2006).

have been attributed to “terrorist groups,” however these groups are defined. These attacks have also led to an increase in deaths and injuries among the civilian population. However, these developments are not unique compared to other regions.

Additionally, the experts put specific emphasis on the impact of *fear* and *social media*. The first step for a “successful” terrorist attack is to induce fear among the public and reduce their trust in governments. The media impact is also essential. The pandemic and social media seem to have decreased the uniformity of the messages of the terrorists and the element of fear. During the pandemic, social gatherings and all major public events were cancelled, and more so, the worry of COVID-19, its variants, and new viruses changed the way that humans started processing fear. People are at times receiving conflicting social media posts, which makes it hard to confirm the information received. In the past years, there have been actions aimed at creating fear in society by sending pathogen agents through letters. It is envisaged that similar actions could be performed using biologically engineered organisms/biomolecules in the future. However, since it is a high-cost technology from biotechnology logistics to human resources, it can be thought that it is still far from the reach of such groups.

In short, according to some experts, these are why we should expect fewer terrorist attacks with traditional explosives on ordinary citizens, but more attacks with unconventional means that would challenge the power of the state.

The experts scored the most likely cases that could best describe a possible new wave of terrorism. In this sense, it could be comprised of the increasing far-right / far-left movements. Some experts claim that *“If the current polarization trend based on the current political-economic world system continues, people’s feelings of deprivation may worsen, leading to an increase in far-right attitudes.”* The new terrorism could be far-right / far-left terrorism such as identity-based radicalization among the majority of society. If the polarization trend based on the current political-economic world system continues, people’s feelings of deprivation may worsen, leading to an increase in far-right attitudes. This has the potential to lead to systemic violence against minority groups.

The second most likely case is a situation where the new wave of terrorism could mobilize the masses, having some anarchic components in it. Furthermore, the experts touch upon the fact that a new wave of terrorism could be more salient, though theoretically debatable. From another point of view, this time, it could be *“the terrorism of the majority”*, while previous waves can be labelled as *“the tool of weak and small groups”*. In addition, the new wave of terrorism could be built on the forceful acquisition of resources by others. Previous waves of terrorism were mostly centred on identity and ideology and aimed at terrorizing large sections of the population to put pressure on governments.

The third scenario revolves around the intersection between new technologies introduced by the Industry 4.0 and radicalized youth. The 4th Industrial Revolution presents new technological advances such as artificial intelligence (AI), robotics, the Internet of Things (IoT) and 3D printing. As soon as any product or service that is provided by Industry 4.0 becomes effective, accessible, cheap, easy to use, portable and concealable, they are quickly adopted and used by violent extremists. In 2011, for instance, Ansar al-Islam built a self-driving car carrying remote-controlled machine guns. Before the far-right terrorist attack in Halle in 2020, one of the attackers tried to produce some parts of his gun by spending \$50 using 3D printers and documents he had accessed over the internet. The

attacker failed to produce the weapon parts he intended. However, his efforts set an example that advanced technologies can be used for terrorist purposes. In November 2021, Iraqi Prime Minister Mustafa al-Kadhimi was attacked in his home via an armed drone. Therefore, new technologies could be one of the most serious outcomes as well as characteristic of a new wave of terrorism.

The new wave could be evolving from targeting physical entities (buildings, people, plants, etc.) to disturbing networks of value creation (grid destabilization, sabotaging data centres, temporarily corrupting data, severing connections, etc.) According to our experts, the terror will emerge from an individual's perception of being cut off from his/her networks, services, etc. The world is transitioning towards a circular logic where individuals become stewards of things rather than their absolute owners. In such a shared economy, access to services will become the Achilles heel of developed societies. This is where terrorists will target, even as simple as through a misinformation campaign.

The fifth challenge that may characterize a new wave of terrorism is *environmental terrorism*. Environmental terrorism is a possible way to influence whole cities and countries. Due to the recent trends to protect the environment - terrorists could use it easily, for example, to threaten to poison water, ruin natural reserves and ignite forest fires.

Lastly, the rise of domestic terrorism could be the new face of terrorist activities, which may combine state, quasi-state, and non-state actors. Possibly, the number of incidents involving nuclear terrorism, in the emerging as well as the traditional sense, will increase. For example, the war Russia is waging in Ukraine not only weakens the Ukrainian nuclear security infrastructure but has also offered an example to other states for how to exploit the existence of nuclear facilities to achieve military and political goals.

Apart from these challenges, the experts conveyed their further concerns over the negative impact of new developments on a number of areas: inequalities; food security; water scarcity; Artificial Intelligence-driven systems; cyber warfare that may also include cyber-criminal organizations; nation-states; and terrorist groups live streaming attacks. In addition to these, economic security threats are becoming serious and widespread. Deprived individuals have often been in the pool of recruitment for terrorist organizations, especially when they have been part of some minorities. Moreover, the ability of the states or governments for fair and efficient public order is diminishing and societies are becoming alarmingly fragmented, as a result of both neo-liberal political economics under globalization and nationalist authoritarian trends in de-globalization. These may unfortunately result in new waves of terrorism.

f. The Relationship between the Rise of Emerging Threats and the Trends in Terrorism

In terms of the relations between emerging threats and trends in terrorism, half of our experts confirmed that “*While the rise of emerging threats will not result in more incidents, it will magnify their effects.*” That is to say, even though the number of terrorist attacks may not be doubling, the devastation that they might cause, empowered by the innovations that emerging technologies allowed them, will be even more terrible. The second popular forecast about this relationship asserted that “*The rise of emerging threats means more destructive terrorist incidents.*” This is followed by the observation that “*The trends in terrorism just reflect the dissemination of the terrorist incidents to the*

widespread of the world public.” Finally, some of our experts strongly remarked there is a growing possibility of increasing numbers of more destructive incidents.

While analyzing the emerging threats and their impact on terrorism, Global Terrorism Index 2022 provides us with valuable insights¹⁵. As mentioned in the report, the global COVID-19 pandemic has had contradicting effects on trends in terrorism. On one hand, the quarantine measures, travel restrictions, and increased border controls have weakened the terrorist groups’ ability to plan and execute terrorist acts. From another point of view, the negative effects of the pandemic on economies increased reactions to governments and fed the ongoing political polarization. Socio-cultural restrictions during the COVID-19 pandemic caused people to spend more time online. Terrorists and violent extremist groups have used this increased online time for propaganda, radicalization, and recruitment activities. Therefore, leaving the restrictions related to COVID-19 behind, in the near future, we can expect an increase in the number of terrorist attacks committed by religiously-motivated, far-right, and far-left, extremists.

The experts explained that far-right/far-left radicalism is closely linked to the rise of emerging threats. What makes it difficult is the inability to identify who the terrorist is. Far-right/far-left terrorism, whether as an organizational form or as lone-wolf violence, means that, for the first time in terrorism’s “history”, it becomes a weapon of the “strong” rather than the “weak” in two ways: the users of terrorist methods are people from the majority in a given society, and they have “accomplices” in the state security structure, at least ideologically. This has also been fuelled by a sense of losing privileges, creating a desire to reclaim them, even violently. This has the potential to lead to identity-based radicalization, similar to religiously-motivated radicalism. Ineffective security measures combined with the radicalization of the identity of the “majority” could result in mass killings, as seen in the Breivik and Charleston cases. This is because “others” are codified by some groups as “alien” or “parasitic” elements of society, thus justifying any type of violence against them.

25

Furthermore, as stated before, terrorist groups are “*learning organizations*” – they have to evolve with changing security dynamics in order to survive. They will find ways to exploit the challenges posed by emerging threats to states. New terrorist tendencies could appear in the near future and we can see even now, the growing role of WMD and cyber-attacks in this process. Using propaganda and mass media, terrorism could be even more popular among certain segments of the population, as it can be popular to seek to punish, for revenge for good purposes. If we are to take cyber security and critical infrastructure into account, experts argue, it might be easier to convince some long-term unemployed youth who are experienced in computer operations to pose cyber security threats to critical infrastructure in their country or elsewhere.

In terms of the ongoing war between Russia and Ukraine, terrorist groups are expected to exploit the Western focus on Russia - the “return of great power competition” could be an opportunity to exploit the West’s distraction from non-state threats.

From a different perspective, the experts also underlined the difference that defines the emerging threats, such as their nature in terms of non-traditional security threats based on ecological, economic or social factors. Terrorist groups are likely to exploit challenges linked to these threats, for example when parts of the population are disenfranchised due to a lack of political participation which

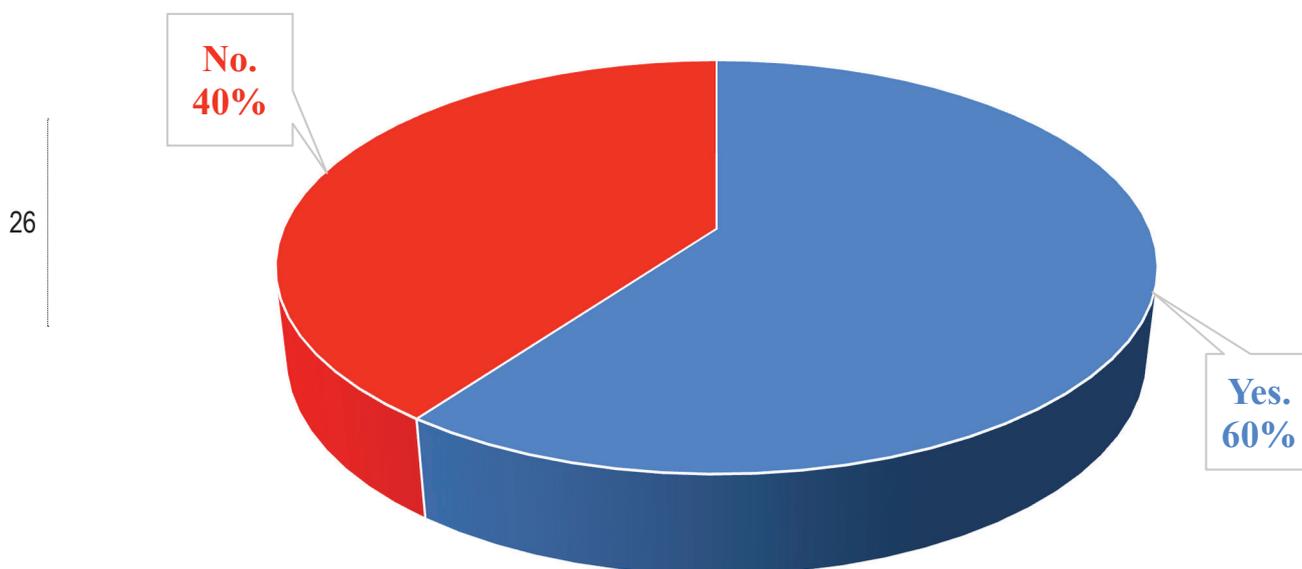
¹⁵ The Institute for Economics & Peace (IEP), “Global Terrorism Index 2022: Measuring the Impact of Terrorism”, May 11, 2022, <https://www.economicsandpeace.org/events/global-terrorism-index-2022-current-and-future-terrorist-threats/>. (Accessed November 15, 2022)

aggravates their problems caused by climate change and demographic factors. This is not different from the modus operandi of terrorist groups in the past, even when technology makes it particularly easy to disseminate information quickly and on a global scale.

g. Non-Aggressive Terrorist Activities

Within the previous sections, we saw experts' repeated emphasis on *fear* as a tool to intimidate the public and create a climate of anxiety, which are commonly employed by terrorist organizations. In this sense, the use of fear without necessarily shedding blood could be possible through the exploitation of such issues as fake news/information, hate speech or discourses against migrants/asylum seekers, the spread of subversive ideology, cyber terrorism, and disturbing networks of value creation (grid destabilization, sabotaging data centres, temporarily corrupting data, severing connections, etc.) In this context, we asked experts whether non-aggressive terrorist activities can be possible (Figure 3).

Figure 3 – Can Non-Aggressive Terrorist Activities be Possible?



Sixty per cent of the experts stated that at the very first glance, the term non-aggressive or non-violent terrorist activities may sound like an oxymoron with controversial meanings. However, there are indeed various non-violent activities related to terrorism including traveling for the purpose of terrorism, funding, organizing or facilitating other persons' traveling abroad for terrorism, incitement to terrorism, providing and receiving training for terrorism, recruitment for terrorism, instructing to commit a terrorist offense, providing financial or material assistance to terrorism, and possession of articles for terrorist purposes. However, if we are to take these non-aggressive dimensions of terrorism into account, experts add, this will require redefining terrorism as acts designed to effect political change without resorting to violence or intimidation.

In addition, the experts emphasized that terrorism is a very loaded term, and a politicized one. This is why the emerging threats described in scholarly literature are kept as a group feature instead of being classified as a separate phenomenon. That said, for all non-state armed actors, terrorism is a tool they can resort to for strategic purposes, and occasionally, under specific circumstances. Hence, in all other times, it can be expected that they might engage in non-aggressive behaviours. Given the nature of new threats affecting larger parts of society, non-violent, yet illegal, methods could be the new buzzword for groups who were previously engaging in terrorism. For example, riots, the irregular spread of petty crimes, or pogroms etc. could be initiated by these groups.

From the viewpoint of these experts, non-aggressive terrorist activities are more probable than ever, as although they may not explicitly promote violence, they can create a climate of fear and distrust after which, violence becomes more likely. A mix of violent and non-violent strategies is better able to attract new recruits and carry out more lethal attacks than those that rely exclusively on violence.

Misinformation is another terrorizing activity. Again, shaking an individual's belief via misleading misinformation - and the cognitive dissonance this misinformation can create may be as terrorizing as a bomb which explodes in a city that an individual lives in. A group of consistently agitated/terrorized individuals may also, in turn, pose security risks for society. The move away from neutrality further exacerbates the problem of "echo chambers," making online communities more vulnerable to targeted misinformation campaigns. The spread of radical propaganda and the practice of discrimination is one such activity. One known radical ideologue, Abu Bakar Bashir, once said "*I make many knives, I sell many knives but I am not responsible for how they are used*". Hence a more important question is to identify the vulnerable group as well as the tipping points.

The new trend might possibly evolve from targeting physical entities (for example buildings, people and plants) to disturbing networks of value creation (grid destabilization, sabotaging data centres, temporarily corrupting data, severing connections). The terror will emerge from an individual's perception of being cut off from his or her network or service provider. In addition, experts expect that poisoning foods that are not ideologically aligned, sabotaging fossil fuel plants and operations, and stopping development activities through terrorist acts will increase in the next few years.

Contrary to perspectives given in detail above, the other group of experts strongly believe that there is no such thing as non-aggressive terrorist activities. Non-state armed actors use terrorist violence; however, they often use other non-violent forms of political action, including civil disobedience as well as participation in the electoral process. Nonetheless, this does not make these activities non-aggressive terrorist activities. In fact, arguably, experts confirm that we would want more groups to move away from terrorist violence and toward non-aggressive activities.

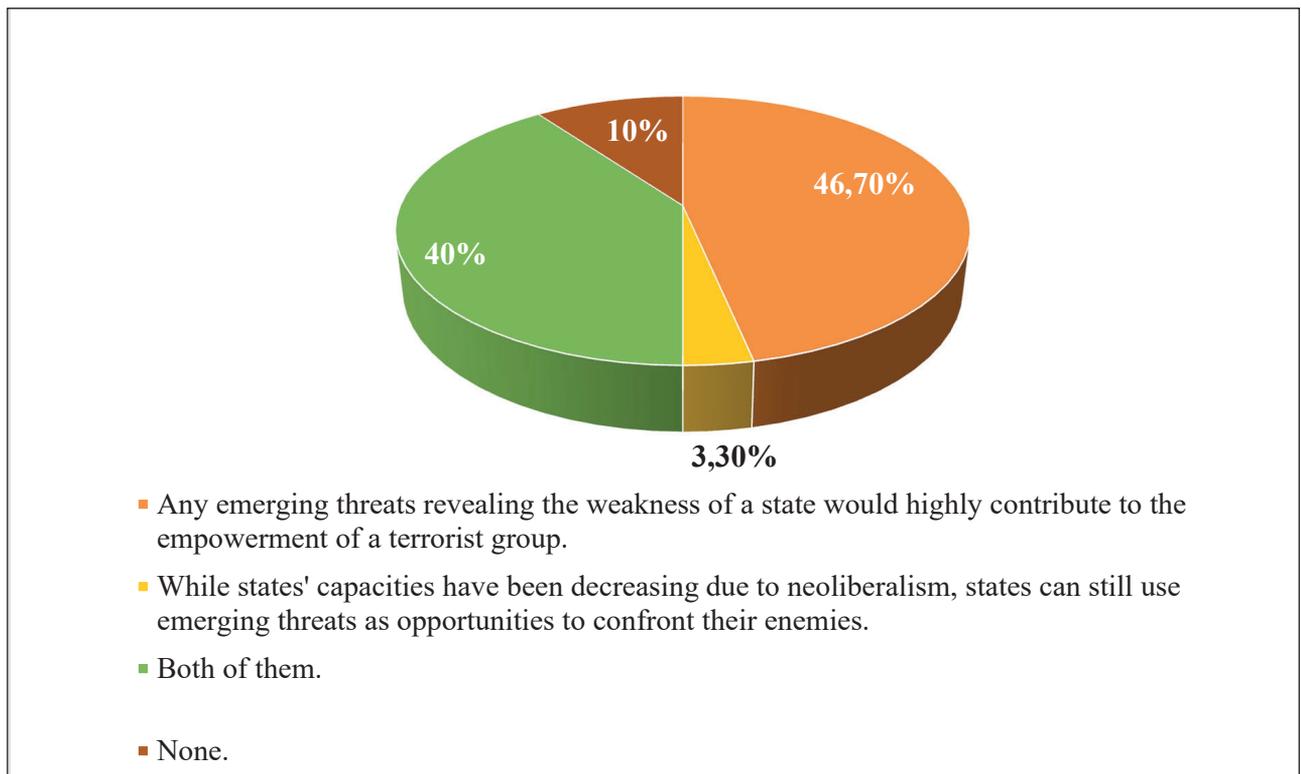
Considering that the spread of fear is generally linked to aggressive activities, non-aggressive terrorist activities are not possible. However, terrorist activities do not have to rely on physical violence against people or places. The spread of misinformation, leading to an increasing amount of fear about certain issues in large parts of a society, may also be caused by terrorist groups. Yet, such campaigns would merely be another, non-physical form of aggressiveness.

Overall, the new types of fear-imposing terrorist acts brought about by technology, indicate a beginning. Nonetheless, there is no guarantee that this fear will not lead to actual violence once it is disseminated into society.

h. Emerging Threats and Terrorist Groups

Since terrorist organizations are in a disadvantageous position in terms of their capabilities, they are willing to overcome this position of weakness by forcing states to act in a more unexpected, unpredictable, and asymmetrical environment. In this sense, it is probable for these groups to create new kinds of threats, or as we call it, emerging threats, making it more difficult to challenge them. To delve deeper into this topic, we asked our experts whether emerging threats empower terrorist groups in their asymmetrical struggle against states.

Figure 4 – “Emerging Threats Empower Terrorist Groups in their Asymmetrical Struggle against the States.” What is your take on this statement?



Nearly half of experts agreed with the idea that “Any emerging threat revealing the weakness of a state would highly contribute to the empowerment of a terrorist group.” One expert emphasized the idea that these non-state armed actors engaging in terrorism are organizations offering alternative governance modalities. Even though this argument is quite controversial, it is obviously the case that many of these organizations intend to challenge the state authority and monopoly to use violence, and to acquire legitimacy. Hence, any emerging threat revealing the weakness of a state dealing with it would highly contribute to the empowerment of a terrorist group. In addition, given that new threats are badly affecting larger parts of the population, they are constituting a more serious threat for states.

Emerging threats empower terrorist groups in their asymmetrical struggle against the states on the grounds that they make those groups even more *invisible* and *efficient*. Furthermore,

according to one of the experts, state capacities are in decline due to the neo-liberal political economy under globalization and the nationalist authoritarian trend in de-globalization. In addition, considering the severity of ecological problems, it seems easier to create fear among the populations with simple moves during extreme weather events. Terrorists can just abandon a car to prevent circulation on a highway during an extreme weather event and increase the fear of those who would be stuck there.

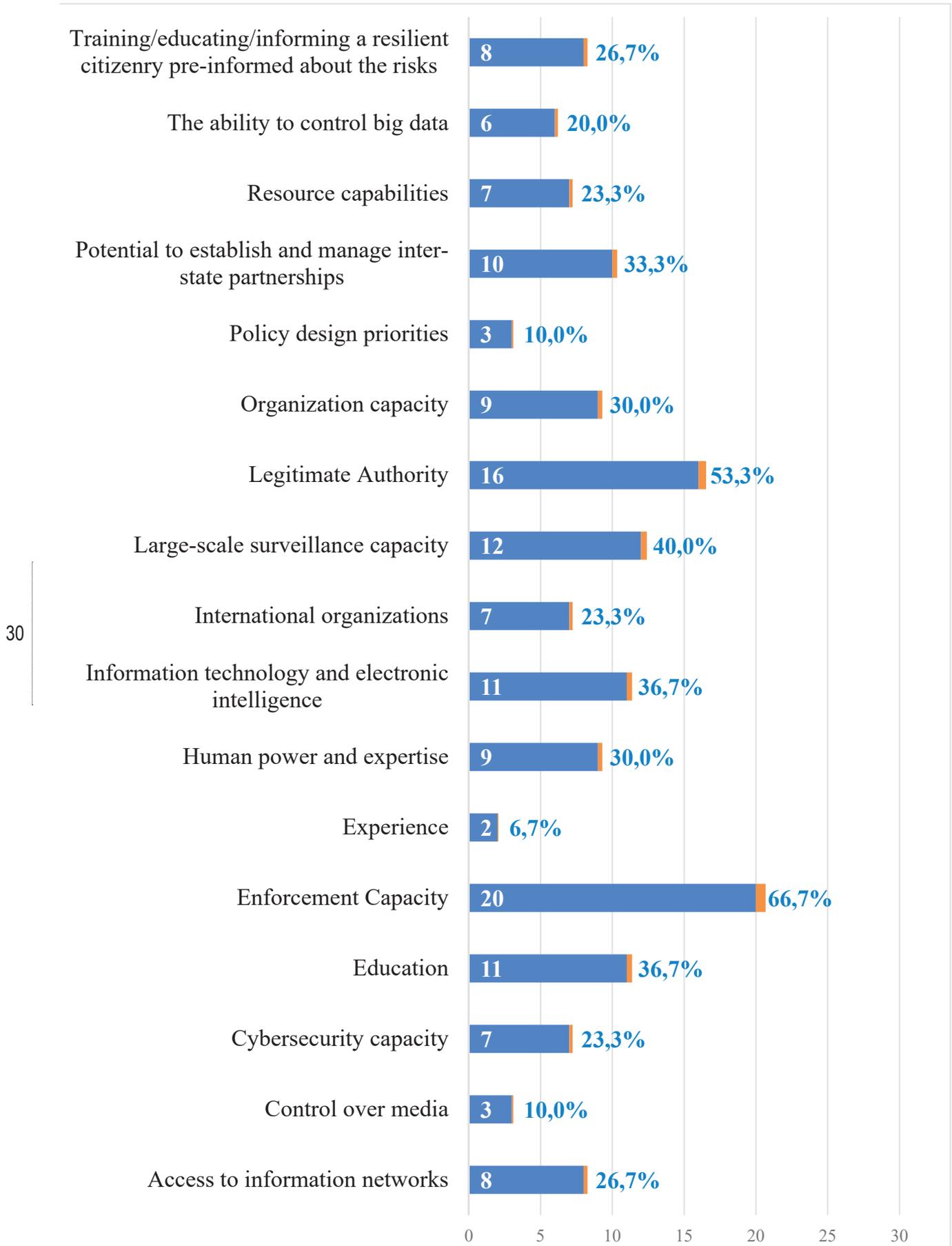
Whether some experts agree or disagree that emerging threats empower terrorist groups in their asymmetrical struggle against states, depends on the context and other factors. It depends on the state and how they have been dealing with terrorism. Any effective counter-terrorism strategy requires a good collaboration between the state and the community, and good governance. Hence, if these safeguards are not present, the emerging threats may be empowered to do what they want. On the one hand, experts drew attention to the ambiguous nature of warfare. That is because we cannot be certain what advantages emerging threats provide these groups. On the other hand, these threats offer no direct opportunities for these groups to wage war. They are inextricably linked to how humanity coordinates all of its resources to deal with them. Far-right radicalization hinders this by putting wider society under suspicion, as opposed to minority groups, who were thought to be potential terrorists and can be easily monitored.

The rest of the experts' approach reflected a more opposing position. They expressed an opinion that states are finding a new area for their power struggle, meaning perceived enemies are emerging from new forms of terrorism. Power struggles might be justified over the constructed issues which will empower states as the inevitably-needed actors of international politics. As the pandemic also confirmed, states have emerged again as the first-resort-actors of governing a crisis, since citizen-state relations are still valid and confirmed by the people. The fear could possibly be construed beyond the real facts which might open more room for the advancement of the state.

i. Capacity of States in Countering Emerging Terrorist Threats

In response to the emerging threats that these vicious terrorist organizations could exploit, we asked our experts what kind of strengths states could prioritize in terms of countering them. The figure below shows the distribution of the answers we collected. Some responses seem to be repetitive. However, considering the fact that these options were extracted from the first round, in this section we are clustering together the categories that were close to each other, in the analysis.

Figure 5 – Strengths of States in Countering Emerging Terrorist Threats



Twenty out of thirty experts evaluated states' *enforcement capacities* as the greatest strength while countering emerging threats. The well-structured security bureaucracy of the states allows them to mobilize agencies, and law enforcement bodies for prevention, detection, and response. In addition, they are able to come up with a policy design and pay greater attention to controlling the borders, which also constitutes a grave danger nowadays. They also have the potential to establish and manage inter-state partnerships which is the most important component in addressing emerging terrorist threats.

In line with a powerful security bureaucracy, another strength of the state has always been possessing "*legitimate authority*". It is very much under threat now because main sources of legitimacy are being seriously challenged: national belonging, rights and freedoms and social security. It should not be forgotten that state authority was able to secure itself and become more legitimate with the democratic welfare states and rule of law after the Second World War. These crucial elements have significantly deteriorated in a neo-liberal political economy, under globalization and nationalist authoritarian trends in de-globalization. National belonging has remained prominent, but has very much eroded due to excessive instrumentalization. To put it simply, states can be stronger if they provide widespread and substantial economic and ecological security to their citizens.

States are practically defenceless in the face of nuclear terrorism. The specific technical parameters involved in operating a nuclear reactor make it impossible to remove radioactive material in a timely fashion. Nuclear power plants are attractive targets because they are immobile and highly vulnerable to a forceful military attack.

From another point of view, as a legitimate authority, state bureaucracy holds the power to access information networks. Even though terrorist groups' access to these networks can be considered a vulnerability for states, if properly thought through, states can also come up with a proper crisis management process. The increasing prevalence of electronic means of communication enables higher interception potentialities. However, control over media is a two-edged sword. In the short term, the ability to control the flow of information and mobilize citizens may be very effective. But once the populace loses interest in certain forms of the medium due to state control, these channels may become irrelevant.

Terrorist groups are relatively disorganized units, and it is costly for them to acquire and hold information about the public. Yet, states can do it, and hence, can be aware of the emerging threats by reading the signals from the public. Democracy will greatly serve in the new era by ensuring the freedom of expression. Hence, democracies could better respond to the grievances of the public, because they will be better equipped to hear their voices.

Another group of strengths that increases the readiness and preparedness of states revolve around their intelligence and technological capacities. In this context, states have the power to set up large-scale surveillance systems and intelligence agencies to prevent terrorist groups from engaging in recruitment, financing or actual operations. However, such surveillance will also have knock-on impacts on other parts of society.

In terms of information technology and electronic intelligence, it is true that terrorist organizations are also highly dependent on communications in plotting and operating terrorist activities. Therefore,

states could take advantage of having enhanced information technology and electronic intelligence capabilities. Experts stated that these advanced technological infrastructures also facilitate states' efforts to counter cyber-attacks. Furthermore, the strict electronic monitoring of smart cities makes it very difficult for terrorists to conduct attacks. The activities of terrorist groups could easily be detected by advanced strict electronic monitoring.

From a more society-based perspective, experts stated that education, human power and expertise, training, educating, and informing a resilient citizenry pre-informed about the risks would strengthen states' efforts to counter these threats. States have the capability to integrate courses, modules, and training programs in research and educational institutions as well as training professionals in related fields. States can design programs to prevent radicalization and to rehabilitate and reintegrate radicalized individuals into society.

States possess

- a. Resource capability (keeping counter-terrorism agencies/units well-funded to keep focused on the threat)
- b. Manpower & expertise (maintaining the sufficient quantity and quality of personnel focused on the terrorist threat)
- c. Experience (including the ability to learn lessons appropriately)

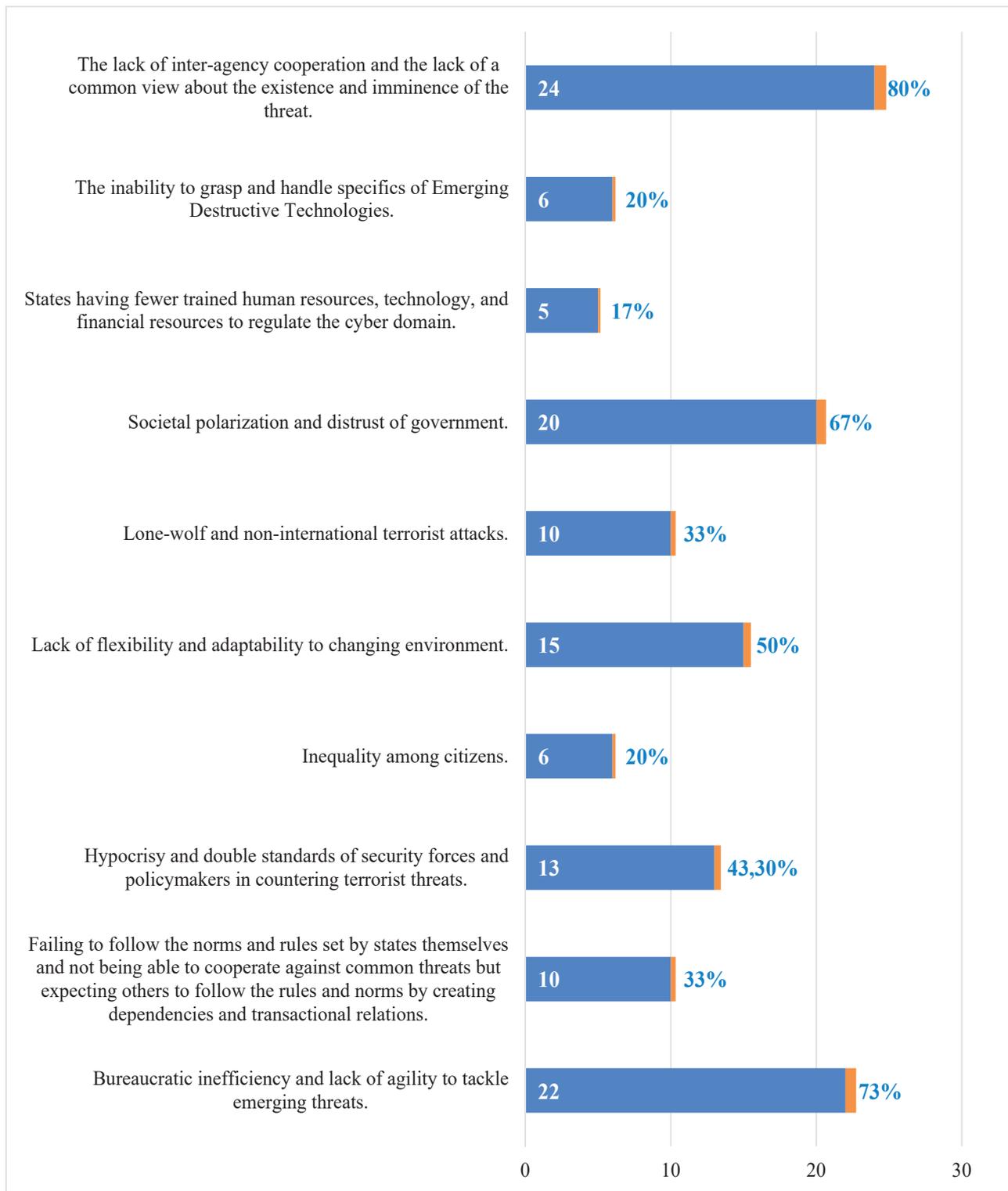
States also have the advantage in terms of being a part of an international organization. They already have divisions that work with technical systems for prevention, detection and response (such as the IAEA) that urge states to adopt these measures domestically and work with international organization, should an emergency take place (with the UNSCR 1540, and the Amended Convention on Physical Protection of Nuclear Material). States can utilize some administrative measures against extremists such as travel bans and re-entry denials (specifically for foreign fighters), house detention, electronic surveillance, and suspension of social benefits.

32

j. Vulnerabilities of States for Countering Emerging Threats

Since the terrorist organizations do not act in patterns and use expected ordinary tactics, states could have several vulnerabilities in detecting and responding to these threats. Our experts specified several threats that states must consider in this sense.

Figure 6 – Vulnerabilities for States in Detecting and Responding to Emerging Threats



The lack of inter-agency cooperation and the lack of a common view of the existence and imminence of the threat. Bureaucratic inefficiency and lack of agility to emerging threats. Lack of flexibility and adaptability to changing environments.

According to our experts, one of the main vulnerabilities could stem from states' current opposite direction of the liberal order. Even though they formulated norms and set rules to create this order, they no longer follow them, nor do they cooperate against common threats. On the contrary, states expect others to follow them by creating dependencies and transactional relations.

Since new forms of terrorism do not have unitary or defined leadership or central headquarters, they are difficult for states to counter. New threats will be “distributed”, i.e., without a centre that the state can address. This creates a strategic tension for a state’s bureaucracy. To let go of control and give agency to its operatives but be more effective, or to keep central command at the expense of efficacy. Also, the nature of the new threats necessitates the responses to be distributed as well. Even if a central part of the country goes offline, the rest should be able to function. This necessitates local or regional resiliency. States, then, should accommodate local governments to develop capacity efficiencies in the best way possible. Such centrifugal tendencies may not be perceived well by a state.

The most important vulnerability relates to a state’s lack of agility to emerging threats. Security thinking that excludes social sciences, humanities, and arts is destined to fall behind. For instance, one of the best engagements in GCC to neutralize potential DAESH sympathizers has been through a well-crafted online response where clerics, IT professionals, sociologists, and graphic designers worked together.

In terms of the concerns for Asia, police forces are again becoming a sectarian internal force rather than the representatives of the democratic rule of law that is essential to all. Armies look as if they are defending more the interests of their capitals abroad, or mere nationalist instrumentalization, than providing security to its own country. In any case, young, less educated and the structurally unemployed are recruited to police forces and the armies, which in turn decrease the capacity and legitimacy of states. In sum, the vulnerability of the states is more ontological, rather than technological.

34 ***Societal polarization, distrust towards government. Hypocrisy and double standards of security forces and policymakers in handling terrorist threats. Inequality among the citizens, and Access to information networks.***

Societal polarization and distrust towards government can weaken the states’ efforts to come up with an integrative and comprehensive counter-terrorism strategy. The reason is that countering terrorism does not only require an inventory, but it is also essential to have great support from the community in terms of putting faith in their leaders. This is an undeniable component of crushing terrorism in the minds of people.

Access to information networks is both a major strength and weakness, as states will be drowning in a flow of information, HUMINT, and SIGINT. This will delay action and increase doubt. As a result, states will depend more on electronic and network surveillance which, over a period of time, is likely to result in positive operations, but degrade human capacity. With the proliferation of social media, states are now more easily “judged” by people and any actions by them are monitored and commented upon by people, which may or may not make things worse.

Extremist and terrorist individuals, groups and organizations extensively exploit the Internet, social media and encrypted messaging applications to be in touch with supporters, spread propaganda, recruit individuals to their cause and even to coordinate and carry out attacks. They also benefit from the unregulated nature of social media. Sites and multimedia platforms, such as Facebook, Twitter, and YouTube still host a large amount of extremist content and propaganda material for terrorist organizations. When states try to exert more pressure on social media companies, they are mostly blamed for repressing the freedom of personal communication.

As an emerging area, concerns are raised that the crypto-currency market could attract terrorist organizations. However, states do not yet exert solid control and proper regulations over crypto-currency. This constitutes an even greater challenge in terms of terror financing.

Lastly, possible vulnerabilities are largely linked to a lack of economic and political opportunities for certain parts of society as well as widespread inequality. This aspect has not changed over time, even though the domestic situation in specific countries can develop significantly.

Failing to follow the norms and rules set by themselves and not being able to cooperate against common threats but expect the others to follow them by creating dependencies and transactional relations.

States are not categorically in a better or worse position in detecting or responding to the emerging threats. Yet, some states will be better equipped, while some will be worse. Furthermore, democratic and developed states can detect the problems arising within the public and respond to them better. All others, though, either might fail to detect it because of the preference for falsification or failure to respond because of a lack of resources.

The inability to grasp and handle specifics of Emerging Destructive Technologies.

States have fewer trained human, technological, and financial resources to regulate the cyber domain. States do not have enough fully skilled work forces. States cannot compete with IT giants such as Google or Microsoft in keeping the experts employed. Many of the government experts are easy targets for private contractors, corporations, and IT giants. This brain drain from the government causes many of private contractors and corporations to become potential malicious actors.

Lone wolf attacks, non-international terrorist attacks.

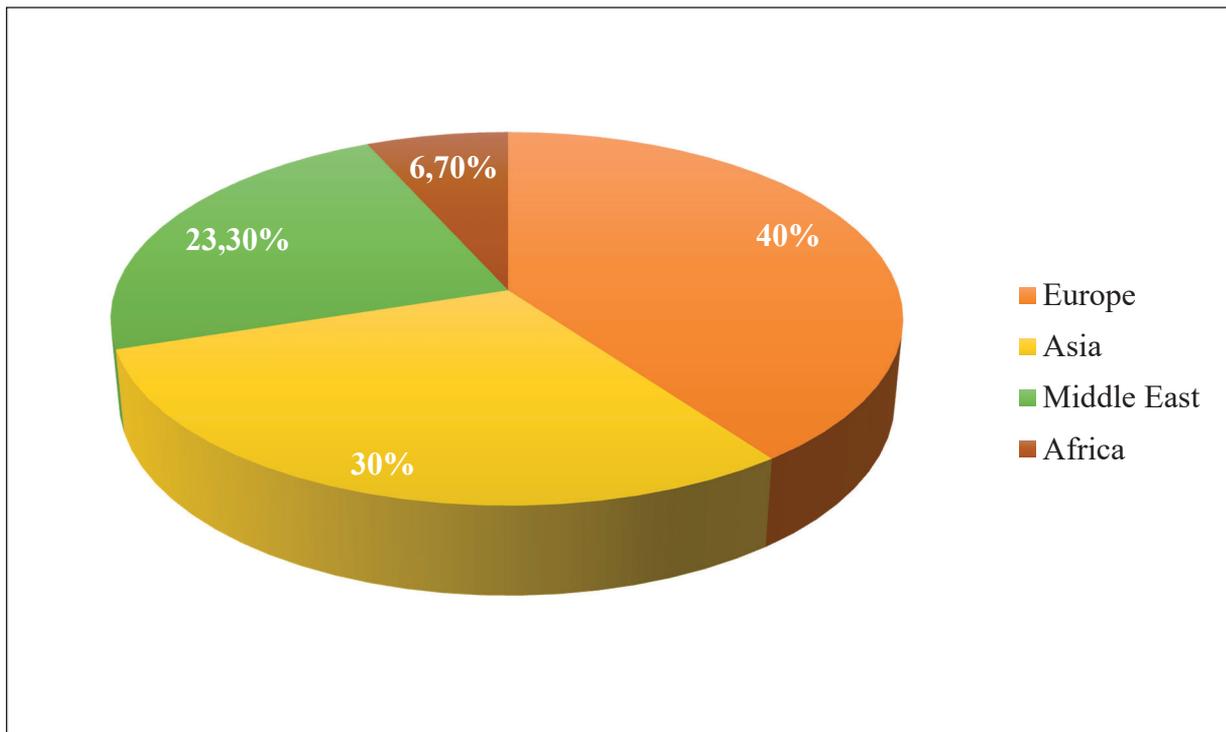
In time, states could detect, in some cases, patterns of a terrorist organizations' behaviour, i.e. the types of possible attacks, a symbolic time period when they are likely to conduct these, etc. However, lone-wolf attacks do not possess these kinds of patterns. It is very hard to timely identify these threats and respond to them.

Trends of homegrown terrorism and extreme violence by individuals who do not have any record are extremely difficult to identify rapidly. This is because these individuals can gain and have unlimited access to any disruptive technologies. Hence, it is critical for governments to work on trust in a democracy and related institutions. If today's trend of losing trust continues, states will not be able to counter-identify threats in timely fashion.

k. International Security Environment's Agenda for the Following Years

In the previous sections, it has been highlighted that the scope of this study covers regions including Africa, Asia, Europe and the Middle East. According to our experts, Europe will be the most vulnerable region compared to others in terms of emerging threats. Europe is followed by Asia, the Middle East and Africa.

Figure 7 – Vulnerabilities of Regions



36

Experts put considerable emphasis on the increasing tensions between great powers and added that great power rivalry will lead to more frequent conflicts by proxy. However, experts do not expect a direct confrontation due to the conflict of perceptions between great powers. The international security agenda is unfortunately very likely to be dominated by questions involving hard power after the return of state-on-state conflict to Europe. However, the aftermath of the war in Ukraine is likely to lead to a deteriorating situation in Ukraine due to the massive influx of weapons as well as the potential for more conflicts in the European periphery as many weapons are likely to be smuggled within the region, e.g., to the Balkans. The situation can be compared to the fall of the Libyan regime and the subsequent conflict across the Sahel region, fuelled by weapons from Libyan arsenals.

At the same time, these concerns are largely relevant in Europe. For Asia, Africa or the Middle East, regional security challenges are very likely to be more significant as security threats generally do not travel far away from a region. However, the trend of looking at security from a more holistic perspective that includes both hard and soft power seems to have been reversed for the time being among Western governments which will complicate international or even regional cooperation on all types of issues, including security concerns, for the coming years around the globe. What we observe in Eastern Europe right now will have more dramatic ramifications in East Asia by making Russia more dependent on China, and providing China with low energy prices. What we observe right now could be read as the challenge to the order, and this challenge will have multiple stages.

In its most conventional understanding, the South China Sea emerges as the most important security issue on the globe. The existing situation is such that the issue can easily escalate to multiparty conflict, with both territory and trade routes under contention. The situation features many of the variables empirically known to catalyse conflict onset and expansion in conflict literature.

In the longer term, how Africa's population growth will translate into the respective countries' foreign policy should also be observed.

In addition to geopolitical and regional conflicts, technological and industrial competition will seriously threaten international security. The next decade will most likely see more aggressive competition between states, while the international relations arena will be dominated by security competition. International cooperation will be more difficult because of national priorities.

Artificial intelligence, cyber security, rivalry in the space domain (capture and manipulation of satellites, dispute over ownership of the moon etc.), security of ground segment of space assets, climate change, vetting of human resources in critical infrastructures, etc. would constitute new areas and more unexpected outcomes in terms of emerging threats. However, some of our experts do not agree with the idea that terrorist organizations will have a chance to acquire these developed technologies.

A dramatic increase in protracted inter-state conflict resulting in political polarization of societies leads to high numbers of casualties, internal and international migration, public health catastrophes, civil unrest, and state failure. In addition, far-right terrorism in the West as a blowback effect regarding their battlefield experience in warzones (Syria, Afghanistan, Ukraine etc.) will probably increase.

As several attacks conducted in Europe, New Zealand, and the US proved, the role of social media and digital platforms in radicalization, extremism, and terrorism is undeniably crucial not only for recruitment but also for propaganda, construction of fear, and personal security.

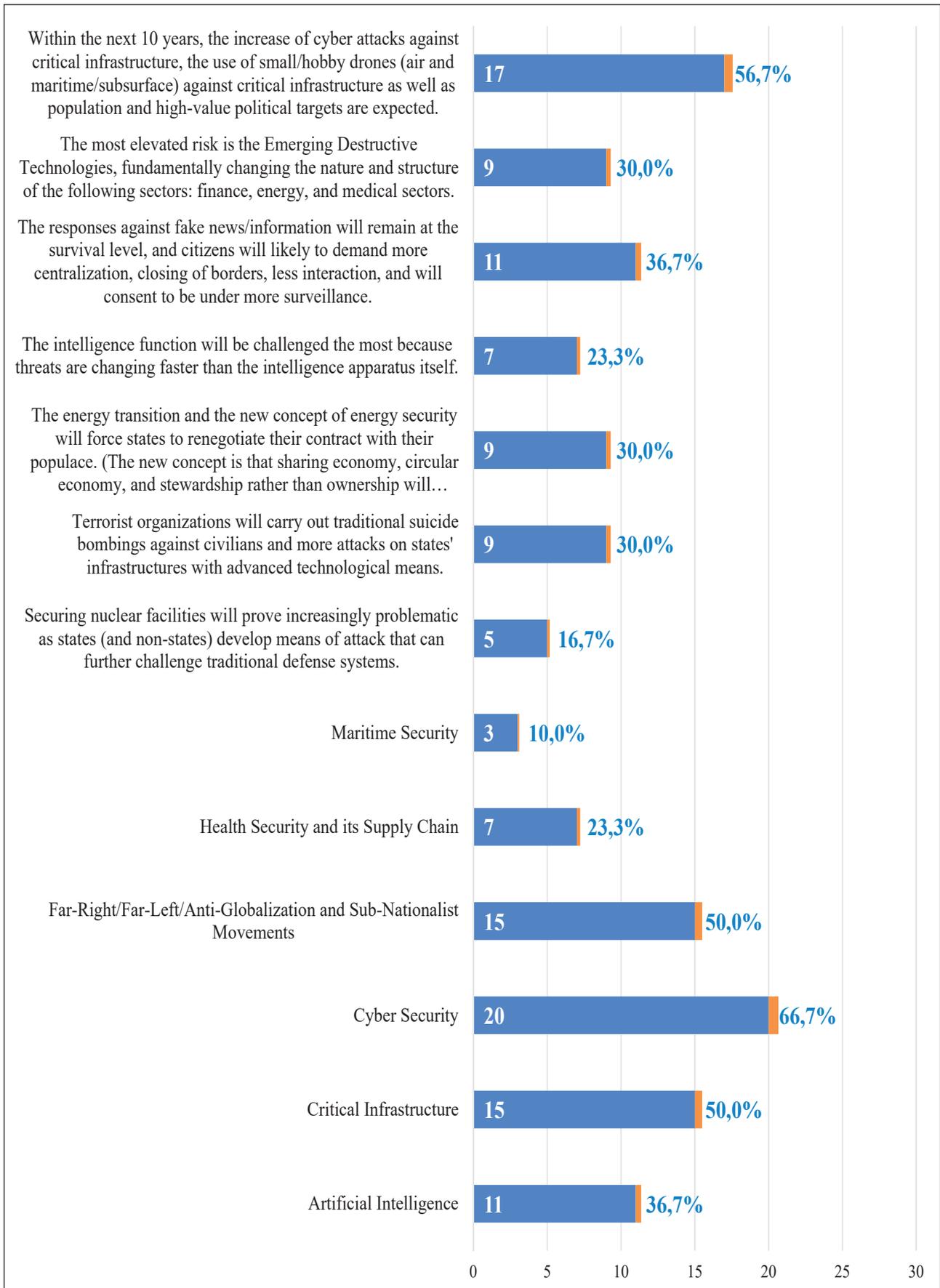
In short, the international security environment will be more volatile than it was in post-Cold War and post-9/11. The Westphalian state system will be challenged by rogue and revisionist state actors and a variety of non-state actors. Furthermore, the agenda should not be determined by specific states depending on their vulnerability or threat perception or construction. By focusing too much on emerging threats, experts stressed, the future agenda should not neglect classical threats.

4. Key Results & Recommendations

The threats are currently highly uncertain, as we observe baby steps in the evolution of the international order. Among others, the first signals of mass migration attempts, demographics, increasing population, and climate change are exponentially growing issues. We are fast approaching a time when these potential problems will become more volatile, and the first half of this century might be the time humankind will not be able to avoid tackling them. Given the intertwined and cyclical nature of these problems, we should start dealing with each without further delay. We gathered our experts' forecasts about which sectors of security will pose the greatest challenges. In this sense, we can categorize the threats as:

- New and Emerging Technology-Related Threats
- Innovative New Threats Against Conventional Sectors
- Accumulation of Classical Terrorist Threats
- Innovative New Threats against Non-Conventional Sectors

Figure 8 – How do you think these Threats will evolve in the next Ten Years and in which Sectors of Security will they pose the Greatest Challenges?



NEW and EMERGING TECHNOLOGY-RELATED THREATS

This section includes the challenges from cyber security, EDTs, AI and the dissemination of fake news/information. Within the next 10 years, cyber-attacks against critical infrastructure, the use of small/hobby drones (air and maritime/subsurface) against critical infrastructure as well as population and high-value political targets are expected. This elevated risk suggests that the Emerging Destructive Technologies can fundamentally change the nature and structure of several sectors, namely the financial, energy, and medical sectors.

Experts stated that the responses against fake news and information will remain at the survival level, and citizens will likely demand more centralization, closing of borders, less interaction, and will consent to more surveillance. Furthermore, the dissemination of fake information through social media creates the feeling of emergency without questioning, keeping people alarmed and anxiety.

INNOVATIVE NEW THREATS against CONVENTIONAL SECTORS

40 According to our experts, terrorist threats will always remain in the conventional sectors, just as the attacks in the past targeted government, public, and tourist establishments. However, there is now an increasing likelihood of attacks involving the cyber and maritime domains and using non-conventional tactics including CBRN. On the other hand, nuclear threats to critical infrastructure were noted highly throughout the responses. Experts indicated that securing nuclear facilities will prove increasingly problematic as states (and non-states) develop means of attack that can evade traditional defence systems. As a new aspect of nuclear threats, state nuclear terrorism is likely to worsen in the next ten years. Securing nuclear facilities will prove increasingly problematic as states (and non-states) develop means of attack that can evade traditional defence systems. For instance, both states and non-state actors can use weaponized drones to attack nuclear facilities, thus turning a nuclear power plant into a fixed radiological dispersal device (RDD). Terrorist organizations will also become more proficient in utilizing social media platforms and gaming sites for the recruitment and radicalization of their prospective militants. They will be able to create high-tech media products in different languages.

ACCUMULATION of CLASSICAL TERRORIST THREATS

There will be greater collaboration among different non-state actors operating in different domains. Jihadis and ethnic sub-nationalists will be using drone technology as part of their operational and tactical doctrines. They will be have 3D weapons-printing capacities. They will also exploit the cyber domain to their great advantages. Far-right and sub-nationalists will be more empowered. That will affect national cohesion and social fabric. In addition, terrorism will continue its traditional suicide—style attacks against civilians and have a more advanced technological attack on state infrastructure. Given these, both traditional and non-traditional security sectors will be vulnerable.

As a result of deep polarization in societies, the current trend of increased racism and xenophobia can feed the radical tendencies of some groups who believe they have lost their status as carriers of the normative existence of subjectivity. This could fuel far-right and far-left terrorism directed at minorities. In this sense, according to the sectoral analysis of security, societal security will be the most threatened as a result of identity-based radicalization.

INNOVATIVE NEW THREATS against NON-CONVENTIONAL SECTORS

Energy transition and the new concept of energy security will force states to renegotiate their contract with their populace. The new concept is that shared economics, circular economics, and stewardship rather than ownership will become the new norms defining a state's energy system.

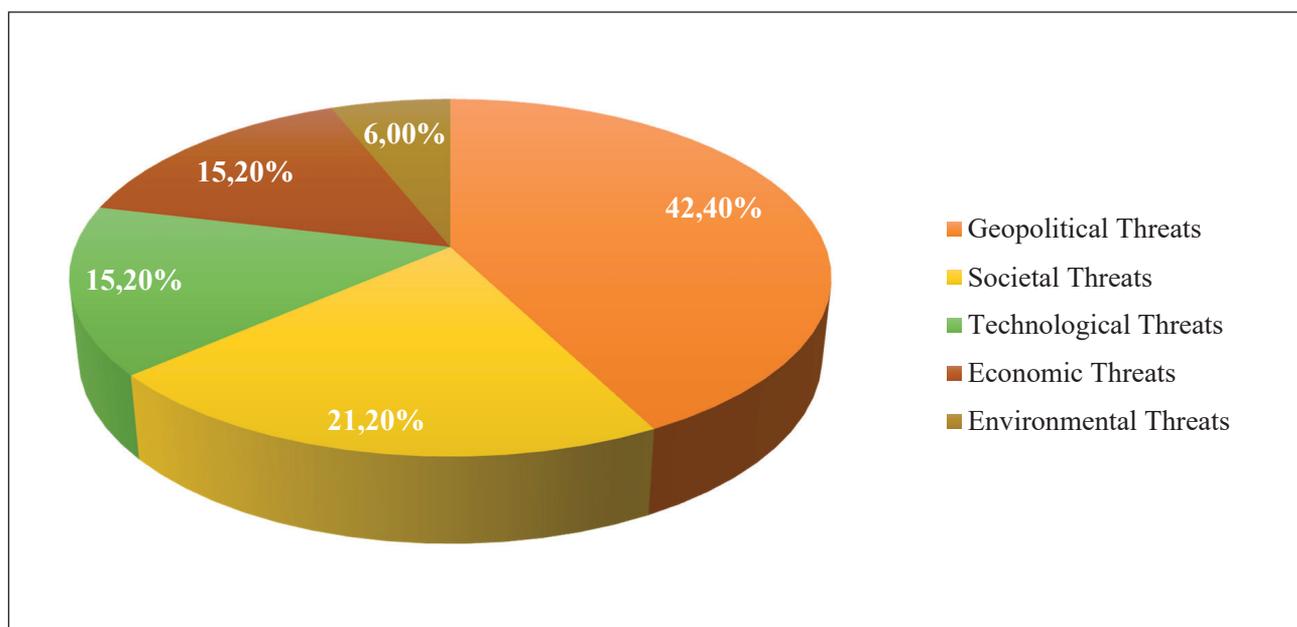
One of the most challenging and serious threats to international security nowadays is climate change, the impacts of which will only intensify over the next decade, and sub-state violent groups could be triggering these negative impacts by exploiting the harsh conditions that climate change may deliver.

As COVID-19 proved, health security and its impact on supply chains has become more significant than ever. Considering the turmoil that a pandemic may cause, the continuation of healthcare systems and supply chains of crucial medication need serious attention. Therefore, we must include health security as a new and important pillar of current international security understanding.

The research team conducted a quick survey during the Terrorism Experts Conference (TEC) 2022, held by the Centre of Excellence Defence Against Terrorism on October 18-19, 2022. The main purpose of this survey was to detect whether there are considerable differences or points where our respondent experts and TEC participants diverge from each other. In this sense, only two questions were directed at participants. First, we asked them to vote what are the most prominent security challenges in the current international environment. In parallel to answers of the Delphi Survey, TEC participants stated that, Geopolitical Threats (42.40%) are the most prominent challenges in the current era. In second place, Societal Threats received a rate of 21.20%. These are followed by Technological and Economic Threats (15.20%) and Environmental Threats (6.00%).

41

Figure 9 – Security Challenges in the Current International Environment (Preparatory Survey)



In terms of the Emerging Threats in Terrorism, the TEC audience stated that the most serious challenge to the current security structures, is *Cyber Threats*. In addition to threats in the cyber domain, *Emerging Disruptive Technologies* have been the second most important challenge raised by the participants. Most of the participants also included the use of UAVs and accessibility of weapons models online for 3D printing by terrorist groups under this category. From a more mixed perspective, the audience specified *Irregular Migration* that could compel states to produce an extensive countering strategy that has security, societal, economic, and geopolitical aspects. The TEC participants also warned about the growing role of *non-state armed actors* and the possibility of increasing *lone-wolf attacks*. These are followed by the use of *cryptocurrencies, metaverse, anti-globalist movements, and eco-terrorism*. Even though the main emphasis was placed on Cyber Security and the proliferation of EDTs, the responses of the audience also showed intensifying concerns over non-traditional aspects such as cryptocurrency, metaverse, and environmental terrorism. Expectedly, in addition to the previous experiences gathered in terms of traditional ways of countering terrorism, states should increase their level of readiness to deal with these different pillars of emerging threats. However, the current indications are not quite clear about to what extent and how exactly these new dangers could threaten the security structures of states. The response to these ambiguous points requires further research and accumulation of experience. Since there has never been a one-size-fits-all solution, information pooling and sharing seem to be vital for countering terrorism.

5. References

- Demir, Cenker Korhan, (2008), “Öğrenen Örgütler ve Terör Örgütleri Bağlamında PKK”, *Uluslararası İlişkiler*, Vol. 5, No. 19, 2008, pp. 57-88.
- Gordon, T.J., (1994), “The Delphi Method,” *Futures Research Methodology*, Vol. 2, Issue 3, pp. 1-30.
- Gordon, Theodore J., and Helmer, Olaf, (1964), “Report on a Long-Range Forecasting Study”, RAND Corp., R-2982.
- Helmer, Olaf and Rescher, Nicholas, (1959), “On the Epistemology of the Inexact Sciences,” *Management Sciences*, Vol. 6, No.1.
- Hoffman, Bruce, (2006), *Inside Terrorism*, (New York: Columbia University Press).
- Kardaş, Şaban, (2008), “The Transformation of the Regional Order and Non-state Armed Actors: Pathways to the Empowerment”, pp. 21-39 in Murat Yeşiltaş and Tuncay Kardaş (eds.), *Non-State Armed Actors in the Middle East: Geopolitics, Ideology and Strategy*, (London: Palgrave MacMillan).
- Mearsheimer, John J., (1990), “Back to the Future: Instability in Europe After the Cold War”, *International Security*, Vol. 15, No. 1, pp. 5-56.
- Moghaddam, Fathali M., (2005), “The Staircase to Terrorism: A Psychological Explanation”, *American Psychological Association*, Volume 60, No. 2, pp. 161-169.
- Rapoport, David C., (2004), “The Four Waves of Modern Terrorism”, pp. 46-73 in Audrey Kurt Cronin and James M. Ludes (eds.), *Attacking Terrorism: Elements of a Grand Strategy*, (Washington: Georgetown University Press).
- The Institute for Economics & Peace (IEP), “Global Terrorism Index 2022: Measuring the Impact of Terrorism”, May 11, 2022, <https://www.economicsandpeace.org/events/global-terrorism-index-2022-current-and-future-terrorist-threats/>. (Accessed November 15, 2022)
- Wolfers, Arnold, (1952), “National Security as an Ambiguous Symbol”, *Political Science Quarterly*, Vol. 67, No. 4, December 1952, pp. 481-502.
- World Economic Forum, “The Global Risks Report 2022”, *17th Edition*, January 11, 2022, <https://www.weforum.org/reports/global-risks-report-2022/>. (Accessed November 15, 2022)

This page intentionally left blank



"Scan to reach the software of this publish and the other products of **COE-DAT**"
www.coedat.nato.int