Centre of Excellence Defence Against Terrorism

COE-DAT

THE EFFECTS OF THE RUSSIA-UKRAINE WAR ON COUNTERING TERRORISM

Edited by Giray SADIK

Centre of Excellence Defence Against Terrorism

COE-DAT

THE EFFECTS OF THE RUSSIA-UKRAINE WAR ON COUNTERING TERRORISM

Edited by Giray SADIK

THE EFFECTS OF THE RUSSIA-UKRAINE WAR ON COUNTERING TERRORISM

Sadık, Giray (ed.) 2025

First Edition, Ankara, 2025
Published by
Centre of Excellence Defence Against Terrorism (COE-DAT)
Publisher Certificate Number: 51450

CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

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 COE-DAT.

Disclaimer
The information and views expressed in this book 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.

134 pages;
ISBN: 978-975-409-782-5
1. Russia-Ukraine War 2. Terrorism 3. Counter Terrorism.

To cite this book: Sadık, Giray (ed.) (2025), The Effects Of The Russia-Ukraine War On Countering Terrorism
(Ankara: Centre of Excellence Defence Against Terrorism)

THE EFFECTS OF THE RUSSIA-UKRAINE WAR ON COUNTERING TERRORISM

TABLE OF CONTENTS

Introduction
Prof. Dr. Giray SADIK, Project Lead Researcher and Editor 7

Chapter 1: Hybrid Warfare and Counter-Terrorism after NATO's New Strategic Concept
Amb. Shota Gvineria 9

Chapter 2: The Effects of the Russia-Ukraine War on NATO's Official Counter-Terrorism Discourse: An Evaluation in Terms International Law
Assoc. Prof. Dr. Arif Bağbaşlıoğlu 25

Chapter 3: Counter-Terrorism Effects of the War in the NATO's Eastern Flank:
The Weaponization of Migration and Implications for Future Terrorism Threats
Dr. Marc Ozawa 37

Chapter 4: War in the Seas: Unmanned Maritime Systems,
Critical Infrastructure Protection, and Maritime Terrorism
Assoc. Prof. Dr. Gordan Akrap 43

Chapter 5: Wagner Group, DAESH, and other Hybrid Actors: Terrorist Strategies and Tactics
Prof. Dr. Stefan Goertz 55

Chapter 6: How have Terrorists Adopted Tactics from the Russia-Ukraine War?
The Crime-Terror-Tech Nexus
Prof. Dr. Daniela Irrera 67

Chapter 7: Emerging Threats: Will the Use of New Technologies in the Russia-Ukraine War
Transform the Capabilities of Terrorists?
Dr. Christina Schori Liang 79

Chapter 8: Terrorist Threats Outside of Warzone: Clashing Narratives, Foreign Information Manipulation & Influence, and Post-Truth
Bernard Siman 95

Chapter 9: Implications of the Russia-Ukrain War on World Order and the Future of Counter-Terrorism
Dr. Nicolas Stockhammer........ 109

Chapter 10: Findings, Conclusions, Lessons Learned, and Recommendations for NATO
Prof. Dr. Giray SADIK........ 125

Biographies of the Editor and Authors........ 131

Preface

The Centre of Excellence Defence Against Terrorism (COE-DAT) is pleased to present this book on the topic of The Effects of Russia-Ukraine War on Countering Terrorism.

Although many political analysts forecasted the inevitable conflict between Russia and Ukraine, none of those strategic minds could foresee the decade-long struggle that stalemated not only the fighting states but also the whole world. Russia avoided using her nuclear power, but invented new warfare strategies and has employed every possible tactics and forces to brake the down-looked, smaller country's will to resist.

However, Ukraine too proved, that the country could do greater power play finding support and allies to successfully fight back with such a fierce power that surprised the whole world. Both sides turned to new technologies, tested off the shelf equipment and also used or countered unconventional, asymmetric approaches in order to achieve their goals, sometimes going to the Grey Zone. The conflict has provided tremendous lessons to the countries in the fight, but also to the Alliance, other nations and groups, who could learn and exploit these regardless of their political side or attitude.

We can see that the war has had indisputable effects on terrorism and COE-DAT as one of NATO's learning and educating facilities and as custodian of the topic, understood the urge to learn about the warfare fought in the invisible space.

In order to analyse these lessons, COE-DAT launched a research project and the gathered knowledge is presented in this book with the aim of serving the Alliance and Partner Nations to enhance their capabilities in their fight against terrorism.

Halil Sıddık AYHAN
Colonel (TUA)
Director COE-DAT

Acknowledgements

The Centre of Excellence Defence Against Terrorism (COE-DAT) is proud to complete this book to address leesons learned from “The Effects of Russia-Ukraine War on Counterıng terrorism”. We would like to thank all of our contributors for their hard work and expertise they shared in this study. By giving you this book, COE-DAT hopes that the world can be a safer place for all of our citizens and their families.

I would like to express our gratitude to Prof. Dr. Giray SADIK, Project Lead Researcher and Editor and the authors, Amb. Shota Gvineria,Assoc. Prof. Dr. Arif Bağbaşlıoğlu, Dr. Marc Ozawa, Assoc. Prof. Dr. Gordan Akrap, Prof. Dr. Stefan Goertz, Prof. Dr. Daniela Irrera, Dr. Christina Schori Liang. Bernard Siman, Dr. Nicolas Stockhammer for their invaluable support of this project that made this book a reality.

Also, I would like to thank the greater interested community, and supporting institutes for providing their support of NATO and Partner Nations.

Last but not least, my gratitude goes to the COE-DAT staff for their dedication and professionalism that ensured the success of this project.

Jose CABRERA
Colonel (USAF)
Deputy Director, COE-DAT

THE EFFECTS OF THE RUSSIA-UKRAINE WAR ON COUNTERING TERRORISM

INTRODUCTION

Prof. Dr. Giray SADIK
Project Lead Researcher and Editor
COE-DAT Project on *Russia-Ukraine War*
Lessons Learned for Counter-terrorism, 2024

According to Strategic Concept 2022, terrorism, which poses the immediate asymmetric and transnational threat, is one of two main threats to NATO. Even though NATO's focus is currently directed to the other main threat, Russia, particularly after its war against Ukraine, terrorism has remained a major threat across the NATO territory and periphery. Besides, the adaptations of terrorist organizations in response to current wars such as the one in Ukraine are likely to exacerbate terrorist threats for NATO Allies and partners. Therefore, there is an ongoing need for research and learning around global terrorism landscape and its implications for NATO. To this end, this research aims to identify the lessons learned for NATO from the Russia-Ukraine war for countering terrorism effectively.

Russia's war on Ukraine since February 2022 has led to dramatic changes in global geopolitics and the all-encompassing domains of security, connectivity, and modern warfare. Although significant and widespread, the effects of this ongoing war on global terrorism have yet to be comprehensively analyzed. To address this gap in a timely manner, this project aims to examine the effects of the Russia-Ukraine war on terrorism through expert discussions on the contemporary trends and lessons learned for global counter-terrorism efforts, and NATO Allies and Partners. To this end, we organized a workshop in hybrid format (in-person and online) with the contributing authors of the edited book. Workshop participants include academics, practitioners, and subject matter experts from various NATO Allies and Partners.

“ THIS PAGE IS INTENTIONALLY BLANK”

CHAPTER 1

HYBRID WARFARE AND COUNTER-TERRORISM AFTER NATO'S NEW STRATEGIC CONCEPT

Shota Gvineria[*]

1. Introduction

This paper examines how today's complex security environment has been significantly shaped by the Russia-Ukraine war and the evolving landscape of asymmetric threats in light of NATO's new Strategic Concept. As NATO transitions from its counter-terrorism pivot post-Afghanistan, the need for a comprehensive security approach becomes evident amid growing interdependencies, technological advancements, and increasing uncertainties. Highlighting NATO's recognition of the speed, scale, and intensity of hybrid methods, the paper evaluates the Alliance's approaches and posture to defend against the range of possible asymmetric threats.

The chapter aims to analyze how NATO's policies on countering terrorism and hybrid warfare have evolved in response to the ever-evolving contemporary security environment. It also seeks to propose solutions on how the concept of resilience can be effectively applied as a response to asymmetric threats, such as terrorism and hybrid warfare. The study will conduct policy analysis by examining primary sources and NATO's official documents, including NATO's new Strategic Concept of 2022 and the latest Washington Summit Declaration of 2024 (NATO, 2022; NATO, 2024). Through this analysis, the chapter will explore NATO's official stance on countering terrorism and hybrid warfare and the concept of resilience. In addition, the chapter analyses expert opinions and relevant literature to complement policy analysis with diverse perspectives. This part of the analysis focuses on identifying shifts in policy and strategy within NATO and evaluating the effectiveness of these adaptations in the context of the current security landscape. This approach critically assesses NATO's strategies and provides insights into how the Alliance can enhance its resilience to asymmetric threats.

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

The chapter is structured into several sections to provide a coherent and comprehensive analysis. Following this introduction, the next section discusses NATO's adaptability in adjusting its roles and functions to the evolving strategic environment, highlighting the historical context and recent developments. The third section examines NATO's approach to countering terrorism, focusing on policy adaptation, global counter-terrorism operations, and challenges faced. The fourth section explores NATO's approach to hybrid threats, analyzing the evolution of hybrid warfare and NATO's response to associated challenges. The fifth section delves into the application of the resilience concept to counter asymmetric threats, linking terrorism and hybrid warfare as interconnected challenges. The last two concluding chapters elaborate on the theoretical framework of resilience, providing recommendations for enhancing resilience strategies as a critical response mechanism to contemporary asymmetric threats.

2. NATO's Adaptability: Adjusting Roles to the Evolving Strategic Environment

Throughout its history, NATO has frequently had to reassess its priorities and functions to adapt to changing strategic environments. Initially established as a military-political alliance to contain Soviet expansion in the Euro-Atlantic area, NATO's future was debated following the end of the Cold War. The 1995 NATO-Russia Founding Act sought to transform Russia, previously viewed as NATO's principal threat, into a partner country. The fundamental principles outlined in the Helsinki Final Act and the UN Charter, such as the equality of all international law subjects, sovereignty, and the inviolability of international borders, were established as the foundational rules of the Euro-Atlantic security architecture and the broader liberal rules-based world order (NATO, 2016).

As these discussions continued, the security environment in the Euro-Atlantic region evolved dynamically. In the 1990s, the conflicts in the Balkans prompted NATO to develop its crisis management capabilities. The rise of religious fundamentalism and the global threat of international terrorism in the early 2000s necessitated a strengthening of NATO's counter-terrorism efforts (Byman, 2018). Adapting to these geopolitical challenges became a defining feature of NATO as a military-political bloc, with its role in the 21st century expanding to include crisis management in global hotspots and combating international terrorism.

The turn of the millennium introduced new challenges for NATO. The rise of authoritarian regimes threatened the foundations of the international order and the Euro-Atlantic security architecture. Russia's military aggression against Georgia in 2008 served as a wake-up call; however, NATO initially perceived it as a localized incident rather than a broader violation of the principles underpinning European security (Asmus, 2010). NATO's response, which included temporarily suspending the NATO-Russia Council and introducing new cooperation mechanisms with Georgia, was insufficient to prevent further aggression (Renz, 2018). Russia's illegal annexation of Crimea in 2014 and its military intervention in eastern Ukraine underscored the need for NATO to return to its core mission of collective defense, particularly in an era increasingly defined by hybrid threats and new technologies (Snegovaya, 2018).

The evolving threat landscape, characterized by diverse challenges—from military and hybrid threats posed by Russia to economic expansion by China, cyberattacks, disinformation, terrorism, irregular migration, and climate change—prompted NATO to adopt a comprehensive 360-degree engagement strategy. In 2020, NATO Secretary General Jens Stoltenberg convened an expert group to analyze these threats and challenges within the modern security environment (NATO, 2020). Their findings informed the development of NATO's Strategic Concept of 2022, which outlines the Alliance's vision and strategic priorities for the next decade (NATO, 2022). Notably, this concept was crafted amid Russia's large-scale war against Ukraine, necessitating a fundamental shift in NATO's threat assessment and response strategies, with a renewed focus on collective defense.

By the end of 2021, Russia had escalated tensions along NATO's eastern flank and openly declared NATO's enlargement a red line. Russia's multi-layered hybrid warfare campaign, initiated during the large-scale "Zapad 2021" exercise, illustrated both military aggression and a clear signaling of its security and military policy priorities. Concurrently, Russia, in collaboration with Belarus, launched hybrid tactics involving the mobilization of irregular migrants to NATO's borders as a form of destabilization (BBC, 2021; Hurt, 2021). This, alongside an unprecedented military build-up near Ukraine's borders, culminated in ultimatums that sought to reverse NATO's enlargement and limit its military presence near Russia (Russian Ministry of Foreign Affairs, 2021). These unfulfillable demands served as a pretext for Russia's full-scale invasion of Ukraine in 2022.

The Alliance recognizes that Russian aggression and hybrid warfare strategies of revisionist regimes are pivotal in shaping the unstable security environment in the Euro-Atlantic region. While systemic challenges from China do not currently pose direct military threats, they aim to gain influence in the economic, informational, and cyber domains, requiring a long-term strategic perspective (Gvineria, 2022). Amid Russia's ongoing war in Ukraine, which poses an imminent threat to peace and stability in the Euro-Atlantic area, one of NATO's most explicit objectives is to maintain a rules-based world order and contain Russian aggression.

Disagreements within NATO regarding defense and foreign policy priorities present challenges to the Alliance's cohesion, credibility, and decision-making. The lack of a unified approach has, at times emboldened Russia's aggressive policies. A key factor in planning and executing Russia's strategy is NATO's readiness for unified positioning and its capacity to reach a consensus on responses to aggression quickly, but NATO's cautious and restrained responses to previous aggressions against Georgia and Ukraine have underscored the effectiveness of Russia's disruptive strategies, potentially encouraging further aggression (Thomas, 2015).

NATO has repeatedly demonstrated its capacity for transformation to address modern threats. Today, the combination of external and internal challenges presents NATO with an unprecedented test. The expert group's recommendation emphasizes the need to strengthen political cohesion and unity within NATO to enhance its effectiveness and capabilities. As

NATO continues to adapt to contemporary security challenges, addressing internal divisions and properly assessing threats is crucial for maintaining its relevance and effectiveness in an increasingly complex global environment (NATO, 2022). NATO's ability to adapt and coordinate responses across a range of asymmetric threats, including terrorism and hybrid threats, highlights the importance of maintaining a unified stance and developing comprehensive resilience strategies to safeguard the security of its member states.

3. NATO's Approach to Counter-Terrorism

NATO's approach to counter-terrorism has undergone significant evolution over the past decade, reflecting a growing recognition of the changing nature of the terrorist threat. The alliance has increasingly integrated counter-terrorism strategies within its broader security framework, focusing on operational, strategic, and policy responses to deter and defend against terrorist activities (NATO, 2024-1).

NATO's counter-terrorism strategy has developed significantly, particularly in the context of its broader security objectives. The NATO Strategic Concept of 2022 reaffirmed the alliance's commitment to counter-terrorism as the key component for all three core tasks: collective defense, crisis management, and cooperative security. This main guiding document identifies terrorism as one of the primary asymmetric threats to the alliance, alongside hybrid warfare, emphasizing a comprehensive approach to "deter, defend, and counter" terrorism through enhanced intelligence-sharing, military preparedness, and partnerships with non-member states and international organizations (NATO, 2022).

The Washington Summit Declaration of 2024 further reinforced NATO's counter-terrorism stance by underscoring a 360-degree approach to security, acknowledging the transnational and evolving nature of terrorism (NATO, 2024). It highlighted the importance of NATO's partnerships, particularly with countries in the Middle East and North Africa (MENA) region, in preventing the spread of extremist ideologies and enhancing counter-terrorism capabilities. The declaration also called for continued investment in counter-terrorism capabilities, including special operations forces, intelligence, and strategic communications (NATO, 2024-1).

NATO's policy adaptation is also evident in its Counter-Terrorism Action Plan, which is regularly updated to address emerging threats. This plan emphasizes addressing the root causes of terrorism, improving situational awareness, and enhancing resilience against terrorist attacks. It integrates counter-terrorism efforts with NATO's broader security and defense objectives, ensuring a coordinated approach across the alliance.

NATO has played a significant role in global counter-terrorism operations, particularly in Afghanistan and Iraq. The International Security Assistance Force (ISAF) mission in Afghanistan and the subsequent Resolute Support Mission (RSM) are examples of NATO's commitment to counter-terrorism in a post-9/11 world (Byman, 2018; Hoffman, 2019). Scholars like Daniel Byman argue that NATO's involvement in these missions has been crucial in disrupting terrorist networks and preventing Afghanistan from becoming a safe haven for terrorist groups.

However, the effectiveness of NATO's military interventions has been debated. Critics argue that NATO's reliance on military force has sometimes been counterproductive, leading to civilian casualties and fueling anti-Western sentiment, which can exacerbate the very threat it seeks to eliminate (Cronin, 2018). Beyond military operations, NATO has increasingly focused on counter-radicalization and prevention as essential components of its counter-terrorism strategy. Addressing the root causes of terrorism, including political, social, and economic factors, has become an obvious necessity (Crenshaw, 2016; Neumann, 2015).

NATO's efforts in this area include supporting partner countries in building resilience against radicalization, promoting good governance, and facilitating dialogue between different communities. This approach aligns with NATO's broader "Comprehensive Approach," which seeks to integrate military and civilian efforts to address complex security challenges. The Washington Summit Declaration of 2024 reaffirmed NATO's commitment to countering terrorism through prevention and resilience-building, emphasizing the importance of promoting stability in regions susceptible to terrorism by enhancing the capabilities of partner countries and supporting their efforts to counter violent extremism (NATO, 2024).

While NATO has made significant strides in countering terrorism, its approach has also faced criticism and challenges. Critics argue that NATO's strategies have sometimes been more reactive than proactive, focusing too heavily on military responses rather than prevention and addressing underlying causes (Sageman, 2018). Furthermore, the effectiveness of NATO's counter-terrorism efforts has been uneven across different geographic areas and domains. The ongoing instability in Afghanistan and Iraq, despite military interventions, raises questions about the effectiveness and long-term sustainability of NATO's counter-terrorism operations.

Coordination among NATO member states, each with its own national security priorities and threat perceptions, presents another challenge. Achieving a unified and coherent strategy within a diverse alliance like NATO is inherently difficult, particularly when dealing with a complex and evolving threat like terrorism.

4. NATO's Approach to Countering Hybrid Threats

Hybrid warfare represents a complex and multifaceted approach to conflict, combining conventional military tactics with irregular warfare, cyber operations, information campaigns, and economic coercion. As global conflicts have evolved, so has the concept of hybrid warfare, necessitating significant adaptations in NATO's strategic and operational approaches to counter these threats (NATO, 2024-2).

The concept of hybrid warfare has developed significantly over the past two decades, influenced by shifts in geopolitical dynamics and advancements in technology. Originally conceptualized by Frank G. Hoffman, hybrid warfare describes the blending of conventional, irregular, and cyber warfare tactics to achieve political objectives without full-scale military engagement (Hoffman, 2007). The evolution of hybrid warfare can be broadly understood through three distinct phases: conceptualization, practical application, and adaptation.

During the conceptual phase, from the late 20th century to the early 2000s, there was a growing recognition among scholars and military strategists of the limitations of traditional, state-centric warfare doctrines. Conflicts in the Balkans, Africa and the Middle East demonstrated that non-state actors and irregular forces could effectively challenge conventional military forces using a combination of tactics (Gvineria, 2022). This period marked the initial conceptualization of hybrid warfare, where both state and non-state actors utilized a diverse array of military and non-military tools to pursue strategic goals, blurring the lines between war and peace.

The practical application phase, from the 2000s to the 2010s, saw the active use of hybrid tactics by various actors. Russia's intervention in Georgia in 2008 marked a significant turning point, demonstrating a sophisticated use of military and non-military tools, including cyber-attacks and information warfare, to achieve political objectives (Renz, 2018). This trend continued with Russia's annexation of Crimea in 2014 and subsequent actions in Eastern Ukraine, showcasing a comprehensive strategy that integrated conventional military operations with irregular forces, cyber-attacks, and propaganda campaigns to create ambiguity and exploit weaknesses in adversaries (Snegovaya, 2018).

The adaptation phase, from the 2010s to the present, saw hybrid warfare tactics becoming increasingly embedded within state military doctrines. Russia, for example, institutionalized hybrid warfare within its military strategy, focusing on integrating conventional and unconventional methods to exploit adversary vulnerabilities (Thomas, 2015). Similarly, China's "Three Warfares" strategy—comprising psychological warfare, public opinion warfare, and legal warfare—reflects an adaptation to the hybrid conflict that prioritizes non-military means to shape the strategic environment (Lewis, 2021).

NATO's approach to countering hybrid threats has evolved significantly in response to the recognition of the complexity and multifaceted nature of hybrid warfare. Initially focused on traditional military threats, NATO has gradually expanded its strategy and operational capabilities to address the full spectrum of hybrid threats (NATO, 2022-2).

The early recognition and strategic shift towards hybrid threats occurred primarily in the 2010s, particularly following the 2014 annexation of Crimea. This event highlighted the effectiveness of hybrid tactics in achieving strategic objectives with minimal conventional military engagement, prompting NATO to adapt its strategy and operational posture to address non-traditional threats more effectively (NATO, 2022). The 2016 Warsaw Summit was a pivotal moment in this strategic shift, with NATO leaders endorsing a comprehensive approach to hybrid threats, including enhanced situational awareness, improved resilience, and rapid response capabilities (NATO, 2016). The summit also led to the establishment of the Hybrid Analysis Branch, which focused on understanding and countering hybrid threats through intelligence gathering, analysis, and sharing among member states (NATO, 2016).

NATO's operational and tactical adaptations to counter hybrid threats include the development of rapid response forces, such as the NATO Response Force (NRF) and the Very High Readiness Joint Task Force (VJTF), designed to respond swiftly to emerging threats, including hybrid tactics. NATO has also bolstered its cyber defense capabilities, recognizing the critical role of cyber operations in the hybrid threat landscape (NATO, 2022). The establishment of the NATO Cyber Defence Centre of Excellence in Tallin, Estonia as early as 2008 and the adoption of a new Cyber Defence Pledge at the Warsaw Summit further underscore these efforts (NATO, 2016).

Building resilience and enhancing cooperation are also central to NATO's approach to countering hybrid threats. This includes strengthening critical infrastructure protection, enhancing civil preparedness, and fostering greater public-private cooperation. NATO has emphasized interoperability and coordination among member states and with external partners, such as the EU, to develop a comprehensive response to hybrid threats (Bourbeau, 2013; Berti, 2018). The establishment of the European Centre of Excellence for Countering Hybrid Threats in Helsinki, Finland, is evidence of enhanced international cooperation in this regard.

Following the strategic concept, the Washington Summit Declaration of 2024 significantly expanded on NATO's strategic approach to countering hybrid threats, emphasizing the need for agility and adaptability in an evolving security environment (NATO, 2024). The declaration underscored the importance of a robust deterrence posture against hybrid threats, integrating conventional and non-conventional capabilities, and highlighted NATO's cooperation with the EU and other international partners in building resilience and enhancing the alliance's ability to operate across multiple domains (NATO, 2024).

Despite significant efforts, NATO faces several challenges in countering hybrid threats. The complexity of hybrid warfare, characterized by the integration of military and non-military tactics across multiple domains, presents a challenge to NATO's traditional military-focused structure (Aradau, 2014). A specific significant challenge is defining the threshold which could be seen uniformly by all Allies as sufficient for evoking chapter five in response to the attacks on the member states in various domains. There are often different views among the member states about legitimacy, legality and proportionality, which makes NATO's response to the hybrid threats a complex political challenge. Moreover, achieving timely intelligence sharing and coordinated responses among member states, each with varying levels of capability and commitment, complicates the alliance's ability to respond effectively to hybrid threats (Kilcullen, 2020).

Looking to the future, NATO's approach to countering hybrid threats will likely involve continued adaptation and innovation. This includes further development of cyber capabilities, enhanced resilience against non-military threats, and improved strategic communications to counter disinformation (NATO, 2022). Additionally, fostering greater cooperation with international organizations, such as the EU, and strengthening partnerships with non-NATO countries will be crucial to building a comprehensive response to the evolving hybrid threat landscape. Incorporating new technologies such as artificial intelligence and machine learning into NATO's strategic and operational planning will also be essential to counter emerging hybrid threats effectively (Lewis, 2021).

5. Applying Resilience Strategies to Counter Asymmetric Threats

As argued in the previous sections, in the current security environment, NATO faces two of the most imminent asymmetric threats: terrorism and hybrid warfare. These threats challenge traditional defense paradigms by combining conventional and unconventional tactics, often exploiting societal and systemic vulnerabilities. Terrorism, characterized by the use of violence and intimidation by non-state actors to achieve political objectives, often operates outside the boundaries of conventional warfare. Similarly, hybrid warfare employs a blend of military and non-military tactics, including cyber-attacks, disinformation campaigns and economic coercion, blurring the lines between traditional understandings of war and peace (Hoffman, 2018).

Given the complexity and unpredictability of these threats, NATO recognizes the importance of comprehensive defense and deterrence strategies. The evolving nature of asymmetric threats, where adversaries exploit the full spectrum of conflict to achieve their strategic aims, requires a more adaptive and comprehensive approach (Bourbeau, 2013). Resilience has emerged as the most effective strategy for countering these threats, providing a framework for societies and organizations to prepare for, absorb, recover from, and adapt to various shocks and disruptions. Drawing on the theoretical insights from the strategic guidance outlined in key NATO documents, such as the NATO Strategic Concept of 2022 and the Madrid Summit declarations, NATO prioritizes leveraging resilience strategies to enhance its defense posture against asymmetric threats, including terrorism and hybrid warfare (NATO, 2022; NATO, 2024).

Terrorism and hybrid warfare are inherently linked as they both represent forms of asymmetric conflict that defy conventional categorization and challenge traditional defense mechanisms. Terrorism often employs guerrilla tactics, Improvised Explosive Devices (IEDs), and suicide bombings, targeting civilian populations and creating psychological and political impacts disproportionate to the physical damage caused. Hybrid warfare, on the other hand, combines conventional military operations with irregular tactics, such as cyber-attacks, economic warfare, disinformation, and the manipulation of social and political structures (Thomas, 2015).

These threats exploit the blurred lines between peace and conflict, challenging NATO's ability to respond effectively with predominantly conventional military power. For instance, hybrid warfare tactics can be used to destabilize regions by creating political and social unrest, which can, in turn, provide fertile ground for terrorist groups to recruit, train, and operate (Lewis, 2021). Similarly, the use of disinformation and cyber-attacks in hybrid warfare can undermine public trust and governmental authority, creating an environment conducive to terrorist activity (Aradau, 2014). Thus, NATO's approach to countering terrorism and hybrid warfare must be integrated and mutually reinforcing, recognizing the interconnected nature of these threats.

Given the interconnected nature of terrorism and hybrid warfare, resilience emerges as a critical strategy for countering these asymmetric threats. Unlike traditional defense strategies that focus primarily on preventing or responding to specific attacks, resilience emphasizes a comprehensive, all-encompassing approach. Resilience is about enhancing the capacity of individuals, societies, organizations, and systems to withstand shocks, recover from disruptions, and adapt to new challenges (Chandler, 2019). This approach aligns with the insights of scholars like David Kilcullen and Benedetta Berti, who argue that resilience must be built across multiple levels—local, national, and international—to effectively counter the broad spectrum of threats posed by terrorism and hybrid warfare (Kilcullen, 2020; Berti, 2018).

Building resilience against asymmetric threats requires strong coordination across various levels of government and active engagement of all layers of society, enabling countries to resist and recover from strategic shocks. The coordinated and synchronized approach across domains and stakeholders allows for adaptability to the dynamic nature of modern threats and is the key feature of resilience. This perspective is particularly relevant for NATO, which must consider its member states' diverse political, social, and economic landscapes when developing resilience strategies (Lewis, 2021).

Many experts extend this argument by highlighting the need for a holistic approach to resilience that integrates military and civilian efforts. Strengthening societal cohesion, promoting good governance, and ensuring that communities are prepared to respond to crises are critical for resilience. By fostering resilience at the societal level, NATO can enhance its ability to counter both immediate and long-term threats posed by terrorism and hybrid warfare (Berti, 2018).

Within the defense and security context, resilience is not just a defensive posture but a proactive and adaptive capacity that enables societies and organizations to thrive in adversity. This concept is particularly suited to countering hybrid warfare and terrorism, where threats are multifaceted and often unpredictable. Experts argue that resilience should be viewed as a dynamic process that involves opposition to external shocks, adaptation to new conditions, and transformation to respond creatively to emerging challenges (Walsh-Dilley, 2015).

NATO's Strategic Concept of 2022 recognizes resilience as a key element in its defense strategy, outlining it as crucial for ensuring continuity of government, essential services, and military support for civil authorities (NATO, 2022). The document emphasizes the need for a comprehensive approach to resilience that integrates military and non-military measures to effectively counter asymmetric threats (NATO, 2022). By focusing on the continuity of essential services and support for civil authorities, NATO acknowledges that resilience extends beyond military strength, encompassing the ability to maintain societal functions and recover quickly from disruptions (NATO, 2022).

The Washington Summit Declaration of 2024 further underscores the importance of resilience in NATO's strategic framework. It calls for an agile and adaptable approach to countering hybrid threats, integrating conventional and non-conventional capabilities to enhance the Alliance's ability to operate across multiple domains (NATO, 2024). This strategic guidance highlights resilience as a core component of NATO's security posture, capable of addressing both immediate and long-term challenges posed by asymmetric threats (NATO, 2024).

NATO's approach to resilience focuses on strengthening the ability of its member nations to prepare for, respond to, and recover from crises, ensuring the continuity of government functions and essential services. Resilience is a critical aspect of collective defense, providing a strong foundation for military capabilities. NATO has established seven baseline requirements to guide member states: assured continuity of government and critical services; resilient energy supplies; ability to deal with the uncontrolled movement of people; resilient food and water resources; ability to deal with mass casualties; resilient civil communications systems; and transportation infrastructure. These requirements help to ensure that societies remain functional under duress and can support military operations when needed (NATO, 2019).

6. Theoretical Framework for Understanding Resilience

To effectively apply resilience in defense and security, it is crucial to understand its theoretical framework and how it can be operationalized. NATO defines resilience as the capacity to prepare for, resist, respond to, and recover from strategic shocks and disruptions (NATO, 2019). This definition aligns with NATO's emphasis on resilience as a key factor in coping with modern security threats and its encouragement of member states to build robust resilience through synchronized civil preparedness and military capacity.

However, resilience should not be seen as a static or one-size-fits-all concept. Resilience must be tailored to different actors' specific needs and vulnerabilities, addressing multiple levels—individual, community, organizational, national, and multinational (Fjäder, 2014). This multi-layered approach ensures that resilience strategies are customized to specific contexts and threats, enhancing their effectiveness in countering both immediate and long-term challenges (Bourbeau, 2013).

Resilience involves several key components and stages:

- Physical elements such as critical infrastructure, resources, networks, and organizational structures are fundamental to maintaining core functions during crises.
- Physical elements such Psychological dimensions, such as determination, social cohesion, and trust in public institutions, are equally important for building societal resilience. These elements ensure that societies remain cohesive and capable of responding effectively to crises, whether they involve terrorist attacks or hybrid tactics.

- Physical elements such The operational stages of resilience—anticipating, managing, adapting, and recovering—highlight the dynamic and adaptive nature of resilience strategies. For NATO, this means not only preparing for potential threats but also learning from past crises to improve future responses. This approach allows NATO to remain flexible and adaptable in the face of evolving threats.

While resilience offers a promising framework for addressing asymmetric threats, its operationalization presents several challenges. One of the primary difficulties lies in the broad and often ambiguous nature of the concept itself. Resilience is frequently conflated with related terms such as resistance, preparedness, and deterrence, and its application in defense and security contexts is still evolving. Moreover, there is no universally accepted theoretical framework for resilience in national and international security, making it challenging to measure the effectiveness of resilience-based strategies.

Despite these challenges, NATO has significant opportunities to enhance its resilience posture. The emphasis on a whole-of-society approach provides a strong foundation for building resilience across multiple domains (NATO, 2022). By fostering cooperation among military, civilian, and private sector actors, NATO can create a more integrated and cohesive response to asymmetric threats. This approach aligns with the principles outlined in the 2022 Strategic Concept, which calls for enhanced civil preparedness and military capacity to ensure the continuity of the Alliance's activities (NATO, 2022).

Moreover, NATO's focus on cyber resilience and technological innovation is particularly relevant in the context of hybrid warfare, where cyber-attacks and information operations are often used to undermine stability and sow discord (NATO, 2022). By investing in advanced technologies and developing robust cyber defenses, NATO can enhance its ability to detect and respond to cyber threats, ensuring that critical infrastructure and services are protected from digital vulnerabilities.

The psychological dimensions of resilience are also crucial for maintaining societal cohesion and stability during crises. Building public trust and fostering a culture of resilience are essential components of NATO's strategy, as they ensure that societies are prepared to face both immediate and long-term threats (Lewis, 2021). This involves promoting civic engagement, enhancing public awareness, and supporting community-based resilience initiatives, all of which contribute to a more resilient and cohesive society.

7. Recommendations for Enhancing NATO's Resilience Strategies

A multiplicity of asymmetric threats stemming from various state and non-state actors severely pressures NATO's resilience. To navigate effectively in a contemporary security environment characterized by uncertainty and constant crisis, NATO should facilitate the formation of a unified vision, policy, and strategy for bolstering resilience within the Alliance. Based on the referenced documents and literature, robust planning and decision-making mechanisms, improvements in unity and coordination among Allies, and effective engagement with external stakeholders can substantially bolster NATO's resilience.

In the process of boosting NATO's resilience, one of the most significant problems is establishing a flexible decision-making system. On the one hand, consensus is one of NATO's fundamental principles that symbolizes the equality of member countries. On the other hand, achieving consensus at all levels in NATO's highest decision-making body, the North Atlantic Council (NAC), requires tremendous effort and threatens the Alliance's unity and effectiveness. Therefore, the possibility of making certain decisions based on a qualified majority principle instead of consensus could be considered. Additionally, the powers of the Secretary General and the international secretariat under his authority could be expanded. This approach could reduce political influence on routine and ongoing issues and bring them within an institutional framework. Furthermore, the authority of NATO's main operational headquarters and the Supreme Allied Commander Europe (SACEUR) could also be increased, including in operational decision-making during the crisis. This would enhance NATO's ability to respond quickly and effectively to asymmetric threats.

An important step toward strengthening NATO's resilience could be establishing a unified threat assessment system, under which the NATO Secretariat, with the involvement of member countries' security and intelligence structures, would develop a joint NATO threat assessment document. The process must be conducted at the expert level rather than the political level to achieve practical results. Otherwise, the document's development process will face the same political difficulties that generally accompany decision-making within NATO. The document agreed upon by experts should be approved at the political level, and the public version of the document should be communicated clearly to the societies of the member states.

One of the foundations of NATO's resilience strategy for the contemporary security environment should be the optimization of partnership and integration formats with like-minded stakeholders. The main format for NATO's cooperation with countries in the Euro-Atlantic area, the Euro-Atlantic Partnership Council (EAPC), includes a range of countries with radically different dynamics, ambitions, and capabilities in their cooperation with NATO. For example, the EAPC includes aspirant countries such as Ukraine and Georgia and neutral countries like Switzerland and Austria. Moreover, the Russian Federation, which is recognized as a threat rather than a partner to the Alliance, is also an EAPC member. A good example of the ineffectiveness of this format is the NATO classified information exchange system, where the access level designated for EAPC member countries (EAPC unclassified) is formally available to all participating countries. Due to the inconsistencies in the EAPC format and the absence of a clear institutionalized process for integrating aspirant countries, NATO has been forced to create new semi-formal mechanisms. The Alliance attempts to achieve logical differentiation among partner countries through additional formats, such as Intensified Dialogue (ID) or Enhanced Opportunity Partnership (EOP). It should be noted that these informal formats do not align with the ambitions of the partners and do not fully realize the potential for cooperation.

Therefore, it is advisable to create a platform based on the EAPC, within which, on the one hand, practical cooperation with relevant countries will be deepened, and on the other hand, the process of integration will be effectively planned and implemented.

In order to make the Alliance more resilient, it is important for NATO to develop a proactive policy aimed at strengthening security in the whole Euro-Atlantic area. Constantly being in a reactive mode to the multifaceted asymmetric threats increasingly complicates the protection of the Alliance's interests and the strengthening of security. A clear example of this is the severe crisis created by Russia and Belarus at the borders of the European Union and NATO through various means of hybrid pressure, such as military exercises, energy crises, and irregular migration. NATO's failure to present its own agenda to Russia convinced the Kremlin that its aggressive policies, the Kremlin's ultimatums, and blackmail were productive, resulting in further escalation and then a full-scale invasion of Ukraine. The consequent security crisis in Europe creates a logical context and urgent necessity for forming a comprehensive and proactive approach to deterrence policies based around the concept of resilience.

As NATO continues to navigate an increasingly complex and uncertain security environment, resilience offers a vital framework for countering the dual challenges of terrorism and hybrid warfare. By integrating resilience strategies into its broader security posture, NATO can better prepare for, withstand, respond to, and recover from a wide range of shocks and disruptions. The insights provided by the literature and the strategic guidance outlined in NATO's key documents provide a robust foundation for operationalizing resilience. Moving forward, NATO must continue to refine and expand its resilience strategies, fostering a culture of resilience within the Alliance and among its member states to ensure the security and stability of the Euro-Atlantic area in the face of evolving asymmetric threats. The following steps could be a good start toward that end:

- **Develop Clear and Comprehensive Resilience Policies**: NATO should refine and expand the physical and psychological components of resilience policies to address military as well as non-military threats comprehensively. This includes integrating resilience into all aspects of its strategic planning and helping member states adopt robust national resilience frameworks. Most importantly, a truly whole-of-society approach should be adopted by including private sector and civil society into planning and execution of resilience policies instead of traditional state-centric civ-mil approach.
- **Promote Societal Resilience and Public Engagement**: Building societal resilience requires active public engagement and fostering a culture of preparedness and vigilance. NATO should support initiatives that promote public awareness, civic engagement, and community-based resilience efforts, ensuring that societies are well aware of both immediate and long-term threats and are prepared to face them.

- **Enhance Multinational Coordination and Cooperation**: Given the cross-border nature of many asymmetric threats, NATO should strengthen cooperation among the Allies and with international partners. Joint exercises, shared intelligence, and coordinated responses are essential for building collective resilience.
- **Invest in Technological Resilience**: As hybrid threats increasingly involve technological solutions and manipulations in and through cyberspace, NATO must prioritize investments in cyber resilience and technological innovation. This includes developing advanced capabilities to detect, deter, and respond to cyber threats, identifying and refuting disinformation, and ensuring that digital vulnerabilities of critical infrastructure are addressed and vital services are protected.
- I**ntegrate Resilience into Military Education and Training**: NATO should incorporate resilience-building scenarios into its military education, training, and exercises, preparing forces to respond effectively to hybrid and terrorist threats. This includes enhancing the adaptability of command structures, ensuring that military operations are integrated with civilian crisis management efforts and that the civilian population is ready to support defensive measures.
- **Adopt a Proactive and Agile Approach**: Resilience is not just about defense but also about adaptation and transformation. NATO should adopt a proactive approach to resilience that anticipates future threats, learns from past experiences, and continuously adapts to new challenges. This includes fostering innovation, flexibility, and learning within the Alliance.

References:

Allied Command Transformation. (2023). *Resilience in NATO*. NATO. https://www.act.nato.int/article/resilience-in-nato/

Aradau, C. (2014). *The promise of security: Resilience, surprise and epistemic politics*. Routledge.

Asmus, R. D. (2010). *A little war that shook the world: Georgia, Russia, and the future of the West*. Palgrave Macmillan.

Audrey Kurth Cronin (2018). *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*. Oxford University Press.

BBC. (2021, November 26). *Belarus border crisis: How are migrants getting there?* https://www.bbc.com/news/world-europe-59400702

Berti, B. (2016). Rebel politics and the state: between conflict and post-conflict, resistance and co-existence. *Civil Wars 18 (2), 118-136*.

Bourbeau, P. (2015). *Resilience and International Politics: Premises, Debates, Agenda*. International Studies Review.

Byman, D. (2018). *Road Warriors: Foreign Fighters in the Armies of Jihad*. Oxford University Press.

Chandler, D. (2019). *Resilience and the City: The Promise of Urbanism in an Age of Uncertainty*. Routledge.

Crenshaw, M. (2016). *Explaining Terrorism: Causes, Processes, and Consequences*. Routledge.

Gvineria, Sh. (2020). Euro-Atlantic security before and after COVID-19. Journal on Baltic Security, 6(1), 5-21.

Gvineria, Sh. (2022). *Hybrid challenge to Euro-Atlantic security*. Latvian transatlantic organization. https://www.lato.lv/shota-gvineria-the-hybrid-challenge-to-euro-atlantic-security/

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies.

Hoffman, F. G. (2018, November 8). Examining complex forms of conflict: Gray zone and hybrid challenges. *PRISM*, National Defense University. https://cco.ndu.edu/News/article/1680696/examiningcomplex-forms-of-conflict-gray-zone-and-hybrid-challenges

Hoffman, B. (2019). *Inside Terrorism*. Columbia University Press.

Hurt, M. (2021, September 14). *Is Zapad 2021 any different from Zapad 2017?* International Centre for Defence and Security. https://icds.ee/en/is-zapad-2021-any-different-from-zapad-2017/

Kilcullen, D. (2020). *The Dragons and the Snakes: How the Rest Learned to Fight the West*. Oxford University Press.

Lewis, P. (2021). Hybrid Warfare and the Role of Resilience. *International Security*. https://direct.mit.edu/isec

Marc Sageman (2018). *Misunderstanding Terrorism*. University of Pennsylvania Press.

Russian Ministry of Foreign Affairs. (2021). *Agreement on measures to ensure the security of the Russian Federation and member States of the North Atlantic Treaty Organization*. https://mid.ru/ru/foreign_policy/rso/nato/1790803/?lang=en

NATO. (2012). *Active engagement, modern defence: Strategic concept for the defence and security of the members of the North Atlantic Treaty Organisation adopted by heads of state and government in Lisbon*. NATO. https://www.nato.int/

NATO. (2016). *Warsaw Summit Communiqué*. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO. (2019). *Resilience: The first line of defence*. NATO Review. https://www.nato.int/docu/review/chapters/2019/02/27/resilience-the-first-line-of-defence/index.html

NATO. (2020). *NATO 2030: United for a new era - Analysis and recommendations of the reflection group appointed by the NATO Secretary General*. https://www.nato.int/nato2030/independent-group/

NATO. (2022). *NATO Strategic Concept 2022*. https://www.nato.int/strategic-concept

NATO. (2024). *Washington Summit Declaration 2024*. https://www.nato.int/cps/en/natohq/official_texts_212330.htm

NATO. (2024-1). *Countering terrorism*. https://www.nato.int/cps/en/natohq/topics_77646.htm

NATO. (2024-2). *Countering hybrid threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm

Neumann, P. (2015). *Radicalized: New Jihadists and the Threat to the West*. I.B. Tauris.

Renz, B. (2018). *Russia's Military Revival*. Polity Press.

Schadlow, N. (2017). *War and the Art of Governance: Consolidating Combat Success into Political Victory*. Georgetown University Press.

Snegovaya, M. (2018). Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare. *Institute for the Study of War*.

Thomas, T. (2015). Russia's 21st Century Information War: Working to Undermine and Destabilize Populations. *Journal of Slavic Military Studies*.

Fjäder, C. (2014). The nation-state, national security, and resilience in the age of globalization. *Resilience*, 2(2), 114–129.

Walsh-Dilley, M., & Wolford, W. (2015). (Un)Defining resilience: Subjective understandings of 'resilience' from the field. *Resilience*, 3(3), 173–182.

CHAPTER 2

EFFECTS OF THE RUSSIA-UKRAINE WAR ON NATO'S OFFICIAL COUNTER-TERRORISM DISCOURSE: AN EVALUATION IN TERMS OF INTERNATIONAL LAW

Arif Bağbaşıoğlu[*]

Abstract

This chapter explores the impact of the Russia-Ukraine War on NATO's official discourse, especially regarding counter-terrorism. Although the war has strengthened the state-based threat discourse against the Alliance, the role of the Wagner Group in the war and the short-lived struggle between its leader and the Moscow administration has added a new dimension to the issue of non-state actors and terrorism. Accordingly, this chapter discusses the Wagner Group's prominent role in the war in terms of international law, specifically the law of international responsibility. The chapter concludes that the group's activities will feature more intensively in NATO's official discourse.

Introduction

The Russia-Ukraine War is a conflict that affects the future of global politics not only because of the current tension, chaos and anxiety it generates in the short term, but also because of the potential risks, such as the danger of nuclear war in the long term. It is obvious that the war had important repercussions for transatlantic relations and NATO, which was established as a regional collective defense organization and entered a period of change after the Cold War. The Russia-Ukraine War not only has effects on the unstable relationship between NATO and the Russian Federation, but also on NATO's enlargement policy, relations between the Alliance member countries, and the Alliance's solidarity discourse. This war strengthened the state-based threat discourse against the Alliance. It can be stated that NATO has tried to develop an approach that focuses on asymmetric threats such as terrorism carried out by illegal structures and the armed forces of a state - in this case Russia - and the conventional

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

and nuclear assets of that state. This war has also brought about the discussion of different aspects of the Wagner Group, which operates as a private military company in various parts of the world, in terms of international law. The United Kingdom (UK) officially declared the Russian mercenary organization, Wagner Group, a terrorist organization in September 2023. The US formally designated the Wagner Group as a transnational "significant" criminal organization in January 2023 and the US officials also constantly draw attention to the connection between the Wagner group and Russia (Fitzgerald, 2023). Accordingly, the chapter claims that the activities of the Wagner Group will feature more intensively in NATO's official discourse.

This study investigates the impact of the Russia-Ukraine War on NATO's official discourse, specifically its counter-terrorism discourse. It argues that the Russia-Ukraine War is partially testing NATO's internal solidarity and its deterrence function, which includes preventing attacks on the political independence or territorial integrity of member states. While Ukraine is not a NATO member state, it has repeatedly requested to join and borders NATO member countries, such as Poland, Hungary, and Slovakia. Hence, NATO member countries perceive the war in Ukraine as a serious threat. This threat perception has also pushed Finland and Sweden towards NATO membership. Thus, the chapter argues that the attitudes of NATO allies, shaped by the war, may play an important role in shaping the Alliance's future.

The study aims to draw attention to the possible implications of the Russia-Ukraine war for the official inclusion of private military companies in NATO's counter-terrorism discourse. In particular, it considers the Wagner group, whose legal status, activities, and responsibilities are highly controversial. The paper will first examine NATO's counter-terrorism discourse created since 2001 and then evaluate the effects of the war on this discourse. Finally, it will evaluate the status of Wagner Group members in terms of international law in relation to the Russia-Ukraine War.

NATO's Evolving Counter-Terrorism Discourse

Fighting terrorism is a relatively new focus for NATO. The September 11 attacks not only changed how people think about security, risk, and threats in global politics but also completely transformed NATO's approach to terrorism. The attacks transformed terrorism from being a domestic issue to an international security problem and threat. Thus, the Alliance accepted the need, as a basic philosophy, for more comprehensive political, economic, policing, and military measures to combat terrorism (Bennett, 2003). The 11 September attacks can therefore be considered as a moment that shifted NATO's security perception from conventional and state-based threats to asymmetric threats, such as terrorism. This is because it was the first and only time that Chapter 5 of the North Atlantic Treaty on collective defence was invoked. Within NATO, it is now accepted that terrorism cannot be fought by a single actor alone (Hallams, 2009: 38) and that terrorism threatens not only the Euro-Atlantic region but also the world.

In its fight against terrorism following the 11 September attacks, NATO initiated counter-terrorism operations outside European territory. The first of these, Operation Eagle Assist (October 2001–May 2002), was launched on 9 October 2001 (NATO, 2002a). The second, Operation Active Endeavour (OAE), was launched in the Eastern Mediterranean on 26 October 2001 to prevent terrorist activities in the Mediterranean. NATO's naval force continued its activities to prevent terrorist activities and ensure security in the Mediterranean until 2004. In 2008, it engaged in anti-piracy operations at the request of the UN in the Gulf of Aden. In 2003, OAE was extended under the mission's name of Task Force Straits of Gibraltar to include the provision of escorts for the non-military ships of NATO member states through the Straits of Gibraltar. This helped to keep trade routes open and strengthened NATO's relationship with Mediterranean Dialogue partners (NATO, 2022a). Thus, the OAE's mandate has expanded beyond counter-terrorism. At the Warsaw Summit in 2016, the operation was downgraded to a non-Chapter 5 mission, to be succeeded by Operation Sea Guardian, which contributed to maritime security capacity building and supporting maritime counter-terrorism (NATO, 2016).

In addition to full-fledged operations, NATO has conducted several military exercises designed to enhancing its counter-terrorism capabilities and increase interoperability among both NATO nations and partners (Sadık and Yalçın-İspir, 2023: 262). In NATO's official discourse, the meaning of the term 'interoperability' includes maintaining solidarity within the Alliance and ensuring cooperation with non-Alliance countries. Particularly significant for interoperability was NATO's operation in Afghanistan, in which it fought a ground war against an asymmetric threat. It was the Alliance's largest military operation in terms of personnel and size of the operational area.

One of the most significant outcomes of the decisions taken under Chapter 5 is that the Alliance demonstrated its political solidarity against terrorist threats. After the September 11 attacks, NATO made significant efforts to reorient its legal doctrine and institutional structure to adapt. NATO adopted counter-terrorism-related legal documents as a basis for its actions in this field. NATO's Military Concept for Defence Against Terrorism MC 472, which was prepared according to NATO's 1999 Strategic Concept and approved in 2002, was particularly valuable in terms of the principles of its counter-terrorism strategy. As part of a broader package of measures, it is significant because it includes definitions for terrorism and counter-terrorism. The adoption of the Policy Guidelines on Counter-Terrorism in 2012 was also fundamental in terms of reassessing NATO's role, responsibilities, and contribution in combating terrorism. In 2016, an updated Military Concept for Counter-Terrorism was published to supersede the 2002 version (North Atlantic Military Committee, 2016). This update was better aligned with both the NATO Policy Guidelines on Counter-Terrorism and the UN Global Counter-Terrorism Strategy, adopted in 2006 and revised biannually (Sadık and Yalçın-İspir, 2023: 256).

As noted in the previous chapter by Ambassador Gvineria, NATO developed an institutional structure and instruments to help combat terrorism. One prominent initiative following the September 11 attacks and endorsed at the 2002 Prague Summit is the NATO Response Force (NRF), which aims to enhance capabilities for combating new security challenges, especially terrorism (NATO, 2002b). It has been modified several times in line with changing needs, as dictated by experiences such as in Afghanistan and Iraq. One of the most significant changes, adopted at the Wales Summit in 2014, was the establishment of the Very High Readiness Joint Task Force, which can be deployed within days. While mainly a land-based unit, it includes air, maritime, and special forces (NATO, 2014). Following Russia's invasion of Ukraine in early 2022, NATO activated for the first time in February that year multinational battlegroups with a deterrent and defensive role in several countries bordering Russia (Latvia, Estonia, Lithuania, and Poland) and is set to increase its presence in other countries.

Originally established to counter a conventional threat, NATO is increasingly focusing on its ability to respond to and neutralize non-traditional security challenges. The establishment of structures like the Centre of Excellence Defence Against Terrorism (COE-DAT) in Ankara, Türkiye to fight against terrorism not only contributes to NATO's transformation but also enhances the collaborative efforts between personnel from member and partner states. Twenty-three years after the September 11 attacks, NATO has established a clearly working legal doctrine and institutional structure, and conducted significant military operations for fighting terrorism.

Despite its transformation and successes in fighting terrorism, NATO faces various limitations and hindrances in implementing its counter-terrorism strategies. These include the inherent complexities of terrorism (Bernasconi, 2011: 1), differing perspectives and capacities among European Alliance members and the United States (Axelrod and Borzutzky, 2006: 303), inadequate intelligence, and problems arising from NATO's enlargement process.

NATO's Agenda and Debates Before the Russia-Ukraine War

In response to the earlier Russian invasion of Crimea directly and decisively impacted NATO's official discourse as well as its activities. At the NATO Summit in Wales on 4-5 September 2014, NATO leaders agreed to strengthen Ukraine's defense capacities, suspend military and civilian cooperation with Russia for its international law violations, and increase NATO forces' readiness against possible attacks. (NATO, 2014) This enhancing of NATO's deterrence against state-centered threats continued at subsequent Alliance summits. These developments initiated a process that placed NATO's collective defense mission and deterrence at the center of its official discourse. However, this discourse, which can be considered as indicating solidarity among member states, could not prevent crises within the Alliance. In the run-up to the Russia-Ukraine War, some NATO member states made a special effort to avoid a rupture in relations with Russia because they were located in the same region, despite imposing sanctions on Russia in line with the United States. This effort was based on social and cultural ties, and economic relations, particularly to ensure energy security (Shakarian, 2014). Differences in perspectives and policies among European allies continued from the invasion of Crimea until the start of the Russia-Ukraine War.

Indeed, NATO members have not always been able to adopt a common stance, while at the same time addressing issues affecting their international political agenda. Prior to the Russia-Ukraine War, their attitudes differed regarding NATO policies towards both Russia and China. In particular, differing geopolitical priorities led the United States to disagree with various NATO allies, especially Germany and France, regarding what measures to take against Russia after it annexed Crimea and what policies to implement in relation to China regarding the Syrian crisis. This dissatisfaction was most visible in French President Emmanuel Macron's interview with The Economist on November 7, 2019, when he commented about NATO's "brain death" and criticized the lack of consultation among NATO member states (Macron, 2019). These disagreements have also been reflected in debates on whether there is fair burden sharing among NATO members (Birnbaum and Rucker, 2018). In fact, behind both Macron's comment and the burden-sharing problem lie divergences among NATO member countries regarding their security understandings and threat perceptions.

The NATO Summit of Heads of Government and State took place in London on December 3-4, 2019, against the backdrop of the events discussed in this chapter. The Summit Declaration also affirmed the commencement of an assessment process to increase unity and cooperation within the Alliance (NATO, 2019). The primary result of this process was the publication of the NATO Strategic Concept 2022, unveiled at the Madrid Summit on June 29-30, 2022. This concept was clearly shaped by the Russia-Ukraine conflict.

The Russia-Ukraine War and NATO's Official Discourse

Russian President Vladimir Putin's initial remarks on the conflict, issued on February 24, 2022, indicate that Russia intended to demilitarize Ukraine, which he described as a constructed entity that historically belonged to Russia, and to prevent NATO from gaining a foothold in Ukraine (Kirby, 2022). Putin's statements emphasized that the US and NATO were trying to encircle Russia through Ukraine and Georgia. NATO's expansion and the threat that Russia perceived from this is clearly the focus of Putin's discourse on the causes and objectives of the war.

In the Western literature, however, the war is seen as a consequence of Russia's "militarized" foreign policy. For example, Fix and Keil (2022: 1-2) claim that Russia's foreign policy approach, which makes much greater use of military methods and tools, is aggressive and and its rhetoric revisionist. Criticism of this approach has also dominated NATO's official discourse since the war started. On February 25, 2022, the NATO Heads of Government and State Meeting condemned the Russian aggression, which it described as a a "full-scale invasion attempt" that threatened regional security (NATO, 2022b). The Declaration of the Meeting stated that NATO was taking all necessary measures under Chapter Four of the North Atlantic Treaty. Thus, NATO activated its defense plans and deployed both national elements of member states and elements of the NATO Response Force on its eastern flank. Finally, NATO and EU adopted resolutions to exclude Russia from the international financial system while the US administration imposed sanctions on Russian officials and increased both security and non-security assistance to Ukraine (U.S. Department of State, 2022). These decisions by NATO members to strengthen both their individual and collective defense, and Sweden and Finland's application for NATO membership, are important concrete indicators that the Russie-Ukraine War has increased solidarity within the Alliance.

The tangible result of this war environment for NATO has been a visible increase in the Alliance's effectiveness and activities. Until 2014, when Russia annexed Crimea, NATO had deployed almost no ground combat forces in those countries that were geographically close to Russia and which joined the Alliance after 1999. This changed, however, after Russia's seizure of Crimea (Pifer, 2022), while the Russia-Ukraine war has increased NATO's military presence on Russia's western borders and led to Sweden and Finland becoming NATO members. At the 2022 Madrid Summit, Sweden, and Finland signed a trilateral memorandum with Türkiye regarding their NATO membership processes. This memorandum is directly compatible with NATO's anti-terrorism discourse and also very important in exemplifying how states that want to be included under NATO's security umbrella have to respect the security needs of existing member states.

Unlike NATO's three previous post-Cold War strategic concepts, the 2022 concept adopted at the Madrid Summit represents a notable shift in the Alliance's official stance. It acknowledges that the Euro-Atlantic region is no longer at peace and identifies the Russian Federation as the primary immediate threat to NATO members (NATO, 2022c). Consequently, the document emphasizes NATO's primary focus on enhancing its defense and deterrence capabilities. The discussion regarding Russia aligns with NATO's actions following the start of the Russia-Ukraine War and is consistent with expectations.

NATO's decisions to increase collective defense, and Sweden and Finland's application for NATO membership are important concrete indicators that the Russian-Ukraine War has increased solidarity within the Alliance. The war has also led to consistency in NATO countries' discourse around the Wagner group. As will be detailed below, first the UK and then the US have designated it as an illegal organization.

The Russia-Ukraine war and counter-terrorism were also high on the agenda of the summit held in Washington on July 9-11, 2024 to mark NATO's 75th anniversary. The Summit Declaration emphasized that Russia is the "greatest and most direct threat" to the Alliance's security (NATO, 2024). The decisions taken at the Summit are important in coordinating NATO allies' assistance and military training in Ukraine and institutionalizing the Alliance's support for Ukraine. In the declaration Russia's aggressive hybrid actions against Allies, including through proxies, in a campaign across the Euro-Atlantic area was condemned. These include sabotage, acts of violence, provocations at Allied borders, instrumentalization of irregular migration, malicious cyber activities, electronic interference, disinformation campaigns and malign political influence, as well as economic coercion. In this context, the summit can be considered a crucial summit for the Alliance's strategy in Ukraine.

Considering Russia's military posture in the Mediterranean and Black Sea, as well as failed states and violent non-state actors on NATO's southern flank, the importance of counter-terrorism is likely to increase in light of the Russian war in Ukraine.

The Status of Wagner Group Members Under The Law of Armed Conflict

Unlike traditional private military companies, the Wagner Group, like other Russian security companies, acts as a "quasi-state agent of influence" (Pokalova, 2023: 1). Since Russia occupied Crimea, the Wagner Group has played an active role as Russia's actor in the field. Wagner was directly involved in actions such as the assassination of the Defense Minister of the Luhank People's Republic, which wanted to operate independently of Russia in Ukraine, and the intense pressure applied to anti-Russian Kazakhs (Sukhankin, 2018). Established by Dmitri Utkin and funded by Russian oligarch Yevgeny Prigozhin, Wagner Group emerged during the Crimea occupation and was labeled Putin's personal army. With centers in Argentina, Hong Kong, and Russia, the group reportedly has over 10,000 members while around 40,000 Russian prisoners are believed to have joined since the start of the Russia-Ukraine War (Letrone and Cabus, 2023). During the war, Wagner troops have been prominently involved on multiple fronts, notably in the Donbas region.

Despite being labeled a private military company, the Wagner Group stands apart from similar entities worldwide due to its unique ties with the Russian military and intelligence apparatus, as evident in its management structure. (Neethling, 2023: 7). The Wagner Group takes an "active combat role" in armed conflicts, in addition to undertaking protection and other auxiliary tasks, which differentiates it from most private military companies (Riepl, 2022: 304). The group, which operates as loose networks of shell companies and financial intermediaries instead of a singular entity (Doxsee, 2022), has gained so much power that it has become autonomous. Hence, Kimberly Marten (2019) describes it as an informal security organization with characteristics similar to those of a "semi-state."

Despite compelling evidence that the company's activities align with Russia's interests, the Russian authorities classify Wagner Group members, not as "Russian soldiers", but as "citizens" who happen to be present in the conflict zone for various reasons (Riepl, 2022: 315-316). Consequently, Russia denies that it uses private military companies as a tool of the state. Ultimately, this policy of concealment means that it is legally uncertain who is behind the group's actions, which undermines accountability mechanisms. This uncertainty is leveraged by the Kremlin in its military strategy to make short-term strategic gains while hindering its adversaries' responses. In addition, by keeping the Wagner Group's violations of international humanitarian law as secret as possible, Russia tries to prevent the Wagner fighters from losing their effectiveness (Linder, 2018: 17).

Undoubtedly, however, Russia is using private military companies to safeguard its cross-border interests. Here, differences should be noted between Russian private military companies and their Western counterparts. Unlike the latter, the former do not avoid engaging in conflict in crisis zones, are involved in complex relationship networks in third countries, and conduct intelligence and psychological operations. Additionally, the Kremlin has used Wagner's lack of legal status in Russia to evade responsibility. This enables Russia to extend its influence internationally by circumventing international law obligations and avoid military casualties. Russia has used such companies in its engagements in Syria, Libya, and elsewhere in Africa. Similarly, Russian private military security companies are actively engaged on the frontline in Ukraine. In particular, Wagner, which employs skilled personnel with combat experience, has recruited individuals with criminal backgrounds and prison inmates in Russia's attempted invasion of Ukraine.

Debate Around the Wagner Group's Legal Status in Terms of International Law

Russia not only does not make national legal arrangements with private military companies like Wagner but also does not participate in international efforts to regulate them, such as the Montreux Document or the International Code of Conduct for Private Security Providers (Bukkvoll and Østensen, 2020: 10). Absent such laws or regulations, Wagner operates in Russia in a gray zone that lacks any legal framework or oversight. Nevertheless, Russia has benefited from its presence as an auxiliary actor for achieving its foreign policy objectives. The main problem here is to determine the status of Wagner Group members in relation to international law.

Under the Law of Armed Conflict, the ongoing conflict between Russia and Ukraine has been categorized as an international armed conflict between two states. In contrast, the same law classifies Wagner Group members involved in the war as mercenaries, combatants, or civilians, which poses several challenges.

First, it should be noted that the Russia-Ukraine war has made the close or even organic relationship between the Wagner Group and Russia clearer to NATO countries. The decisions taken by the UK, the European Parliament and the US in this respect are very significant. In January 2023, the Biden Administration designated Wagner a Transnational Criminal Organization while several US bills imposed sanctions, reporting requirements, and other measures on the Wagner Group (Congressional Research Service, 2023). While the USA designates Wagner a "transnational criminal organization", the UK designates it a "terror organization" (UK Government 2023; U.S. Department of the Treasury 2023).

On July 11, 2023, the declaration following the NATO Summit of Heads of Government and State in Vilnius specifically mentioned the Wagner Group. It also stated that NATO would closely monitor the potential deployment of such so-called private military companies in Belarus (NATO 2023).

The legal regime applicable to the ongoing armed conflict between Russia and Ukraine consists of the Geneva Conventions of 1949, the 1977 Additional Protocol I, and the 1907 Hague Conventions as well as customary international law. Russia and Ukraine are parties to the 1949 Geneva Conventions and Additional Protocol I. Although Russia describes its attempted invasion of Ukraine as a "special military operation", its denial of the nature of the conflict's status does not change the fact that it is an international armed conflict.

The international law of armed conflict defines two categories of combatants: lawful and unlawful. It is therefore crucial to determine whether Wagner Group members participating in the Russian-Ukrainian War are lawful combatants under Article 43 of Additional Protocol I. It is also important to determine whether they are operating under a command responsible to Russia. In fact, Russia is officially connected to the group in various ways that contradict its attempts at plausible deniability. These include issuing Russian passports to Wagner Group members by Central Migration Office Unit 770-001 to individuals linked to the Russian Ministry of Defense, and the treatment and rehabilitation of its members in Russian military hospitals (CSIS, 2020). Yet, this does not imply a clear case that the Wagner Group has been operating under a command accountable to Russia.

The Wagner Group has played various roles in Ukraine, such as acting under the command of Russian military forces in Severodonetsk and acting under its own chain of command in the capture of Bakhmut (Williams and Maddocks, 2023). Moreover, on June 23, 2023, Prigozhin, then Wagner Group leader, revolted against the Russian army on the grounds that the group had not been provided with sufficient ammunition. The group's forces quickly took control of Rostov and Voronezh, close to the Ukrainian border (CNN Türk, 2023). Belarus mediated an end to the mutiny. Russia lacked effective or general control over the Wagner Group in Ukrainian territory. It can be said that as of today, state oversight of the Wagner Group is clearly more restrictive and greater than before. Therefore, changing roles and actions made it difficult to reach a clear conclusion on the group's status. However, today, according to Marten state oversight of the Wagner Group, is confusingly split between three organizations: the Russian National Guard; Chechen leader Ramzan Kadyrov's Akhmat special forces group (which is technically part of the National Guard); and Russia's military intelligence agency (Marten, 2024). In this case, it can be said that the Kremlin has completely taken control of Wagner.

The conventional military forces of the two parties in the Russia-Ukraine War are legal combatants, whereas the status of Wagner Group members occupies a gray area and emerges as unlawful combatants. Illegal combatants are often civilians, spies, terrorists, and mercenaries who directly participate in an armed conflict. Hence, it is critical to determine whether Wagner Group members who actively participated in the war are mercenaries. The main criteria for identifying private military company members, or mercenaries, are "citizenship ties and the nature of the armed conflict in which they are involved" (Miroshnichenko, 2023).

Lessons Learned and Conclusion

It is clear that NATO's counter-terrorism strategy has expanded its global area of struggle and intervention, as demonstrated especially by NATO activities outside the North Atlantic region. Since the September 11 attacks, NATO has made significant progress in counter-terrorism, although cooperation among member states has not always reached the desired levels, given, for example, French President Emmanuel Macron's comment that NATO is 'brain dead'. The most important challenge while developing NATO's counter-terrorism role has been transatlantic and intra-European disagreements over the nature of terrorism and how to deal with this threat. Given that the Russia-Ukraine War has increased solidarity within the Alliance, NATO has clearly contributed positively to cooperation among member states in the fight against terrorism.

It is reasonable to claim that the Wagner Group has close relations with Russia and is directed by Russia. However, it differs from other private military companies in being declared illegal under both the Constitution of the Russian Federation and the Russian Criminal Code. While Russia evidently sought to use the Wagner Group to achieve its foreign policy objectives before the Russia-Ukraine War, the absence of a direct causal connection between the group and the Russian state left a gray area for the latter. After certain NATO countries designated Wagner as a terrorist organization after Russia's invasion of Ukraine, this gray area has disappeared. It would be very valuable for NATO's counter-terrorism discourse if NATO countries determine a common definition for Wagner and its related elements and impose joint sanctions against them within this framework. In this regard the UK's definition of the Wagner Group as a terror organization has set a positive precedent.

Decisions taken by the UK, the US, the European Parliament, and NATO since the Russia-Ukraine War broke out have helped to clarify the close relationship between the Wagner Group and Russia. This creates the potential to increase Russia's responsibility and accountability in the international arena by documenting the clear violations of the law of armed conflict committed during military operations involving Wagner forces. Furthermore, determining the group's international legal status will set a precedent for determining the responsibility and accountability of other private military companies and the states that directly or indirectly employ them in future conflict situations. Hence, the stance taken by NATO as a collective defense organization will be crucial in determining the responsibilities stemming from various actions of military companies, whether deliberate or accidental, and their implications under international law.

References

Axelrod, R. and Borzutzky, S. (2006). "NATO and the War on Terror: The Organizational Challenges of the Post 9/11 World", *The Review of International Organization*, 1, 293-307.

Bennett, C. (2003). "Combating Terrorism", *NATO Review,* https://www.nato.int/docu/review/articles/2003/03/01/combating-terrorism/index.html.

Bernasconi, C. (2011). *NATO's Fight Against Terrorism Where Do We Stand?,* Rome: NATO Defense College Research Paper.

Birnbaum, M. & Rucker (2018). P. "At NATO, Trump Claims Allies Make New Defense Spending Commitments After He Upends Summit," *The Washington Post,* 07.12.2018. https://www.washingtonpost.com/world/europe/trump-upends-nato-summit-demanding-immediate-spending-increases-or-he-willdo-his-own-thing/2018/07/12/a3818cc6-7f0a-11e8-a63f-7b5d2aba7ac5_story.html.

Bukkvoll, T., & Østensen, Å. G. (2020). "The Emergence of Russian Private Military Companies: A New Tool of Clandestine Warfare". *Special Operations Journal*, *6*(1), 1-17.

Congressional Research Service (2023). *Russia's Wagner Private Military Company (PMC),* 01.08.2023, https://crsreports.congress.gov/product/pdf/IF/IF12344.

Doxsee, C. (2022). "Wagner: The Cornerstone of Russia's Strategy in Africa". *ISPI* https://www.ispionline.it/en/publication/wagner-cornerstone-russias-strategy-africa-37141.

Fix, L. and Keil, S. (2022), "NATO and Russia after the Invasion of Ukraine", *The German Marshall Fund of the United States*, 04.04.2022, https://www.gmfus.org/news/nato-and-russia-after-invasion-ukraine.

Hallams, E. (2009). "The Transatlantic Alliance Renewed: The United States and NATO Since 9/11". *Journal of Transatlantic Studies*, 7(1), 38-60.

Kirby, P. (2022). "Why did Russia Invade Ukraine and has Putin's War Failed?". *BBC News*, 16.11.2022 https://www.bbc.com/news/world-europe-56720589.

Letrone, W. and Cabus, T. (2023). "The Wagner Group and the Question of the Legal Attribution of the Acts of Private Actors to a State". *Cambridge Core Blog* , 24.07.2023, https://www.cambridge.org/core/blog/2023/07/24/the-wagner-group-and-the-question-of-the-legal-attribution-of-the-acts-of-private-actors-to-a-state/.

Linder, A. (2018). "Russian Private Military Companies in Syria and Beyond", *New Perspectives In Foreign Policy*, 16, 17-21.

Macron, E. (2019). "Emmanuel Macron in his own words", *The Economist* 07.11.2019, https://www.economist.com/europe/2019/11/07/emmanuel-macron-in-his-own-words-english.

Marten, K. (2019). "Russia's Use of Semi-State Security Forces: The Case of the Wagner Group". Post-Soviet Affairs 35(3), 181-204.

Marten, K. (2024). "Where's Wagner Now? One Year After the Mutiny". *PONARS Eurasia,* 21.06.2024, https://www.ponarseurasia.org/wheres-wagner-now-one-year-after-the-mutiny/.

Miroshniçenko, S. (2023). "Wagner Group. Why They Are Not Mercenaries, And Russia Is Equally Responsible For Them Like For Its Regular Armed Forces". *Media Initiative for Human Rights,* 04.01.2023 https://mipl.org.ua/en/wagner-group-why-they-are-not-mercenaries-and-russia-is-equally-responsible-for-them-like-for-its-regular-armed-forces/.

Neethling, T. (2023). "Russian Para-Military Operations in Africa: The Wagner Group as a De Facto Foreign Policy Instrument", *Scientia Militaria*, 51(1), 1-23.

NATO (2002a). "Statement by the Secretary General on the conclusion of Operation Eagle Assist", 30.04.2002, https://www.nato.int/docu/update/2002/04-april/e0430a.htm.

NATO (2002b). *"Prague Summit Declaration",* 21.11.2002, https://www.nato.int/cps/en/natohq/official_texts_19552.htm.

NATO (2014). "Wales Summit Declaration", 05.09.2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO (2016), "Warsaw Summit Communiqué", 09.07.2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

NATO (2022a). "Operation Active Endeavour", https://www.nato.int/cps/en/natolive/topics_7932.htm.

NATO (2022b). "Statement by NATO Heads of State and Government on Russia's attack on Ukraine", https://www.nato.int/cps/en/natohq/official_texts_192489.htm?selectedLocale=en

NATO (2022c). "NATO 2022 Strategic Concept," 29.06.2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf.

NATO (2023). "Vilnius Summit Communiqué", 11.07.2023,https://www.nato.int/cps/en/natohq/official_texts_217320.htm?selectedLocale=en.

North Atlantic Military Committee, (2016). *Military Concept for Counter-Terrorism*, https://www.nato.int/nato_static_fl2014/assets/pdf/topics_pdf/20160905_160905-mc-concept-ct.pdfi.

NATO (2024). "Washington Summit Declaration", 10.07.2024, https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

Pifer, S. (2022). "The Russia-Ukraine War and Its Ramifications for Russia, Brookings. 08.12.2022 https://www.brookings.edu/chapters/the-russia-ukraine-war-and-its-ramifications-for-russia/.

Pokalova, E. (2023). The Wagner Group in Africa: Russia's Quasi-State Agent of Influence. *Studies in Conflict & Terrorism*, 1-23.

Riepl, M. (2022). *Russian Contributions to International Humanitarian Law: A Contrastive Analysis of Russia's Historical Role and Its Current Practice*, Baden-Baden: Nomos Verlagsgesellschaft Mbh & Co.KG.

Sadık G. and Yalçın-İspir A. (2023). "Counter-terrorism", ed. Sebastian Mayer, *Research Handbook on NATO,* Northampton: Edward Elgar Publishing, 253-267.

Shakarian, P. (2014), "Sanctions against Russia are Dividing Europe More than You Think". *Russia Direct*. 22.09.2014, http://www.russiadirect.org/opinion/sanctions-against-russia-are-dividing-europe-more-youthink.

Sukhankin S. (2018), "Continuing War by Other Means': The Case of Wagner, Russia's Premier Private Military Company in the Middle East", Eurasia Daily Monitor, 15(60), 6.

Østensen, Åse Gilje, and Tor Bukkvoll. 2022. 'Private Military Companies – Russian Great Power Politics on the Cheap?' Small Wars & Insurgencies 33(1-2):130–51. doi: 10.1080/09592318.2021.1984709.

U.S. Department of State (2022). "Imposing Sanctions on President Putin and Three Other Senior Russian Officials". 25.02.2022 https://www.state.gov/imposing-sanctions-on-president-putin-and-three-other-senior-russian-officials/.

CHAPTER 3

COUNTER-TERRORISM EFFECTS OF THE RUSSIA-UKRAINE WAR FN THE NATO'S EASTERN FLANK: THE WEAPONIZATION OF MIGRATION AND IMPLICATIONS FOR FUTURE TERRORISM THREATS

Marc Ozawa[*]

Abstract

This chapter examines the impact of the Russian-Ukraine war on terrorism risks and counter terrorism strategies on NATO's Eastern Flank. The war has raised the risk of terrorist and asymmetric events in the region for two reasons. First, there is the proliferation of state-based hybrid tactics aimed at sowing division in societies of the region and undermining support for Ukraine. This coincides with an information war to appeal to aggrieved segments of society to sympathize with Moscow's position. Second, the war has created a fluid security environment that both state and non-state actors will use to their advantage. The chapter explores three events, their links to the war, and terrorist related ripple effects. These include the Poland-Belarus border crisis and the Moscow theater attack.

Introduction

NATO's Eastern Flank is becoming a nexus for military and hybrid confrontation which raises the risk of terrorism that is both directly and indirectly connected with the war and geopolitical events. Russia's invasion and continued war with Ukraine presents not only a military and security threat to NATO member states, but also raises the short and long-term risk of terrorism within NATO's borders. In the near-term, traditional deterrence and defense will focus on events in Ukraine but Russia's direct contact with the Eastern flank will be in the grey zone. NATO's approach to countering terrorism focuses on three areas: building awareness; expanding capabilities; and engaging with allies, stakeholders, and partners.

War creates an environment of fluidity, one in which terrorism can flourish in the form of asymmetric events through political, economic and information warfare which all occur below the threshold of conventional war.

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

Information war surrounding the Russia-Ukraine war is also impacting the risk of homegrown domestic terrorism. This type of information warfare is targeting politically extreme groups to sow division in society, create instability, and undermine western support for Ukraine while promoting sympathy for Russia's actions. For domestic terrorist threats, the primary risk groups come from the far right, religiously motiviated extremist groups, and otherwise aggrieved minority groups.

Across the region, states have raised terrorism threat levels in response to the increased fluidity of the security environment since the war began. Actors may be originally state based in terms of hybrid aggression, but they work and deploy non-state actors, and there is link with ethnic, religious groups and disenfranchised groups in society with grievances. Border security can become vulnerable, which raises risk of external state and non-state actors moving across the region who can then stoke grievances and deploy hybrid tactics, working alone or with homegrown elements.

This chapter examines the links between the state-on-state war taking place in Ukraine along with recent sub-war attacks on NATO's Eastern Flank that are both state and non-state in origin. The chapter explores one case in detail and draws implications for future risks of terrorism in the region. This is the artificial border crisis involving Belarus and Poland, one that was likely orchestrated by both Minsk and Moscow. This case demonstrates the links, either intentional or unintentional, between state-sponsored hybrid aggression and terrorism. Emphasis is paid to border security, migrant weaponization, and radical extremism in the context of the ongoing information war concerning Russia's war with Ukraine. The chapter concludes with implications for NATO's approach to counter terrorism.

Migration and Terrorism

The relationship between migration and terrorism is multifaceted with links that are both direct and indirect. For example, migration can be a result of terrorism when people must flee their homes to seek refuge in safer regions or further abroad. There were instances of terrorism induced migration in the wars and civil unrest in Syria, Afghanistan, and Iraq. Likewise, terrorism can contribute to humanitarian crises which can also lead to people to move. On the other hand, migration can also lead to the spread of terrorism because it presents routes that terrorists may use to enter other countries. While this presents a risk for countries that receive migrants, the vast majority of migrants are not terrorists. Yet indirectly, the experience of migration can create conditions for some migrants to radicalize and become terrorists in the future. Conditions such as poor societal integration, economic and health hardship, isolation, and connections with other disenfranchised migrants or extremists in the adopted countries can contribute to grievances among migrants leading to radicalization. This is an indirect link between migration and terrorism, one that most European countries are focused on. Large scale migration can also lead to tensions within host country communities. These may be between new migrants and migrants who arrived earlier or between migrants and indigenous communities. These tensions may be exploited by terrorists and other radical organizations for recruitment purposes and to justify their actions.

At the same time, migrant communities that are well integrated may contribute to counter terrorism by cooperating with authorities, sharing information, and denying safe haven to known terrorists and radicalized individuals. While terrorism can drive migration and certain migration-related factors may influence terrorism, the link is not straightforward. It is important to approach the issue with nuance, recognizing that the majority of migrants are not involved in terrorism, and that migration can play a positive role in preventing and countering extremism. Oversimplifying this relationship can lead to counterproductive and excessive policies.

In the case of the border migration crisis at the Belarus-Polish border, there is an added layer complexity because the concern from Warsaw, and what appears to be Minsk's intention, is uncontrolled migration. Thus, the link between migration and terrorism is the notion that environments where there is chaos and a breakdown of create conditions where terrorism can thrive. Specifically, an open or poorly controlled border provides a route for terrorists and radicalized individuals to enter Poland and ultimately move freely in the Schengen zone countries. Loose borders also offer opportunities for terrorist organizations to move resources, weapons, and supplies that may be used for future attacks.

The Belarus Border Crisis with Poland

The Belarus border crisis with Poland is inextricably linked to the Russia-Ukraine war. The crisis began with the Russian military buildup along Ukraine's borders in 2021 against the backdrop of growing 'saber rattling' from Russia and Belarus. The crisis began at the same time that Minsk announced a deeper military cooperation with Moscow and that Russian troops and military equipment would be positioned in Belarus. Because of the link between the war and border crisis, Moscow and Minsk's intentions are clear – to create chaos, disrupt elections and domestic politics, influence European and especially Polish public opinion, and create additional costs, both financial and personnel, for Poland, the countries of NATO's eastern Flank, and Europe broadly. While Moscow short term intentions may be obvious, the secondary effects related to future terrorist threats are not as evident.

The intentions of Russia and Belarus in orchestrating the border crisis appear to be four-pronged. The first was to create chaos for Polish authorities. The second was to force the adversary, in this case Polish and European leaders, to incur additional costs through resources devoted to securing the border. In this case, Poland and the EU have had to devote additional border guards and staff. Moreover, Polish authorities have erected a 110 km long border fence, partially funded by the EU, at a cost of 450 million euros. Next, the weaponization of migrants can also influence domestic politics in Poland and Europe in Russia's favor by creating an artificial crisis used by opposition and far-right parties many of whom are sympathetic to Russia. Finally, there is a Russian domestic propaganda utility to the border crisis, when Russian media portray Polish and European authorities as cruel by allowing a humanitarian crisis to unfold. This reinforced a narrative of western hypocrisy concerning human rights.

While Russia's possible intentions for the migration crisis are evident, it is unclear if the secondary and long-term impacts are on deliberate or accidental. As previously mentioned, there is a complex relationship between migration and terrorism, which is exacerbated when security conditions are chaotic and authorities lose control over their borders. Not only is it easier for radicalized individuals or those susceptible to radicalization with links to extremist groups to cross borders, the difficulties presented to migrants and their future obstacles to integration depending on where they eventually settle. This could create vulnerabilities to radicalization in the long-term. Much of the existing analysis of Russian hybrid warfare tactics examines the short term and political goals of the weaponization of migration, not the secondary and long-term impacts such as radicalization and terrorism.

However, considering that Russian authorities have cooperated in counter-terrorism with their western counterparts, and because Moscow continues to struggle with domestic terrorism threats as evidence by the recent Moscow theater attack, the terrorism dimension migration weaponization is probably unintentional. In the case of the Moscow theater attack, Washington even warned Moscow of an imminent threat despite over two years of Russia's war with Ukraine. Whether or not Moscow heeded the warning, the fact that these lines of communication are still active suggests that both sides acknowledge the value continued cooperation in counter terrorism.

Beginning in the winter of 2021, migrants began to arrive and accumulate at the border between Belarus and Poland. The sheer number of migrants and their countries of origin raised suspicion among Polish and European leaders. The migrants sought to enter the EU to seek asylum. They were primarily form the Middle East, Africa, and Afghanistan, and it was unclear how they made it to the Polish border or even into Belarus in the first place. The numbers suggested that they had help from Belarus authorities. As more migrants arrived, Polish border guards struggled to maintain border security. At the same time, the winter conditions created a humanitarian catastrophe with migrants stranded in the forest at the border with little to no supplies or shelter. This crisis took place against the backdrop of growing popular hostility towards migrants in Europe, a mood that began with the first wave of refugees fleeing the war in Syria from 2011 onwards, reaching a peak in 2015.

While Polish authorities focused the dangers of uncontrolled migration flows, western media often concentrated the humanitarian catastrophe of families stranded in a forest in the freezing cold with many migrants falling ill and succumbing to the elements. In Russia, however, the events were portrayed as a humanitarian crisis of Europe's making, with Polish authorities leaving migrants to die rather than allow them sanctuary and asylum.

As humanitarian workers gained access to those at the border, it became clear that the crisis at the border was likely intentional. Many of the migrants had Russian visas, and their accounts illustrated how Belarus authorities often transported them to Polish border by service or by force. Moreover, the most common routes for these migrants was either through Russia, with Russian authorities transporting them to Belarus through Russia or flying them directly to Belarus via flights between Minsk and destinations in the Middle East. Migrants explained that how they were offered quick and easy visas to both Russia and Belarus. The intentions of what appeared to be state-sponsored transportation operations became clear when migrants were also transported to Belarus's border with Lithuania and Latvia. Russian authorities even announced new flights between the Russian enclave of Kaliningrad and capitals in the Middle East.

The number of migrants attempting to cross into Poland through Belarus were at their highest ranging around 800 attempts per day in 2021 and 2022, just before and after Russia's invasion of Ukraine. With EU support and the development of Polish border security operations, the number of illegal crossing attempts dropped in 2023. This included the construction of a 110 km fence along the Polish-Belarus border. However, the number rose again to approximately 400 attempts per day in the spring of 2024 shortly before federal elections in Poland and other European states. After the elections, the numbers dropped to around 8 attempts per day. This pattern illustrates the link and likelihood that Russian and Belarus weaponization of migrants for political purposes, in this case, to put pressure on Polish and European authorities through direct costs and political pressure through their populations by stoking fears of uncontrolled migration and exacerbating xenophobia.

Conclusions

Security and the risk of terrorism in the Black Sea region are intertwined. Therefore, events in the Russia's war with Ukraine have directly impacted the threat of terrorism in the region. One way is with respect to migration and specifically, the border crisis between Belarus and Poland. This is an instance whereby state sponsored hybrid aggression, in this case the weaponization of migration, has created a situation that heightened the risk of terrorists and their resources being allowed to cross into NATO territory and move freely on into the Schengen zone. However, the chaotic conditions under which migrants have crossed this border could have long term ripple effects on migrant communities and individuals who may be radicalized in the future depending on their future life circumstances. The preceding case also illustrates the overlapping conditions of war, hybrid warfare, and terrorism.

For counter terrorism, the immediate priority is to secure the border. Poland and EU authorities took steps to stop uncontrolled migration by shoring up law enforcement personnel and building infrastructure. This has had the desired effect, however, despite the lower numbers of illegal border crossings and crossing attempts, the border experienced another wave of migrants arriving at the border in June 2024 coinciding with Polish and European elections. It appears that the weaponization of migration will continue to be part of Russia's hybrid tool kit. States subservient to Russia, such as Belarus, can also play a role, as this case demonstrates. While this hybrid tactic raises the costs of securing the borders, the Poland-Belarus border case study also illustrates how states can minimize and even deter the weaponization of migration by rendering the tactic ineffective.

For NATO, this means that successful measures to counter hybrid aggression and counter terrorism cannot be separated. The better policy makers understand the complex links between hybrid warfare and terrorism, the more they can design effective strategies to secure the eastern Flank. One step in this direction would be to resist stove piping analysis and operations of hybrid warfare and counter terrorism by greater cooperation among the relevant Centers of Excellence like the Centre of Excellence Defence Against Terrorism (COE-DAT) in Ankara, Türkiye and COE Stability Policing in Vicenza, Italy.

References

Amnesty International. “Poland: 17 Afghans at the Border Violently Pushed Back to Belarus,” October 20, 2021. https://www.amnesty.org/en/latest/news/2021/10/poland-17-afghans-at-the-border-violently-pushed-back-to-belarus/.

Bove, Vincenzo, and Tobias Böhmelt. “Does Immigration Induce Terrorism?” *The Journal of Politics* 78, no. 2 (April 2016): 572–88. https://doi.org/10.1086/684679.

Consilium. “The EU’s Response to Terrorism.” Accessed October 2, 2024. https://www.consilium.europa.eu/en/policies/fight-against-terrorism/.

dw.com. “How Will EU React to Poland-Belarus Border Crisis? – DW – 11/09/2021.” Accessed October 3, 2024. https://www.dw.com/en/how-will-eu-react-to-poland-belarus-border-crisis/a-59770240.

dw.com. “Poland, Baltics Step up Border Controls amid Migrant Crisis – DW – 06/16/2024.” Accessed October 3, 2024. https://www.dw.com/en/poland-baltics-step-up-border-controls-amid-migrant-crisis/a-69350351.

dw.com. “Poland Border Wall Hasn’t Stopped Migrants – DW – 09/21/2022.” Accessed October 3, 2024. https://www.dw.com/en/polands-border-wall-hasnt-stopped-the-flow-of-migrants-from-belarus/a-63193152.

euronews. “Poland to Tighten Belarus Border Controls in the Name of EU Security,” February 22, 2024. https://www.euronews.com/2024/02/22/poland-to-tighten-controls-on-belarus-border-as-estonia-warns-of-russian-threat-to-eastern.

Massicot, Dara, Michelle Grisé, Kotryna Jukneviciute, Marta Kepe, Casey Mahoney, Krystyna Marcinek, Yuliya Shokh, and Mark Stalczynski. “Cooperation and Dependence in Belarus-Russia Relations.” RAND Corporation, June 20, 2024. https://www.rand.org/pubs/research_reports/RRA2061-3.html.

“Migration Outlook Report: Possible Second Wave of Refugees from Ukraine and Further Weaponisation of Migration - ICMPD.” Accessed October 3, 2024. https://www.icmpd.org/news/migration-outlook-report-possible-second-wave-of-refugees-from-ukraine-and-further-weaponisation-of-migration.

OECD. “Migration.” Accessed October 2, 2024. https://www.oecd.org/en/topics/policy-issues/migration.html.

Ptak, Alicja. “Poland Publishes Data on Thousands of Migrant ‘Pushbacks’ at Belarus Border for First Time.” *Notes From Poland* (blog), February 7, 2024. https://notesfrompoland.com/2024/02/07/poland-publishes-data-on-thousands-of-migrant-pushbacks-at-belarus-border-for-first-time/.

Treistman, Jeffrey, and Charles J. Gomez. “European Migration and Terrorism: Humanitarian Crisis, Political Rhetoric, or Pragmatic Policy?” *Conflict, Security & Development* 21, no. 3 (May 4, 2021): 337–70. https://doi.org/10.1080/14678802.2021.1940781.

“U.S. Intelligence Warning to Moscow Named Specific Target of Attack - The New York Times.” Accessed October 3, 2024. https://www.nytimes.com/2024/04/02/us/politics/moscow-attack-us-warning.html.

Walker, Shaun, Shaun Walker Central, and eastern Europe correspondent. “Belarus Protests: Putin Ready to Send Lukashenko Military Support.” *The Guardian*, August 27, 2020, sec. World news. https://www.theguardian.com/world/2020/aug/27/belarus-protests-putin-ready-to-send-lukashenko-military-support.

“Why Poland Says Russia and Belarus Are Weaponizing Migration to Benefit Europe’s Far-Right | AP News.” Accessed October 2, 2024. https://apnews.com/chapter/poland-belarus-migrants-russia-ukraine-59d6050c2ea6853de3154150e8c9dcb5.

CHAPTER 4

WAR IN THE SEAS: UNMANNED MARITIME SYSTEMS, CIP, MARITIME TERRORISM

Gordan Akrap[*]

Abstract

This paper analyzes the impact of Russian aggression on Ukraine on the development of unmanned systems and new techniques and technologies on conflicts and wars in the maritime domain. By the term maritime domain we mean all water surfaces, regardless of whether they are seas, lakes or rivers. New knowledge, techniques and technologies developed in defensive and offensive actions are available to the general public thanks to the fast and wide distribution of information and knowledge (in text and especially video formats). Therefore, their use by individuals and groups prone to violent and even terrorist acts is easily achievable. The NATO alliance must pay special attention to the protection of its interests (that is, the interests of the Allies) in the maritime domain from new, very serious security risks and threa, by considering possible negative consequences s.

Introduction

Water is one of the essentials in the life. The first human communities were necessarily located near waters due to the necessity of ensuring the basic life needs: uninterrupted and safe availability of drinking water necessary for human use, for agriculture, as well as the possibility of growing and collecting different foodstuffs from the water. The most important civilizations developed lived by and with water. Moving on and later under the water led to the development of additional abilities and opportunities with which humanity accelerated its development by harnessing the potential of water.

Maritime, lake and river trade allowed further strengthening of societies and states and these developed in many different areas. The sea unites and connects people, enables traffic and trade, and creates a sense of freedom. Nowadays even the bottom of the sea is used as a base for laying numerous different critical infrastructures that humans depend on.

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

Exploitation of water surfaces represented, both then and now, a significant advantage but they are very vulnerable and can become a source of numerous risks and threats.

The second Russian aggression against Ukraine (from February 24, 2022) changed the existing security paradigms in all domains including the maritime domain. This chapter asks: what can be learned from this Russian aggression and the Ukrainian responses to it? Are there any possibilities that new knowledge, means, technology and techniques, as well as methods, may be used for harmful forms of action, such as violence and terrorism?

This chapter therefore focuses on lessons identified and lessons learned from the Russia-ukraine war in order to better understand possible threats in maritime domain. The question is not whether some terrorist organization, group or radicalized individuals will analyze the available data and information on war activities, but when: and with what means and with what success they will try to organize a terrorist act related to maritime domain. This is based on Russian offensive operations, Ukrainian defensive operations, and also previous conflicts and wars.

We must not, for example, ignore and experiences of the war in Syria, considering the fact that a large number of members and sympathizers of terrorist organizations such as al-Qaida and DAESH are now trained to use drones for combat, violent and terrorist purposes. Although drones that operate in air were mostly commonly used then, the possibility of terrorists mastering the use of drones in the maritime domain should not be ignored. As a result, counter-terrorism experts argue that the maritime transport will be the first upcoming major terrorist target as it was mentioned in al-Qaida manual from 2003 (Prodan, 2017)

Vulnerabilities

Water and water surfaces connect people, cities, states, continents. The surface area of the earth is covered by 71% water, that of which 96.5% is sea water (Prodan, 2017). Their security and safety are extremely important for NATO and NATO led peacekeeping activities and operations. By the term of water surfaces in this paper we mean fresh water areas and flows, rivers and lakes, as well as seas and oceans. There are three groups of areas, objects, structures and activities that needs to be part of any counter-terrorism analysis in maritime domain:

1. Near water
2. Offshore
3. Underwater

This analysis shows possible targets of violent terrorist activities, by the attacking of which terrorist can obtain their goals at the tactical, operational and strategic level:

1. Harbors/ports, especially those for human transport where huge number of humans (with or without their vehicles) assemble and wait for transfer to other ports
2. Passenger and commercial waterways, trade routes and different kinds of maritime/water transportation vehicles
3. Production and transportation of drinking water

4. Areas and systems used to supply population, flora and fauna with drinking water
5. Business activities related to food production (such as agriculture, fisheries)
6. Tourist maritime activities which many countries depend upon economically
7. Energy critical infrastructure located next to water surfaces due to their cooling requirements (such as nuclear power plants) or terminals for gas/oil storage and subsequent transportation
8. Off shore energy critical infrastructures that pump, produce and transfer individual energy sources (platforms, wells, wind and solar power plants on water surfaces)
9. Underwater key critical infrastructure (communication and electrical cables, water supply, sewage, gas and oil pipelines, traffic tunnels)
10. Protection of water and underwater life (flora and fauna) where disrupting its integrity and functionality would negatively affect people's lives
11. Bridges, especially in narrow passages and canals

There is a possibility that in the foreseeable future ferry passenger traffic will become the target of violent and terrorist activities in the way that certain terrorist groups have already done in the past by hijacking airplanes. There are well-known historical examples (Prodan, 2017) of hijackings and the use of passenger ships as means to promote the goals and ideas of terrorist organizations (as was the case with the ship Achile Lauro in the Mediterranean in 1985).

We should also not ignore the possibility that some sparsely or uninhabited areas next to water bodies, which are nonetheless habitable, are used by terrorists for the preparation, planning and conduct of other forms of illegal activities such as electronic data collection (SIGINT), creating conditions for electronic warfare (EW) or the creation of training and logistics bases to support other forms of violent and illegal activity (Warsaw Institute, 2018; The Warzone, 2018; New York Times 2018).

When we look at the extent of the security and safety challenges for maritime area, one can see numerous vulnerabilities. We can also notice complexity of those challenges that preventive, protective and security organizations need ensure the security and safety of water areas, both freshwater and salt sea.

LI & LL from the Russia-Ukraine War

The second Russian aggression against Ukraine (February 2022) posed numerous questions about the security and safety of seas and waters and their use as a means to fulfill terrorist goals. In preparation for the second aggression against Ukraine, Russia strengthened the composition of its Black Sea Fleet with parts of the Baltic and Northern Fleets (Semenenko, 2022). Immediately before the aggression, Russia had in the Black Sea 71 naval ships and 7 submarines at its disposal. (Boyse et al., p. 36) but by mid-2024, about 30% of the Russian fleet has been destroyed by the offensive actions of the Ukrainian armed forces, primarily through the use of unmanned multi-functional assets. (Boys, p. 65).

Given that the Russian armed forces at the time of aggression had a significant advantage at sea, air and land (with a special emphasis on armored mechanized forces, artillery-missile assets and electronic warfare systems), Ukraine had to adapt very quickly to new challenges. This adjustment was very effective considering the failure of Russian military operations to achieve their strategic goals (Akrap, Mandić, Rosanda Žigo, 2022). The fact that numerous members of the Ukrainian armed forces underwent high-quality training in the period from 2014-2022 also contributed to the quality of Ukrainian capacity for adaptation. It is especially necessary to emphasize that Ukraine's defensive, and later offensive, successes are also based on the connection and motivation of the private, state and academic sectors with the aim of developing new means, methods, techniques and technologies. Their goal is very clear: the defense of Ukrainian national sovereignty and identity on land, in the air, and on and under water. Also, as is the case with all attacked parties who are forced to defend themselves with what they have, they had focus on research and innovation as well.

Ukraine had developed

> *"...small-sized high-speed surface platforms with long-range and medium-range missiles on board, other sea platforms to replace the lost ones, as well as unmanned aircraft and underwater reconnaissance-strike complexes, the latest means of communication and complexes automation of force management, provision of intelligence information in real time."* (Yakymiak, 2023)

Thanks to these innovations, which integrated several different capabilities, the Ukrainians were able to successfully defend themselves at sea and forced the strengthened Russian Black Sea Fleet to retreat to safe ports located on the eastern side of the Black Sea, several hundred kilometers away from the front line. As a result, their operational power and ability to act is significantly reduced (Atlantic Council, 2024).

It is also necessary to acknowledge that Russia has supported a series of activities aimed at provoking high-intensity conflicts and even war in other areas that are in a state of constant low-intensity conflict. A typical example is the attack by Hamas on Israel, the Iranian attack on Israel, as well as the activities of the Yemeni Houthis in the Red Sea.

This is precisely the subject of our interest: the possibility of adapting existing capabilities and the use of such means and models by individual state and non-state factors in planning, supporting and carrying out terrorist attacks.

Ukraine, realizing all the advantages that the organized and integrated action of attack with unmanned drones has, has organized units at the level of specialist brigades fully dedicated to the planning and execution of attacks with these weapons systems. As well as their further development and subsequent use as factors that increase and multiplies the effects of other human organizations and weapon systems.

One of the important features of the war in Syria is also the widespread use of commercially available drones in the offense, intelligence collection, command and control, and reconnaissance. Terrorists quickly and effectively turned these cheap drones into means for committing offensive actions (Akrap, Kalinić, 2018). The threat posed by drones to key critical energy infrastructure has also long been recognized (Ranson, 2017).

Cases of Interest

Given these considerations, several cases are interesting because they provide examples of significant present and future security challenges.

1. Attacks on Kerch Bridge

The Kerch Bridge (or Crimean Bridge) has a length of about 19 km and consists of two parallel traffic structures. One is intended for road traffic and the other for rail traffic. The bridge connects Crimea with Russian territory and separates Azov from the Black Sea. It is important for the supply and movement of the Russian occupation forces located in the territory of Crimea as well as the occupied southern part of Ukraine. As a result, it was repeatedly the target of offensive operations by the Ukrainian armed forces with the aim of damaging it and possibly destroying it. Autonomous unmanned multi-functional vehicles, as well as vehicles filled with explosives, were most often used in the attacks (The Guardian, 2024).

2. Attack on Nord Stream 2 Gas Pipeline

Nord Stream 1 (NS1) and Nord Stream 2 (NS2) are two gas pipelines that connect Russia and Germany. They lie in Baltic Sea and have a length of 1234 km. On September 26, 2022, an explosion destroyed part of the NS2 pipeline near the island of Bornholm, effectively disabling the pipeline to the extent that it would not be functional again without serious repair. It is still not yet officially known who is responsible for this attack but the quantity of explosive devices used and the expertise required to conduct this kind of attack in deep water would be significant. However, on August 14, 2024, the German prosecutor's office filed charges against Ukrainian citizens whom it accuses of NS2 pipeline sabotage (CNN, 2024).

3. Demolition of Nova Kahkovka Dam

Assessing the current situation on the front line and the possibility that the Ukrainian armed forces would be able to liberate the occupied parts of Ukraine, on June 6, 2023 the Russian occupation forces decided to destroy the Nova Kahkovka dam, part of Kakhovka Hydroelectric Power Plant. The water wave flooded a large number of settlements downstream. A particular problem resulting from the attack was the large number of mines as well as other explosive devices that have changed their location under the onslaught of the water wave and are located in new and unknown places both downstream of the Dnieper River and in the Black Sea (BBC, 2023).

In the Croatian Homeland War of ?, the Croatian side faced similar threat. Although members of the occupying Yugoslav army and rebel Serbs placed explosives on the dam on Lake Peruča and detonated it, thanks to the actions a high-ranking British Army officer, the explosion did not completely destroy the dam, preventing a dangerous situation for tens of thousands of residents who live downstream of that dam. (Hrvatski Vojnik, 2021).

4. Attack on seaports in Ukraine, Crimea and Russia

Russia halted commercial maritime traffic by imposing a ban on the navigation of all ships, which directly affected the stoppage of the export of Ukrainian grain to third countries for which this grain is essential for the food supply of the population. The naval blockade is shown in Figure 1. (Semenenko, 2022).

Russia also threatened the communication and navigation systems of civilian ships located in the Black Sea area through its unauthorized electronic activity. At this time Russia carried out numerous powerful attacks on Ukrainian ports on the Black and Azov seas. In particular, cities Mariupol, Bednjansk, Skladovsk, Kherson, Mykolaiv and Odesa were targeted. Some of them were occupied by the Russian aggressor after heavy and devastating battles.

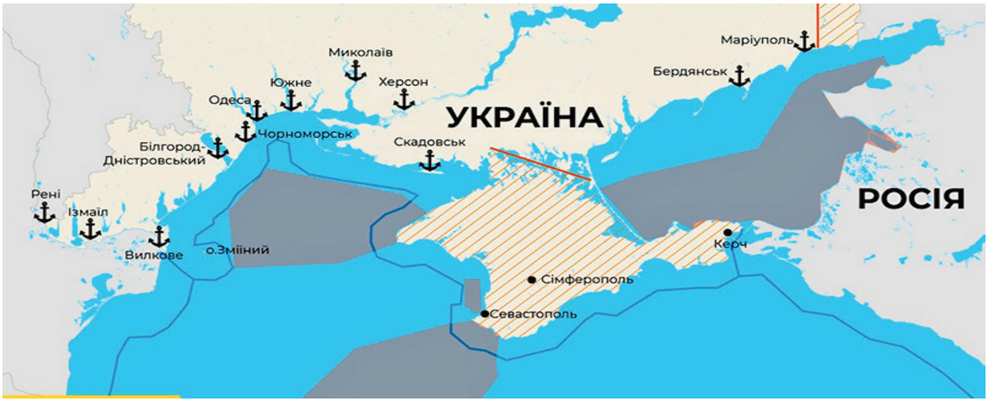

Figure 1: Russian Naval blockade at Black Sea (Semenenko, 2022)

In response, the Ukrainian armed forces developed systems that destroyed or damaged the Russian fleet in areas that were, according to the conventional Russian military way of thinking, beyond the reach of Ukrainian combat capabilities, including as the Russian command ship, the missile cruiser Moskva as shown on Figure 2 (Yakimiyak, 2023).

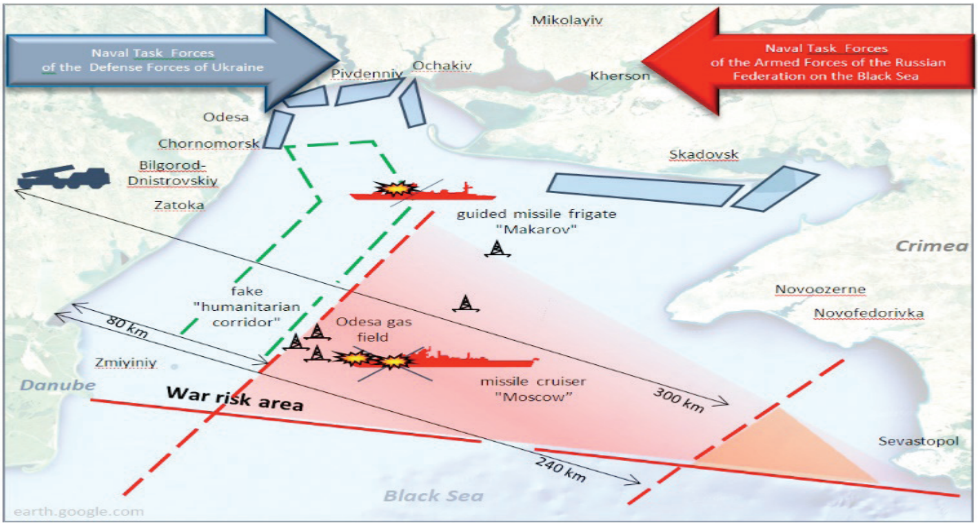

Figure 2: The sinking of the missile cruiser “Moscow” (Yakymiak, 2023)

The neglect of security measures and procedures on the Russian side, and the development of a system by which the Ukrainian armed forces brought their own combat assets to distant parts of the Black Sea where the Russian fleet was located, thereby destroying ports, ships, submarines and bridges, led to Ukraine, which has almost no navy, forcing the Russian Navy into a strategic retreat (Al Jazeera, 2024).

5. Gas and Oil Platforms in the Black Sea

At the beginning of the aggression against Ukraine, Russia occupied gas and oil platforms in the Black Sea that were owned by Ukraine. Russia also used these platforms to block navigation systems, as well as the places from which Russia launched various forms of attacks and threats against Ukraine. Therefore, Ukraine had to undertake offensive activities with the aim of liberating them (AL Jazeera, 2023), i.e. neutralizing the existence of threats (RFE/RL, 2024).

6. Ever Given Blacking of the Suez Canal

The Suez Canal was blocked for six days from 23 to 29 March 2021 by the Ever Given, a container ship that had run aground in the canal. Although this event is not directly related to the Russian aggression against Ukraine, it should be seen as a potential course of action that terrorists can mimic. Attacks on ships passing through sea routes such as narrow canals can have a dramatic impact on the world economy, on the cost to the end consumer, and on perceptions security and the effectivesness of institutions among many citizens. (NY Times, 2021).

7. Croatia LNG Terminal Case

Croatia decided to build Liquid Natural Gas terminal off the island of Krk in order to diversify supply routes and end gas dependence on Russia in 1995. During the process of planning and building up the terminal it was possible to notice intensive malign influence organized, conducted and financed by Russia and their assets. The Russian concept was to either take full control over this facility or to stop its construction. Russia used, wittingly or unwittingly, politicians and political groups, the local population, NGOs and persons with very strong business relations with the former Soviet Union and the present Russian Federation. The Croatian government realized this and, after intense activity, successfully finished building the floating LNG terminal on January 1, 2021 (NATO STO SAS 161, 2023). Then, on August 23rd, around twenty ‘activists’ endangered the working processes of LNG terminal by their illegal activities. Thirteen were arrested (13 of them) but police found that, mysteriously, no one had ID documents with them (HRT, 2024).

8. Pearl of Airisto Case in Finland

At the end of September 2018, Finnish authorities launched raids on properties connected with Russian citizen Pavel Melnikov who had bought a significant quantity of real estate in a coastal part of Finland, the Turku Archipelago (The Warzone, 2018). Melnikov's front company, Airiston Helmi bought several locations/islands next to strategic sea lanes. On those locations it was possible to build up Russian secret services base (The Warsaw Institute, 2018) for electronic warfare (EW) and signal intelligence (SIGINT) activities, and as potential location for Russian miliary units (The New York Times, 2018).

The above-mentioned examples have a direct connection with the preparation, planning and implementation of Russian attacks on Ukraine, as well as threats to the security and stability of other countries, show the modus operandi of Russian exploitation of the vulnerability of democracy in maritime domain.

Another key element which NATO should consider is international cooperation. An excellent example of this cooperation in the face of the Russian aggression against Ukraine, was the agreement between the three allies, Türkiye, Romania and Bulgaria, to countering mine warfare in the Black Sea (Defensenews, 2024).

Multifunctional Unmanned Systems

The hallmark of Ukrainian combat at sea, on the surface as well as below it, is innovation and the integration of various capabilities, which increase the overall effectiveness of all the means used. Drones have become multi-functional unmanned systems/platforms that can simultaneously or sequentially operate underwater surface or on the surface as a launch pad for various types of rockets and performing other tasks, from laying mines and explosives, collecting intelligence, electronic jamming/warfare, and the delivery of logistic support to military units. Ukraine, regardless of the fact that at the beginning of the second Russian aggression it was almost without its own navy, managed, as it seems now, to defeat the significantly superior Russian navy. This was primarily thanks to wisdom, courage, and innovation. It is precisely these innovations that are the subject of our interest because there is a genuine threat of terrorists exploiting this knowledge and experience to carry out terrorist attacks.

What should be learned is that these multi-functional unmanned platforms should be used rationally as an integral part of future mobile units with an area of action on land, air, water. They could have also very important scope of activities as a means of facilitating access to the digital space of adversary. It may be necessary to organize units that can be added to existing military formations (infantry, artillery, armor, navy, aviation, cyberspace) with the aim of increasing their basic efficiency and as a force efficiency multiplier. Such units would also be able to provide rapid and comprehenseive support also to counter-terrorist activities.

In order to be effective in the training of pilot-operators who operate those platforms, two necessary training should be included: analysis and study of counter-drones' platforms and solutions of an adversary, as well as combat against enemy drones in all domains of activity.

Terrorists, as well as others prone to violent acts, have shown that they are able to learn from experiences elsewhere and apply those lessons in planning and carrying out their own attacks. Therefore, the lessons which arise as a result of the second Russian aggression against Ukraine, are also available to those who have neither friendly nor constructive intentions. Our civilization still depends on the safety of water and water surfaces as one of only a few key critical infrastructures. The use of cheap, easily available, easy-to-use drones and their quick and efficient transformation into means for carrying out offensive and/or terrorist actions represents a serious challenge for all security organizations.

A special problem will also be posed by so-called homemade drones that will use a different frequency spectrum to communicate with the environment (pilot-operator, objects in area of activities) than commercially available drones. These drones will act as multi-functional platforms ready to carry out complex and different kind of multiple attacks or those with a delayed action: these are also convenient for terrorist activities.

Recommendations

It should also be noted that terrorists adapt their modus operandi and choose targets depending on the level and effectiveness of preventive and protective security and counter terrorist measures. It is noticeable that terrorists have shifted their focus from attacks on airplanes (which, like airports, have become extremely well-protected places), to large human gatherings which are difficult to protect completely, such as different forms of festivals (religious, musical, cultural, theatres) in open/closed areas that represent an easier target. Now, when they are planning their activities, terrorists are very often guided by the idea of how to achieve the maximum effect in the fastest way with the least possible casualties from their own side.

The experiences of recent and existing conflicts and wars indicates the following needs:

1. To encourage Research & Innovation activities of the private, state, public and academic sectors in the development of new technologies and means with the aim of detection and mitigating existing and future multi-functional unmanned platforms. That is especially relevant to the development of defense systems in the domain of electronic warfare, because unmanned platforms must use different types of receivers/senders to communicate with their environment and even with remote pilot-operators unless the systems are not autonomous.
2. To establish a communication channel with a full exchange of information and knowledge with colleagues from Ukraine in order to understand the advantages and disadvantages of using unmanned platforms.
3. The protection of harbors and piers is extremely important because, especially during the tourist season, a large number of people and vehicles of various types and sizes are gathered in them. A terrorist attack in such a location could lead to numerous casualties, possibly from many different countries and causing significant political and social disturbance.

4. The protection of underwater key critical infrastructure shows serious deficiencies. Therefore, it is necessary to protect this infrastructure with systems for the detection and recognition of objects (living and non-living) that approach them and the quick and uninterrupted sending of warning signals to the nearest monitoring center in order to for the threat to be mitigated.
5. Offshore platforms, especially those that are active but unmanned, must have the highest level of protection (physical, technical, technological, electronic), with simultaneous and reliable connection to the nearest defense system that can send help in case of need.
6. It is necessary to work on the organization of special combat units that will manage unmanned platforms and as such will be attached to conventional combat units to support their operations: from the processing of data and intelligence collection, management of the battlefield, all the way to direct offensive action. These units should also work on systems to combat adversary unmanned platforms in order to enhance the defensive efforts of their own systems and improve their own offensive capabilities by reducing their vulnerabilities during peacetime, together with responsive civilian institutions.
7. It is necessary to work on strengthening NATO preventive capabilities primarily in the domain of cooperation between national intelligence communities and policing organizations, strengthening cooperation with the media, with specialized and expert organizations close to NATO and the EU (Jacobs and Samaan, 2015, pp. 288-289) and all stakeholders engaged with the concept of homeland security.

References

Akrap, G., i Kalinić, P. (2018). ‘Bezposadne letjelice i terorizam’, *National Security and the Future*, 19(1-2), str. 213-219. Preuzeto s: https://hrcak.srce.hr/206497 (Datum pristupa: 13.08.2024.)

Akrap, G., Mandić, I., & Rosanda Žigo, I. (2022). ‘Information Supremacy, Strategic Intelligence, and Russian Aggression against Ukraine in 2022’. *International Journal of Intelligence and CounterIntelligence*, *36*(4), 1254–1277. https://doi.org/10.1080/08850607.2022.2117577

Al Jazeera (July 3, 2024) Ukrainian maritime attack on Black Sea port Novorossiysk repelled: Russia, 15.07.24, https://www.aljazeera.com/news/2024/7/3/ukrainian-maritime-attack-on-black-sea-port-novorossiysk-repelled-russia

Al Jazeera (September 12, 2023) Ukraine says Black Sea gas, oil platforms recaptured from Russian control, 26.7.24, https://www.aljazeera.com/news/2023/9/12/ukraine-says-black-sea-gas-and-oil-platforms-recaptured-from-russia-control

Atlantic Council, by Peter Dickinson (July 16, 2024): Russia’s retreat from Crimea makes a mockery of the West’s escalation fears, https://www.atlanticcouncil.org/blogs/ukrainealert/russias-retreat-from-crimea-makes-a-mockery-of-the-wests-escalation-fears/

BBC, by the Visual Journalism & BBC Verify Teams (June 8, 2023): Ukraine dam: Maps and before and after images reveal scale of disaster, 20.07.24, https://www.bbc.com/news/world-europe-65836103

BBC. By Laura Gozzi (July 23, 2024): Ukrainian attack on ferry kills one in Russian port, 26.07.24, https://www.bbc.com/news/chapters/cgrldn8d65wo

Boyse, M., Scutaru, G., Colibasano, A., Samus, Mykhailo. (2024). The Battle for the Black Sea Is Not Over. New Strategy Center & Hudson Institute, Bucharest, Washington D.C.

CNN World, By Rob Picheta (August 14, 2024): Ukrainian man wanted over Nord Stream pipelines explosions, 22.08.24, https://edition.cnn.com/2024/08/14/europe/nord-stream-explosions-suspect-arrest-warrant-germany-intl/index.html

DefenseNews by Cem Devrim Yaylali (December 1, 2024): Three NATO allies activate Black Sea task force, Jul 2. 2024, https://www.defensenews.com/naval/2024/07/02/three-nato-allies-activate-black-sea-task-force/

HRT vijesti, (August 23, 2024): Aktivisti prosvjedovali ispred LNG terminala, 13 ih je uhićeno [Activists Protested in Front of the LNG Terminal – 13 of them were Arrested], 25.08.24, https://vijesti.hrt.hr/hrvatska/prosvjed-aktivista-ispred-lng-terminala-uhiceno-12-prosvjednika-11721202

Hrvatski vojnik, by Vesna Pintarić (February 4, 2021) The Royal Marine who helped save the Peruća Dam, 26.08.24, https://hrvatski-vojnik.hr/108683-2/

Jacobs, A., Samaan, J-L. (2015) 'Player at the Sidelines: NATO and the Fight against ISIL' (pp: 277-294*)*, in *NATO's Response to Hybrid Threats,* ed. By Guillaume Lasconjarias and Jeffrey A. Larsen, NATO Defense College, Forum Paper 24

Prodan, T. (2017). 'Maritime terrorism and resilience of maritime critical infrastructures', *National Security and the Future*, 18(1-2), pp. 101-122., 14.08.24, https://hrcak.srce.hr/189671

Ranson, A. (2017). 'The 2014 UAV threat to French nuclear power plants', *National Security and the Future*, 18(1-2), pp. 125-142., 14.08.24, https://hrcak.srce.hr/189675

RFE/RL by RFE/RL's Ukrainian Service (August 10, 2024): Ukrainian Forces Attack Black Sea Gas Platform Used By Russia For GPS 'Spoofing,' Navy Says, 21.08.24, https://www.rferl.org/a/ukraine-russia-war-platform-black-sea-attack-pletenchuk/33073780.html

Semenenko, C.V. and Ivashenko, C.A. (2022). 'Russia's Total War: A Challenge and a Threat to Europe'. *National security and the future*, 23 (2), 53-87. https://doi.org/10.37458/nstf.23.2.2

The Guardian, by Luke Harding (April 4, 2024) 'No choice': Ukraine eyes Kerch bridge in Crimea for drone attack. 23.08.24, https://www.theguardian.com/world/2024/apr/03/ukraine-eyes-kerch-bridge-crimea-drone-attack

The NATO STO SAS-161 Research Task Group (RTG) – Military Aspects of Countering Hybrid Warfare: Experiences, Lessons, Best Practices Volume V: Military Implications, (October 18, 2023), 22.08.24, https://zagrebsecurityforum.com/analysis/id/4381

The New York Times, by Andrew Higgins (October 31, 2018): On a Tiny Finnish Island, a Helipad, 9 Piers — and the Russian Military?, 23.08.24, https://www.nytimes.com/2018/10/31/world/europe/sakkiluoto-finland-russian-military.html

The New York Times, by Vivian Yee and James Glanz (July 19-21, 2021): How One of the World's Biggest Ships Jammed the Suez Canal*,* 24.08.24, https://www.nytimes.com/2021/07/17/world/middleeast/suez-canal-stuck-ship-ever-given.html

The Warzone, by Jospeh Trevithick (November 1, 2018). Rumors of Covert Russian Ops Swirl After Finland's Police Raid Bond-Esque Private Island, 23.08.24, https://www.twz.com/24616/rumors-of-covert-russian-ops-swirl-after-finlands-police-raid-bond-esque-private-island

Warsaw Institute: BALTIC MONITOR, (September 26, 2018): The Finnish secret services operation in the Turku Archipelago, 23.08.24, https://warsawinstitute.org/finnish-secret-services-operation-turku-archipelago/

Yakymiak, S. (2023). 'Hybrid and war Actions of the Russian federation at Sea: Lessons Learned, Cooperative Countering and Prospectives'. *National security and the future*, 24 (1), pp.67-81.,22.08.24, https://doi.org/10.37458/nstf.24.1.7

CHAPTER 5

WAGNER GROUP, DAESH, AND OTHER HYBRID ACTORS: TERRORIST STRATEGIES AND TACTICS

Prof. Dr. Stefan Goertz[*]

1. Hybrid Actors, Strategies and Tactics in the 21st Century

Frank Hoffman first introduced the concept of ‘hybrid warfare’ in 2007 during the Western Counterinsurgency-campaigns in Afghanistan and Iraq as a type of war, in which many methods and means of war are being used simultaneously in a way best suiting the current circumstances. It is therefore now meaningless, or only academic, to classify wars as large/small wars or regular/irregular wars. Hoffman explained in 2007 that in the future, conventional forces (regular forces), irregular warfare, terrorist groups and organised crime organisations would be present within the same operational area concurrently, using asymmetrical, hybrid tactics and means.

Giray Sadik explained in 2020, that “as hybrid threats to international security have evolved, their analysis in scholarly and policy debates have become a source of on-going confusion” (Sadik, 2020: 73). Consequently, this chapter is not an academic debate about different definitions and concepts of hybrid threats to international security, but will analyze instead various current hybrid actors on different levels in order to let the analysis become a first step of lessons learned for NATO and EU.

The twenty first century, with the terrorist attacks on 9/11, first brought two decades of small wars between state and non-state actors, the Western counter-insurgency campaigns in Afghanistan and Iraq and the US-“war on terror“ against non-state actors in the MENA-region. The major non-state opponents were the terrorist organisations, Al Qaeda and DAESH, which were and are hybrid terrorist actors.

With the illegal annexation of the Crimea by Russia in 2014 other hybrid actors appeared, specifically the ‘Wagner Group and the ‘little green men’, active Russian soldiers in uniforms but without insignia.

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

This chapter on the one hand describes the strategy and tactics of the Wagner Group as, in the beginning at least, a clandestine, hybrid actor of Russian military politics, operating in Russian shadow wars in Crimea, Syria and African countries. On the other hand the strategy and tactics of the terrorist organisations al Qaeda and DAESH are examined, hybrid terrorist actors who used and are still using terror tactics, war crimes, torture and (organised) crime. Hybrid actors and hybrid warfare can be used by non-state actors and state actors alike to pose a threat NATO and EU-countries.

2. The Actors

2.1. The Wagner Group

Until its official dissolution as Private Military Company in June 2023, the Russian Wagner Group was Putin's shadow army, a paramilitary organisation, part of a corporate network around the oligarch Yevgeny Prigozhin, who was considered a close confidant of Russian President Putin until he allegedly planned a coup against the Russian military leadership at the end of June 2023. Wagner mercenaries were involved in the annexation of Crimea in 2014 in violation of international law but had been active in Ukraine since autumn/winter 2021 at the latest in preparation for the current Russian war of aggression against Ukraine, at the beginning of the war in Kiev and in subsequent battles, often sustaining heavy losses.

The Wagner Group (Russian: Группа Вагнера, Gruppa Wagnera), also known as PMC Wagner, ChVK Wagner or CHVK Vagner, parts of which were also called 'Task Force Rusich', was a Russian Private Military Company that was labelled Putin's shadow army. A PMC called Wagner Group was never officially registered (no entry in the Russian commercial register). The Wagner Group was a network of dozens of interwoven companies behind the Wagner brand. In Russia, private military companies are not officially permitted by law, but de facto they were and are paramilitary contract forces, hybrid actors of Russian military politics.

But the Wagner Group more likely was a Private Military Company until the preparation of the current Russian war of aggression (autumn/winter of 2021) and was credited with numerous mercenary missions as part of covert operations in Ukraine, Syria and various African countries, including Mali. Covert operations as means of hybrid Russian military politics have been conducted in Sudan, where Wagner supported the former dictator Omar Al Bashir, in the Central African Republic it supported President Faustin-Archange Touadéra, and in Mozambique the government briefly hired the Wagner Group to fight extremist groups.

The Wagner Group was more than a 'private military company, it was hybrid. Even in 2018, being part of a private military company did not necessarily mean that such companies operated independently of the Russian state. The Wagner Group, for example, was not a classic mercenary company that simply offered its services to the highest bidder. A striking feature of the Wagner Group was its proximity to the Russian military: Its training ground was located on a GRU military intelligence site in Southern Russia and its operations were part of the Russian interventions in Ukraine and Syria (Goertz, 2022).

Until the war of aggression against Ukraine in 2022, the Russian government tried to cover up its direct involvement in the war in Donbass. Shortly after the fall of Yanukovych, Ukraine's new pro-Western government was confronted with a Russian military invasion and the annexation of Crimea. In April 2014, according to Kremlin-propaganda 'pro-Russian separatists' occupied administrative buildings in several cities in eastern Ukraine, in the Donetsk and Luhansk districts. Russian fighters were then deployed in Crimea and eastern Ukraine, who wore no national insignia and were referred to as "little green men" (Pifer, 2014). The "little green men" had been efficiently and discreetly supporting the pro-Russian forces within Ukraine since 2014 and as a hybrid actor were a means of clandestine Russian military politics until 2022, when Wagner Group played a central and overt role in the Russian-Ukraine war.

2.2. DAESH and Other Terrorist Organisations

International terrorism is one of the greatest threats to security worldwide. Since 9/11 the interaction, cooperation and in some cases even fusion of terrorism and transnational organised crime has become a new and hybrid threat for Western-states as well as for states in the MENA-region.

New terrorism, the international extremism of the twenty-first century, poses an asymmetric threat to Western democracies. It neither recognises national nor international boundaries and blurs the frontiers between offensive and defensive tactics, war and peace, domestic security and foreign policy as well as organized crime.

In the period from 2014 to 2015, DAESH-affiliated terrorist organizations controlled territory in parts of Syria and Iraq the size of Great Britain and were present in nine other states: Syria, Iraq, Libya, Afghanistan, Pakistan, Egypt, Yemen, Saudi Arabia and West Africa. In just one country, Pakistan, 33 different Salafi-Radicalist organisations were detected in the year 2017. Since the summer of 2011, more than 100 Salafi-Radicalist organisations, groups, brigades and units have been fighting in Syria.

New terrorism, the international terrorism, its actors, strategies and tactics cannot be strictly separated in established categories like terrorism, guerilla warfare, small war, insurgency and revolutionary warfare, because it was operating and still is operating in all these categories at the same time, but with differing degrees of intensity (Goertz/Streitparth, 2019: 1).

Afghanistan once again sees conspicuous activity by militant groups in terms of presence, attacks carried out and recruitment. The Islamic State Khorasan Province (ISKP) and al Qaeda are both active in Afghanistan. On the other hand, foreign terrorist groups, including Jaish-e-Mohammad ('the Army of Mohammad') and Lashkar-e-Tayba ('the Army of the Good'), maintained only a limited presence in Afghanistan. The largest externally focused terrorist group in Afghanistan is Tehreek-e-Taliban Pakistan (TTP, 'Taliban Movement Pakistan'), that increased its attacks against Pakistan in 2022 (EUROPOL, 2023: 41).

Despite the major difficulties the ISKP faced after the Taliban returned to power in August 2021, ISKP has demonstrated great resilience. Tactically it has focused on attacks in the cities, partly to spare its forces. Parallel to that it invested massively in propaganda, which helped it convey an image of much greater strength than it actually had.

In 2022, ISKP increased its attacks across Afghanistan, tactically mainly targeting Taliban leaders, as well as soft targets such as the Shia and Sikh communities, as well as the broader civilian population. In addition to carrying out operations in the group's traditional bases in Nangarhar and in Kabul, ISKP expanded its activities to Kandahar and parts of the Afghan north where it was previously less present prior to the Taliban takeover in August 2021 (EUROPOL, 2023: 41).

The strategy of ISKP in Afghanistan is more than just terror tactics, it is hybrid. On the one hand terror attacks as constant component of their strategy. On the other hand, ISKP's strategic goal is to establish governance structures. So in Afghanistan in the last few years ISKP divided the territory where it operates into provinces. The IS-governor is called *wali* and under him operate various *amirs* (Giustozzi, 2022: 94). The sub-provincial *amirs* have a primarily military role. The sub-provinces of DAESH in Afghanistan are Farah, Zabul, Ghazni, Logar, Nangarhar, Kunar, Bagdis, Kunduz, Badakshan, Parwan, Minroz, South Waziristan, North Waziristan, Kurram, Kyber and others (Giustozzi, 2022: 94-95).

To finance its military and political activities is paramount to the ISKP. ISKP-Finance Commission is in charge of fundraising from businessmen, mosques and government entities. In 2015 ISKP invested significant resources in the development of an intelligence apparatus and had approximately 500 members. This apparatus had the task of infiltrating the Afghan security apparatus. The top military structure of the ISKP is the Military Shura or Council, composed of 25 to 40 members. In the Military Council there are sector commanders, responsible for so-called 'battalions' of 150-200 fighters (Giustozzi, 2022: 106). The Council also includes a general staff, a commander of 'special commandos' and suicide groups.

The civil war in Afghanistan, that lasted from 2001 to August 2021, created a professional military class of fighters, insurgents with different fighting skills and technological skills. Afghanistan seems to promise a never-ending conflict or civil war, so consequently there will always be recruitment possibilities for Salafi-Radicalist and international terrorists. Overpopulation in the rural areas of Afghanistan and the tribal areas of neighboring Pakistan have been generating and will generate huge numbers of poor young men, who are looking for a 'task' and basics.

Since mid-2014, al Qaeda and its associated regional affiliates have been in direct competition with DAESH and its networks. The previous supremacy of al Qaeda within international terrorism has been permanently undermined by DAESH and its military and propaganda successes. Nevertheless, al-Qaeda continues to see itself as the vanguard of its community and continues to call for attacks against Western targets. However, the claim and reality are far apart (Bundesamt für Verfassungsschutz, 2024: 119).

It is difficult to estimate the size of the global personal potential of al Qaeda supporters. Despite the loss of personnel, al Qaeda has so far proven its resilience and has repeatedly adapted to changing conditions. Accordingly, Al-Qaeda's tactics have also changed over the years: Although large-scale attacks with a long planning time are still desired, a more 'pragmatic' approach has now prevailed in practice. According to this approach, the West is to be attacked primarily by 'inspired' individual perpetrators and small groups of attackers. These are encouraged to plan and carry out politically-motivated offences on their own initiative. A formal connection to or tactical coordination with al Qaeda is no longer fundamentally necessary for this. Rather, the decisive factor is that the offence itself (or its preparation) takes place in accordance with the guiding principle propagated by al Qaeda. Above all, this 'pinprick tactic' is intended to maintain a permanent presence of threat.

3. Their Strategies and Tactics

3.1. The Wagner Group

Wagner fighters supported Syria's dictator Bashar Al Assad as ground troops, while Russia officially only provided air support. In the Libyan civil war, Wagner mercenaries intervened on the side of the renegade General Khalifa Haftar, who was closely networked with Russia. In the Central African Republic, Mozambique and, since 2021, Mali, the Wagner Group acts as a training unit for the local armed forces.

There were – and are – presumably dozens of countries worldwide in which Wagner troops were active. It was driven by the interests of the Russian government or Russian state-affiliated companies. For example, the Wagner Group became active when Venezuela's head of state, Nicolás Maduro, came under pressure and the Russian oil company Rosneft feared for its investments.

The Wagner Group's involvement in Syria vividly illustrated how its business operating model worked. The energy company EvroPolis, which was part of the Wagner Group, concluded a contract with the Syrian state-owned General Petroleum Corp. This contract stipulated that EvroPolis would receive a quarter of the oil and gas production in the areas that Wagner fighters liberated from DAESH.

In mid-January 2022, US media also discovered images on Instagram that had been circulated by Wagner mercenaries Members of the 'Rusich' force, which had already been deployed in eastern Ukraine in 2014, had already published images in October 2021 showing them conducting reconnaissance near Kharkiv, Ukraine's second largest city (Goertz, 2022b: 72).

According to the British newspaper 'The Times' dated February 28, 2022, around 400 mercenaries of the Wagner Group had been in Kiev since the end of January 2022 to attack around 20 high-ranking politicians, including the Ukrainian President Volodymyr Zelenskyi and the Mayor of Kiev, Vitali Klitschko (The Times, 2022). On April 28, 2022, Time Magazine reported at least three foiled attempts by mercenaries from the Wagner Group and forces of the Chechen President, Ramzan Kadyrov, to assassinate the Ukrainian President Vlodimir Zelenskyi (Time, 2022).

There are are reports on the Russian breakthrough near Popasna at the end of May 2022 which state that a mixture of airborne troops, marines from the Baltic and Pacific fleets, infantrymen from the Far East and forces of the Wagner Group fought there. A few days after the start of the war in Ukraine, it was reported internationally that the Wagner Group was also recruiting fighters in Syria at the time for the rural and urban warfare with likely heavy losses, offering wages of up to 3,000 US dollars per month (Goertz, 2022b: 73).

According to the British intelligence services, the Wagner Group probably achieved ‘important tactical territorial gains’ in the Donbass at the end of July 2022. The mercenaries had advanced in the vicinity of the Vuhlehirska coal-fired power plant in eastern Ukraine and the nearby village of Novoluhanske, the British Ministry of Defence announced on Twitter on 27 July 2022. As a result, some Ukrainian troops in the area then withdrew. (Goertz, 2022b: 74).

3.2 DAESH and Other Terrorist Organisations

The international conflict between al Qaeda, DAESH and other terrorist organisations as non-state actors and governmental actors, like Western democracies or countries of the MENA-region is characterised by the principle of asymmetry. This asymmetry affects the interaction between international terrorist organisations and countries on various levels. On the one hand, for example, non-governmental irregular forces of extremist organisations break the international law by using tactical capabilities like terrorist attacks, crimes against the civilian population. On the other hand, they wear no uniforms or insignia so they cannot be identified as combatants. In these asymmetric conflicts, non-state actors and irregular forces without combatant status operate beyond traditional rules of war, and the borders between war, terrorism and organised crime become blurred.

Due to organisational and financial disadvantages, a terrorist organisation aims at destabilising a political system and at questioning the legitimacy of a government. This terrorist objective w usually regionally limited. As terrorist organisations are definitely weaker than Western countries when it comes to organisational, technica, and financial realms, it uses asymmetric tactics when attacking the liberal political order of Western countries. Extremist groups use the logic of terrorism as a strategic means in order to spread fear of terrorist attacks among the civilian population, thereby questioning the democratic states’ monopoly on the use of force.

At the present time, and for the foreseeable future, there are two main terrorist scenarios threatening the Western world: on the one hand, the threat of large-scale attacks and multiple tactical scenarios by international terrorist organisations, such as DAESH and al Qaeda, and, on the other hand, low-level attacks by ‘inspired’ lone actors.

Large-scale attacks and multiple tactical scenarios by international extremist organisations are planned and conducted pursuant to the hierarchical top-down principle, exemplified by the Mumbai, Paris, Brussels, Barcelona style of attacks. This kind of large attack is operated by hit teams with or without paramilitary training and/or combat experience. Due to their simultaneous or nature, such attacks pose a considerable challenge for security forces and rescue services in Western countries and countries of the MENA-region.

4. Recruitment

4.1 The Wagner Group

The Wagner Group in Eastern Ukraine model of operating went worldwide after 2014. It developed into a Russian strategy, a hybrid actor of Russian security and military policy. Clandestine, without laying direct tracks to Russian armed forces or taking the risk of Russian soldiers being killed. Before the current Russia-Ukraine war, the Wagner Group said to have had 10,000 fighters, growing to over 50.000 men during the Russia-Ukraine war, primarily through the recruitment of detainees from Russian prisons.

Until the current Russian war against Ukraine, Wagner mercenaries were mainly recruited from Russians who no longer had a military career ahead of them. They were said to receive around 3,000 to 4,000 euros a month in pay.

According to its own information, the Ukrainian secret service, the SBU, identified the names of more than 2,000 people who had fought for the Wagner Group on Ukrainian territory. Former soldiers, police officers, extremists and men from the criminal milieu operated for the Wagner Group in eastern Ukraine and committed war crimes there. The majority of the Wagner mercenaries are said to have come from Russia, some from Ukraine, as well as in Moldova, Serbia, Armenia and Bosnia (Goertz, 2022b: 68).

According to British intelligence services in mid-July 2022, the Russian armed forces in Ukraine were increasingly short of personnel and mercenaries from the Wagner Group were increasingly filling the gaps (Goertz, 2022b: 75). At the same time, however, the British intelligence services also assumed that the Wagner Group had suffered heavy losses, which in turn led to lower standards in the recruitment of new fighters, including convicted criminals and previously rejected applicants. These new recruits were then trained less thoroughly, which reduced the combat value of the Wagner Group in the war against Ukraine. In the summer of 2022, videos of the Wagner Group's recruitment efforts in prisons were repeatedly circulated on social media. The fact that Wagner mercenaries were used for attrition battles in hot spots documented the difficult personnel situation of the Russian armed forces.

British intelligence services also indicated that the Russian military leadership transferred responsibility for some front sections in eastern Ukraine to Wagner Group at the end of July 2022. This was an indication that the Russian armed forces were facing a major shortage of infantry soldiers, the British Ministry of Defence explained at the end of July 2022. This decision by the Russian military leadership was a significant change from the previous operations of Wagner Group, as it had previously been primarily involved in operations that differed from the large-scale operations of the regular Russian armed forces (news@orf.at 2022).

4.2 DAESH and OtherTterrorist Organisations

Recruitment continues to take place both online and through gatherings in informal religious buildings, as well as in correctional facilities. According to EUROPOL the Salafi-radicalist movement in Europe is fragmented. Consequently, radicalist groups or cells coexist with individuals acting on their own or as part of fluid cells. These groups and cells see themselves as parts of various national and transnational terrorist networks, both online and offline (EUROPOL, 2023: 29). Extremists involved in the planning of terror attacks frequently combine concrete tactical preparation activities with an extensive use of terrorist online platforms. At the strategic level Salafi-radicalists appeal to members of groups on social media platforms and instant messaging channels to pursue terrorist attacks, to pledge allegiance to terrorist organisations and, in some cases, they announced their intent to commit a terrorist attack. According to EUROPOL, at the level of nation states, Salafi-radicalist groups are progressively multi-ethnic, while links at regional levels are frequently based on the members' common language. For example, Salafi-radicalist in Germany and Austria often share contacts and propaganda content with German-speaking peers (EUROPOL, 2023: 29).

The loosely structured extremist groups, where in many cases there are no clear differences between non-militant or militant, typically lack formal hierarchies among the members. EUROPOL points out, that in the majority of cases the Salafi-radicalist groups are based locally, from time to time with a wider geographic scope, with members living in several European states (EUROPOL, 2023: 29).

According to EUROPOL the release of radicalised individuals from prisons in Europe remain a concern for European States as they can continue actions of proselytism outside prisons and become actively involved in the preparation of terrorist attacks.

Individuals in prisons under observation for violent extremist views include both prisoners convicted of terrorism-related offences and prisoners convicted of criminal offences who became radicalised in prison. Apart from the radicalisation and recruitment of other prisoners, the threat of radicalised individuals can also materialise in the form of attacks on other prisoners and prison staff.

5. Terrorism, Terror Tactics, War Crimes, Atrocities

5.1. Wagner Group

In 2019, two former Wagner mercenaries told the BBC that "prisoners are sometimes executed" so that "no extra mouths have to be fed". At the end of 2019, a clip circulated on Russian social networks, which was investigated in a report by Frontline Forensics, an initiative run by Arizona State University. The video, which according to Frontline Forensics was first posted on the Reddit platform in 2017, shows the brutal murder of a man named Muhammad Taha Al Abdullah in Syria (The Moscow Times 2019). Several Russian-speaking men torture Abdullah with a sledgehammer before beheading him. They then dismember the body and set it on fire. They subsequently take photos of the remains. The murder of Al

Abdullah, known by his nickname Hamdi Bouta, took place on the site of a Syrian gas field called Al Shaer, which was controlled by a subgroup of the Wagner Group called EvroPolis, according to Frontline Forensics' analysis. EvroPolis, like other sub-companies of the Wagner Group, was working on behalf of the Russian gas company Stroytransgaz at the time of the crime. According to documents obtained by Frontline Forensics, Wagner mercenaries were tasked with protecting the gas plant where Abdullah was brutally tortured and executed. By analysing the video and comparing it with known accounts of members of the Wagner Group on social media, the authors of the report, like the British Guardian newspaper before them, came to the conclusion that Abdullah was murdered by mercenaries from the Wagner Group.

Then, at the end of April 2022, international sources reported major losses by the Wagner Group in Ukraine, with around 3,000 mercenaries reported killed. A former member of the Wagner Group told the investigative research network Bellingcat, whose managing director, Christo Grozev, told the Foreign Affairs Committee of the British House of Commons that some Wagner mercenaries fought for the "fun of killing". The proportion of these members was around 10 to 15%: "They are murderous, they are not just adrenaline junkies" (Stern, 2022).

Sean McFate, a professor at the US National Defence University, explained that the brutality of Wagner Group was "part of their selling point" [...] "If you look at Butscha and others, you see the same pattern as in Syria, where they interrogate, torture and behead people," he said. "One reason I think this has become one of Putin's favoured weapons is that it allows plausible deniability between the excesses on the ground, the failures on the ground and the policy." According to McFate, Western states have not taken the threat posed by the Wagner Group seriously enough so far and have not tracked the movements of its members (Stern, 2022).

5.2. DAESH

Since the proclamation of the so called 'DAESH Caliphate' in June 2014, the public presentation of excessive and sadistic 'innovative' violence quickly developed to a medially transported trademark of DAESH. Most of DAESH propaganda videos show uncensored and almost inconceivable brutality. This very archaic brutality in the guise of modern aesthetics appeals to adolescent target groups. The spectrum of published DAESH violence ranges from mutilation of human bodies (e.g. ears, lips, genitals), being driven over with tanks, stoning, drowning and burning with flamethrowers or slower with methylated spirit poured over clothes to decapitation videos and deliberately dehumanizing presentation of the enemy's mutilated bodies. This glorification of practiced and published violence presents an alternative concept to Western democracies with humanist norms, against which IS fights on various terrorist levels—here on the level of psychological warfare (Goertz, 2017: 348-352).

The terrorist logic of spreading fear and horror among the civilian population was taken to a new and up till now unknown level, because DAESH let its child soldiers execute adversaries and published clips of it worldwide from the scene. DAESH video 'The Nations

Will Gather Against You', released on August 26, 2016, showed the execution of at least 14 Kurds and no less than 5 of them being executed by children of DAESH fighters. The Intelligence Group website identified British, Tunisian, Egyptian and Uzbek citizens in the video (Prince, 2016).

Target groups for this tactic of psychological warfare are extremist groups and sympathisers, on the one hand, and "the" (perceived) adversary, civilian population and journalists on the other hand. The excessive and stylized violence in DAESH execution videos follow the principle of "kill one - frighten ten thousand" and aims to manipulate a global audience in social media. In order to reach the largest possible audience, new terrorism uses aesthetically stylised archaic violenc, especially on social media platforms.

In the 24 months after the proclamation of the Caliphate in June 2014, the terrorist organisation executed at least 4000 people and recorded the executions on video. In 2015 alone, DAESH issued video clips showing the killings of more than 1000 captives. During the first 18 months of its occupation of Syrian territory, DAESH brutally executed more than 2000 Syrian civilians, who were clearly not combatants (Syrian Observatory for Human Rights, 2015).

On a strategic level, these execution videos are a means of securing the attention of modern mass media in order to exploit their multiplicator function for DAESH propaganda and justify the executions on a 'religious' (extremist) basis as examples for Sharia law. Additionally, these published execution videos demonstrate the terrorist power DAESH has to decide on life or brutal, slow and agonizing death in order to deter and intimidate (perceived) adversaries. Execution videos are also intended to satisfy DAESH members' and supporters' desire for revenge.

6. Summary and Lessons Learned

This chapter has shown that hybrid actors – non-state actors such as terrorist organisations or state-influenced actors such as the "PMC" Wagner Group and numerous other Russian PMCs – as well as strategies and tactics are shaping the conflicts and wars of the 21st century.

Until its coup attempt in June 2023, the Wagner Group was the most important player in Russia's hybrid military policy. After the death of Yevgeny Prigozhin and his deputies, the Wagner Group was subordinated to the Russian National Guard and the Russian armed forces. The current Russian PMCs are Private Military Medical Company, Berkut, Zvezda, Redut, Moran, Mar, Yastreb, Patriot, Vega Strategic Services, Konvoy, RSB Group and E.N.O.T.. The civilian and military intelligence services of NATO and EU- states must therefore gather and exchange more intelligence on the activities of these Russian PMCs – as well as their connection to the Russian armed forces and intelligence services.

NATO and the EU must recognise that the vast majority of Russian PMCs are different from Western PMCs. They are not at the disposal of the public market, but primarily or exclusively perform tasks for the Russian government, Russia-friendly states and Russian companies.

Sanctions against offences committed by Russian PMCs should be better developed and applied in a more coordinated manner by NATO and EU.

International terrorism continues to threaten the human security of numerous MENA states. Added to this is the threat of terror attacks against member states of the NATO and EU. Both politicians and the armed forces and intelligence services of NATO and EU must recognise and implement the fact that international terrorism cooperates with transnational organised crime and therefore combat the financing of terrorism more effectively.

The intelligence capabilities of NATO and EU should be improved, both in terms of human intelligence capabilities and SIGINT with regard to digital terrorist data. Digital terrorist knowledge has been spread for many years, both on the www and on the darknet. The SIGINT-capabilities of NATO and EU states have to be improved.

Afghanistan was a safe haven for Al-Qaeda in the 1990s, various terror attacks against the USA (the East African Embassy bombings in Nairobi, Kenya and Dar es Salaam, Tanzania on August 7, 1998, plane attacks against New York and Washington on September 11 2001) were planned and initiated there. Today, the ISKP has its base in Afghanistan, Pakistan and other neighbouring countries and the attack against the Crocus City Hall near Moscow in 2024 has shown that the ISKP can and will now also carry out attacks in Europe.

Returning foreign fighters represent a current and future challenge for NATO and EU and the exchange of information between the authorities involved (intelligence and police) should be improved. Some returning foreign fighters are currently in prison. Various attacks by lone actors who were previously in prison deradicalisation programmes (for example the lone actors attacks in Vienna and Dresden attack in the 2020s) show that both the quality of deradicalisation programmes and the state's influence on these programmes, which are often run by NGOs, should be improved.

Strengthening the border security of NATO and EU is currently just as important as protective measures for critical infrastructure. For hybrid actors, both non-state and state-influenced, critical infrastructures are important high-profile targets.

To conclude: When analysing and combating hybrid threats and hybrid actors, it is also important to review your own mindset as quickly and thoroughly as possible. It is not about categorising academically what a hybrid actor is. It should be about recognising hybrid threats, improving awareness capabilities and developing strategies against hybrid threats as well as monitoring and combating hybrid threats and actors.

References

Bundesamt für Verfassungsschutz (2024). Kompendium 2024. Köln/Berlin.

EUROPOL (2023). TE-SAT, European Union Terrorism Situation and Trend Report 2023, Den Haag.

Giustozzi, A. (2022): The Islamic State in Khorasan, 2nd edition. London.

Goertz, S. (2022a). Die „Gruppe Wagner“ – Putins Söldner im Ukrainekrieg, https://www.reservistenverband.de/magazin-loyal/die-gruppe-wagner-putins-soeldner-im-ukrainekrieg-2/

Goertz, S. (2022b). Der Krieg in der Ukraine und die Folgen für Deutschland und Europa. Wiesbaden.

Goertz, S./Streitparth, A. (2019). The New Terrorism. Actors, Strategies and Tactics. Wiesbaden.

Goertz, S. (2017). Analyse der Motivation und der psycho-sozialen Konstitution der Foreign Fighters des sog. Islamischen Staates. Österreichische Militärische Zeitschrift 3/2017, p. 348-352.

Pifer, S. (2014). Watch Out for Little Green Men; July 7, 2014, https://www.brookings.edu/chapters/watch-out-for-little-green-men/

Prince, S. (2016). New ISIS Video Shows Child Soldiers Executing & Beheading 5 ‘Kurdish Fighters’. 26.8.2016. http://heavy.com/news/2016/08/new-isis-islamic-state-amaq-newspictures-videos-kurdish-ypg-peshmerga-execution-beheading-by-boy-child-foreignsoldiers-raqqa-syria-telegram-full-uncensored-youtube-mp4-download/

Sadik, G. (2020). Terrorism and Hybrid Threats: Analyzing Common Characteristics and Constraints for Counter-Measures, *EICTP Vienna Research Papers on Transnational Terrorism and Counter Terrorism: Current Developments Volume I*, 73-80. https://www.eictp.eu/wp-content/uploads/2020/06/EICTP-Transnational-Terrorism-Publication_April-2020.pdf

news@orf.at (2022). GB: Wagner-Gruppe mit stärkerer Rolle an der Front, 29.7.2022, https://orf.at/stories/3278635/

Stern (2022). Ukraine 3000 Söldner der Wagner Gruppe laut Medienberichten getötet https://www.stern.de/gesellschaft/ukraine--3000-soeldner-der-wagner-gruppe-laut-medienbericht-getoetet-31795712.html

Syrian Observatory for Human Rights (SOHR), www.syriahr.com/en/?p=41663

The Moscow Times (2019). Russian mercenaris linked to gruesome syrian torture and beheading-video, https://www.themoscowtimes.com/2019/11/21/russian-mercenaries-linked-to-gruesome-syrian-torture-and-beheading-video-a68261

The Times (2022). War in Ukraine. Volodymyr Zelensky: Russian mercenaries ordered to kill Ukraine’s president, February 28, 2022, https://www.thetimes.co.uk/chapter/volodymyr-zelensky-russian-mercenaries-ordered-to-kill-ukraine-president-cvcksh79d

Time (2022). World. Inside Zelensky’s World, 28.4.2022, https://time.com/6171277/volodymyr-zelensky-interview-ukraine-war/?utm_source=twitter&utm_medium=social&utm_campaign=editorial&utm_term=world_ukraine&linkId=162789913

CHAPTER 6

HOW HAVE TERRORISTS ADOPTED TACTICS FROM THE RUSSIA-UKRAINE WAR? THE CRIME-TERROR-TECH NEXUS

Daniela Irrera[*]

Introduction

The war in Ukraine, that began in 2014 and militarily intensified in 2022, has demonstrated modern warfare tactics, many of which have been observed and could potentially be adopted by terrorist groups. The nexus between terrorism and organised crime is seen as a strategic alliance between two non-state actors able to exploit illicit markets and influence policy-making at the global level. The ability of criminals and terrorists to progressively develop their capabilities on a global scale, to establish themselves in failed and fragile states, and to interact with other violent non-state actors such as insurgents, paramilitaries and contractors, has largely benefited from the war and has been strengthened, particularly through the use of technology and the cyber environment.

This chapter analyses the impact of the relationship between organized crime and terrorism on the global security agenda and countermeasures strategies in the light of technological advances. In particular, it argues that the crime-terror nexus has changed significantly in the aftermath of the war in Ukraine and now represents a renewed threat capable of challenging the security of the NATO alliance and shaping its counter-strategy.

The chapter aims to answer the following research questions:

- Has the Crime/Terror nexus changed and evolved as a result of recent events in Ukraine?

- Does technological progress pose new challenges to the nexus?

- What is NATO's potential role in addressing these new challenges?

The chapter is divided into three sections. First, the crime-terror nexus is discussed in order to understand the extent of its impact at both regional and global levels. It is then

[*1] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

analyzed in the light of the additional threats posed by insurgency, armed conflict and weak and failed states. Second, it examines the current challenges posed by technological advances, as demonstrated during the war in Ukraine, to analyze the likelihood of a third component of the nexus. The third section examines NATO's role in meeting these growing challenges. Finally, it draws some conclusions about perceptions of the nexus and future prospects.

The Crime-Terror Nexus: How it Emerged and How It has Evolved

The study of the crime-terror nexus has consolidated within the scholarly community of International Relations and Security Studies, producing various theoretical and empirical insights (Ljujic, van Prooijen, & Weerman, 2017; Felbab-Brown, 2019; Makarenko, 2021; Carrapico, Irrera, & Tupman, 2014). It has been associated with two very different actors, each with diverse identities, goals and methods but which sometimes share common grounds and goals that converge and produce different forms of connection (Makarenko, 2000; 2009).

Initial analyses have focused on the process and the factors that may facilitate convergence.

As Makarenko described in her seminal works, criminal or terrorist groups may begin by adopting each other's tactics for mutual benefit; it may continue with the appropriation of these methods or tactics, leading to the fusion of groups into a functional alliance; and finally, it may lead to an evolution by which the tactics and motivations of one entity may be transformed by the other. All the different stages can be placed on a *continuum* and describe a variety of gradations depending on different conditions and causes (Makarenko, 2004).

Successive studies have offered a tripartite conceptualization of the crime-terror nexus, encompassing three types of (a) interaction, (b) transformation/imitation, and (c) similarities. For each type, different potential categories have been identified, ranging from zero (no interaction, transformation or similarity) to one (fusion, complete transformation or complete overlap). It is argued that only the 'heavier' categories of the first type - regular cooperation, alliance formation and fusion - require the co-existence of organized crime and terrorist organizations in each location and are rare. Other types may occur more frequently, but they vary depending on a variety of facilitating factors and the different performances of actors (Paoli & Fijnaut, 2022).

Other analyses have used different categories (cooperation, coexistence, convergence) to include more flexible and changing characteristics and to encompass different gradations of activity (Irrera, 2016). Cooperation refers to established alliances between terrorist and criminal groups. Short-term or *ad hoc* relationships may be frequent and outweigh the risks mechanically associated with this set of relationships, especially when focused on specific operational needs. Coexistence may be in an intermediate position, resulting in a situation where criminal and terrorist groups operate in the same business, but explicitly prefer to remain separate entities, unless a union is rationally and functionally required through an occasional or temporary link. Convergence is more difficult to observe and study and can refer to a very common condition in which the two actors use their respective techniques for practical purposes without necessarily forming an alliance. Organised criminal networks have long used terrorist tactics to protect their business interests and work environments, but terrorist groups are also increasingly using criminal expertise to meet operational needs.

As terrorists and criminals are non-state actors, the debates have also intersected with the literature on non-state actors (NSAs) and their impact on various policy fields. The nature and *modus operandi* of NSAs can vary, as can their ability to engage with actors in the global system, to exert influence and to develop their networking capacities in different policy areas. All NSAs are subject to internal and external factors and respond to them by developing strategies, agendas and actions. The extent to which they are able to respond positively to changes in their environment can make a big difference. This is particularly relevant for the subversive ones analyzed in this chapter. Discussions of the environment in which they operate, their interactions with other subversive actors, and the impact on the conflict zones in which they proliferate can be useful in understanding how they develop and what countermeasures are needed.

With the transnational expansion of markets and services offered by the cyber-environment, terrorist groups have adopted new structural forms, often very similar to those of organised crime syndicates. Post-Cold War terrorist groups such as Al-Qaeda and the DAESH appear to be sophisticated networks that combine largely autonomous cells and structures (Hutchinson & O'Malley, 2007). These groups are also more likely to engage in crimes such as drug smuggling, money laundering, theft, extortion, although they do not consider themselves to be common criminals (Hoffman, 2006). Drug trafficking is the largest source of income for organised crime groups and terrorists, along with robbery, extortion, kidnapping, arms trafficking and smuggling. However, such activities require extensive organizational capabilities and are likely to be carried out by more structured terrorist groups rather than individuals or isolated cells. Advances in technology are therefore perceived as necessary and useful (Hutchinson & O'Malley, 2007). For example, terrorist groups are increasingly using decentralized financial tools, such as cryptocurrencies, to evade financial controls, launder money and fund their operations. Cyber capabilities are being used by terrorist groups to launch attacks or steal financial assets to fund their operations. Artificial intelligence (AI) and big data analytics are used to sift through large amounts of information for strategic purposes. Terrorist groups could adapt these methods to identify targets, recruit individuals more effectively and plan attacks. The way in which extremist, armed and terrorist groups around the world have embraced technological innovation to gain an advantage over their adversaries has already been highlighted (Holt, 2012; Musotto & Wall, 2020).

Changes in nature and performance are relevant not only to understanding how terrorists and criminals interact, but also to identifying links with other actors or non-state armed groups, such as insurgents, paramilitary groups or private military companies (PMCs) hired by states to provide security services (Sullivan & Bunker, 2014; Jones & Johnston, 2013). These fighters, also labeled as mercenaries, bring with them not only combat skills but also links to international criminal networks, further blurring the lines between terrorism and organized crime.

Troubled and conflict-ridden environments are ideal for subversive actors to flourish. In contexts where terrorist groups and organized criminal groups are already active and consolidated, closer forms of cooperation between them are more likely. At the same time, some exceptional conditions may facilitate their presence and even give rise to new forms or entities (Kalyvas, 2015; do Ceu Pinto, 2022). These conditions can be observed in States affected by political, economic or social weaknesses; in States or regions where competitive illicit markets are largely or entirely controlled by existing organized crime syndicates; and in states or regions where various forms of non-state armed groups are already active (Alesina, Piccolo, & Pinotti, 2019; Petrich, 2021).

The links between criminals, terrorists and other armed groups, facilitated by the use of advanced technology, can take a variety of flexible forms that defy easy categorization. In some areas, the use of terrorist tactics by criminals is more visible. In conflict zones such as eastern Ukraine, existing groups blur the lines between organized crime and insurgent or terrorist activity. They control territory and engage in various illegal activities such as drug production, arms and human trafficking, all of which can fund terrorism, creating a hybrid crime-terror structure. The global political system is thus entering a new phase of increasing cooperation between violent NSAs.

The Impact of the War in Ukraine on the Crime-Terror Nexus

The Russia Ukraine war has clearly contributed to the amplification of several military and political potentialities and shortcomings at the regional and global level that are already part of the new security architecture, and to the intensification of the activities of armed NSAs, either individually or as part of nexuses. The attacks in Ukraine and the military escalation have had a significant impact on the activities of terrorist and criminal groups, increasing the likelihood of alliances and cooperation. This impact can be assessed in terms of three main features, that have been analyzed in the previous section: sources of funding for subversive activities; recruitment of alternative 'personnel' and changes in *modus operandi*; and the increasing use of technology.

In terms of funding, conflict zones have always provided additional space for illicit trafficking. Former Soviet countries and the Balkans have long been centers of organized crime, and war has exacerbated the black-market trade in arms and military equipment (Feinstein & Holden, 2004; Tan, 2023). These networks provide terrorist groups with access to sophisticated weapons and logistical support. Even in Ukraine, the influx of weapons has been substantial, benefiting criminal organizations in the first instance, but potentially also terrorist groups. War has created an environment in which financial institutions are vulnerable to abuse by organized crime and terrorist groups. Money laundering and terrorist financing through complex international networks are increasingly common, often facilitated by corrupt officials or weak regulatory systems. Both sides in the Ukrainian conflict have relied on decentralized financial instruments to finance their war efforts, particularly local volunteer units.

The recruitment of fighters, mainly foreigners, has been greatly affected by the war as well.

Ukraine has attracted fighters from different parts of the world, motivated by ideology, nationalism or mercenary work. Terrorist groups have long recruited foreign fighters. However, the war has revealed new models of cross-border recruitment that may be mirrored by terrorists, particularly in the recruitment of individuals without formal affiliation. The abandonment of the logic of the state has been even more radical. Instead of ethno-nationalist terrorist groups or extremist ideologies pursuing a separatist process or a change in the structures of government, groups are now provided with global aspirations whose goal is to influence global governance (Marrero Rocha, 2019). These fighters bring with them not only combat skills but also links to international criminal networks, further blurring the lines between terrorism and organized crime. In addition, some have returned home with enhanced combat skills and links to criminal networks, potentially fueling terrorism in other regions (Kaunert et al., 2023; de Roy et al. 2023).

The war has also improved the *modus operandi* of terrorists. Many organizations, especially after the collapse of DAESH, have adopted a decentralized model. Autonomous cells carry out attacks with little oversight, making them harder to disrupt. This tactic has been adopted by groups across Europe, the Middle East and Africa. The practice was particularly evident in Ukraine, where many groups began to operate in a decentralized manner, especially in the early stages with separatist groups (Pearson, et al., 2017). The absence of centralized command structures made it much easier to interact with criminals and other armed groups. Finally, as much of the fighting in Ukraine has taken place in urban areas, with both sides using the cover of civilian infrastructure, terrorist groups have increasingly engaged in urban warfare, adopting tactics that involve embedding fighters among the civilian population in order to deter direct military strikes or to exploit the consequences of civilian casualties for propaganda purposes.

Many of these tactics have been shaped or introduced by the increasing use of technology and cyber warfare. This is the area where the Ukrainian war has contributed most to the rise of the crime-terror nexus.

Two main features should be highlighted. The first one is the ‘improvisation’ of techniques and tools, which has been a constant for terrorist groups in many conflict zones due to the precarious local conditions or the uncertainty of cooperation with other local actors. In Ukraine this practice has improved, becoming less improvised and more professional and consolidated. The second is the 'weaponization' of tools and techniques and their deliberate use in a hostile or aggressive manner to achieve political, or military objectives (Riemer & Sobelman, 2023).

This is the case of Improvised Explosive Devices (IEDs) and the use of drones for surveillance. The conflict in Ukraine has popularized the use of commercial drones for surveillance and combat purposes. Ukrainian military and irregular forces have used drones to target Russian positions, and terrorist groups are learning to use drones for reconnaissance and attack or to employ tech-enabled tools to raise propaganda [2]. Groups such as DAESH and others in the Middle East and North Africa have increasingly adopted drones for similar purposes. They are using them for surveillance to gather intelligence on enemy positions, as well as weaponizing them to drop explosives on targets. In addition to drones, the 'de-improvisation' process involves guerrilla tactics, including ambushes and hit-and-run operations, which have been used to target Russian convoys and positions. More sophisticated remote placement and detonation techniques are now being used by armed groups. They are also often reinforcing civilian vehicles with makeshift armor and weapon mounts, creating more mobile and protected platforms for attacks.

Both features can also be seen in the transformation of cyberspace into a domain of conflict and warfare, where information technology is used as a weapon to cause harm, whether by disabling critical infrastructure, stealing sensitive data, spreading disinformation, or influencing events such as elections. Cyber warfare has been used intensively by Ukrainian and Russian forces (and their proxies) to target each other's critical infrastructure, communications and databases, but it has easily become a critical tool for both state and non-state actors. State-affiliated hacking groups have targeted infrastructure in Ukraine and beyond. Criminal groups, often linked to the Russian government, have launched cyber-attacks to destabilize Ukraine and its allies. Terrorist groups have moved into the cyber domain, targeting state infrastructure, banks and other institutions to create chaos and weaken governments. They also use cyber capabilities to spread propaganda or recruit new members. The complexity of the security and economic situation, along with emerging challenges such as hybrid warfare, cyber threats, and terrorism, may push NATO and the EU toward deeper cooperation (Holt, 2012).

De-improvisation and weaponization are two sides of an already existing process of empowerment of subversive actors, especially when they are linked, which the war has only made more visible. The forms that the crime-terror nexus is taking are more than a traditional offence enabled by new tools and technological devices, but rather a new form of offence that has no parallel. Because the war has had a significant impact on the capabilities and

[2] The NotPetya ransomware attack in 2017, which originated in Ukraine, is an example of cybercriminal activity that had a global impact. Such tactics can be used by terrorist organizations to create chaos or undermine state authorities.

technological advances of subversive actors, and because technological capacity and political stability are inextricably linked, the war should also have an impact on the countermeasures developed by NATO and its allies.

NATO's Role in New Challenges

In the post-Cold War era, NATO's focus has shifted from collective defence to crisis management to ensure Euro-Atlantic security against various risks, including terrorism and its connections. The fight against terrorism has been a priority in the Alliance's post-Cold War transformation, as set out in NATO's 2010 Strategic Concept. In the aftermath of 9/11, this strategy has been shaped by cooperation and among competition its various policies, as well as with international institutions such as the EU, which some NATO member states perceived as equally or better equipped to deal with these new challenges (Pomarede, 2024; Lupovici, 2023).

So far, the approach developed to counter proliferation has been a mix of deterrence, defense, non-proliferation, arms control and international cooperation. Its strategies cover conventional weapons, weapons of mass destruction, cyber capabilities and emerging technologies to ensure that the Alliance is prepared to meet modern threats and prevent the proliferation and misuse of weapons around the world.

At the same time, the challenges posed by violent NSAs, their growing capacity to implement more sophisticated practices and weaponized tools, such as the use of drones or in cyber domains, definitely require a deeper reflection and probably a rethinking of current counter-strategies. Capacity building, including improving infrastructure resilience and strengthening cyber defenses, and information sharing are at the heart of such considerations. This will require not only an overhaul of NATO's deterrence and collective defense pillars, but also an increase in the Alliance's technological innovation and strengthening NATO countries' resilience to hybrid threats such as cyber-attacks and disinformation campaigns (Morcos & Simon, 2022).

Dealing with Emerging and Disruptive Technologies (EDTs), which encompass technologies with significant military potential and associated risks, is a growing aspect of NATO's strategic focus (NATO Strategic Concept, 2022). This is consistent with the need to access innovation in the private sector, with the aim of identifying dual-use cases and regulating the use of emerging technologies. This approach allows NATO to stay at the forefront of technological advances, particularly in areas such as AI, where China and Russia are also investing heavily. Strong US leadership remains essential in almost all aspects of NATO decision-making. The US commitment to the Alliance, including its military presence in Europe, is critical to credible collective deterrence and defense (Olsen, 2020). As has been observed, member states and the Alliance should become more resilient by adopting a common strategic culture that embraces technological complexity (Gottemoeller et al., 2022). Furthermore, an integrated strategy is needed to capture the hybrid environment in which violent NSAs operate, and communities need to start looking at strategic learning and inter-agency collaboration (Sadik, 2021).

In this sense, partnership with international organizations and regional allies is also essential, as is the establishment of standards for interoperability between allied and partner defense systems, ensuring the smooth exchange of information and the compatibility of AI algorithms and data sets. This focus recognizes the different pace of implementation and regulatory approaches between the United States and Europe. By actively engaging in the development and regulation of emerging technologies, NATO aims to maintain its technological edge, address security challenges posed by illiberal actors, and establish norms for responsible use. Reducing harmful dependencies in the strategic sectors and preventing supply strains, and countering manipulation may also preserve Europe's capacity for independent decision-making.

One of the most challenging consequences of the Russia-Ukraine war may be the need to replace existing US capabilities. That the concept of NATO's European Allies plays a major role in maintaining the regional balance of power is not entirely new. NATO members have been working to improve their defense capabilities, increase their defense spending and contribute more actively to NATO operations and missions.

Although the war in Ukraine has already shown that significant changes are taking place and that a different landscape is emerging, it is not easy to identify the various components of the new security architecture and to understand how the relationship between NATO and the EU will evolve in the field of counter-terrorism.

From NATO's perspective, a reaffirmation of roles is needed. Allies committed to a significant increase in troop numbers and rapid deployment capability. This is also a reaffirmation of what members expect from NATO. While it upholds democratic values and the rules-based order, it focuses on areas directly related to its defense competence. This focus enables the Alliance to effectively address security challenges, deter potential adversaries and ensure the collective defence of its members (Larsen, 2022).

From the EU's point of view, a reaffirmation of independence is needed. The EU has increased its role as a conflict manager in the war, but it is still indirect and incomplete. The emphasis on state-building and the security nexus, as opposed to an exclusive focus on democratization and transformation, reflects a recognition of the need to address immediate security challenges and strengthen state capacity.

The EU's increased influence and ambition to play a more significant role beyond technical assistance is evident in the pragmatism and political involvement of EU representatives on the ground in Ukraine. This signals a deeper commitment and a desire to have a tangible impact on the security and stability of the region. However, there may be limitations in terms of flexibility and capacity to respond adequately to security developments in the region. This may pose challenges in responding rapidly to evolving security situations. Addressing these limitations and enhancing the flexibility and capabilities to respond adequately to security developments is an ongoing challenge for the EU and its Member States in the framework of the Common Security and Defence Policy (Härtel, 2023).

It is evident that the NATO-EU partnership plays an important role in enhancing the Alliance ability to respond to external influence and potential coercion in various areas. While the concept of European strategic autonomy often refers to the EU's quest for a more independent defense posture, the NATO-EU partnership focuses on broader security and resilience challenges, including civilian aspects. Enhanced cooperation would allow for coordination and cooperation in addressing common security challenges beyond traditional military defense, such as the fight against illicit financial flows. In the area of technology import/export controls, NATO and the EU can work together to establish common rules and standards to mitigate risks and prevent the misuse of emerging technologies.

Conclusions: Navigating Troubled Waters

The fluid and dynamic nature of modern conflicts, including the one in Russia-Ukraine war, provides a learning ground for asymmetric warfare strategies that can be adopted by non-state actors, such as terrorist and criminal groups. The war has introduced and demonstrated a wide range of tactics, from drone warfare to cyber operations, urban warfare and decentralized structures, many of which have been or could be adapted to terrorist contexts around the world. In terms of the crime-terror-technology nexus, the war has helped to exacerbate its impact. Criminal networks facilitate the flow of weapons, illicit goods and finances that support both state and non-state actors in the conflict. Meanwhile, technological advances in cyber warfare, propaganda and surveillance are increasingly being adopted by terrorist organizations. Criminals and terrorists have consolidated relations with other violent local NSAs, identified additional channels for recruiting new fighters (not necessarily linked to ideology or extremism, but also to the use of contractors), and improved and enhanced sources of funding. The Ukrainian battlefield provided an ideal context for testing and consolidating new tools and practices. In particular, the war has offered terrorists and criminals the opportunity to learn how technology can improve the use of drones, vehicles and weapons, and how the cyber environment can facilitate illicit activities to fund warfare. De-improvisation and weaponization have rapidly transformed subversive performances. This will inevitably have implications for regional security, but also for NATO's counterstrategy and relations with its allies.

Various scenarios could develop. The EU has taken steps to strengthen its defense cooperation through initiatives such as the Permanent Structured Cooperation (PESCO) and the European Defence Fund. These efforts aim to enhance the defense capabilities of EU and improve coordination on security and defense issues. The EU could be one element of the Global West, working closely with other conceptually homologous economic, cultural and defense entities from different regions. In this case, NATO could function as a sub-structure within a broader global defense alliance composed of Western and West-supporting states. Co-ordination between EU defense policy and extended NATO structures would largely depend on the specific institutional arrangements and agreements between these entities. It could include cooperation on defense planning, information sharing, joint exercises and, potentially, shared defense capabilities. The precise nature and extent of such coordination would require detailed negotiations and agreements between the parties involved.

References

Carrapico H. Irrera D. & Tupman B (2014), Transnational Organised Crime and Terrorism: different peas, same pod? Double Special Issue of Global Crime, 15 (03-04).

de Roy van Zuijdewijn, Jeanine, and Edwin Bakker. "Twenty years of countering jihadism in Western Europe: from the shock of 9/11 to 'jihadism fatigue'." Journal of Policing, Intelligence and Counter Terrorism 18.4 (2023): 421-434.

do Céu Pinto Arena, Maria. "The Impact of Ethnic Groups on International Relations. In M. Charountaki & D. Irrera (eds). Mapping Non-State Actors in International Relations. Cham: Springer International Publishing, 2022, pp. 73-94.

Felbab-Brown, V., 2019. The crime-terror Nexus and its fallacies. In Chenoweth E. (eds.), The Oxford handbook of terrorism, Oxford University Press, Oxford, pp. 366-383.

Feinstein, Andrew, and Paul Holden. "Arms trafficking." The Oxford handbook of organized crime. Oxford: Oxford University Press, 2014. 444-59.

Fiott, Daniel, 'The Fog of War: Russia's War on Ukraine, European Defence Spending and Military Capabilities', *Intereconomics* 57.3, 2022, pp. 152-156.

Freudlsperger, Christian, and Frank Schimmelfennig, 'Rebordering Europe in the Russia-Ukraine war: community building without capacity building', *West european politics* 46.5, 2023, pp. 843-871.

Gottemoeller, Rose, et al. "Engaging with emerged and emerging domains: cyber, space, and technology in the 2022 NATO strategic concept." Defence Studies 22.3 (2022): 516-524.

Härtel, André, 'EU Actorness in the Conflict in Ukraine: Between 'Comprehensive'Ambitions and the Contradictory Realities of an Enlarged 'Technical'Role', Ethnopolitics 22.3, 2023, pp. 271-289.

Hoffman, B. (2006). Inside terrorism. New York: Columbia University Press.

Holt, Thomas J. "Exploring the intersections of technology, crime, and terror." Terrorism and Political Violence 24.2 (2012): 337-354.

Hutchinson, S. and O'Malley, P. (2007), 'A Crime–terror Nexus? Thinking on Some of the Links between Terrorism and Criminality', Studies in Conflict Terrorism, 30(12): 1095–1107.

Jones, Seth G., and Patrick B. Johnston. "The future of insurgency." Studies in Conflict & Terrorism 36.1, 2013, pp. 1-25.

Kalyvas, S.N. (2015), 'How Civil Wars Help Explain Organized Crime – and How They Do Not', Journal of Conflict Resolution, 59(8): 1517–1540.

Kaunert, Christian, Alex MacKenzie, and Sarah Léonard. "Far-right foreign fighters and Ukraine: A blind spot for the European Union?." New Journal of European Criminal Law 14.2 (2023): 247-266.

Irrera D. (2016), The crime-terror-insurgency 'nexus'. Implications on multilateral cooperation in S. Romaniuk (eds.) Insurgency and Counterinsurgency in Modern War, CRC Press, New York, pp. 39-52.

Irrera, D. (2024), Criminality and Delinquency: the impact on Regional and Global Security, in S. Kaempf & A. Gruszczak (eds.) Routledge Handbook on the Future of Warfare, 2024.

Larsen, Henrik, 'Adapting NATO to Great-Power Competition', *The Washington Quarterly* 45.4, 2022, pp. 7-26.

Ljujic, V., van Prooijen, J.W. and Weerman, F., 2017. Beyond the crime-terror nexus: socio-economic status, violent crimes and terrorism. Journal of Criminological Research, Policy and Practice, 3(3), pp.158-172.

Lupovici, Amir. "Deterrence by delivery of arms: NATO and the war in Ukraine." Contemporary Security Policy 44.4 (2023): 624-641.

Makarenko T. (2000), Crime and Terrorism in Central Asia, Jane's Intelligence Review 12 (7), pp. 16-17.

Makarenko T. (2004). "The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism." Global Crime 6:1, pp. 129-145.

Makarenko T. (2009), 'Terrorist Use of Organised Crime: operational tool or exacerbating the threat?' in F. Allum, F. Longo, D. Irrera, P. Kostakos (eds.), Defining and Defying Organised Crime: Discourse, Perceptions, and Reality, London, Routledge, pp. 180-193.

Makarenko, T., 2021. Foundations and evolution of the crime–terror nexus. In Allum F., Gilmour S. The Routledge Handbook of Transnational Organized Crime, London, Routledge, pp. 253-269.

Morcos, Pierre, and Luis Simón. NATO and the South after Ukraine. Center for Strategic and International Studies (CSIS), 2022, https://www.jstor.org/stable/pdf/resrep41413.pdf

Musotto, Roberto, and David S. Wall. "More Amazon than Mafia: analysing a DDoS stresser service as organised cybercrime." Trends in Organized Crime (2020): 1-19.

NATO Strategic Concept, adopted by the Heads of States and Governments, NATO Summit, Madrid, 28 June 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

Olsen, John Andreas. "Understanding nato." The RUSI Journal165.3 (2020): pp. 60-72.

Paoli L. & Fijnaut, C. (2022), Conceptualizing the nexus between organized crime and terrorism. In Paoli L. & Fijnaut, C. (eds.), The Nexus Between Organized Crime and Terrorism, Edward Elgar Publishing, 48-84.

Pearson, F.S., Akbulut, I. and Olson Lounsbery, M. (2017), 'Group Structure and Intergroup Relations in Global Terror Networks: Further Explorations', Terrorism and Political Violence, 29(3): 550–572.

Pomarede, Julien. "Deadly ambiguities: NATO and the politics of counter-terrorism in international organizations after 9/11." Security Dialogue (2024): DOI 09670106241240426, pp. 1-19.

Riemer, Ofek, and Daniel Sobelman. "Coercive disclosure: The weaponization of public intelligence revelation in international relations." Contemporary Security Policy 44.2 (2023): 276-307.

Rocha, I. M. (2019). Global system dynamics in the relationships between organized crime and terrorist groups. In V. Ruggiero (eds.). Organized Crime and Terrorist Networks, Routledge, London, 100-116.

Sadık, Giray. “How can NATO effectively counter terrorism and hybrid threats? Analyzing the benefits and pitfalls of joint synergies.” PERCEPTIONS: Journal of International Affairs 26.1 (2021): 54-72.

Sperling, James, and Mark Webber, ‘NATO and the Ukraine crisis: Collective securitisation’, *European journal of international security* 2.1, 2017, pp. 19-46.

Struwe, Lars Bangert, et al. “The Ukraine crisis and the end of the Post-Cold War European order: options for NATO and the EU.”, 2014, Centre for Military Studies, University of Copenhagen.

Sullivan, John P., and Robert J. Bunker. “Multilateral counter-insurgency networks.” Networks, terrorism and global insurgency. Routledge, London, 2014, pp. 183-198.

Tan, Andrew TH. “Global Arms Trade.” Security Studies. Routledge, London, 2023, pp. 535-551.

CHAPTER 7

EMERGING THREATS: WILL THE USE OF NEW TECHNOLOGIES IN THE RUSSIA-UKRAINE WAR TRANSFORM THE CAPABILITIES OF TERRORISTS?

Dr. Christina Schori Liang[*]

Introduction

On 24 February 2022 Russia launched an unprovoked war against sovereign Ukraine, expanding a bloody conflict that started in 2014 with the Russian annexation of Crimea. The 2022 invasion of Ukraine is exceptional in that it should have ended quickly, given the fact Russia had a significant advantage in both manpower and firepower. However, Ukraine continues to prevail, with many, including its leadership, attributing this success to both the exceptional will and determination of the Ukrainian people and to their skill and ingenuity in leveraging the latest technologies with the aid and support of multiple private companies, countries, and international organizations. With round-the-clock international and social media coverage, terrorists worldwide can monitor the unfolding war in real time through encrypted messaging apps, social media platforms, niche forums, image boards, video-sharing platforms, and the dark web. Access to these technologies enables them to continually adapt and learn about new technologies and assess their effectiveness in combat.

Wars are not merely battles of weapons and resolve; they also serve as testing grounds for the future. The war in Ukraine has become a distinctive laboratory, a terrible Silicon Valley of sorts that is actively experimenting with the technological advancements of the past two decades. It has been described as a “technology” war, where newly developed apps, cutting-edge technologies, and sheer human determination are continuously fortifying the war effort.

The Russia-Ukraine war has been depicted as the first commercial space war, the first full-scale drone war and the first AI war (Suess, 2023; Khurshudyan, Ilyushina and Khudov,

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

2022). The war is also stealthily ushering in a new age of intelligent killer robots (Mozur and Satariano, 2024). The Russia-Ukraine war blends the technologies of the twenty-first century with the tactics of the Second World war, the attrition rate of the First World War and the devastating humanitarian consequences that is a hallmark of all wars. As of February 2024, the Office of the United Nations High Commissioner for Human Rights (OHCHR) verified 10,582 deaths of civilians in Ukraine which has been matched with a massive humanitarian crisis as thousands of Ukrainians were internally displaced and over 17.3 million leaving the country (Statista, 2024). As of May 2024, some estimates put Russian troop deaths at over 150,000 (France24, 2024).

While the Russia-Ukraine war displays all the characteristics of a large-scale combat operation, it has multiple unique characteristics that make it truly exceptional. The conflict is predominantly a land war, where manned aerial systems have been mostly neutralized by air defenses. It has become a *Materialschlacht*—a battle characterized by the massive deployment of Soviet-era tanks that exemplifies old-fashioned attrition warfare, marked by large-scale engagements involving manpower, artillery, tanks, explosives and ammunition. Simultaneously, the conflict is also highlighting how technology is reshaping the modern battlefield, with the industrial-scale use of drones, AI and information power. It is a war fought close-up in the form of guerilla style tactics and at a distance with neither side ever actually seeing each other.

This analysis primarily aims to examine the twenty-first-century tactics used in this war, with a focus on understanding what new insights the Russia-Ukraine conflict may provide to violent non-state actors and in particular terrorists. Historically, terrorists have been eager adopters of innovative technologies. The key question is how this conflict will inspire violent non-state actors to devise new and more innovative strategies and tactics.

Drones

Drones have played an important role in the Russia-Ukraine war since the unlawful incursion of Russian forces into its territory. They are being used with growing frequency by unidentified operators to strike targets within Russia, including in the heart of Moscow. Both sides in the conflict have integrated drones into every aspect of fighting from precision fire and strike coordination to intelligence, surveillance, reconnaissance (ISR) and psychological operations.

For Ukraine, the drone has become the ultimate symbol of resistance. Drones helped prevent Russia's military invasion into Kyiv in the early days and weeks of the war. The Aerorozvidka drone operators unit, with the support of Ukrainian special forces, ambushed Russia's armored vehicles and supply trucks and prevented convoys from reaching the capital. The Russian offensive ground to a halt within days, largely due to these tactics which were able to destroy two or three vehicles at the head of the convoy, blocking the progression of the other vehicles (Borger, 2022). The Aerorozvidka unit also claims to have helped defeat a Russian airborne attack on Hostomel airport using drones to locate, target and shell about 200 Russian paratroopers concealed at one end of the airfield (Borger, 2022).

Drones have become the eyes on the battlefield. A special reconnaissance drone team called "ochi" (Ukrainian for "eyes") effectively give eyes to their artillery. The drones are linked to Starlink satellites of the American company SpaceX which supplies high-speed internet connection so everything the drone sees can be streamed to nearby brigades. Ochi teams observe Russians and identify targets while being in constant contact with artillery units. According to T.J. Holland, soldier in America's XVIII Airborne Corps "around 86% of all Ukrainian targets are derived from drones. They vigilantly watch the enemies every move – posting their every move like a nature movie while they are planning, fighting, eating and sleeping."

Multiple drone types are fielded in Ukraine. One of the most cost-efficient drones in the war is the small Mavic quadcopter produced by the DJI, a Chinese company which costs less than USD 4,000 online. They are used for surveillance and to drop small munitions, sometimes fashioned in soda cans. Although the Chinese have stopped supplying the drones to either side, supporters of both sides buy them in bulk from retailers. Among the cheapest small drones were those supplied in 2023 by Ukrainian high-school students who built them by welding Chinese-supplied components on to carbon-fibre frames costing USD 350 a piece. These were then strapped with two or three pound explosives for kamikaze-style missions to either kill Russian artillery brigade operators or to immobilize armored vehicles.

Larger drones are being used to hunt down smaller ones. Ukraine has introduced the Drone Hunter F700, a six-rotor drone equipped with radar-supported autonomous technology and two "net heads" that can launch webs to capture smaller enemy drones. Once ensnared, these drones can be dragged away. Larger drones are also caught in nets, but instead of being dragged, they are released; the net disrupts their flight, causing them to fall to the ground under their own weight. A parachute attached to the net deploys to cushion the landing. The Drone Hunter has hindered Russia's ability to use their drones for gathering artillery-targeting intelligence on Ukrainian troops and has also slowed down larger Russian kamikaze drones targeting critical infrastructure (Sherman, 2023).

Drones are crowd-sourced from all parts of the world through a UNITED24 platform "Army of Drones" initiative, supported by the Ukrainian government and the Ukrainian World Congress. The program with this new initiative which focuses on fundraising for the procurement, delivery, and maintenance of professional drones for aerial reconnaissance, and training pilot-operators. In August 2024, the "Army of Drones" website maintains that 10,000 operators have been trained and the government has allocated $867 million to create 60 drone strike companies. Ideally, Ukraine plans to produce or purchase 200,000 combat UAVs in 2024. Contributions from various sources included cardboard drones from Australia, 3D-printed suicide drones from Britain, AI-supported surveillance drones from Germany, and small military drones like Norway's Black Hornets.

Ukraine has become a testing ground for diverse and evolving drone technologies. Direct feedback from troops is driving innovation. Eric Schmidt, previously at Google, and other investors set up a firm called D3 to invest in emerging battlefield technologies in Ukraine. Other defense companies, such as Helsing, are also teaming up with Ukrainian firms (Conger and Metz, 2022). Some of the most advanced drones are being used in collaboration with AI.

Drones and AI

Generative AI will profoundly impact global security by enabling the creation of new weapons and methods for malicious actors worldwide. Recent advancements in commercially available drones have equipped them with high-level sensors, user-friendly controls, and first-person view capabilities at a lower cost than military-grade systems. These drones, while less durable and less protected than their military grade counterparts, allow forces to absorb losses more easily. Ukrainian forces utilize a mix of civilian and military drones, ranging from small loitering munitions like the U.S.-supplied Switchblade to larger systems with greater range.

AI technologies are enabling drones and other machines to operate autonomously. AI is enhancing drone operations by automating processes like take-off and landing, and helps the drone navigate to the target while avoiding obstacles and minimizing detection. This involves real-time adjustments to the drone's flight path based on environmental conditions and potential threats.

Drones use AI to make decisions on what to strike by processing vast amounts of data and leveraging advanced algorithms to identify, analyze, and prioritize potential targets. They can also use computer vision algorithms to interpret visual data. This involves recognizing objects, differentiating between civilians and military assets, and identifying patterns or anomalies. AI systems are trained to recognize and classify various objects—such as vehicles, buildings, or people—using deep learning models. AI algorithms assess the potential threat level of identified objects or entities. This might involve evaluating the object's size, movement, heat signature, or location. Based on the threat assessment, the AI system prioritizes targets.

Drones are equipped with various sensors, including high-resolution cameras, infrared sensors, radar, and LiDAR (Light Detection and Ranging). These sensors collect data from the drone's surroundings, such as visual imagery, thermal signatures, and geographical information. By coordinating the data from these sensors which are integrated in real-time, soldiers are presented with a comprehensive view of the environment.

If a target is confirmed, the AI system can guide the drone to deliver a payload, such as a missile or bomb, with high precision. AI ensures that the strike is as effective as possible, minimizing collateral damage.

Depending on the level of autonomy programmed into the drone, the AI can either autonomously decide to strike or assist human operators by suggesting targets. Autonomous systems operate within predefined rules of engagement, while human operators typically make the final decision. In most cases humans are asked to confirm selected targets and information is sent to Ukrainian battle management systems. This has enabled the time of detection of a target to its destruction to be reduced to approximately 30 seconds.

After a strike, AI systems can undertake a post-strike analysis to analyze the aftermath using the drone's sensors to determine the effectiveness of the strike and assess any remaining threats. AI enables drones to operate with a high degree of autonomy, making split-second decisions based on complex data analysis. This allows them to be highly effective in modern warfare, though it also raises significant ethical and legal concerns regarding the use of autonomous weapons.

Furthermore, the Ukrainians have also effectively employed AI for facial recognition through ClearviewAI and for voice recognition, transcription, and translation services through PrimerAI: this also allows them to understand what the enemy is saying (Paresh and Dastin, 2022).

Special Unit for Drone Warfare

The ongoing conflict in Ukraine underscores the advantages of deploying multiple drones simultaneously for an operational advantage. Among the many military tactics that Napoleon Bonapart employed that led to success on the battlefield was partly due to his ability to use maneuver to mass his forces at multiple points of enemy weakness, allowing him to defeat armies larger than his own. He attacked the enemy as a cohesive system and created synergetic effects.

Transitioning to a theory of warfare for swarm weapons, going beyond just mass, a swarm of drones can exploit this same principle of maneuver to attack the enemy system at hundreds of dispersed weak points simultaneously. The effectiveness of swarming tactics relies on the drones' ability to communicate, coordinate, and act cohesively. Employed as a system to attack a system, militaries can multiply the effects a swarm weapon by exploiting synergetic effects to gain a larger operational advantage (Williams, 2018). A 2018 study demonstrated that drone swarms could boost the lethality of attacks by up to 50% while simultaneously reducing drone losses from enemy fire by the same margin (Williams, 2018).

According to Mykhail Federov, Ukraine's Minister of Digital Transformation, "[t]hese technologies are fundamental to our victory" (Satariano, 2022). Makeshift factories and labs have emerged across Ukraine, producing remote-controlled machines of various sizes, ranging from long-range aircraft and attack boats to inexpensive kamikaze drones—known as F.P.V.s, or first-person view drones, guided by pilot-operators wearing VR-like goggles that provide the drone's perspective. Many of these machines are early versions of what will eventually operate autonomously. Some autonomous drones are "already in high demand, especially the ones that are able to prevent jamming. These drones can pilot-operator on their own, the pilot-operator simply needs to lock on to the target and the device does the rest" (Mozur and Krolik, 2023).

Ukrainian entrepreneurs, engineers and military units are using code found online and components from hobbyist computers like Raspberry Pi that can be purchased from hardware stores or Best Buy (Satariano and Scott, 2023). Technologically these gadgets are not as expensive or advanced as the military-grade systems that are made by military behemoths like China, Russia and the US. These new weapons are much cheaper – just thousands of dollars or even less and except for munitions these weapons can be built with code found online.

Entrepreneurs, engineers, and military units in Ukraine are developing swarms of self-guided drones capable of coordinating attacks. These drones can independently assess targets, scan areas for safety, and provide aerial support. However, when integrated into swarms, their collective intelligence grows exponentially, enhancing both surveillance and combat effectiveness.

In June 2024, Ukraine established the Unmanned Systems Forces, a new military branch dedicated to drone warfare, claimed to be the first of its kind globally. This initiative reflects Ukraine's significant reliance on drones, as highlighted by President Volodymyr Zelenskyy who announced that they "have proven their effectiveness in battles on land, in the sky and at sea" (Zelenskyy, 2024).

Corporates

Corporates have identified Ukraine as the ideal testing ground for their latest AI tech. This has enabled Ukraine to access some of the most advanced AI technologies in the world. Multiple corporates have had an important impact on the war, among them SpaceX and Palentir (Satariano, Reinhard, Metz, Frenkel and Malika, 2023). SpaceX has helped ensure Ukraine's access to high-speed internet for the country. It is according to Elon Musk "the backbone of Ukraine's military communications," and according to Federov "the blood of our entire communications infrastructure" (Satariano, Reinhard, Metz, Frenkel and Malika, 2023).

Without Starlink's access to the internet, Ukrainian President, Volodymyr Zelenskyy would not have been able to rally the world's leaders, citizens and corporates to protect and support Ukraine from being swallowed up by Russia. Starlink also allowed him to meet with world leaders, communicate with his people via social media and have the bandwidth to counter the Russia's powerful information campaigns (Miller, Scott and Bender, 2022).

Palantir, a U.S. data analytics firm assists Ukraine with military intelligence, refining its targeting capabilities in artillery strikes and target tanks. The Ukrainian Ministry of Defense utilizes Palantir's AI software to analyze open-source data, satellite imagery, and drone footage, creating reports from the ground that present military options to commanders.

Ukrainian intelligence analysts use Palantir's MetaConstellation tool to quickly access commercial satellite data through AI-assisted searches, providing crucial information when and where it is needed. Palantir's data analytics also contribute to collecting battlefield intelligence, gathering evidence of war crimes, clearing landmines, and resettling refugees (Bergengruen, 2023).

A Ukrainian drone manufacturer, Saker, has developed an autonomous targeting system using AI technology that was originally intended for sorting and classifying fruit. During the winter, the company began deploying this technology on the front lines, testing various systems with drone pilot-operators. As demand grew, Saker increased production, and by May, it was mass-producing single-circuit-board computers preloaded with its software. These computers can be easily attached to FPV drones, enabling them to automatically lock onto targets. Once a target is locked, the drone crashes into it. Saker currently produces 1,000 of these circuit boards monthly, with plans to increase output to 9,000. Several Ukrainian military units have already used Saker's technology to strike Russian targets on the front lines, as confirmed by the company and verified videos. Recently, Saker has made further advancements, successfully deploying a reconnaissance drone that uses AI to identify targets and then directs autonomous kamikaze drones to eliminate them one target was 25 miles away (Mozur and Satariano, 2024).

Significant questions nonetheless remain about the acceptable level of automation in warfare. Currently, drones require a pilot-operator to lock onto a target, ensuring a 'human in the loop' - a concept frequently emphasized by policymakers and AI ethicists. In the future, such constraints on these weapons may no longer exist. Autonomous weapons are already being used to strike Russian ships, significantly affecting naval security. But Ukrainian soldiers have expressed concerns about the possibility of malfunctioning autonomous drones mistakenly targeting their own forces.

Naval Drones to Attack Ships

Naval drones are also having an important impact. Ukraine has used remote-controlled boat drones packed with explosives to attack Russia's fleet located off the coast of Sevastopol. According to unofficial reports, an amphibious Russian landing ship was targeted with two unmanned maritime drones subsequently sinking sinking the Ivanovets, a seventy million dollar Russian missile Corvette (Seawanderer, 2024). According to multiple news agencies, at least 20 medium to large Russian naval vessels have been sunk in the Black Sea (Carey, Kostenko and Pennington, 2024).

A vast arsenal of millions of autonomous drones presents a significant threat to naval fleets. Ukraine has already demonstrated this potential by repelling large-scale Russian mechanized attacks and crippling Russia's Black Sea fleet. Several countries that had previously been developing naval drones are now intensifying their efforts, particularly after witnessing their effectiveness in striking Russian ships in the Black Sea.

In 2021, the U.S. Naval Forces Central Command established Task Force 59, which focuses on unmanned operations in the Middle East. "The Pioneers" aim to enhance maritime security by integrating unmanned systems with manned operations across the U.S. 5th Fleet's area of responsibility, which spans approximately 2.5 million square miles of water, including the Arabian Gulf, Red Sea, Gulf of Oman, Gulf of Aden, Arabian Sea, and parts of the Indian Ocean. This region, encompassing 21 nations, includes three critical chokepoints: the Strait of Hormuz, the Suez Canal, and the Bab al-Mandeb Strait.

Then, in the summer of 2024, U.S. Indo-Pacific Command unveiled a new "hellscape" strategy, which involves saturating the waters around Taiwan with tens of thousands of unmanned boats, submarines, and drones to hinder any Chinese attempt to capture the island. A new manufacturing initiative, the Replicator Initiative, has been launched to support the build-up necessary for this strategy (Kluth, 2024).

In parallel, NATO forces currently have drone arsenals numbering in the hundreds or low thousands, but this is rapidly changing. Six NATO countries—Estonia, Finland, Latvia, Lithuania, Norway, and Poland—are joining forces to build a European version of the "hellscape" plan by creating a "European drone wall" to prevent Russian incursions, creating a new kind of defensive landscape (Meier and Ferguson, 2024).

For the first time this year, both Ukraine and Russia have started producing drones on an industrial scale, moving from single-drone operations to managing entire swarms with just a few operators. By the end of 2024, we will likely witness the deployment of an autonomous mass — thousands of drones controlled by a small number of operators with minimal ground oversight. The shift toward unmanned warfare is becoming seemingly inevitable. For the United States, initiatives like the Replicator Initiative and the "hellscape" plan are just the beginning; the next step is to develop a comprehensive Unmanned Systems strategy, which other countries are likely to follow. Drones are fundamentally changing the nature of warfare.

Drones and UAWs are Reinventing Military Opus Operandi

Drones therefore, have significantly changed military strategies and could significantly change how militaries engage in the future. The implications for traditional military hardware are significant. Today's drones, akin to the early biplanes of World War I, are primitive compared to future advancements. We are already witnessing the emergence of advanced "deep-strike" drones, such as Iranian Shahed drones used by Russia and long-range drones developed by Ukrainian startups. In large numbers, these drones can surpass even sophisticated air defenses. Unlike traditional large standing armies, reserve drones require minimal space, no sustenance, and no salaries. Drones are also becoming easy to acquire and if needed, upgraded, repurposed and if broken, rebuilt.

‘Do-it-Yourself’ Weapons by Citizens, Reservists and Military

Drones have introduced the concept of the ‘do-it-yourself’ weapons. The war in Ukraine has changed the way people and their militaries are approaching weapons. The widespread availability of easily designed software, off-the-shelf devices and 3D printing has accelerated the ability for innovative minds to build their own weapons.

Ukraine is also a new laboratory for 3D printing. Since Ukraine is greatly underequipped compared to Russian military forces and armor, 3D printing is an important strategic enabler enabling Ukraine to print crucial munitions including artillery shells. The grenade, once considered obsolete due to its limited range, has now evolved into a powerful anti-personnel weapon. Quadcopters can now drop grenades directly onto targets, equipped with 3D-printed stabilizing fins for accuracy. Multiple organizations are harnessing 3D printing to enhance Ukraine’s offensive capabilities, designing, printing, and donating personal protection and medical equipment. Tech Against Tanks connects 3D printing support efforts, producing items such as window barricades, elbow and knee protection, tourniquets, smoke grenades, and diversionary mines.

The U.S. Department of Defense has donated Warp SPEE3D metal 3D printers, allowing Ukraine’s soldiers and engineers to quickly manufacture metal parts needed for repairing damaged machines in real-time, often within hours. Having these metal 3D printers readily available in the country provides a significant advantage in the field, where replacing parts is otherwise challenging.

Ukraine also receives support from volunteer organizations with 3D printing capabilities. WildBees Poland, part of a global network of volunteers using 3D printers to aid the war effort, operates in more than 20 countries with hundreds of volunteers working independently. These “BeeHives” around the world provide essential items at cost, including lifesaving gadgets like trench periscopes, clips to securely attach FPV goggles to helmets, drone launching platforms, casings for Starlink satellite receivers, magazine clips and drone recovery claws to retrieve drones downed by electronic warfare.

3D printing is creating new weapons too. A 23-year-old reservist in Ukraine has trained four soldiers to use the latest futuristic weapon: a gun turret with autonomous targeting that works with a PlayStation controller and a tablet. It can auto-lock on a target up to 1,000 meters away. The gun uses A.I.-trained software to automatically track and shoot targets. Not dissimilar to the object identification featured in surveillance cameras: software on a screen surrounds humans and other would-be targets with a digital box, the shooter then needs only to activate the trigger with a video game controller. Another soldier in Ukraine is strapping bombs to racing drones, adding larger batteries so they can fly longer and night vision so they can hunt in the dark.

We have seen the numerous technological developments which have emerged from the Russia-Ukraine war. What potential lessons are violent non-state actors such as terrorists poetically learning from the conflict?

Conclusions/Lessons Identified

Lesson One: All-Out Wars' are long, devastating and costly.

One of the key lessons that is being learned from the conflict is that an 'all-out war' against Western forces would be much longer and more devastating than, say, what has been experienced by Middle Eastern armed groups in Homs, Mosul and Raqqa.

The war in Ukraine is underscoring the exorbitant costs of all-out wars. Modern wars need modern equipment, fuel, ammunition, mechanical maintenance and combatants. Multiple states and international actors have helped to support the war in Ukraine by supplying munitions and financial help. The European Union (EU) institutions, including the Commission and the EU Council have provided 39 billion Euros in bilateral financial, humanitarian, and military aid from January 24, 2022 to June 30, 2024. The United States has donated the highest value of allocations at 75.1 billion Euros (Statista, 2024).

War also has an enormous human cost. Russia will suffer the consequences of the war in Ukraine for many decades to come with an older, more fragile and less educated society. As many as half a million young men in Russia have been killed or wounded, women are choosing to forego having children and some are being sent to fight in Ukraine, and more than one million mostly young and highly educated people left Russia (Balzer, 2024). In Ukraine, young men 25 and upwards are being drafted, tens of thousands have been killed or seriously injured, while 800,000 Ukrainian women aged 18 to 34 have fled Ukraine. This will impact Ukrainian demographics for generations to come (Kramer, Holder and Leatherby, 2024).

Lesson Two: Drones will empower violent non-state actors enormously.

Drones are not a new phenomenon for terrorists; a variety of non-state actors, including the Afghan Taliban, Nigeria's Boko Haram, the Yemeni Houthi rebels, and DAESH, have utilized drones in combat. In 2016, French Special Operations Forces in Syria were among the first to encounter small commercial drones repurposed for warfare when attacked by DAESH fighters. By 2017, DAESH had conducted 70 drone missions over a 24-hour period in Syria, using both commercial and homemade drones to pin down Iraqi security forces. In 2016, DAESH terrorists used cheap drones to counter US advances in the city of Raqqa, and Mosul by dropping grenade-sized munitions from the sky and thus making it hard for the local armed forces. The Yemeni Houthis today are able to send drones 200 kilometers away to attack ships in the Red Sea and the Bab al-Mandeb Strait which has tripled the cost of shipping from Asia to Europe.

The conflict in Ukraine has demonstrated to terrorists the potential of drones for ISR (intelligence, surveillance, and reconnaissance) and psychological operations, and how they can be easily deployed with AI capabilities. Ukrainian innovations have shown that drone attacks can be highly precise and effective at long distances. For example, a Houthi drone was able to fly for some 16 hours from Yemen over a distance of more than 2,600 kilometers to strike Tel Aviv in July 2024 (Nevola, 2024).

In Ukraine, innovation has transformed even the cheapest drones into effective guided missiles, both human-operated and AI-guided. Terrorists are discovering that low-cost drones, particularly in swarms, can be highly effective. Although high-tech military drones remain largely beyond the reach of non-state actors, terrorists are mastering the use of civilian drone technology, which is widely available due to the ongoing conflict in Ukraine.

Lesson Three: Non-state actors worldwide who are sharing their expertise.

Drones are increasingly used by non-state actors around the world, with videos of drone attacks and group chats facilitating knowledge sharing among these groups. According to the Centre for Information Resilience, fighters in Myanmar have documented 1,400 online videos of drone flights from October 2021 to June 2023. Drone operators are turning to chat apps like Discord and Telegram to access 3D printing blueprints for fixed-wing drones, get information on tactics and tips on pilot-operator training and learn how to bypass default software on commercial drones to conceal their locations. In both Ukraine and Myanmar, videos of drone strikes are often edited with dramatic music and shared on social media to boost morale (CIR, 39).

In the future, these new weapons could include self-guided drone swarms with computer vision and the lethal power of machine guns that could shoot military personnel. There are already unmanned helicopters with mounted machine guns under development (Mozur and Satariano, 2024). As urban warfare becomes more prevalent, even robotic dogs could be abused by non-state actors to conduct guerilla warfare (Milley and Schmidt, 2024).

Lesson Four: 3D Printing means non-state actors can print whatever they need wherever and whenever they need it.

Due to the widespread availability of off-the-shelf devices, user-friendly software, specialized AI microchips and powerful automation algorithms are now within reach of anyone with a few thousand dollars and strong technical skills. People around the world now have access to the tools necessary to create lethal robots. Although these systems may not match the sophistication of military-grade technologies from major powers like China, Russia, or the United States, the concern lies in the potential for these less expensive systems to be re-designed and developed by terrorists globally with little effort.

Lesson Five: New wars need new strategies and new modus operandi.

Wars are no longer solely determined by the number of jets, ships, or tanks a country can deploy. Instead, the focus is shifting to how these assets are equipped to defend against a surge of drones (Milley and Schmidt, 2024). As Milley and Schmidt suggest, future conflicts will increasingly be influenced by autonomous weapons systems and powerful algorithms (Milley and Schmidt, 2024). Success in future wars will depend on the ability to continually adapt to new technological innovations. This requires what Schmidt terms "innovation power," the capacity to invent, adapt, and deploy new technologies more swiftly than adversaries. Effective strategies at the onset of a conflict involve disrupting the enemy's fighting force, as demonstrated in the early stages of the Russia-Ukraine war. It is also crucial to delay battles through tactics such as using booby-trapped vehicles, suicide bombers, and IEDs, both on the ground and in the air, ideally deployed by drones. According to Deputy Defense Minister Ivan Havryliuk, Ukraine's new Unmanned Systems Forces could potentially lead to the creation of an international coalition dedicated to advancing new generations of autonomous drone technology, which could revolutionize warfare (Kushnir, 2024).

Lesson Six: David and Goliath: New asymmetry in wars.

Terrorists will never achieve the air superiority over a state, given that most nations possess advanced defense systems like Patriot anti-air and anti-missile systems, or MIG aircraft. However, terrorists can still access MANPADS and drones, as seen in the past. The war in Ukraine has demonstrated the significant advantages these drones offer for ISR (intelligence, surveillance, and reconnaissance). International allies' support has made it nearly impossible for Moscow to secure air superiority against a much weaker Ukraine, showcasing the effectiveness of combining various assets, from MANPADS to drones.

Drones have also shifted the dynamics for terrorists. The conflict has highlighted how smaller states can leverage commercial space technologies, unmanned systems, AI, and open-source intelligence to wield considerable power. The spread of these technologies among non-state actors introduces a new asymmetry in warfare, allowing them to conduct lethal attacks from a safe distance and evade counterattacks. This pattern has been evident in past conflicts in Iraq, Afghanistan, and Syria, where IEDs emerged as a highly lethal, low-cost threat to military personnel. In the Russia-Ukraine conflict, drones and unmanned aerial systems (UAS) have proven increasingly effective for targeting and reconnaissance. Drones have become crucial for gathering evidence, enhancing targeting precision, and supporting battlefield operations. The war has also revealed an accelerated pace of conflict and highlighted the global nature of support, showing that assistance can come from beyond national borders.

Lesson Seven: Companies are expanding AI.

Technology is transforming the nature of warfare. The shift toward increasingly autonomous weapons systems has been developing over decades, though the moral discussion has largely remained within the realm of a small group of academics, human rights advocates, and military strategists rather than in broader public discourse.

The growing demand for combat tools that integrate human and machine intelligence has led to substantial investments in companies and government agencies that promise to enhance the efficiency, cost-effectiveness, and speed of warfare. This demand for advanced AI and autonomy has been a boon for tech and defense companies, resulting in large contracts for developing a range of weaponry, including lethal autonomous drones, unmanned fighter jets, and underwater vehicles.

Lesson Eight: The Oppenheimer moment: The AI military race.

The rise of AI-enabled warfare and autonomous weapons systems is being likened to the "Oppenheimer moment," drawing parallels to the creation of the atomic bomb. This comparison represents a pivotal point that could either mark the beginning of a new era of American dominance or serve as a warning of potential catastrophic consequences. The U.S. military is currently involved in over 800 AI-related projects and has requested $1.8 billion in funding for AI in its 2024 budget. As investment in AI rapidly increases, experts caution that these technologies could profoundly change society's relationship with war and technology, potentially leading to greater reliance on machines for critical decision-making. The prospect of autonomous weapons raises fears of a dystopian future reminiscent of apocalyptic fiction. "The substantial investments being made in autonomous weapons and AI targeting systems are deeply troubling," said Catherine Connolly, monitoring and research manager for Stop Killer Robots.

Lesson Nine: The world is becoming increasingly transparent.

The world is becoming more transparent due to advancements in technology. For example, Human Rights Watch uses satellite imagery to document ethnic cleansing in Myanmar. Nanosatellites track vessels engaged in illegal fishing through their identification systems. Amateur sleuths assist Europol in investigating child sexual exploitation by analyzing geographical clues in photos. As the world becomes more transparent, terrorists will have fewer places to hide both in the real and virtual worlds.

Lesson Ten: The importance of regulation of autonomous weapons.

Generative AI will have an enormous impact on global security generating new weapons and modus operandi to malicious actors worldwide. The heightened focus on autonomous weapons systems and AI over the past year has given regulation advocates some optimism that political pressure for international treaties might increase. Despite differing global visions on governance, both the U.S. and China share a concern about preventing terrorists from acquiring autonomous weapons. Advocates point to historical successes, such as the campaign to ban landmines—where Human Rights Watch's Mary Wareham played a prominent role—as evidence that states can indeed reverse their stance on a type of weaponry.

There is significant international support for regulating autonomous weapons, yet major countries including Russia, China, the U.S., Israel, India, South Korea, and Australia are resistant to new laws governing their production and use. Defense companies and their leaders also oppose regulation. For instance, Anduril's founder, Palmer Luckey, has made vague assurances about maintaining a "human in the loop" in the company's technology, while publicly opposing regulations and bans on autonomous weapons. Similarly, Palantir's CEO, Alex Karp, has frequently invoked the Oppenheimer analogy, portraying autonomous weapons and AI as part of a global race for dominance against geopolitical rivals like Russia and China. Experts caution that the lack of regulation is a broader issue, as current international laws struggle to address technological failures or errors in warfare. Regulating these weapons once they are integrated into military forces may then become even more difficult. "Once weapons are embedded into military support structures, it becomes more difficult to give them up, because they're counting on it." As Scharre said. "It's not just a financial investment – states are counting on using it as how they think about their national defense."

References

Balzer, H. (2024). "A Russia Without Russians: Putin's Disastrous Demographics", *Atlantic Council*, August, 2024, https://www.atlanticcouncil.org/content-series/russia-tomorrow/a-russia-without-russians-putins-disastrous-demographics/

Bergengruen, V. (2023). "How Ukraine is Pioneering Ways to Prosecute War Crimes", *Time*, 6.11.2023, How Ukraine is Pioneering New Ways to Prosecute War Crimes | TIME

Borger, J. (2022). "The Drone Operators Who Halted Russian Convoy Headed for Kyiv",*The Guardian.* 28.3.2022, https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv

Carey A., Kostenko M.and Pennington J. (2024). "Ukraine says it hit two Russian naval vessels in major attack on Crimea", CNN 24.3.2024, https://edition.cnn.com/2024/03/24/europe/ukraine-strikes-russian-naval-vessels-sevastopol-intl/index.html

CIS (2024). Centre for Information Resilience (info-res.org)

Conger, K. and Metz, C. (2021). "I Could Solve Most of Your Problems' Eric Schmidt's Pentagon Offensive, *New York Times,* 3.11.2021,'I Could Solve Most of Your Problems': Eric Schmidt's Pentagon Offensive - The New York Times (nytimes.com)

France24 (2024). "France estimates that 150,000 Russian soldiers have been killed in the Russia-Ukraine war", *France24,* 3.5.2024, France estimates that 150,000 Russian soldiers have been killed in the Russia-Ukraine war (france24.com)

Ivshina O., Dale, B. and Brewer, K. (2024). "Russia's meat grinder soldiers 50,000 confirmed dead", *BBC News*, 17.4.2024, https://www.bbc.co.uk/news/world-68819853

Kallenborn, Z. (2024) Swarm Clouds on the Horizon? Exploring the Future of Drone Swarm Proliferation, Modern War Institute, 3.20.2024, https://mwi.westpoint.edu/swarm-clouds-on-the-horizon-exploring-the-future-of-drone-swarm-proliferation/

Kluth, A. (2024). "US drones will create a 'Hellscape' in the Taiwan Strait", *Bloomberg*, 7.7.2024, US Drones Will Create a 'Hellscape' in the Taiwan Strait - Bloomberg

Khurshudyan I., Ilyushina, M., and Khudov, K. (2022)."Russia and Ukraine are fighting the first full-scale drone war", *The Washington Post,* 2.12.2022, Russia and Ukraine are fighting the first full-scale drone war - The Washington Post.

Kramer, A. E., Holder, J., and Leatherby L. (2024)."Can Ukraine Find New Soldiers Without Decimating a Whole Generation", *New York Times,* 11.4.2024, https://www.nytimes.com/interactive/2024/04/11/world/europe/ukraine-demographics.html

Kushnir, N. (2024) "Ukraine focuses on drone warfare, its military creates new Unmanned Systems Forces branch", ABC News, 12.6.2024, As Ukraine focuses on drone warfare, its military creates new Unmanned Systems Forces branch - ABC News

Meier L. and Ferguson, N. (2024) "Why the U.S Military Needs to Imitate Ukraine's Drone Force", *Time,* 13.8.2024, https://time.com/7010426/us-military-drone-force/

Miller, C., Scott, M. and Bender B. (2022) "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground, *Politico,* 8.6.2022, UkraineX: How Elon Musk's space satellites changed the war on the ground – POLITICO

Milley, M. A. and Schmidt E. (2024) "America Isn't Ready for the Wars of the Future", *Foreign Affairs,* September/October 2024, p. 28-32, https://www.foreignaffairs.com/united-states/ai-america-ready-wars-future-ukraine-israel-mark-milley-eric-schmidt

Mozur, P. and Krolik A. (2023) "The Invisible War in Ukraine Being Fought Over Radio Waves", *The New York Times,* 19.11.2023, https://www.nytimes.com/2023/11/19/technology/russia-ukraine-electronic-warfare-drone-signals.html

Mozur, P, Satariano, A. (2024) "AI begins ushering in a New Age of Killer Robots", *New York Times,* 2.7.2024, https://www.nytimes.com/2024/07/02/technology/ukraine-war-ai-weapons.html

Mozur, P. and Satariano, A. (2024), "A.I. Begins Ushering In an Age of Killer Robots", *New York Times,* 2.7.2024, https://www.nytimes.com/2024/07/02/technology/ukraine-war-ai-weapons.html

Nevola, L. (2024). "Six Houthi warfare strategies: How Innovation is shifting the regional balance of Power, ACLED, 6.8.2024, https://acleddata.com/2024/08/06/six-houthi-drone-warfare-strategies-how-innovation-is-shifting-the-regional-balance-of-power/

Paresh, D. and Dastin J. (2022)"Exclusive: Ukraine has started using Clearview AI's facial recognition during war", *Reuters,* 14.3.2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/

Russia-Ukraine War (2022-2024) - Statistics & Facts, Statista, https://www.statista.com/topics/9087/russia-ukraine-war-2022/#topicOverview

Satariano, A. (2022) "Ukrainian Minister Has Turned Digital Tools int Modern Weapons of War, 12.3.2022, Ukrainian Minister Has Turned Digital Tools Into Modern Weapons of War - The New York Times (nytimes.com)

Satariano, A., Reinhard, S., Metz, C., Frenkel, S. and Khurana M. (2023). "Elon Musk's Unmatched Power in the Stars, *New York Times,* 28.7.2023, https://www.nytimes.com/interactive/2023/07/28/business/starlink.html

Sherman, J. (2023). "Drone-on-Drone Combat in Ukraine marks a new era of ariel warfare, *Scientific American,* 3.4.2023, Drone-on-Drone Combat in Ukraine Marks a New Era of Aerial Warfare | Scientific American

Seawanderer (2024)."Ukraine's surface drones sink Russian Black Sea Fleet's Ivanovets missile boat" (2024). Seawanderer, 1.2.2024, https://seawanderer.org/ukraines-surface-drones-sink-russian-black-sea-fleets-ivanovets-missile-boat

Statista (2024)."Total bilateral aid allocations to Ukraine between January 24, 2022 and June 30, 2024, by donor and type (in billion euros, Statista, *https://www.statista.com/statistics/1303432/total-bilateral-aid-to-ukraine/*

Suess, J. (2023)."The First Commercial Space War", RUSI, Featured on 'This Means War' podcast, 19.1.2023, The First Commercial Space War | Royal United Services Institute (rusi.org)

Williams, S. M. (2018). "Swarm Weapons: Demonstrating a Swarm Intelligent Algorithm for Parallel Attack", Technical Report, US Army School for Advanced Military Studies, Fort Leavenworth, USA, May 2018, https://apps.dtic.mil/sti/pdfs/AD1071535.pdf

Zelenskyy, V. (2024), Speech, 6.2.2024, Official Website of President of Ukraine,

I signed a decree initiating the establishment of a separate branch of forces – the Unmanned Systems Forces – address by the President of Ukraine — Official website of the President of Ukraine

CHAPTER 8

THE EFFECTS OF RUSSIA-UKRAINE WAR ON COUNTER-TERRORISM TERRORIST THREATS OUTSIDE OF WARZONE: CLASHING NARRATIVES, FIMI, AND POST-TRUTH

Bernard Siman*

Abstract

The illegal Russian war of aggression against Ukraine (IRWAAU) produced a number of valuable lessons in how terrorism might evolve in the Cognitive Domain, and possible associated kinetic and non-kinetic consequences, and consequently lessons also for counter-terrorism.

In this chapter we will deal with two headline themes in these areas, as well as present at the outset what possible 'enablers might become factors in terrorism. These are the key constituent components that make the transfer of the tools and experiences employed by Russia into the terrorism sphere possible and even make their adoption by terrorists probable. In particular we will highlight the role of Cognitive Warfare (in addition to the use of new, disruptive, technologies).

Cognitive and Information Warfare Can Cause Kinetic Effects

The first area covers the way in which the non-kinetic tools in the Hybrid Threats spectrum, chiefly those of Narratives and Disinformation along with their cyber enabler, can be turned into kinetic terrorist threats both in general terms, but also specifically in Force Protection. Cognitive Warfare and Information Warfare play a key role in this area.

The second area concerns itself with how the combined operations of techno-military capabilities (such as Electro-Magnetic Warfare) with other tools in the Hybrid Threats spectrum (such as the use of cyber space, Disinformation and social media), that have been employed in the IRWAAU theatre against individual soldiers and their families and friends, may end up being used by terrorist organizations. In other words, the well-being of individual deployed soldiers has become a threat factor and an attack vector , undermining morale,

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

cohesion and the public's support back at home for military deployments. They can also have a direct kinetic effect when a non-kinetic combined operation as described above leads to kinetic and violent outcomes, such as when radicalization turns into terrorist behavior. For Counter-Terrorism the key will in all likelihood be to be able to sift through mass data covering radicalized individuals for example to be able to predictively spot signs of change of behavior towards committing terrorist acts.

As alluded to above, these threats are both kinetic as well as non-kinetic, offering the possibility to turn non-kinetic Hybrid Threats, such as Dis/Mis/Malinformation (DDMI), into direct terrorist kinetic threats and violence against specific targets.

This chapter, therefore, aims to highlight a limited number of such developments, emerging from the IRWAAU, as pertains to the possible shifts in the terrorist threat environment in order to draw the necessary lessons for Counter Terrorism in general and how it might evolve, but also in specific areas such as enhanced Force Protection during deployments.

In both of the above-mentioned areas of interest, Cognitive Warfare has been a key driver of the planning and delivery of effect in a targeted, deliberate and dynamic manner (i.e. the mix and match of Hybrid tools over time adjusted as required) to achieve specific objectives. The delivery of effect spans the full range from inducing kinetic terrorist violence by third parties to be inflicted on deployed Forces and Missions (such as radicalizing local populations in the deployment areas with the aim of affecting a change of behavior to execute terrorist acts), to undermining morale and weakening the well-being of soldiers deployed in operations as well that of their families, and further (at the strategic level) to weakening social and political cohesion in society, in pursuit of both kinetic as well as non-kinetic subversive and violent effects and maximizing damage.

Cognitive Warfare in IRWAAU: A Pernicious and Persistent Threat - Lessons for Counter Terrorism

Cognitive warfare has become a constant, persistent and pernicious weapon in the IRWAAU. For terrorists, it is extremely likely (if not indeed is the case already) that its practice and applications will grow in importance exponentially. A parallel and equal level of detailed attention is very likely to accompany such growth and will be required, in the area of Predictive Counter-Terrorism.

Cognitive Warfare concerns itself chiefly with shaping '*how* an adversary thinks', as compared to Information Warfare that mainly focuses on impacting '*what* the adversary' thinks. Cognitive Warfare, therefore, is essential in shaping and manipulating perceptions in the adversary's mind. This impact includes narrative formation and delivery, as well as how to foment conflict in the adversary's society and community (utilizing the social, ethnic, linguistic, cultural, religious, sectarian, economic and other fault lines), and creating alternative realties. "Post-truth" in this area is not simply a matter of general conversational discussion and media quips: it is a sinister and effective tool that is now likely to make its way from how it has been practiced by Russia including in the IRWAAU to other hostile actors, including rogue states and terrorist groups.

A key lesson from the RWAAU is that combinations of Hybrid Tools in the design and delivery of Cognitive Warfare operations can, moreover, create a more sympathetic (or at least empathetic) acceptance by sections of society for a narrative that justifies the execution of violence. In other words, the terrorist narrative that there are legitimate reasons for the conduct of terrorist action starts to gain a certain degree of acceptance in sections of society. It can ultimately undermine counter-terrorism efforts should that sympathetic or empathetic narrative gain momentum in the public discourse. This would be a dangerous evolution, as it will create a more accommodating "hinterland" effect, as well as a larger maneuver space for terrorist action and generating pre- as well as post-attack support.

In this regard, Cognitive Warfare forms a common and dominant underlying denominator and a backbone supporting the use of practically all tools in the Hybrid Warfare & Threats spectrum. This covers both the design of hostile and malign operations, as well as in terms of the delivery of effect, including creating circumstances conducive to providing direct support for terrorist action, as well as supporting their narratives.

It is important to note that Cognitive Warfare employed by a hostile adversary actor can have tactical aims (such as against a particular and specific force, mission or deployment), strategic objectives (such as, over time, undermining public and political support for a policy of military deployments or a particular foreign policy choice); or indeed both, in which a succession of successful tactical cognitive effects can combine to create a strategic advantage in favor of the adversary.

This last combination can alter the terrorist threat environment by creating new longer-term strategic shifts in perceptions through raising the 'Threshold of Tolerance' in a society for terrorist action. These shifts may initially be hard to detect, thus offering better and larger terrorist operating space to hostile actors. 'Raising the threshold of tolerance' gradually over time is a particularly pernicious threat that acts as an enabler in planning and delivering effect in terrorism situations.

Turbo Charging Cognitive Warfare through the Powers of Cyber and A.I.

Weaponizing perceptions is perhaps one of the key take aways that terrorist organizations might have learned from Russia's Cognitive strategies in the Ukraine.

A good example is the evolving landscape of information warfare in the IRWAAU in which AI and social media are combined to deliver malign effect: this may yet prove to be a key emerging terrorist threat. The malign effect may encompass persuasion campaigns against a more active military, political, economic or diplomatic role in a geographic region, creating fear (collectively or targeted at specific individuals), or attempting to affect actual kinetic consequences (physical violence, bodily harm, fatalities) through the use of non-kinetic Hybrid tools (e.g. by inciting violence, harnessing cyber operations to cause physical damage in the physical world, causing financial loss and so on).

The IRWAAU in Cyberspace and in the Cognitive and Information Domains has already expanded beyond its specific and geographically defined theatre of operations to cover not only Europe, but also the Middle East, Africa, Asia and generally in the so called 'Global South'. The 'Cognitive War' conducted by Russia, for example. through cyberspace and by utilizing A.I., through creating narratives and by disseminating disinformation, has aimed to dominate the cognitive domain, to gain cognitive advantage and then superiority and, by doing so, impact the outcome of the war, but also to compensate for its losses in the military field. Terrorist groups' likely take away is that they can compensate for their weaker military capability not only through the adoption of an asymmetric operational armed model and the creation of terrorist networks, but also through manipulating perceptions. This may well become a new front in Counter Terrorism. These terrorist groups have already been engaged in some form of perception manipulation through radicalisation for example, but the Russians have shown that combining disruptive technologies, behavioural patterns and analyses, data and information and other Hybrid and techno-military tools can have a vastly wider and more persistent impact across large swaths of the globe. From the narrow perspective of assessing terrorist action (in other words focusing exclusively on the terrorist action itself rather than the broader politics of a situation) DAESH started, as mentioned above, with successfully applying those lessons in combining Cognitive Warfare with technology and social media. The result was a wave of support across certain parts of the world not just the Middle East, to create an altered reality that justified terrorist action. This is very likely becoming a standard operating procedure for terrorist groups.

The Russian cognitive effort has been reasonably successful across the Middle East and Africa, and in some parts of the Global South. It provided not only a renewed 'favourable' backdrop to the narrative of terrorists, but also created the illusion of an alliance with a great power in a new front that can confront "the west" and win. The war front therefore, from a terrorist's perspective, extends perceptibly beyond the physical lines of confrontation between Russia and Ukraine into those areas where a particular terrorist group operate. They started to see their 'struggle' as forming part of a broader global confrontation against the West, thus not only enhancing their claim to legitimacy among segments of society and the Global South, but also gaining credibility in recruitment and support.

This cognitive evolution was aided by the perception, in many parts of the Global South (and among certain groups in Europe, including far right extremist groups as detected in their online chatgroups), that NATO's withdrawal from Afghanistan was not only chaotic, but that it had proven that the "west" can be defeated by non-conventional "insurgency" irregular forces, employing asymmetric and terrorist tactics and strategies.

This dimension should not be underestimated in creating a more fertile environment for the recruitment of youth (for example in the Middle East and Sahel), and the motivation of would-be terrorists to commit heinous acts of terrorism.

Beyond "Branding" and into Cognitive Warfare

The IRWAAU has been moving the Cognitive Terrorism dials beyond the influence of 'branding' on a limited social and demographic pool, and into a broader global confrontation that is larger geographically as well as demographically (i.e. covering more areas of the world with exponentially more people exposed to the possibility of perception manipulation and alternative realities).

It is useful to briefly analyse DAESH's skilful use of Cognitive Warfare and Strategic Communication tools to deliver the desired effect, from its perspective.

DAESH can perhaps be called the 'Coca Cola' brand of terrorism: if it were a multinational commercial enterprise, it would have achieved similar heights of brand recognition, followers and market penetration through its direct engagement with would be customers, its use of unique symbols, visual impact and mannerisms, and the creation of brand loyalty.

It very effectively combined commercial branding techniques with the anthropological tribal identification markings of a sub-culture: its own music, signages, gestures, dress code and its trademark Hollywood style well-produced videos, with their other trademark theme, extreme violence (using some of the techniques employed in popular video games). In a nutshell, it employed all the effective marketing and Strategic Communications techniques employed by multinationals, across different cultures in the world markets where they operated since the mid-60s in achieving top "branding" and brand loyalty. What DAESH achieved is dominance among its competitors, i.e., the other terrorist groups. It also achieved stronger commitment and loyalty (including brand loyalty) among its potential recruits and followers (customers) by engaging directly with them, mostly on one-on-one basis, and by understanding their motivation. We identified six motivations: moral, idealistic, political, religious, romantic, and idealist. To engage with a moralist on the basis of political motivation is a losing preposition. That means that DAESH their "customers" extremely well and at an individual level. Their primary goal, from a Cognitive perspective, seems to have been to cause direct and maximum terrorist damage by primarily influencing a global pool of potential recruits, supporters and followers, and to instil fear globally (as well as in the areas they controlled).

This means that DAESH invested heavily in gaining cognitive advantage, defining narratives, and in intrusive perception formation, all of which rely heavily on access to data and information, intrusive and thorough surveillance, as well as persuasion and coercion. To make this process more efficient online they employed self-identification (i.e. searching for those individuals who click searching for relevant topics) to identify potential recruits and supporters so that they would then use a real human to engage with the target.

The IRWAAU pushed this approach further and in immeasurably more efficient ways through the use and timely application of new and disruptive technologies. What the terrorists are learning is to combine technology, human behavior, Hybrid Threat tools, Cognitive and information warfare tools to design and deliver effect. AI-enabled bots can not only identify profiles online of would-be supporters and recruits without the need for an expensive and difficult to find skilled human resource, but can also engage directly with targets on the basis of the motivation as identified from chats and online profiles (based for example on one of the six motivations mentioned above).

Such automated human-like engagement by bots clearly enhances the efficiency in terms of numbers and sustained 24/7 engagement with the target, a feat not possible if a human terrorist acts as a recruiter or "radicaliser" for example. It is also clear that the motivational aspects of engagement online that are based on "clicking" are shifting to creating an emotional dependency element by the human on the bot. The key question from a Cognitive superiority perspective is "who seeks confirmation and approval from whom?". It is likely that in some cases the human will, over time, seek approval from the bot. This is already opening the door for the evolution of the terrorist branding effort to move to this higher level of cognitive effect particularly as terrorists and rouge states, such as Iran, interact with rogue cyber and AI syndicates emerging from the IRWAAU.

This direct "cross-fertilisation" between groups operating in the shadows of the IRWAAU acting as guns for hire on the one hand, and rogue states and terrorist groups on the other, is perhaps one of the key developments and impacts in the area of both Cognitive Warfare as well as terrorism that has emerged from the IRWAAU.

An actual operational example may be useful and instructive. Russian-speaking Ukraine volunteers are using AI-generated synthetic data images of females to be put on Russian dating websites to engage with Russian soldiers deployed on the various fronts. This is yielding tremendous real time intelligence such as locations, state of morale, provisions, and so on. This is relatively cheap, quick to deploy with quick results. It can clearly have kinetic as well as non-kinetic effects. It is only a matter of time before terrorists will upgrade their Cognitive operations, that were so central to DAESH's early successes, from branding and human-based engagement activities, to automated operations utilizing Deepfakes and synthetic data to achieve a higher level of Cognitive Warfare performance.

Counter-terrorism thinking and practice must evolve to recognize that this new threat environment requires operating across silos, with a better understanding of how terrorists can potentially combine different instruments in the Hybris Threat spectrum to design and deliver effect.

Common Authoritarian Culture with Russia: Key Factors

The reason that terrorist organizations succeed in legitimizing their authoritarian culture internally, and thus are generally able to successfully adopt Russian Hybrid Threats tools, is that they basically share a common authoritarian culture with Russia. The utilization of technological, data and digital tools in the pursuit of terrorist aims thus becomes a matter of practical planning and delivery, rather than an ideological or moral dilemma that would have otherwise played a role in distracting and weakening these organizations. Essentially these terrorist organizations and networks are not only authoritarian; they are also revisionist, many of them backed by authoritarian rogue states. They, therefore, are able to combine their (sub)cultures, with advanced technological and digital tools, utilizing speed of dissemination of data, physical operations and human behavior, and invading the private digital spaces of individuals and organizations, thus putting such operations in the service of either targeted or indiscriminate terrorist acts. This affirmation of a basic common cultural understanding with Russia has enhanced their view of themselves as not being isolated, and as being part of a bigger front combating the West.

FIMI as a Security Threat, Not Just a Communication Challenge

The EU has identified Foreign Information Manipulation and Influence (FIMI) as a key hybrid threat.

> "A mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors including their proxies inside and outside of their own territory."

This is akin to an umbrella description of disinformation, mal-information and other forms of malign operation in both the information and cognitive domains.

Disinformation is "the creation, presentation and dissemination of verifiably false or misleading information for the purposes of economic gain or intentionally deceiving the public."

Misinformation is unintentionally doing so, whilst mal-information entails deliberately designing and employing dis- and mis-information to cause harm to specific individuals and organizations. It is easy, therefore, to see why FIMI has largely been viewed as a communications threat in the first instance, undermining the soft cornerstones of democratic order, such as trust, legitimacy, and cohesion.

While this is an accurate description and diagnosis in a broad sense, it does not deal with FIMI as a security threat with consequences on the ground (such as civil disorder and terrorism). These consequences include increased radicalization, recruitment of terrorists, and incitement to attack. Examples include accusing Western soldiers in the Sahel of abusing the local population. In one case, false photographs were published in Sahel countries purporting to depict a destroyed village due to French Air Force activities. This was deliberate disinformation aimed at rejecting French forces presence, encouraging terrorist recruitment and inciting terrorist attacks. Russia-linked websites and social media outlets both in Africa and in Europe were and are the key propagators of such FIMI.

As such, FIMI poses a narrower, more focused and direct military and mission security dimension in the area of Force Protection and military operations, including against civilian missions. The examples of deepfake photos, videos or audio falsely depicting for example UN peacekeepers, EU or NATO mission personnel torturing or abusing locals, can have the consequence of increasing the radicalization and recruitment of terrorists locally on the one hand, but also creating a backlash in public opinion back home in the sending countries against deploying troops overseas, on the other.

Russia's experience in Africa was honed and ultimately became transferable to the battlefields of Ukraine and beyond into Europe, as well as the so called "Global South". Russia used Dis-mis-mal information in the form of social media, Deepfakes and printed and visual media to disseminate the Russia narrative on the war, such as the war being waged by the whole of NATO against Russia and that this is essentially an imperialist and Neo-Colonial pattern of geopolitical behavior.

There is a strong relationship, and continuity, between Russia's development and use of FIMI and other Hybrid Threat tools in Africa, and its FIMI operations in the war against Ukraine. The FIMI operations since the IRWAAU did not just target Ukraine or the Ukraine military in theatre. In fact, they aimed at influencing the public's perception across Europe as well the US, at times linking Russia's cause with that of the confrontation of Iran with the west, supporting to varying degrees of clarity acts of terrorism in the Middle East conflict, thus in effect encouraging the sort of evolution of radicalization that can lead to terrorist action on the European mainland. This approach places the terrorist organization's agenda, narrative, and terrorist acts in a broader context, that of the narrative falsely propagating that there is a wider confrontation between the neo-colonial expansionist West against 'the rest'.

A great deal of emphasis in Russia's narrative post-Ukraine has played on its past close and friendly Soviet ties with the Global South, during the phase of the post-colonial liberation movements, to create a new (false) reality that Russia's current geopolitical posture is a reflection of past Soviet anti-colonial anti west support. It aims to create the perception that equates past post-colonial liberation movements' struggles for independence with the current crop of terrorist organizations.

This broader international context, as presented by the Russian narrative, has been a welcome additional breathing space for terrorists and non-state actors designated as terror organizations. They have presented the Russian narrative as evidence that their aims and acts are not 'loony', 'deranged', 'criminal', 'terrorist' or stand alone; rather that they are an integral part of the broader global struggle against western dominance, ideals and values. This has naturally been an unwelcome extra 'oxygen' to terrorist organizations and would be lone terrorists.

Counter-terrorism work and counter DDMI efforts have to be more closely coordinated, utilizing a broader set of tools in their technical conduct of operations that should incorporate the broader geopolitical dynamics. This is particularly the case in dealing predictively with counter-terrorism, as an added tool in the toolbox of Counter-terrorism.

Clearly, Russia's use of FIMI is not just a communication challenge that needs to be resolved by correcting the record on cold facts, or by addressing the communication issues in a general manner. It is a larger, pernicious and longer-term security threat including in the area of force protection and mission safety against terrorist attacks.

A related strategic threat resulting from FIMI involves undermining public and political support in the countries that participate in sending personnel on these missions, duly undermining their commitment or continuity.

It is, therefore, critical that Strategic Communication should become an integral and more important component of planning UN, EU and NATO deployments and Force Protection well beyond straight-forward tactical 'cultural' and classic tools of the 'communications functions', moving to the more complex and sophisticated realm of formulating and disseminating narratives.

Micro-Targeting and the Well-Being of Individuals: Terrorists may see Micro-targeted Acts as a Lesson from Russia's Playbook

A key lesson to terrorists from the Hybrid Russian operations in the Ukraine theatre is that there are many ways to skin a cat. In other words, blowing things up and random acts of terrorism can be augmented with more intelligent, harder to detect, and effective forms of integrated Hybrid operations that can combine lethal force with technology.

Since the IRWAAU started, Russia targeted the well-being of individual soldiers, including with fatal kinetic effect, as well as their family and friends through integrated operations. These operations combine utilizing geo-location tools to locate soldiers in theatre utilizing their mobile devices, subsequently kinetically targeting those soldiers, then producing a video clip of the event, and finally disseminating the video to the contact list extracted from the individual soldiers' mobile devices utilizing electro-magnetic warfare tools.

The lessons for terrorists, particularly well-funded and state-backed terror groups, is that combined operations utilising a cocktail of electro-magnetic capabilities, kinetic effect, social media and the possible doctoring of video and audio clips through creating AI-enabled Deepfakes, can be very rewarding. Counter terrorism thinking will need, therefore, to move beyond its classic modus operandi to contemplate the possibilities in civilian and urban contexts of random or targeted acts of terrorism mirroring to varying degrees what Russia has employed in the Ukraine theatre. AI-enabled DeepFakes can be used to augment and enhance effect.

Fake news, as well as deepfakes, have been exploited in the IRWAAU, by both state and non-state actors, to attack the well-being (physical, mental and emotional) and safety of individuals in the field, as well as their families back in their home countries. This might have also been inspired by the experience of Russia in Africa. An AI-generated deepfake video circulated widely just days after the military junta in Burkina Faso ordered French troops to leave the country following the successful coup in 2023. The video urged support for the junta and its leader. A similar video targeting the presence of French troops circulated widely in Mali around the same time. DeepFakes of soldiers "committing (fictitious) acts were sent to their family members back home, undermining marital relationships, community support and friendships thus affecting morale in theatre. Less worryingly are the “cheap fakes” that are on the other end of the technical specifications spectrum from AI-enabled deepfakes. Cheap fakes are quicker and require much less resources. Although less realistic than Deepfakes, fast social media distribution makes them reasonably effective. Cheap fakes generally alter videos and audios to manipulate perceptions of specific events.

This form of FIMI, in which AI-enabled deepfakes utilize synthetic data coupled with microtargeting, is very likely to be an attractive area of operations for terrorists as a Hybrid Threats tool in the context of individuals participating in overseas missions, as well as for terrorists acting in the west to undermine confidence in the political system, and to deliver non-kinetic terrorist effect.

Moreover, a key aim of FIMIs is to whip up resentment against the mission and the individual participants both in the recipient and in the Troop Contributing Countries. This latter objective can undermine the physical security of the individuals and their missions as local populations become enraged by fake news and deepfakes. Moreover, the public and political sentiment in the home countries of the individuals participating in the missions can turn hostile against the individuals, their families, and the missions, including in the local communities where the individuals reside and their families live. At the conference on “75 years of UN peacekeeping: how can UN peacekeeping missions tackle the challenge of disinformation?” at the Egmont Institute (June 2024), it became clear from the various contributions that such activities further undermine the safety and mental well-being of the individuals and their families, as well as budgets, recruitment and support for participation in future missions.

Deepfakes, Social Media and Technical Skills as Tools of Terrorism

Deepfakes are video and audio clips that depict individuals doing and saying things they never did or said, or situations that never took place. They were already being deployed even when the technology and software required actual human actors and considerable time.

As technology has rapidly developed, the time, cost, and technical skills required to produce convincing Deepfakes have exponentially shrunk. This makes deepfakes more accessible, including the individual terrorist spending time online in their homes.

With the emergence of AI, however, AI-enabled deepfakes, utilising totally newly created synthetic images, are likely to become a key security threat in the hands of malign actors operating in the hybrid domain. This is mainly because Deepfakes can currently be produced using completely synthetic data: the faces of people who never existed speaking with voices that never existed in all existing languages and dialects, or utilizing cloned voices, doing and saying things they never did. Cloning actual voices of specific individuals is now quite straightforward requiring roughly 30 seconds of the actual voice to create a very hard to detect clone. The potential for abuse of such capability is not hard to imagine. These are all technological add-ons to the key lessons terrorists may extract from Russia's operations in Ukraine: that integrated physical, technical and social media/cyber/AI operations can produce the damaging effects, particularly given that, in principle, they can have higher frequency of occurrence.

A multi-modal operation has the potential to be both cheap and effective. For example, a deepfake depicting mission personnel torturing a local individual can be combined with social and traditional media campaigns. The dissemination of this deepfake can also target the deployed individual's family and friends back home. The deepfake could then cross into the digital sphere, leading to diverse repercussions. These range from security threats related to force protection because of an outraged local population, to concerns about the physical safety of the individuals involved and that of their families. There is also the risk of psychological and mental strain on the families, potentially leading to social ostracisation in their home communities, for example. A snowball effect of incremental tactical security threats can lead to broader malign strategic threats, such as undermining political support for continuing a particular operation, and the creation of new social and political fault lines in a community.

Quo Vadis Counter Terrorism?

Whereas facts play a key role in the Information Domain, the battle in the Cognitive Domain involves emotions as much as it does facts. Narratives also play a crucial role in shaping perceptions. Yet efforts to counter (adversary) emotive narratives and those aimed at shaping perceptions using cold facts only have not yielded the desired results.

Achieving Cognitive dominance is one of the decisive aims of modern non-conventional military operations as well as 'Political Warfare', simultaneously using information and cyber warfare. Operationally, these Cognitive operations rely on access to and extraction of data and information, technical surveillance, persuasion and/or coercion, as well as new and disruptive technologies as outlined above. The battle to achieve Cognitive Dominance is not a new invention. However, cyber and disruptive technologies have turbo-charged operations and possibilities in the Cognitive Domain affecting all activities in society, politics and the economy.

Russia had been fully deploying Cognitive tools, well before the IRWAAU, but particularly since the war started. This presents rich pickings for the evolution of terrorist strategies, tactics, ways, means and methods. It is essential, therefore, for counter-terrorism thinking, to evolve by understanding and incorporating the broad field of Hybrid Threats in a sophisticated, inter-disciplinary and across the bureaucratic silos.

This is particularly true when employing pre-emptive and predictive counter-terrorism strategies and methods. What makes this rising area particularly critical is the emerging phenomenon of what can be called 'Democratization of Influence'. One may speculate that this approach was at least partially inspired by the Russian tactics in Africa and Ukraine.

Digitalization and its use by the public and the economy has democratized information and data access. However, Cyberspace as an unlimited and boundless space has also undermined the sovereignty of the state, by damaging the state's monopoly on physical power with new forms of violence. Malign actors are able to influence almost every target audience by setting, undermining, or enabling certain narratives. AI-bot-enabled microtargeting will turbo charge this ability, as will combining techno-military tools with disruptive technologies and social and digital media. Russia has been a very active practitioner of Hybrid Warfare well before the IRWAAU whether in the "west", or more clearly in Africa. It is likely that that terrorist groups have learned many lessons from the Russia playbook- first of which is combining tools to deliver maximum damage.

At a strategic level, the key challenge for the western democracies will be how to counter such malign threats without undermining their core democratic values as they face a totally new wave of terrorist challenges that will push the balance of security, privacy, rule of law, human rights and the right to free speech to their absolute limits in areas of the law and the constitutions that were designed for an age that had naturally inbuilt limitations of geography or by law.

Developing an Emotive Narrative Key for Defeating FIMI

A key long-term step in preventatively countering FIMI is to stop relying on cold facts alone to defeat and counter emotively formulated FIMI. This became clear during the war against ISIL/DAESH. Counter-radicalization efforts focused on highlighting factual defects in what DAESH was offering. In fact, the motivation for many would-be recruits to ISIL/DAESH's cause was driven by emotive, idealist, or romantic motivations, or a mixture of the three drivers. These drivers could not be effectively countered by restating cold objective facts without their emotive context.

Europe and the West, in general, have targeted minds for far too long by using blunt facts and, perhaps more often than not, by ignoring hearts. Europe, in particular, needs to deploy a positive emotive narrative and reclaim dominance in the cognitive domain. It has a great story to tell – but facts alone will not win hearts in many regions of the world where missions are deployed. There is currently a sufficiently large space that is being filled with hostile narratives. It is essential to re-occupy this space in the information and cognitive domains through content development and dissemination, which should become an integral part of mission planning.

Disinformation is not just a Communications challenge, It is a Force Protection Threat

FIMI operations have been largely viewed as a communications' threat undermining the soft cornerstones of the democratic order, e.g. trust, legitimacy and cohesion. This is an accurate description and diagnosis in a broad sense. There is, however, a more narrow, focused, and direct military security dimension. FIMI poses a malign, dangerous, and direct security threat to UN and EU missions overseas potentially leading to lethal outcomes. It is in effect a force protection threat during deployments, whether civilian, military or in peacekeeping operations. FIMI is the umbrella description for disinformation, misinformation, malinformation and other form of malign operation in both the information and cognitive domains. FIMI can also undermine public and political support in the countries that participate in sending personnel for these missions, thus undermining the commencement or continuity of such missions.

Wellbeing of Individuals is the Other Face of Maintaining Political Support

A variety of Hybrid tools, such as fake news as well as Deepfakes, are deployed to attack the wellbeing (and possibly the physical safety) of individuals in the field, as well as their families. This can affect the psychological and mental wellbeing of the individual's and their families. Moreover, a key aim of FIMIs is to whip up resentment against the mission and the individuals participating in these missions, both in the recipient as well as the Trrop Contributing Countries. This latter objective can lead to undermining the physical security of the individuals and their missions as local populations become enraged by fake news and Deepfakes. Moreover, the public and political sentiment in the home (sending) countries of the individuals participating in the missions can turn hostile against the individuals, their families, and the missions. This not only further undermines the safety and mental wellbeing of the individuals and their families, but also budgets, recruitment and participation in future missions.

DeepFakes are video and audio clips that depict individuals doing and saying things they never did or said. They were already deployed even when the technology and software required g actors and a great deal of time. As technology rapidly developed, the factors of time, cost, and technical skills required to produce convincing Deepfakes have been shrinking exponentially. This is making DeepFakes more accessible. With the advent of A.I., however, A.I.-enabled DeepFakes are likely to become a key security threat in the hands of malign actors operating in the Hybrid domain. This is mainly the case as DeepFakes currently can be produced using completely synthetic data- the faces of people who never existed speaking with voices that never existed doing things they never did. Combining, for example, a DeepFake depicting mission personnel torturing a local individual, with a social media campaign spreading this Deepfake, including targeting the deployed individual's family and friends back home, and crossing then into the digital and other media, can lead to wide ranging consequences: from security threats related to force protection because of an outraged local population, to the physical security of the individuals concerned and that of their families, to the latter's psychological and mental wellbeing (through for example social ostracization in their home communities). A snowball effect of incremental tactical security threats can lead to broader malign strategic threats, such as undermining political support for continuing a particular operation, or budgetary cuts.

Developing an Emotive Narrative Key to Defeating FIMI

A key longer-term step is to stop relying on facts alone to defeat and counter emotively formulated FIMI. We have targeted the minds for far too long using blunt facts, and perhaps more often than not ignored the hearts. We need to deploy our own positive emotive narrative and reclaim dominance in the cognitive domain. We have a great story to tell- but facts alone will not win us the hearts in many regions of the world where we have been deploying missions. A strategic communications approach should be structurally incorporated into the Global Gateway, not as an exercise in “communications”, but as an integral part of the strategic objectives underpinning values and interests.

CHAPTER 9

IMPLICATIONS OF THE UKRAINIAN WAR ON WORLD ORDER AND THE FUTURE OF COUNTER-TERRORISM

Nicolas Stockhammer[*]

Abstract

The Russian offensive war in Ukraine has far-reaching implications for global affairs, potentially reshaping the international security architecture and influencing NATO's counter-terrorism efforts. Against the backdrop of these developments, this analysis examines the war's overall impact on the geopolitical and the evolving terrorist threat landscape, and the necessary adaptations in Western counter-terrorism strategies. The conflict has created opportunities for terrorist groups, particularly ISKP, to exploit security vacuums and acquire advanced weaponry. Key trends emerging from this context include the persistence of low-level terrorism, the growing exploitation of the digital "value chain" by terrorist organizations, and the potential proliferation of arms. These and other developments suggest a selective reevaluation of NATO's counter-terrorism approach.

1. Impact on International Order

The Russian offensive war in Ukraine certainly has a wide-ranging impact on global affairs, potentially resulting in significant tectonic shifts concerning the international security architecture (Kotoulas/Pusztai 2022). Propelled by dynamics and changes within the international arena on both sides the violent conflict simultaneously exerts its own influence on that playground.

As this violent conflict unfolds, it will continue to mold the future geopolitical landscape, particularly in terms of security policy dynamics. Interestingly Gao Jian, a Chinese scholar, while traditionally advocating official Chinese government positions and propaganda, called the Russian invasion of Ukraine and the ongoing battle there rightly a '*touchstone for great power politics*' and even more a '*catalyst for* (a) *new international order*'. (Jian 2024). The ongoing erosion of the unipolar power order and the associated system of rules

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

must be considered in an analysis of geopolitical conditions that shape the current war in Ukraine. Globally relevant spheres of influence are gradually emerging, which are managed autonomously by regional hegemons, i.e., according to their own ideas of power and interests. In this context, the distinguished German political scientist Herfried Münkler refers in the last chapter of his recent book '*Welt in Aufruhr*' (best translated as '*world in turmoil*') to a '*multipolar constellation of five global players*' - a global *pentarchy*, that includes - with different relative power resources and ambitions - the United States, China, Russia, Europe and as emerging hegemon India (Münkler 2023: 401-457).

Münkler further argues that power is more or less condensed in the center of the regional influence spheres (Münkler 2023). Great Powers in consolidation like the US or Europe tend to be predominantly interested in maintaining their competitive position in the Great Game, rising powers (China, India) focus on themselves and want – at least for the time being– to remain unaffected by international confrontation. In contrast, declining revisionist powers such as Russia may be tempted to strive for power expansion rooted in the intent to rewrite history. Substantially this culminates in a '*war of narratives*' (Harper /van der Vugt 2024). Given this kind of ideological confrontation, the emphasis lies clearly more on the narrative dimension than the mere factual details. The Russian narrative, an eclectic self-portrait, is characterized by a complex and ambivalent self-assurance, which is expressed through the construction of a Russian identity both in differentiation from and connection with Europe. In its excessive Great Power ambitions Moscow perceives itself as Slavic 'Third Rome' (Poe 2001). This narrative is also supported by the idea of a 'Russian world' (*russki mir*) and a Eurasian mission that is distinct from Western values and represents an alternative, spiritual and anti-materialist vision. Most prominently has Alexander Dugin, the notorious illiberal right-wing philosopher of the Kremlin articulated this anti-Western Russian culturalism (Umland 2023).

However, recent events, particularly the Ukrainian War and other- comparably minor- military interventions by Russia, have led to these imperial claims to a global political role being called into question. The Russian government under Vladimir Putin is now in conflict with the West and other neighboring states. With its expansionist imperialistic narrative and its brutal practice of subjugation, Moscow has become a serious threat for Western security interests. American diplomat Geoffrey Pyatt called the Russian annexation of Crimea in 2014 "*the most naked manifestation of his* (Putin's) *revisionist agenda*" and he coined the term "*Putinism*" for it (Sciutto 2024: 140). It describes President Putin's strategy to establish political *faits accomplis* by exerting brute military force and a constant provocation of the West and NATO in particular.

As former judoka, Putin is tempted to utilizing '*juji*', a martial arts tactic where the opponent's force is directed against them. Such approach involves sensing the opponent's movements and using precise timing and positioning to exploit their momentum. By subtly guiding the opponent's force in a different direction, the skilled judoka can unbalance them and create openings for counterattacks or throws. This approach emphasizes efficiency and adaptability, allowing the apt martial arts fighter to overcome stronger opponents through skillful manipulation of physics and leverage. A fundamental principle in Kano Jigoro's (the founder of Judo) philosophy was *'seiryoku zenyo'* which emphasizes maximizing efficiency by utilizing available resources to their fullest extent (Patrick 2022). Putin, who is said to bluntly admire Jigoro, allegedly has a bust of him on his desk. Given the most recent efforts of Putin's, we may well assume that he has become a *ronin* instead of a *samurai*. A *ronin* ('drifter') was a former samurai warrior in feudal Japan who, often due to the loss of their master or some other dishonor, became a masterless and wandering individual. They typically sought employment or redemption through various means, sometimes becoming mercenaries. Putin has in the past years turned into a geopolitical drifter oscillating between the boundaries of the possible.

If Ukraine were to suffer defeat either militarily or politically in the 'war of narratives', this could fuel President Putin's confidence to target other states, such as Estonia or Moldova, which he has already shown interest in (Sciutto 2024: 125). Additionally, such attempts might prompt China's Xi Jinping to pursue a military resolution to the 'Taiwan question', a move that some observers fear could escalate into a global conflict.

This altogether should remind us that Great Power interests are at the core of the Russian war of attrition in Ukraine. The Transatlantic community for good reasons aims at preserving Ukrainian sovereignty, whereas a revisionist Russia is seeking to subjugate and fully control Ukraine (Watling /Reynolds 2024). The Kremlin continuously attempts to drag China and other global players such as Iran on its side or even into its theatre of war, while asking for direct (military) support. Any kind of potential fully-fledged trilateral engagement of a '*rogue coalition*' (Russia-China-Iran), however doubted by experts, would probably pursue to undermine, "*disrupt and challenge the U.S.-led international rules-based order*" (Winter et al. 2024).

The war's impact stems from its nature as an alleged proxy conflict- at least on the intellectual and political battlefield- and the complex network of both declared and undisclosed strategic alliances among the involved parties, many of which operate behind the scenes. Russian cross-domain warfare includes prototypical hybrid measures and draws from a customized toolkit of disinformation (*deception, distraction and paralysis*), power pressure (*provocation and deterrence*) and exhaustion – refer to Clausewitz: "*Ermattung*" (Marahrens 2023). Besides wide-ranging disinformation campaigns against the West, Moscow has rolled out cyber-attacks and likely conducted unattributed or denied attacks on pipelines and critical infrastructures all over Europe (Marahrens 2023). Commonly attributed to the infamous 'Gerasimov Doctrine', named after Russian General Valery Gerasimov, the use of non-military means to achieve strategic objectives, has become a strategic trademark of Russian warfare (Bilban/Grininger et al. 2019). While it emphasizes the integration of political, economic, informational, and military tools to achieve desired military-strategic or political outcomes, in some constellations it even contributes to blurring the lines between war and peace. This approach has in the past two years for a good reason been associated with Russia's offensive war in Ukraine and its continuing efforts to influence elections and public opinion in other countries. The guiding playbook behind all that seemingly follows the overarching and holistic Russian concept of strategic deterrence ('*strategicheskoe sderzhivanie'*) (Ven Bruusgaard 2016: 9). A constant propensity of military violence and readiness for escalation, even war on other fronts, is a significant deterrent threat, that Moscow uses for intimidation purposes. The Kremlin's hybrid warfare is usually accompanied by a nuclear deterrence component – covert or openly manifested (Luxmoore 2024; Wachs 2022).

On the larger, grand-strategy scale, Russia embraces China and is constantly seeking to expand a dragon-bear axis in opposition to the West (Tchakarova 2020). Despite Chinese concerns regarding Russia's actions and effectiveness in waging the war Ukraine, both autocratic regimes maintain a basic alignment in their shared criticism of the neoliberal international order. China has largely embraced Russia's narrative on the conflict, depicting it as a proxy struggle between the West and Russia, wherein Russia's actions are framed as a "*legitimate response to an existential threat*" (Wilson 2023).

The notion of a 'New Cold War' may be in essence right, but it should not oversee the complex interactions and dynamics of such a multipolar world order (Niblett 2024). Substantially, Taiwan could be regarded as the elephant in the room, but the war in Ukraine and its further pathway will entail a strong leverage on this bipolar confrontation between the US and China in a confrontative multipolar setting. Niblett refers to a geopolitical contest that is "*far less binary*" because of the direct or indirect involvement of so many other great and middle powers, such as Russia, India, Japan, Saudi Arabia, Iran and Brazil.

Players possibly seeking confrontation with the West could profit from the current developments and might in/directly engage in/or support activities that could become a substantial security challenge for Western CT ambitions and even more so for NATO partners. Such a development will by nature also affect the trajectory of terrorism as a phenomenon.

The EU's anti-terrorism coordinator Bartjan Wegter presently identifies a more diffuse extremist threat, particularly in its Salafi-radicalist specification, coming from many different directions and spreading online, something he refers to as "*mutant jihadism*". (France 24 / 2024). This should be understood within the framework of the emergence of ISIL/DAESH offshoot ISKP ('Islamic State – Khorasan Province') is empowering its terrorist propaganda and radicalization in Western societies. The Kremlin has more or less taken sides against Israel, as Putin provocatively hosted representatives of Hamas in Moscow after the militant attack against Israel (Haseldine 2023) As a result of the war in Ukraine, Russia's relations with Iran have become a strategic alliance. Given the importance of this coalition, Moscow has pursued a policy that is sympathetic to Iran's allies, including Hamas. Russia may therefore support pro–Palestinian / pro–Hamas riots or even violence in the West. Moreover, Hamas has declared transnational ambitions and is inclined to expand its campaign against the West (Benoit 2023). Salafi radicals, both organizations as well as micro-structures are seeking advantage from growing polarization and online radicalization, that is the outcome of prevailing conflicts.

But not only Salafi radicals. Right–wing extremists are likewise profiteers of excessive extremist propaganda and societal divisions, with Russia selectively supporting far–right populist movements and associated extremist structures (Rekawek/Renard/Molas 2024). The current dynamic will impact the terrorist landscape and the resulting necessities of counter-terrorism.

2. The Emergence of ISKP in the Russian Context

Without doubt Central Asia is yet another territory of strategic interest for Russia. IS-Khorasan Province (ISKP), a notable Afghan rooted branch of the ISIL/DAESH, operates across regions spanning Afghanistan, Pakistan, Iran, and Central Asia. While the core organization of DAESH experienced significant military setbacks in Syria and Iraq by 2018/2019, the strength of ISKP has surged notably since 2021 (Stockhammer/Clarke 2024). Some analysts consider this regional affiliate to be among the most formidable radical groups globally, boasting a membership estimated to exceed 10,000 individuals (Steinberg / Albrecht 2022). Despite its opposition to the Taliban and al-Qaeda, ISKP shares a common political objective with al-Qaeda: the establishment of 'a so-called unified Islamic caliphate'. Until mid-2021, ISKP faced substantial weakening due to robust counter-terrorism efforts, Taliban offensives, and internal strife. However, the withdrawal of Western coalition forces has facilitated its resurgence (Wilson Center 2021). Following the US military departure in August 2021 and the Taliban's rise to power in Afghanistan, hostility between them and ISKP has intensified (Ahmadzai 2022). The separatists assert their sole legitimacy in establishing a so-called Islamic state and caliphate, demanding Taliban submission. Yet, the Afghan Taliban leadership remains steadfast in rejecting this demand. Regardless, ISKP has managed to carry out sporadic attacks in Afghanistan in recent times (Kozlov/Rynda 2021). In defiance of vast preventive security measures, the ISKP marked a significant milestone in August 2021 when it perpetrated a devastating terrorist attack at Kabul airport, resulting in over 180 casualties, including 13 US soldiers, and nearly as many injuries in a suicide bombing (Bertrand / Liebermann /Atwood 2023). Despite specific intelligence warnings beforehand, the ISKP managed to execute this large-scale terrorist operation in plain sight of the world (Deutsche Welle 8/2021). In late December 2023, it came to light that a small group of ISKP terrorists from Central Asia, who were living in and around Germany, had plotted terrorist attacks on symbolic Catholic churches in at least three major European cities during the Advent season. (Schmitt 2024). The suspected targets reportedly included the Cologne Cathedral, the St. Stephen's Cathedral in Vienna, and unidentified churches in Madrid (Parth 2023).

This foiled plot has been followed by several other high-profile attacks, such as the assault earlier in the year at a funeral service in Kerman, Iran, where ISKP affiliated attackers killed almost 90 people in a suicide bombing, despite tight security measures following the US drone strike that killed the deceased, Iranian General Qasem Suleimani (Hafezi/Elwelly/Tanios 2024). Subsequently, in January 2024, terrorists from Central Asia targeted a church in Istanbul, resulting in one fatality (Shahbazov 2024). Moreover, since the Quran burnings in the Netherlands and Sweden, the ISKP has also threatened attacks in these countries (Lister 2024).

The most recent large-scale terrorist attack occurred in Moscow on March 22, 2024, revealing the ISKP's capability to orchestrate meticulously planned terror scenarios with multiple perpetrators. The synchronized attack at Crocus City Hall bore striking similarities to the Paris Bataclan attack in November 2015, indicating a meticulously orchestrated and tactically disciplined terrorist operation. Notably, individuals with a Central Asian background, predominantly Tajiks, are suspected of playing key roles in most of these attacks, with Tajikistan serving as a preferred recruiting ground for the ISKP (Burke 2024). In a first reaction the Kremlin claimed Ukraine was responsible for the attacks (Melkozerova 2024).

In response to the Moscow attack, a court ordered that four suspects - aged 19, 25, 30, and 32, all from Tajikistan - be held in custody until trial, facing potential life sentences if convicted. Of specific relevance is the health condition of the suspects: Dalerdzhon Mirzoyev, Shamsidin Fariduni, and Saidakrami Rachabalizoda appeared reasonably stable despite signs of torture, while Muhammadsobir Fayzov, seriously injured during arrest and interrogation, appeared in court in a wheelchair and initially refused to plead guilty (Sauer 2024).

The public dissemination of video footage and images depicting the torture of detained individuals, including acts such as electric shocks, severe beatings, and even mutilation, raises profound ethical and legal concerns. The use of such imagery for internal purposes suggests that Russian security services may aim to instill a deterrent effect by showcasing toughness and unwavering resolve in countering terrorism, possibly intending to shape public opinion positively. Many observers have questioned why Russia, often falsely perceived as an atypical terrorist target, has become a focus of recent ISKP attention (Vision of Humanity 2024). This shift may transcend mere ideological or geographic factors, possibly rooted in military and strategic considerations. Russia's historical involvement in combating ISIL/DAESH and other terrorist organizations while advocating its own strategic interests, both through military intervention in Syria and diplomatic initiatives in Central Asia and the broader Middle East, has placed it in a prominent position. By actively supporting the Assad regime and confronting terrorist forces in Syria, Russia has positioned itself as a direct target for retaliation by Salafi groups (Lister 2024). The involvement in Syria and the cultivation of relations with the Taliban in Afghanistan might constitute elements of a broader Moscow strategy aimed at securing and extending its influence in strategically significant regions (Kozlov/Rynda, 2021). However, some argue that these actions represent more symbolic gestures than a coherent strategy (Suleymanov 2023). Certainly, Russia's strategic positioning regarding the Taliban following the fall of Kabul and the Western withdrawal has further complicated its relationship with ISIL/DAESH. Russia's historical focus on Abu Bakr al-Baghdadi, coupled with its repeated military interventions in Syria and growing presence in Africa through entities like the Wagner mercenary group, has drawn the attention and enmity of IS. The significance of narratives should not be underestimated: longstanding grievances stemming from the Soviet invasion of Afghanistan in 1979 may be as crucial as more recent military maneuvers against religiously motivated factions. Additionally, the Chechen War serves as *lieu de mémoire* for extremists in Central Asia. Furthermore, Russia's aspirations for power in Central Asia present a challenge to terrorist organizations operating in the region (Stockhammer 2024).

The war in Ukraine has led to a significant shift in Russia's regional security priorities, also resulting in a reduced focus on security efforts in broader Central Asia. This strategic reallocation has created a security vacuum that the Islamic State Khorasan Province (ISKP) and its Central Asian affiliates (predominantly Tajiks) are exploiting, posing an emerging threat to Western interests in the region and increasingly abroad. As Russia has diverted much of its resources and attention to the Ukrainian front, ISKP is seizing the opportunity to expand its influence and operational capabilities from Afghanistan across Central Asia to Europe and beyond. NATO now faces the challenge of addressing this evolving threat landscape, as the diminished Russian regional presence in security efforts (widely considered as oppressive) leaves a gap that could potentially be filled by extremist elements. This situation underscores the need for increased vigilance and potentially more active engagement from Western nations in regional security matters to mitigate the growing threat posed by ISKP and its affiliates.

The collective series of ISKP terrorist attacks, whether executed or prevented, have bolstered the reputation of the local DAESH affiliate in the Hindukush within its community. This organization is increasingly perceived as highly capable, garnering attention, and attracting followers globally (Ali 2024). Ultimately ISKP seeks to "*outperform rival groups by carrying out more audacious attacks to distinguish its brand and assert leadership of the global jihadi extremist*" (Goldbaum 2024). This competitive approach and the firm intention combined with existing capabilities to conduct terrorist operations make ISKP a significant threat for the West- on both sides of the Atlantic.

3. The Influence of the War on Terrorist Capabilities Abroad

Pretty much a consequence of the ongoing war in Ukraine, the availability and systematic proliferation of war material/arms that may flood into Western states and thus nourish terrorist capabilities could significantly contribute to an accelerated terrorist engagement in relevant – most likely European – states. Terrorist groups and associated perpetrators– both Radicalists or Right Wing – have shown the will and capacity to carry out attacks using illicit weaponry in the UK and Western Europe in the past. In general, arms trafficking from conflict zones remains a significant concern for Western counter-terrorism ambitions. Such illicit trade potentially involves the smuggling and sale of weapons, ammunition, and other military equipment from the battlefields in Ukraine. A recent example is the attempt of an ISKP splinter cell to acquire arms from Ukraine to attack civilians in an amusement park in Germany in 2023 (Spilcker 2024a). After the arrest of the Central Asian ISKP terrorist commando, an informer provided the authorities with information that the terrorist entrepreneur of the group planned a buy a Stinger missile via a contact from Ukraine who had offered it to him for 5,000 US dollars (Spilcker 2024b). Allegedly the seller was fighting in the Donetsk Basin then, but occasionally traveled to Germany to sell weapons.

Moreover, the war has so far been a striking proof of the effectiveness of commercial drones delivering explosives and even for their transformation into low-cost ammunition (Kunertova 2023: 576–591).

Weapons and associated technologies, but also relevant know-how could find their way into the hands of terrorist organizations from all ideological backgrounds, providing them with the means to carry out attacks and sustain their operations (Crisp 2023). The profitability and accessibility of arms in war zones like Ukraine create a lucrative market for traffickers, exacerbating instability and violence in conflict-affected areas and beyond. Combatting arms trafficking from war zones remains an essential task for international organizations and law enforcement. Disrupting the supply chain of weapons to terrorist groups is subject to enhanced global security efforts. The Europol "TESAT Report 2023" suggests that the Russian war of aggression against Ukraine "*raises concerns about CBRN material from the war zone potentially being smuggled into the EU and ultimately used for terrorist purposes*" (Europol 2023: 18). The proliferation of weapons of mass destruction is a serious challenge for NATO and other Western security organizations.

4. Implications on Western Counter-terrorism (CT)

As Russia's war of aggression in Ukraine continues, there are growing concerns about how Vladimir Putin might respond to potential further "*humiliating battlefield defeats*" perhaps on Russian soil or even simple adverse developments (Clarke 2022). Russian-backed terrorist attacks against Western targets, most likely European, may still be considered a legitimate response by Russia. As the Kremlin is casting the conflict as one between Russia and NATO, Russia could resort to terrorist tactics, potentially targeting European military sites, NATO-related facilities, or even civilian areas. Also, a direct Russian support of terrorist groups active in the West is conceivable (Rekawek 2024).

The underlying strategic approach of "inter-state terrorism" (*mezhgosudarstvenny terrorism*), had been conceptualized Russian military theorists, rooted in the belief that this could become advantageous for Russia in future (hybrid) conflicts. Dmitry Rogozin, then Russian Deputy Prime Minister, defined "inter-state terrorism" already in 2016 as

> "*a method of intimidating an adversary state by an aggressor state [while] influencing it with means of terrorism. The purpose of this kind of action is the physical elimination of the representatives of the political leadership and military command of the adversary state, or provoking mass panic and chaos via organizing terrorist acts against the civilian population*"

(Varga et al. 2022). Inter-state terrorism is hence a part of the Russian warfare toolkit.

Western – and specifically European – CT will undoubtedly have to adapt as large-scale conflicts like the Russian-Ukrainian war tend to trigger new or intensify existing phenomenological dynamics and trends in terrorism, that concern i.e., *modi operandi*, tactics, targeting and manifestations.

First, we should be aware of the major ramifications of information warfare and psyops against the West, conducted by Russia and its allies. Russian information warfare utilizes various methods to manipulate information and shape perceptions, both domestically and internationally (Boksa 2019). Cyber space has become an opaque battlefield for propaganda, false narratives, and fake news. By spreading such disinformation through traditional channels and social media platforms it targets Western audiences. Typically, the objective is to influence public opinion, destabilize adversaries, and advance Russian interests. Russian information warfare can indirectly relate to terrorism against the West through different mechanisms:

- *Disinformation and Radicalization*: Dissemination of false narratives and propaganda by Russian actors or Internet bots can contribute to the radicalization of individuals or groups prone to extremist ideologies. Fake news campaigns may amplify grievances or exploit existing tensions within Western societies, potentially leading to acts of terrorism (Roberts-Ingleson /McCann 2023).
- *Destabilization and Vulnerabilities*: By exacerbating social, political, or cultural divisions within Western states, Russian information warfare can create an environment conducive to extremism and terrorism. Instability and societal discord may create vulnerabilities that terrorist organizations seek to exploit (Edwards 2016).
- *Weaponization of Information*: Russian actors may exploit terrorist incidents in the West to sow further discord or undermine confidence in Western institutions and governments. By amplifying fear, confusion, or mistrust following a terrorist attack, they can weaken Western solidarity and resilience against future threats (Braddock 2020: 21).
- *Proxy Warfare Dynamics*: In some cases, Russian support for proxy groups or governments that sponsor terrorism can indirectly contribute to terrorist activities against Western interests. This support may include weapons transfers, funding, or political backing, amplifying the threat posed by terrorist organizations to the West (Rondeaux/Sterman 2019).

When it comes to amplification, the soaring digitalization and ultra-fast emergence of AI are to be considered as quantum leaps for our human development. This applies of course as well to terrorist violence, where these new opportunities and modalities will likely become a game changer (NCTC/DHS/FBI 2022). A second trend therefore concerns the growing exploitation of the digital "*value chain*" of terrorism which refers to the increasing use of digital technologies and online platforms by terrorist organizations and individuals to conduct their operations: An essential criterion along the terrorist 'supply chain' is "*the role of the internet and the associated virtualization of terror - from initial contact with extremist propaganda, to radicalization and recruitment, to planning and logistical support, including the exchange of information on the effective execution of an act of terror - almost everything takes place online*" (Stockhammer 2023a: 30). Such exploitation thus encompasses various stages of the terrorist lifecycle, from recruitment and radicalization to planning, execution, and propaganda dissemination.

Online platforms provide a global audience for terrorist propaganda and extremist ideologies, inspiring predominantly young individuals around the world to carry out attacks in the name of a particular cause or ideology. Lone actors and small cells are usually radicalized online, in most cases without direct contact with a terrorist organization. In this light, social media platforms serve as powerful tools for terrorist propaganda and recruitment. Extremist organizations produce and distribute slickly produced videos, social media posts, and online magazines to spread their message, recruit new members, and incite violence. Extremism, radicalization, and terrorism have moved online. It goes without saying that the advocates of extremism intensely leverage social media platforms, online forums, and encrypted messaging apps to recruit new members and radicalize individuals. They use sophisticated online propaganda campaigns to appeal to vulnerable individuals (preferably 'Generation Z' and 'Generation Alpha'), exploiting grievances, and promoting extremist ideologies. Furthermore, digital technologies (encrypted messaging) facilitate communication and coordination among terrorist networks, enabling them to plan and execute attacks with greater efficiency and secrecy. Unsurprisingly, terrorist organizations exploit online financial networks and cryptocurrencies to raise and transfer funds to finance their operations and evade traditional banking regulations. Social media play a key role in that process (Keatinge et al. 2019: 13). Virtual currencies provide terrorists with a secure and anonymous means of fundraising and money laundering. However, there are currently tendencies towards an old-fashioned cash-money laundering approach to evade counter measures.

Last not least, terrorist groups but also state actors like Russia and China are increasingly using cyber-attacks as a means of achieving their illegal, extremist objectives, including disrupting critical infrastructure, stealing sensitive information, and spreading fear and chaos (CSIS 2024). These attacks can target government agencies, businesses, and individuals, posing a significant threat to national security and economic stability.

In a nutshell, the growing exploitation of the digital value chain of terrorism poses significant challenges for counter-terrorism efforts, requiring innovative approaches to monitor and disrupt terrorist activities in cyberspace. Despite this rapid digital transformation, terrorist actors will most likely stick to simple and flexible tactics while executing attacks.

A third persisting trend indicates that low-level terrorism will remain the preferred tactic and modus operandi. The phenomenon of low-level terrorism refers to a specific type of terrorist activities characterized by smaller-scale attack scenarios or acts of violence perpetrated by individuals or small groups with limited resources, minimal or no organizational support, and limited strategic objectives (Stockhammer 2023b: 445). This type of terrorism is characterized by its reliance on decentralized structures, being more tactically oriented, and tending to focus on symbolic or ideologically exploitable rather than strategic targets. Low-level terrorism by lone actors or micro-cells relies on the simplest tactical principles and means of action, such as easily accessible (bladed and stabbing) weapons or everyday items - knives and cars - to which drones could possibly be added in the near future. Low-level terrorism is based on tactical simplicity in planning, logistics, and operational execution. The terrorist landscape will be further characterized by low-threshold-attack scenarios that point unmistakably toward simple planning, rapid execution, and the provision of corresponding, relatively easy-to-obtain armaments for the attackers (automatic rifles and explosive vests). The war in Ukraine will likely intensify the current dynamic, as Western counter-terrorism is mostly oriented vis à vis spontaneous attack scenarios by lone perpetrators. Low-cost DIY drones, as frequently used in the Ukrainian battlefield, could be appealing to terrorist organizations such as DAESH given a multitude of potential application scenarios (Franke 2023).

Against this backdrop, the rise of ISKP suggests that group-based, projected scenarios involving small or micro cells may become more plausible. Why is low-level terrorism likely to persist? The main reason is that low-level terrorism, as mentioned, primarily relies on easily accessible weapons such as knives, vehicles, or even everyday items, facilitating attacks by individuals or small groups without needing sophisticated weaponry or extensive resources (The Flemish Peace Institute 2018). DIY drones perhaps originating from Ukraine or Russia may become a welcomed addition to the existing repertoire. Low-level terrorism is characterized by simple tactics and minimal planning which allows perpetrators to adapt quickly to changing circumstances and evade detection by authorities. This simplicity also makes it difficult for security agencies to anticipate and prevent such attacks (Stockhammer 2023b: 445). The ongoing virtualization of extremism and terrorism favors rapid connections and online dispersion. Social media platforms provide a fertile environment for the dissemination of extremist propaganda and the radicalization of individuals, inspiring lone actors, or small cells to carry out attacks without direct organizational support (Braddock 2020). Moreover, the spread of extremist ideologies is transcending borders, potentially radicalizing individuals anywhere. The accelerating internationalization of extremist rhetoric is fueling a quick expansion of low-intensity, sometimes stochastic, terrorism.

5. Conclusion: Implications for NATO / NATO Defense Against Terrorism

Russia's aggression against Ukraine has significantly reshaped NATO's security landscape, necessitating a reevaluation of its counter-terrorism strategy. The conflict has elevated state-based threats in NATO's strategic calculus, potentially altering the balance between these and non-state terrorist threats. Undoubtedly, the war has underscored Russia's proficiency in hybrid warfare, encompassing cyber-attacks, disinformation campaigns, and the deployment of irregular forces. In response, NATO must expand its counter-terrorism capabilities to address these hybrid threats, particularly focusing on combating false narratives and propaganda that could exacerbate divisions and foster radicalization within Western societies. As the conflict expands, the risk of radicalizing individuals or groups sympathetic to either side increases, potentially spawning new terrorist threats that demand NATO's vigilance and preemptive action. Moreover, the widespread use of advanced weaponry, including drones, in Ukraine could provide terrorist groups with new tactical insights and capabilities. Consequently, NATO should prioritize enhancing its counter-drone and counter-IED capabilities. Without doubt, the war-induced instability and proliferation of weapons in the region present opportunities for terrorist groups to acquire arms and exploit the situation. While this primarily concerns the acquisition of weapons for use against Western targets, it's not limited to this scenario. Therefore, implementing effective and coordinated measures to counter the proliferation of such materials is crucial. Since February 2022, intelligence sharing and cooperation among NATO members has become even more critical. Existing counter-terrorism efforts should leverage and build upon this enhanced collaboration, creating a more robust and responsive security framework. In conclusion, NATO's counter-terrorism strategy must evolve to address these emerging challenges, balancing traditional threats with new hybrid warfare tactics and potential spillover effects from the Ukraine conflict.

References

Ahmadzai, A. (2022): *“IS-Khorasan: Organizational Structure, Ideological Convergence with the Taliban, and Future Prospects”*, in: *Perspectives on Terrorism*, vol. 16, issue 5 (Oct 2022); https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2022/issue-5/atal-ahmadzai.pdf [15.09.2024].

Al Jazeera (2024): “*Hamas says October 7 attack was a ‘necessary step,’ admits to ‘some faults’*”, *Al Jazeera.com*, (21. Jan. 2024), URL: https://www.aljazeera.com/news/2024/1/21/hamas-says-october-7-attack-was-a-necessary-step-admits-to-some-faults [15.09.2024].

Ali, J. (2024): “*The Islamic State’s Afghanistan-based affiliate is emerging as a global menace”, (*Defense One), available at: https://www.defenseone.com/ideas/2024/03/islamic-states-afghanistan-based-affiliate-emerging-global-menace/395223 [15.09.2024].

AP (2023): “Has Israel invaded Gaza? The military has been vague, even if its objectives are clear”. *Associated Press*. (31 Oct. 2023).

Benoit, B. (2023): “*Germany Uncovers Alleged Hamas Terror Plot in Europe. Prosecutors say four men were detained under suspicion of stashing weapons to target Jewish sites”* in: Wall Street Journal (14 Dec. 2023), URL: https://www.wsj.com/world/europe/germany-uncovers-alleged-hamas-terror-plot-in-europe-a367eb70 [15.09.2024].

Bertrand, N. /Liebermann, O. /Atwood, K. (2023): “*ISIS-K leader behind deadly 2021 suicide bombing at Kabul airport killed by Taliban, White House says”*(CNN) available at https://edition.cnn.com/2023/04/25/politics/isis-k-leader-killed-taliban-kabul-airport-bombing/index.html [15.09.2024].

Bilban, C. / Grininger, H. et al. (eds.) (2019): „*Mythos ‚Gerasimov-Doktrin‘. Ansichten des russischen Militärs oder Grundlage hybrider Kriegsführung?“*, in: *Schriftenreihe der Landesverteidigungsakademie*, Bundesministerium für Landesverteidigung, Vienna.

Boksa, M. (2019): *Russian Information Warfare in Central and Eastern Europe: Strategies, Impact, Countermeasures*. The German Marshall Fund of the United States, available at: https://www.gmfus.org/sites/default/files/Russia%2520disinformation%2520CEE%2520-%2520June%25204.pdf [15.09.2024].

Braddock, K. (2020): *Weaponized Narratives. The Strategic Role of Persuasion in Violent Radicalization and Counter-Radicalization*, Cambridge: Cambridge University Press, 21.

Burke, J. (2024): “*Islamic State ‘recruiting from Tajikistan and other central Asian countries’*” (The Guardian), available at: https://www.theguardian.com/world/2024/mar/24/islamic-state-recruiting-militants-from-tajikistan-and-other-central-asian-countries#:~:text=Islamic%20State%20launched%20a%20major,other%20intelligence%20services%20have%20said [15.09.2024].

Cafiero, G. (2020): “*What do Russia and Hamas see in each other*?”, *Middle East Institute* (02. April 2020), available at: https://www.mei.edu/publications/what-do-russia-and-hamas-see-each-other [15.09.2024].

Clarke, C. P. (2022): Op-Ed: “*How Russian battlefield defeats in Ukraine could lead to terrorism in the West”,* LA Times (Oct 2, 2022); https://www.latimes.com/opinion/story/2022-10-02/russian-military-defeats-ukraine-terrorist-attack-west [15.09.2024].

Collinson, F. (2024): “*Biden’s Rafah warning sends immediate shockwaves through US and global politics*”, *CNN* (9 May 2024), URL: https://edition.cnn.com/2024/05/09/politics/bidens-rafah-warning-is-turning-point-in-us-israel-relations-and-a-belated-but-inevitable-rupture-with-netanyahu/index.html [15.09.2024].

Crisp, J. (2023): “*New IRA believed to have Russian grenades stolen from Ukraine front line*“, (Telegraph), available at: https://www.telegraph.co.uk/world-news/2023/09/09/new-ira-grenades-russia-ukraine-war-northern-ireland/#:~:text=New%20IRA%20believed%20to%20have%20Russian%20grenades%20stolen%20from%20Ukraine%20front%20line&text=The%20New%20IRA%20is%20thought,grenades%20in%20Londonderry%20on%20Thursday [15.09.2024].

CSIS (2024): "*Significant Cyber Incidents*", available at: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents [15.09.2024].

Deutsche Welle (2021): „*Terrordrohungen haben sich massiv verschärft",* available at https://www.dw.com/de/terrordrohungen-haben-sich-massiv-verschärft/a-58986195 [15.09.2024].

Edwards, P. (2016): "*Closure through Resilience: The Case of Prevent*", in: *Studies in Conflict and Terrorism*, 39 (4), 292-307.

Europol (2023): *European Union Terrorism Situation and Trend Report*, Publications Office of the European Union, Luxembourg, 18, URL: https://www.europol.europa.eu/cms/sites/default/files/documents/European%20Union%20Terrorism%20Situation%20and%20Trend%20report%202023.pdf [15.09.2024].

Fabian, E. (2023): "*IDF says it has notified families of 242 hostages being held in Gaza*," *Times of Israel* (02. Nov. 2023), URL: https://www.timesofisrael.com/liveblog_entry/idf-says-it-has-notified-families-of-242-hostages-being-held-in-gaza [15.09.2024].

Fabian, E./ Pacchiani, G. (2023): "*IDF estimates 3,000 Hamas terrorists invaded Israel in Oct. 7 onslaught*," *Times of Israel* (01. Nov. 2023), URL: https://www.timesofisrael.com/idf-estimates-3000-hamas-terrorists-invaded-israel-in-oct-7-onslaught [15.09.2024].

France24 (2023): "*Israel social security data reveals true picture of Oct 7 death*," *France24* (15 Dec. 2023), https://www.france24.com/en/live-news/20231215-israel-social-security-data-reveals-true-picture-of-oct-7-deaths.[15.09.2024].

France 24 (2024): "*'Mutant jihadism' spreading across borders and online: EU's anti-terrorism coordinator*", (31 May 2024) available at: https://www.france24.com/en/tv-shows/talking-europe/20240531-mutant-jihadism-spreading-across-borders-and-online-eu-s-anti-terrorism-coordinator [15.09.2024].

Franke, U. (2023): *Drones in Ukraine and beyond: Everything you need to know*. (European Council of Foreign Relations), URL: https://ecfr.eu/chapter/drones-in-ukraine-and-beyond-everything-you-need-to-know/ [15.09.2024].

Goldbaum, C. (2024): "*ISIS-K, Group Tied to Moscow Attack, Has Grown Bolder and More Violent", (*New York Times), available at: https://www.nytimes.com/2024/03/24/world/europe/isis-k-moscow-attack.html [15.09.2024].

Hafezi, P. /Elwelly ,E. /Tanios, C. (2024): "*Islamic State claims responsibility for deadly Iran attack, Tehran vows revenge*", (REUTERS), available at: https://www.reuters.com/world/middle-east/iran-vows-revenge-after-biggest-attack-since-1979-revolution-2024-01-04 [15.09.2024].

Hafezi, P. / Rose, E. and Tolba, A. (2024): "*Iran plays down Israel's strikes, says they caused 'limited damage'*" (Reuters), available at https://www.reuters.com/world/middle-east/explosions-heard-iran-syria-middle-east-braces-israeli-retaliation-2024-10-25/ [26.10.2024].

Harper, E. / van der Vugt, R. (2024): "*The Narrative War That the West Must Win*", (*IPI Global Observatory*), URL: https://theglobalobservatory.org/2024/08/the-narrative-war-that-the-west-must-win/ [15.09.2024].

Haseldine, L. (2023): "*Why Putin hosted Hamas at the Kremlin"* in: The Spectator (27 Oct. 2023), URL: https://www.spectator.co.uk/chapter/has-putin-picked-a-side-by-hosting-hamas-at-the-kremlin/ [15.09.2024].

Hill, F. / Huggard, K. (2024): "*What is Russia's role in the Israel-Gaza crisis?*", *Brookings* (31. Jan. 2024), URL: https://www.brookings.edu/chapters/what-is-russias-role-in-the-israel-gaza-crisis [15.09.2024].

Hodge, N. (2023): *„An anti-Jewish riot in Russia's Dagestan region shows the risks of Putin's balancing act on Hamas*", *CNN* (31. Oct. 2023), available at https://edition.cnn.com/2023/10/31/europe/dagestan-riot-putin-hamas-balancing-act-analysis-intl-hnk/index.html [15.09.2024].

Jian, G. (2024): "*The Russia-Ukraine conflict is a catalyst for new international order*", in: *Global Times*, URL: https://www.globaltimes.cn/page/202402/1307696.shtml [15.09.2024].

Jones, R. / Said, S. (2024) "*Hostage—Video Release Aims to Head Off Attack,*" *Wall Street Journal,* (26. Apr. 2024); see also: "Hamas hostages: Stories of the people taken from Israel", *BBC* (01. Sept. 2024), URL: https://www.bbc.com/news/world-middle-east-67053011 [15.09.2024].

Keatinge, T. et al (2019): "*Social Media and Terrorism Financing. What are the Vulnerabilities and How Could Public and Private Sector Collaborate Better*?" in: *Global Research Network on Terrorism and Technology*: Paper No. 10, *Royal United Services Institute* 2019, 13, available at: https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf [15.09.2024].

Kilani, F. (2024): "*Hamas leader refuses to acknowledge killing of civilians in Israel*", *BBC* (07. Nov. 2023), URL: https://www.bbc.com/news/world-middle-east-67321241 [15.09.2024].

Kotoulas, I. E., & Pusztai, W. (2022): "*Geopolitics of the War in Ukraine*" (*Foreign Affairs Institute*), URL: https://www.aies.at/download/2022/Geopolitics-of-the-War-in-Ukraine-FINAL.pdf [15.09.2024].

Kozlov P. / Rynda, A. (2021): "*Afghan crisis: Russia plans for new era with Taliban rule*" (BBC), available at https://www.bbc.com/news/world-europe-58265934 [15.09.2024].

Kunertova, D. (2023). *Drones have boots: Learning from Russia's war in Ukraine*. In: *Contemporary Security Policy*, *44*(4), 576–591. https://doi.org/10.1080/13523260.2023.2262792 [15.09.2024].

Lister, Tim (2024): "*How ISIS has Europe and the US in sights after deadly Moscow attack"* (CNN), available at https://edition.cnn.com/2024/03/30/europe/how-isis-has-europe-and-the-us-in-sights-after-deadly-moscow-attack/index.html [15.09.2024].

Luxmoore, M. (2024): "*Russia to Carry Out Exercises for Tactical Nuclear Weapons*", Commentary (06 May 2024) in: *Wall Street Journal* (WSJ), URL: https://www.wsj.com/world/russia/russia-to-carry-out-exercises-for-tactical-nuclear-weapons-923622df [15.09.2024]. For a more elaborated account see: Wachs, L. (2022): "*The Role of Nuclear Weapons in Russia's Strategic Deterrence. Implications for European security and nuclear arms control*" (*Stiftung Wissenschaft und Politik*), *SWP Comment* 2022/C 68, 25.Nov.2022, URL: https://www.swp-berlin.org/publications/products/comments/2022C68_NuclearWeaponsRussias_Deterrence.pdf [15.09.2024].

Marahrens, S. (2023): "*The Russia-Ukraine Conflict from a Hybrid Warfare Perspective – A Year in the War*", in: *The Defence Horizon Journal* (18. Sept. 2023), URL: https://tdhj.org/blog/post/russia-ukraine-hybrid-warfare [15.09.2024].

Melkozerova, V. (2024): *„Russia ups blame-shifting for terror attack to Ukraine, brags it's boosting recruitment", (*POLITICO), available at https://www.politico.eu/chapter/russia-ups-efforts-to-shift-blame-for-crocus-terror-attack-to-ukraine-brags-its-boosting-recruitment-for-front/ [15.09.2024].

Münkler, H. (2023): *Welt in Aufruhr. Die Ordnung der Mächte im 21. Jahrhundert*, Berlin: Rowohlt Berlin, 401-457.

NCTC/DHS/FBI (2022): "*Emerging Technologies May Heighten Terrorist Threats*", available at: https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/134s_-_First_Responders_Toolbox_-_Emerging_Technologies_May_Heighten_Terrorist_Threats.pdf [15.09.2024].

Niblett, R. (2024): *The New Cold War. How the Contest Between the US and China Will Shape Our Century*, New York: Atlantic Books.

Parth, C. (2023): "*Terrorgefahr an Heiligabend*" (Die Zeit), available at: https://www.zeit.de/gesellschaft/zeitgeschehen/2023-12/anschlagsplaene-islamisten-koeln-wien-faq [15.09.2024].

Patrick, P. (2022): Does Putin's Judo philosophy explain his sanctions response? In: *The Spectator* (18. March 2022), https://www.spectator.co.uk/chapter/does-putin-s-judo-philosophy-explain-his-sanctions-response [15.09.2024].

Poe, M. (2001): "Moscow, the Third Rome: The Origins and Transformations of a 'Pivotal Moment'", in: *Jahrbücher für die Geschichte Osteuropas*, *49*(3), 412–429. http://www.jstor.org/stable/41050783 (07.09.2024).

Rekawek, K. (2024): "*Russian State Terrorism and State Sponsorship of Terrorism*", ICCT ReportSeptember 2024, https://www.icct.nl/publication/russian-state-terrorism-and-state-sponsorship-terrorism [15.09.2024].

Rekawek, K. / Renard, T. / Molas, B. (eds.) (2024): *Russia and the Far-Right Insights from Ten European Countries***.** The Hague: ICCT Press 2024, available at: https://www.icct.nl/sites/default/files/2024-04/Russia%20and%20the%20Far-Right%20Insights%20from%20Ten%20European%20Countries%20-%20A4%20e-book_0.pdf [15.09.2024].

Roberts-Ingleson, E. M. / McCann, W. S. (2023): "*The Link between Misinformation and Radicalisation: Current Knowledge and Areas for Future Inquiry*", in: *Perspectives on Terrorism*, *17*(1), 36–49; available at: https://www.jstor.org/stable/27209215 [15.09.2024].

Rondeaux, C./ Sterman, D. (2019): "Twenty-First Century Proxy Warfare", (New America), available at: (https://www.newamerica.org/future-security/reports/twenty-first-century-proxy-warfare-confronting-strategic-innovation-multipolar-world/rethinking-proxy-warfare [15.09.2024].

Rubin, S. / Warrick, J. (2023): "*Hamas envisioned deeper attacks, aiming to provoke an Israeli war*," *Washington Post* (13. Nov. 2023), URL: https://www.washingtonpost.com/national-security/2023/11/12/hamas-planning-terror-gaza-israel [15.09.2024].

Sauer, P. (2024): "'*I noticed nothing strange': suspect's colleagues express shock at Moscow attack*", (The Guardian), available at: https://www.theguardian.com/world/2024/mar/26/moscow-concert-hall-attack-tajik-gunmen-russia [15.09.2024].

Schmitt, E. (2024): "*ISIS Affiliate Linked to Moscow Attack Has Global Ambitions"* (New York Times), available at https://www.nytimes.com/2024/03/25/us/politics/moscow-attack-isis.html [15.09.2024].

Sciutto, J. (2024): *The Return of Great Powers: Russia, China, and the Next World War.* NY: Dutton.

Shahbazov, F. (2024): *What Does a Recent ISIS-K Terror Attack Mean for Turkey?,* Stimson, available at https://www.stimson.org/2024/what-does-a-recent-isis-k-terror-attack-mean-for-turkey [07.04.2024].

Simon, S. / Stevenson, J. (2023): "*The Gaza Horror and US Policy*," in: *Survival*, vol. 65, no. 6, 38; see also, Segev, T (2024): "Israel's Forever War," *Foreign Affairs*, vol. 103, no. 3, May/June 2024, 110.

Singh, M. (2023): "*Why China Is Taking Sides Against Israel—and Why It Will Likely Backfire*", *The Washington Institute for Near East Policy,* Policy Watch 3818 (29. Nov. 2023), available at: https://www.washingtoninstitute.org/policy-analysis/why-china-taking-sides-against-israel-and-why-it-will-likely-backfire [15.09.2024].

Spilcker, A. (2024a): „*Mutmaßliche Terroristen spähten am Ostermontag Deutzer Kirmes aus*", (Kölner Stadt-Anzeiger), available at: https://www.ksta.de/koeln/koeln-mutmassliche-terroristen-spaehten-deutzer-kirmes-aus-711590 [15.09.2024].

Spilcker, A. (2024b): „*Terror in Deutschland mit Waffen aus Ukraine - die irren Pläne der IS-Terroristen*", (Focus), available at: https://www.focus.de/panorama/welt/vermerke-des-bundeskriminalamts-terror-mit-waffen-aus-ukraine-in-deutschland-die-irren-plaene-der-is-terroristen_id_259543379.html [15.09.2024].

Steinberg, G./Albrecht, A. (2022): „*Terror gegen die Taliban: der Islamische Staat zeigt in Afghanistan neue St*ärke"; in: *SWP Aktuell* (Februar 2022), available at: https://www.swp-berlin.org/publications/products/aktuell/2022A08_IS_Afghanistan.pdf [15.09.2024].

Stockhammer, N. (2023a): *Trügerische Ruhe. Der Anschlag von Wien und die terroristische Bedrohung in Europa*. Vienna. (translated by author).

Stockhammer, N. (ed.) (2023b): *The Routledge Handbook of Transnational Terrorism*, Abingdon, Oxon; New York, NY: Routledge.

Stockhammer, N. (2024): *„Der IS schießt sich in Erinnerung“,* (Die Presse), available at: https://www.diepresse.com/18316109/der-is-schiesst-sich-in-erinnerung [15.09.2024].

Stockhammer, N. /Clarke, C. P. (2024): "*Learning from Islamic State-Khorasan Province's Recent Plots*", in: *Lawfare* (11 August 2024), available at https://www.lawfaremedia.org/chapter/learning-from-islamic-state-khorasan-province-s-recent-plots [15.09.2024].

Suleymanov, R. (2023): "*Russia's Growing Ties with Afghanistan are more Symbolism than Substance*", (Carnegie), available at: https://carnegieendowment.org/politika/90584 [15.09.2024].

The Flemish Peace Institute (2018): *Triggering Terror: Illicit Gun Markets and Firearms Acquisition of Terrorist Networks in Europe*, URL: https://vlaamsvredesinstituut.eu/en/report/triggering-terror-illicit-gun-markets-and-firearms-acquisition-of-terrorist-networks-in-europe [15.09.2024].

Tchakarova, V. (2020): "*The Dragonbear: An Axis of Convenience or a New Mode of Shaping the Global System?*“, IRMO Brief 5/2020, (Institute for Development and International Relations-IRMO), URL: https://irmo.hr/novosti/the-dragonbear-an-axis-of-convenience-or-a-new-mode-of-shaping-the-global-system/ [15.09.2024].

Times of Israel (2023): "*Death count from Re'im music festival massacre reportedly updated to 364—a third of Oct. 7 fatalities*," *Times of Israel* (17. Nov. 2023), URL: https://www.timesofisrael.com/liveblog_entry/death-count-from-massacre-at-reim-music-festival-reportedly-updated-to-364-a-third-of-oct-7-deaths [15.09.2024].

Umland, A. (2023): *„Der gefährlichste Philosoph der Welt – Alexander Dugin und die Rolle von Russlands extremer Rechten bei dem* völkermör*derischen Eroberungskrieg Russlands gegen die Ukraine“*, Commentary (18. Nov. 2023) in: „Neue Zürcher Zeitung“ (NZZ), URL: https://www.nzz.ch/meinung/r-gefaehrlichste-philosoph-der-welt-aleksandr-dugin-ld.1764246 [15.09.2024].

Varga, T. et al. (2022): "*Terrorism Threat During Peer-to-Peer Conventional War. A Background Study*," in: *Defence Against Terrorism Review*, vol. 14, 2022,16-18, available at: https://dgap.org/sites/default/files/chapter_pdfs/coedat_terrorismandpeer-to- peerconventionalwar.pdf [15.09.2024].

Ven Bruusgaard, K. (2016): "Russian Strategic Deterrence", in: *Survival*, 58:4, 7-26: 9; doi:10.1080/00396338.2016.1207945 [15.09.2024].

Vision of Humanity (2024): "*Why is ISIS targeting Russia?",* available at: https://www.visionofhumanity.org/why-is-isis-targetting-russia/ [15.09.2024].

Watling, J. /Reynolds N. (2024): "*Russian Military Objectives and Capacity in Ukraine Through 2024*", Commentary (13.Feb.2024) for "*The Royal United Services Institute*" (RUSI), https://www.rusi.org/explore-our-research/publications/commentary/russian-military-objectives-and-capacity-ukraine-through-2024 [15.09.2024].

Wilson Center (2021): Explainer: ISIS-Khorasan in Afghanistan, available at https://www.wilsoncenter.org/chapter/explainer-isis-khorasan-afghanistan [15.09.2024].

Wilson, J. L. (2023): *„Russia, China, and the Russia-Ukraine war: Tensions in the 'No Limits' Relationship*“, in: *The Diplomat* (15.Sept. 2023), URL: https://thediplomat.com/2023/09/russia-china-and-the-ukraine-war-tensions-in-the-no-limits-relationship [15.09.2024].

Winter, L. et al (2024): "*The Axis Off-Kilter: Why an Iran-Russia-China "Axis" is Shakier than Meets The Eye*", in: *War on the Rocks* (19. Apr. 2024), available at: https://warontherocks.com/2024/04/the-axis-off-kilter-why-an-iran-russia-china-axis-is-shakier-than-meets-the-eye [15.09.2024].

CHAPTER 10

FINDINGS, CONCLUSIONS, LESSONS LEARNED, AND RECOMMENDATIONS FOR NATO

Prof. Dr. Giray Sadık[*]

Findings, conclusions, lessons learned, and recommendations put forward in this chapter are direct reflections from the chapters of our project expert authors. As project lead researcher and editor of this volume, I led the project from the planning to workshop organization and preparation of this final deliverable on ***the effects of Russia-Ukraine War on counter-terrorism***. From the beginning until the end, authors have always been encouraged to be free in their assessments and recommendations. Therefore, the views expressed below can only be attributed to the mentioned authors. To keep this chapter focused, I point to the most directly CT-relevant findings and recommendations, for detailed overview with examples about the lessons learned, readers need to refer to the full chapters of the authors. In the following two sections expert assessments and lessons from the Russia-Ukraine war are presented under the *Findings and Lessons Learned from the Authors* section, while their actionable insights are put forward in the section on the *Conclusions and Recommendations for NATO*. In this chapter, to highlight the authors' findings and recommendations I added ***italics and bold*** for the most directly relevant lessons learned for NATO counter-terrorism efforts.

Findings and Lessons Learned from the Authors

In his chapter on *Effects of the Russia-Ukraine War on NATO's Official Counter-terrorism Discourse: An Evaluation in Terms International Law* Associate Professor Arif Bağbaşlıoğlu puts forward that NATO's counter-terrorism strategy has expanded its global area of struggle and intervention, as demonstrated especially by NATO activities outside the North Atlantic region. ***Since the September 11 attacks, NATO has made significant progress in counter-terrorism, although cooperation among member states has not always reached the desired levels***. The most important challenge while developing NATO's counter-terrorism role has

[*] The information and views expressed in this publication are solely those of the author and do not necessarily represent the views and policies of NATO, COE-DAT, NATO member states or institutions with which the author is affiliated.

been transatlantic and intra-European disagreements over the nature of terrorism and how to deal with this threat. Given that the Russia-Ukraine War has increased solidarity within the Alliance, NATO has clearly contributed positively to cooperation among member states in the fight against terrorism.

In his chapter on *Counter-Terrorism Effects of the War in the NATO's Eastern Flank: The Weaponization of Migration and Implications for Future Terrorism Threats* Dr. Marc Ozawa points out that terrorism risk and security in the Black Sea region are intertwined. Therefore, ***events in the Russia's war with Ukraine have directly impacted the threat of terrorism in the region***. One way is with respect to migration and specifically, the border crisis between Belarus and Poland. This is an instance whereby state sponsored hybrid aggression, in this case ***the weaponization of migration, has created a situation that heightened the risk of terrorists and their resources to cross into NATO territory*** and move freely in the Schengen zone. To address these challenges on the borders of NATO Allies such as Poland and Türkiye, the expertise of NATO Stability Policing Center of Excellence and NATO Center of Excellence Defence Against Terrorism can offer further elaborations about the good practices for border security. (*See* COE-DAT Report on Border Security, 2024)

In his chapter on *War in the Seas: Unmanned Maritime Systems, CIP, and Maritime Terrorism* Associate Professor Gordan Akrap highlights the key finding and lesson for NATO that ***terrorists adapt their modus operandi and targets depending on the level and effectiveness of preventive and protective security and counter terrorist measures***. It is noticeable that terrorists have shifted their focus from attacks on airplanes (which, like airports, have become extremely well-protected places), to large human gatherings which are difficult to protect completely. It is primarily about different forms of festivals (religious, musical, cultural, theatres) in open/closed areas that represent an easier target.

In her chapter on *How have Terrorists Adopted Tactics from the Russia-Ukraine war? The Crime-Terror-Tech Nexus* Professor Daniela Irrera points out that that the war has introduced and demonstrated a wide range of tactics, from drone warfare to cyber operations, urban warfare and decentralized structures, many of which have been or could be adapted to terrorist contexts around the world. In terms of the crime-terror-technology nexus, the war has helped to exacerbate its impact. Criminal networks facilitate the flow of weapons, illicit goods and finances that support both state and non-state actors in the conflict. Meanwhile, ***technological advances in cyber warfare, propaganda and surveillance are increasingly being adopted by terrorist organizations***. For similar lessons learned and a detailed overview on the effects of crime-terror-nexus for NATO and beyond, reading the recent *Columbia Lessons Learned* offers insights about the potential global spill-over effects of these underground networks. (*See* COE-DAT Report on Columbia Lessons Learned, 2023).

In her chapter on *Emerging Threats: Will the Use of New Technologies in the Russia-Ukraine war Transform the Capabilities of Terrorists?* Dr. Christina Schori Liang highlights various interrelated findings and lessons learned including but not limited to the following ones:

The conflict in Ukraine has demonstrated to terrorists the potential of drones for ISR (intelligence, surveillance, and reconnaissance) and psychological operations, and how they can be easily deployed with AI capabilities. Ukrainian innovations have shown that drone attacks can be highly precise and effective at long distances. In Ukraine, innovation has transformed even the cheapest drones into effective guided missiles, both human-operated and AI-guided. Terrorists are discovering that low-cost drones, particularly in swarms, can be highly effective. Although high-tech military drones remain largely beyond the reach of non-state actors, ***terrorists are mastering the use of civilian drone technology, which is widely available due to the ongoing conflict in Ukraine.***

Conclusions and Recommendations for NATO

In his chapter on *Hybrid Warfare and Counter-terrorism after NATO's New Strategic Concept* Ambassador Shota Gvineria highlights several interrelated recommendations including but not limited to the following ones, where NATO needs to:

Enhance Multinational Coordination and Cooperation: Given the cross-border nature of many asymmetric threats, NATO should strengthen cooperation among the Allies and with international partners. Joint exercises, shared intelligence, and coordinated responses are essential for building collective resilience. ***Invest in Technological Resilience***: As hybrid threats increasingly involve technological solutions and manipulations in and through cyberspace, NATO must prioritize investments in cyber resilience and technological innovation. This includes developing advanced capabilities to detect, deter, and respond to cyber threats, identifying and refuting disinformation, and ensuring that critical infrastructure is protected from digital vulnerabilities. To this end, he suggests integrating ***resilience into counter-terrorism education and training***: NATO should incorporate resilience-building scenarios into its military education, training, and exercises, preparing forces to respond effectively to hybrid and terrorist threats. This includes ***enhancing the adaptability of command structures, ensuring that military operations are integrated with civilian crisis management efforts*** and that the civilian population is ready to support defensive measures.

Professor Stefan Goertz identifies several critical lessons learned from Russia-Ukraine war and its regional ramifications for NATO counter-terrorism efforts including the following ones:

NATO and the EU must recognize that the vast majority of Russian "PMCs" are different from Western PMCs. They are less or not at the disposal of the public market, but primarily or exclusively perform tasks for the Russian government, Russia-friendly states and Russian companies.

When analyzing and combating hybrid threats and hybrid actors such as terrorists, it is also important to review your own mindset as quickly and thoroughly as possible. It is not about categorizing academically what a hybrid actor is. It should be about recognizing hybrid threats, ***improving awareness capabilities and developing strategies against hybrid threats as well as permanently monitoring and combating hybrid threats such as terrorists***.

Associate Professor Gordan recommends encouraging research and innovation activities of the private, state, public and academic sectors in the development of new technologies and means with the aim of detection and mitigation of existing and future multi-functional unmanned platforms. That is especially related to the development of defense systems in the domain of electronic warfare, because unmanned platforms must use different types of receivers/senders to communicate with their environment and even with remote pilot-operators(if the systems are not autonomous. His core argument is expanded to devising AI-related CT-strategies by Dr Christina Schori Liang by pointing out to ***the accelerating trend that technology is transforming the nature of warfare***. The shift toward increasingly autonomous weapons systems has been developing over decades, though it has largely remained within the realm of a small group of academics, human rights advocates, and military strategists rather than in broader public discourse. Furthermore, Gordan puts forward various policy recommendations to better address the multifaceted global counter-terrorism landscape NATO needs to:

Establish a communication channel with full exchange of information and knowledge with colleagues from Ukraine in order to understand the advantages and disadvantages of using unmanned platforms that can cause serious damage and produce negative consequences for the attacked target – or targets – in real time.

Protection of harbors and piers is extremely important, as is the protection of undersea key ***critical infrastructure (CIP)***

Work on strengthening NATO preventive capabilities primarily in the domain of cooperation with the national intelligence communities and police organizations, strengthening cooperation with the media, with specialized and expert organizations close to NATO and the EU (Jacobs and Samaan, p. 288-289) and all stakeholders covered by the concept of homeland security.

In his chapter on *Findings, Conclusions, Lessons Learned, and Recommendations for Nato* Dr. Prof. Dr. Giray Sadık observes that the Russian offensive war in Ukraine has far-reaching implications for global affairs, potentially reshaping the international security architecture and influencing NATO's counter-terrorism efforts. and the evolving terrorist threat landscape, which necessitates adaptations in Western counter-terrorism strategies. The conflict has created opportunities for terrorist groups to exploit security vacuums and acquire advanced weaponry. ***Key trends emerging from this context include the persistence of low-level terrorism, the growing exploitation of the digital "value chain" by terrorist organizations, and the potential proliferation of arms***. As the conflict expands, the risk of radicalizing individuals or groups sympathetic to either side increases, potentially spawning new terrorist threats that demand NATO's vigilance and preemptive action. Moreover, the widespread use of advanced weaponry, including drones, in Ukraine could provide terrorist groups with new tactical insights and capabilities. Consequently, ***NATO should prioritize enhancing its counter-drone and counter-IED capabilities. Without doubt, the war-***

induced instability and proliferation of weapons in the region present opportunities for terrorist groups to acquire arms and exploit the situation. While this primarily concerns the acquisition of weapons for use against Western targets, it's not limited to this scenario. Therefore, implementing effective and coordinated measures to counter the proliferation of such materials is crucial. ***Since February 2022, intelligence sharing and cooperation among NATO members have become even more critical. Existing counter-terrorism efforts should leverage and build upon this enhanced collaboration, creating a more robust and responsive security framework.***

In conclusion, for NATO, successful measures to counter hybrid aggression and counter terrorism cannot be separated. The better policy makers understand the complex links between hybrid warfare and terrorism, the more they can design effective strategies to secure the eastern Flank. One step in this direction would be to resist stove piping analysis and operations of hybrid warfare and counter terrorism by greater cooperation among the relevant centers of excellence. Building on expert capacities of NATO Centers of Excellence such as COE-DAT, SP-CoE, CCD-CoE, MARSEC, JWC, and others such as Hybrid-CoE can be counted as a step in the right direction to countering growing terrorist exploitations of ***Emerging Disruptive Technologies (EDT) and Artificial Intelligence (AI)*** in the blurring lines of crime-terror-tech nexus.

References

Report on “Border Security in Contested Environments” published by *NATO Centre of Excellence Defence Against Terrorism (COE-DAT)*, Ankara, Türkiye, 2024.

Workshop Report on “Colombia Lessons Learned on Terrorism Workshop Report” published by *NATO Centre of Excellence Defence Against Terrorism (COE-DAT)*, Ankara, Türkiye, 2023.

BIOGRAPHIES OF THE EDITOR AND AUTHORS

Editor's Biography

Prof. Dr. Giray SADIK is Professor and Chair in the Department of International Relations, Faculty of Political Science and *Director of European Studies Research Center*, both at Ankara Yildirim Beyazit University, Türkiye. Previously, he was Eisenhower Fellow at *NATO Defense College*, Rome, Italy, and Swedish Institute Postdoctoral Fellow in the Department of Global Political Studies at Malmö University, Sweden. Prof. Sadik received his Ph.D. in Political Science from the University of Georgia, USA, specializing in International Relations and Comparative Politics. His current research focuses on international security, Transatlantic relations, counter-terrorism, hybrid threats, European security and foreign policy, border and maritime security. In addition to his contributions to various COE-DAT projects and as lead researcher and author, Prof. Sadik was the Academic Advisor of *Terrorism Experts Conference and Defence Against Terrorism Executive Level Seminar* (TEC-DATELS-2024).

Author Biographies

Associate Professor Gordan Akrap is Vice-Rector of the "Dr. Franjo Tuđman" Defence and Security University in Zagreb, Croatia. He graduated at Zagreb Faculty of Electronics and Computing in 1994. In 2011 he received a PhD at the University of Zagreb, in the field of Information and Communication sciences. The title of his PhD was "Informational Strategies and Operations in Public Knowledge Shaping". He had an active role in Croatia's Homeland war for independence. During his career in diplomatic and security structures of Croatia he completed a number of professional courses, including Diplomatic Academy. He is active in research of national and regional security, intelligence and history of Homeland War. He published a number of books, and papers in journals and proceedings. He is editor-in-chief-of National Security and the Future journal from February 2021, and member of the Board of International Intelligence History Association from 2017.

Arif Bağbaşlıoğlu is an associate professor in the Department of International Relations at the Faculty of Economics and Administrative Sciences, Izmir Democracy University, Türkiye. His field of study is international relations focused on international security, Transatlantic relations, European security and international organizations in particular. He graduated from the Department of International Relations, Gazi University, Ankara/Türkiye in 2002 and he completed his M.Sc. degree in The Department of International relations at the same university in 2004. His Masters thesis was 'The US intervention in Afghanistan and the evaluation of its legal dimensions'. He received his Ph.D. degree on 'NATO's Enlargement in the Balkans' from the Department of International Relations, Gazi University, Türkiye in 2011. He worked in the Turkish Partnership for Peace (PfP) Training Centre from November

2005 to January 2009 as an international relations specialist and as a course director. He was postdoctoral fellow at the University of Ottawa between Sept 2012 and Sept 2013. Between January 2009 and February 2019, he worked as a research assistant and faculty member at Kırşehir Ahi Evran University. Between February 2019 and November 2023, he worked as a faculty member and head of the Department of International Relations at Çanakkale Onsekiz Mart University, Faculty of Political Sciences. He has written for a number of academic publications and contributed conference papers on NATO's partnership policy, international security, European security, peace research, and conflict resolution.

Bernard Siman is a Senior Associate Fellow at Egmont-Royal Institute for International Relations in Brussels in charge of Hybrid Warfare and Threats. The Egmont Institute is the think tank associated with the Belgian Foreign Ministry. He is also Head of Cyber Diplomacy and Statecraft at the Brussels Diplomatic Academy of the Vrije Universiteit Brussel (VUB). He lectures at the Defence College of the Belgian Royal Military School and at the European Security & Defence College. Regionally he specialises in Maritime Geopolitics, Black Sea, Mediterranean and Middle Eastern affairs.

Dr. Christina Schori Liang is Head of Counter-terrorism and Preventing Violent Extremism at the Geneva Centre for Security Policy (GCSP) in Switzerland. At the GCSP, she designs and directs courses on Preventing Violent Extremism and on Transnational Organized Crime. She leads GCSP's Geneva Security Debates and offers academic and policy guidance for global security actors worldwide. She is on the advisory board of the RESOLVE Network of the US Institute for Peace and an expert for the Global Initiative Against Transnational Organized Crime. Since 2016, Dr. Schori Liang has served as an Adjunct Faculty Member at the Paris School of International Affairs, Sciences Po where she teaches courses within the Global Risks and Intelligence Studies departments. She is the editor of *Europe for the Europeans: The Foreign and Security Policy of the Populist Radical Right* and has contributed to six Global Terrorism Index (GTI) reports. Dr. Schori Liang holds a doctorate in International Relations and an MA in History and International Politics from the Graduate Institute of International and Development Studies, Geneva, Switzerland.

Daniela Irrera is Professor of Political Science and International Relations at the School of Advanced Defence Studies, CASD, Rome, Italy. She is Chair of the European Consortium for Political Research (ECPR), associate editor of the Journal of Contemporary European Studies, co-editor of the Springer book series on Non-State Actors in International Relations. She is Visiting professor of Political Violence and Terrorism and Civil Society and Sustainability at the OSCE Academy, Bishkek.

She is a member of the Management Committee of the COST CA21133 – Globalization, Illicit Trade, Sustainability and Security (GLITSS) and also leads the Working Group 2: Platform: the governance of illicit trade. She is an ERCOR researcher, part of the Radicalisation Awareness Network Policy Support (RAN PS) European Research Community on Radicalization (ERCOR) Researchers' Directory.

She has served as member of the ISA Governing Council (2019-2021), Secretary General of the Italian Political Science Association (SISP) (2018-2021), Chair of the ECPR Standing Group on International Relations (2019-2021) and President of the European Peace Research Association (EuPRA) (2017-2022). She has been Visiting Scholar at several Universities and Research Centres in Europe, US and Asia. She has been awarded with a DAAD Fellowship at the Peace Research Institute Frankfurt and with a research grant at the European Union Center of Excellence, University of Alberta, Canada. She has been Associate Faculty at IBEI, Barcelona, teaching within the MUNDUSMAPP Erasmus Mundus program and Marie Curie Fellow at the Universidade Federal de Santa Caterina, Florianopolis, Brazil.

Dr. Marc Ozawa is an author, lecturer, and Associated Researcher of the Energy Policy Research Group at the University of Cambridge. He was previously Senior Researcher at the NATO Defense College. His current research examines the role of trust in international relations, NATO-Russian relations, the geopolitics of energy, and Russian and Eurasian affairs. He has previously held teaching, research, and editorial positions at the University of Cambridge, IHS CERA, and Yale University. Marc has taught and supervised both undergraduate and graduate level students in the subjects of international relations, the geopolitics of energy and intrastate conflict. He has published works on Russia's relations with its neighbors, energy security, and European-Russian relations. Marc is a graduate of the University of Alaska (BA), Yale University (MA) and the University of Cambridge (MSt, PhD). Additionally, he conducted coursework at Lomonosov Moscow State University and North-Eastern Federal University in Yakutsk.

Amb. Shota Gvineria joined the Baltic Defence College as a Defence and Cyber Studies lecturer in 2019. He is also a non-resident fellow at the Economic Policy Research Center since 2017. Before, Shota has been working on various positions in Georgia's public sector. Among other positions, he served as the Deputy Secretary at the National Security Council of Georgia. Earlier, he held the position of the Foreign Policy Advisor to the Minister of Defense of Georgia. Through 2010-14, Shota served as the Ambassador of Georgia to the Kingdom of the Netherlands. Amb. Gvineria holds an MA in Strategic Security Studies from Washington's National Defense University. He also earned MAs in International Relations from the Diplomatic School of Madrid and Public Administration from the Georgian Technical University. Shota Gvineria's main areas of expertise include hybrid warfare, cyber defense policy, Russia's foreign & security policy, Black Sea security and the Eastern partnership region.

Dr. Stefan Goertz is Professor for Security Studies at the German Federal University of Applied Administrative Sciences/Federal Police (Bundespolizei) in Lübeck, Germany. He is a researcher in the fields of Salafist-extremism, international terrorism, Right-wing extremism and terrorism. He studied political sciences in Berlin and Damascus/Syria and received his PhD (Security Studies) from the Bundeswehr University in Munich. He is reserve officer of the Bundeswehr and was deployed in the EUFOR and UNIFIL-missions.

Dr. Nicolas Stockhammer is a political scientist with focus on security policy and terrorism research. From 2004 to 2006 he was research fellow and university lecturer at the chair for Political Theory (Prof. Dr. Herfried Münkler) at Humboldt-University Berlin, Germany. Until 2021 Dr. Stockhammer had been a senior post-doc researcher of the research group Polemology and Legal Ethics at the University of Vienna. With numerous publications in academic journals, chapters published in print media as well as many media appearances as an expert for terrorism and terrorist developments, Stockhammer's expertise on security policy-related issues continues to meet great interest in Austria and abroad. Currently Dr. Nicolas Stockhammer is heading the Research Cluster "Counter-Terrorism, CVE (Countering Violent Extremism) and Intelligence" in the Department of Law and International Relations at Danube-University Krems (Austria). Recent publications: "*Routledge Handbook on Transnational Terrorism*," London: Routledge 2023; "*Lehrbuch Terrorismusbekämpfung und Extremismusprävention*," Wiesbaden: Springer VS (with Stefan Goertz); „*Trügerische Ruhe. Der Anschlag von Wien und die terroristische Bedrohung in Europa*", Wien: Amalthea Signum 2023.

NATO OTAN

NATO OTAN

Centre of Excellence Defence Against Terrorism

COE-DAT

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
2004
TÜRKİYE

ISBN 978-975-409-782-5
9 789754 097825

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