Centre of Excellence
Defence Against Terrorism

EMERGING DISRUPTIVE TECHNOLOGIES AND TERRORISM

NATO COE-DAT Research Project

Edited by Mitat ÇELİKPALA

Centre of Excellence Defence Against Terrorism
Ankara, Türkiye, 2026

EMERGING DISRUPTIVE TECHNOLOGIES IN COUNTER-TERRORISM

NATO COE-DAT
Research Project

Mitat ÇELİKPALA
Editor

Centre of Excellence - Defence Against Terrorism
Ankara, Türkiye, 2026

EMERGING DISRUPTIVE TECHNOLOGIES IN COUNTER-TERRORISM

Çelikpala, Mitat (ed.) 2026

Emerging Disruptive Technologies in Counter-Terrorism – NATO COE-DAT / Research Project by Mitat Çelikpala (ed.)

Authors: Özgün Erler Bayır, Seray Baykal, Mehmet Fatih Ceylan, Mitat Çelikpala, Sıtkı Egeli, Paul Hurmuz, Tacan İldem, Krešimir Mamić, Robert Mikac, Aleksander Olech, Zeynep Sütalan, Ashok Vaseashta,

First Edition, Ankara, March 2026

Published by

Centre of Excellence Defence Against Terrorism (COE-DAT)
Publisher Certificate Number: 47344
Address : Devlet Mahallesi İnönü Bulvarı Süleyman Emin 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 Öztepe Matbaacılık
Zübeyde Hanım Mahallesi Kazım Karabekir Caddesi No: 31/107 İskitler/ANKARA

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.

228 pages;
ISBN: 978-975-409-785-6

1. Emerging Disruptive Technologies 2. Dual-Use 3. Counter Terrorism.

To cite this book: Mitat Çelikpala (ed.) 2026, Emerging Disruptive Technologies in Counter-Terrorism – NATO COE-DAT Research Project -
Ankara: Centre of Excellence Defence Against Terrorism

CONTENTS

Preface

The convergence of Emerging Disruptive Technologies (EDTs) and terrorism has garnered significant attention in the modern world. These technologies are driving profound changes in organizational and industrial practices while simultaneously having a profound impact on existing security frameworks. As dual-use technologies, EDTs present a range of risks and opportunities that involve a diverse array of stakeholders, including private sector actors, governments, and international organizations. Their growing influence affects all areas of society, necessitating a reassessment of security approaches that must now address new threats posed by both state and non-state actors in both military and civilian environments. NATO is particularly influenced by the developments of EDTs, which play a crucial role in shaping the operational strategies and strategic planning of its member nations and allies. The advent of these technologies presents new opportunities for NATO's military forces, enhancing their effectiveness, resilience, cost-effectiveness, and sustainability while also addressing immediate capability gaps and fulfilling their established objectives. However, the introduction of these technologies also brings new vulnerabilities due to threats from both state and non-state actors, targeting both military and civilian assets. To capitalize on these opportunities while minimizing the risks associated with EDTs, NATO has pursued collaborative initiatives with member states to create responsible, innovative, and adaptive policies regarding such technologies. Furthermore, NATO is actively promoting the rapid adoption and integration of new technological advancements among its Allies. By cultivating partnerships with key stakeholders in academia and the private sector, NATO seeks to maintain its technological edge and military dominance, thus enhancing its ability to deter aggression and safeguard Allied nations.

To equip key decision-makers with a thorough understanding of the challenges posed by terrorism and to enhance the capabilities of NATO Allies and Partners in their defence efforts, the Centre of Excellence for Defence Against Terrorism (COE-DAT) offers subject matter expertise to member countries and partners. By introducing relevant new topics to interested audiences, COE-DAT has established itself as an internationally recognized and esteemed resource for expertise on terrorism. It functions as NATO's central hub for research, education, and collaboration within the global counter-terrorism community. Supporting the publication of new agenda items, such as EDTs and terrorism, is a vital aspect of its mission.

This edited volume, titled 'Emerging Disruptive Technologies and Terrorism', consists of ten articles designed to explore how EDTs are reshaping the capabilities of terrorist groups. Terrorists may leverage these technologies for multiple objectives, such as boosting radicalization and recruitment, enhancing the planning, training, and

execution of attacks, and employing new remote tactics to carry out assaults. The transformation brought about by EDTs also complicates the efforts of responders and investigators to address the latest threats generated by these technologies. Given the pressing nature of these issues, first responders and policymakers must understand how technological advancements can enable terrorist tactics, techniques, and procedures. This comprehension will facilitate the implementation of effective countermeasures.

To support this discussion, the following ten articles are beneficial. The article authored by Ambassador (Retired) Mehmet Fatih Ceylan, titled 'EDTs, Terrorism and Counter-terrorism in a Multi-Domain Context', aims to clarify the complex relationships between EDTs and the spheres of terrorism and counter-terrorism strategies. The author argues that EDTs serve as fundamental components, offering elaborate insights from various scholars on the implications of these technologies within the context of terrorism and counter-terrorism efforts in a multi-domain context.

Professor Ashok Vaseashta, in his comprehensive article titled 'Human Factors in Terrorism: Countering the Dual-Use of Emerging Disruptive Technologies', thoroughly investigates the dual-use nature of EDTs. The rapid advancement of these technologies is fundamentally altering critical sectors, including precision healthcare, defence, cybersecurity, and international security systems. Nonetheless, the intrinsic dual-use quality – where these technologies can be utilized for both positive and harmful ends – raises significant concerns regarding their potential misuse by adversaries and terrorist organizations. Importantly, military and civilian critical infrastructures are key targets for global aggressors due to their vital importance in various operational scenarios.

In their article titled 'Terrorist Threats Emanating from Cyberspace: Disinformation, Radicalization, and Recruitment', Professors Robert Mikac and Krešimir Mamić examine crucial research questions regarding how terrorist and criminal organizations exploit disinformation in the online environment. They focus on the tactics these groups use to promote radicalization and recruitment, the primary platforms and tools for spreading propaganda, and the impact of artificial intelligence and deepfake technologies on the dissemination of disinformation and the enhancement of propaganda efforts.

In the article 'Terror-AI-sm: The Future of Artificial Intelligence in the Hands of Terrorists', Dr. Aleksander Olech discusses the substantial threat that terrorism poses to international security. He coined the term 'Terror-AI-sm' to emphasize the importance of understanding the future of AI in relation to terrorist actors. Dr. Olech highlights the increasing capabilities of artificial intelligence and the evolving nature of terrorist threats, illuminating the complex interplay between technological progress and the associated security risks. He identifies a worrying trend where terrorist

organizations are progressively leveraging AI for various activities, including the spreading of propaganda, cyberattacks, and physical assaults using autonomous combat systems. This development is transforming operational capabilities and fundamentally reshaping the dynamics of asymmetric warfare.

Ambassador (Retired) Tacan İldem offers an in-depth examination of the relationship between social media and terrorism in his article, 'Social Media and the Shadow of Terrorism: Impacts, Risks, and the Way Forward'. Utilizing his significant experience in diplomacy and security, he addresses pressing concerns at the intersection of extremism and digital technologies. The growth of social media has introduced a variety of intricate and serious risks, including the rise of cyberterrorism and the dissemination of misinformation. While these platforms can encourage connections and discussions among people and institutions, they also offer a more troubling potential: the accelerated radicalization of individuals.

Dr. Zeynep Sütalan's article, 'The Role of Digital Ecosystems in the Evolution of Terrorist Strategy of Radicalization and Recruitment,' presents a detailed examination of how open digital ecosystems inherently facilitate radicalization. Dr. Sütalan identifies open digital ecosystems by their heightened visibility, widespread engagement, and content curated by algorithms. Platforms like YouTube, TikTok, Instagram, and X (formerly Twitter) shape user experiences with automated recommendations that emphasize engagement patterns. Terrorist groups take advantage of this framework to create settings of ambient radicalization, where individuals are subtly and gradually exposed to extremist ideologies. Conversely, closed digital ecosystems depend on encrypted, smaller-scale, trust-based communication. Platforms such as WhatsApp, Signal, and private Telegram groups offer end-to-end encryption, low discoverability, and enhanced user control, making them particularly conducive to relational radicalization.

In the article The Future of Counter-terrorism for Intelligence and Security Agencies in the Age of Emerging and Disruptive Technology', Major General (Retired) Paul Hurmuz analyses the current state and future direction of counter-terrorism and intelligence operations, particularly in light of the EDTs. He carefully assesses how intelligence and security agencies can effectively reassess their strategic intelligence priorities while adopting technological advancements without sacrificing their core missions and operational effectiveness.

Professors Özgün Erler Bayır and Seray Baykal explore new and relatively unexplored themes in their article 'Cyber Diplomacy in the Space Age: Fostering the Responsible Use of Space for Global Security'. This work examines the role of cyber diplomacy in mitigating cybersecurity threats, particularly those targeting national digital infrastructures and space-based systems. Additionally, it examines how EDTs, when combined with the responsible use of space, can be harnessed for the collective

benefit. The authors highlight the potential of diplomatic initiatives to convert disruptive forces into opportunities that enhance global peace and security.

In his comprehensive article, 'Innovative Tools Available to Non-State Actors: Aerial Drones and Unmanned Systems at Sea and on Land', Professor Sıtkı Egeli elucidates the transformative impacts of uncrewed vehicles – on modern warfare. Egeli examines how a variety of entities, including lone wolves, terrorist organizations, and organized crime syndicates, have increasingly incorporated drones into their hybrid warfare tactics. This change has fundamentally altered how nations globally perceive threats and security priorities.

In the final article of the collection, titled 'The Potential Use of Emerging Disruptive Technologies by Non-State Actors in the Energy Domain', Professor Mitat Çelikpala investigates the significance and role of EDTs in the energy sector, particularly their potential applications by non-state actors. The energy sector, with its extensive connections to critical industries and focus on technology and innovation, frequently utilizes EDTs. Private companies, both domestic and international, play crucial roles in this sector as both owners and operators, presenting significant opportunities alongside inherent risks linked to technological progress. Thus, EDTs are essential for transforming key energy infrastructures and revolutionizing the way energy is generated, distributed, and consumed. Given the ongoing global challenges of climate change and the limited availability of fossil fuels, these technological innovations offer a strategic pathway to a more sustainable and resilient energy future. In this context, EDTs are vital as we shift from reliance on fossil fuels to a foundation of renewable and clean energy.

In summary, this study, comprising a series of insightful articles authored by leading experts in the field, aims to deepen understanding of the counter-terrorism approaches supported by COE-DAT for NATO Allies and Partners, while also making a meaningful contribution to the scholarly dialogue on these critical issues. Although the articles do not cover all dimensions of this rapidly evolving field, it is anticipated that these gaps will be addressed in future studies. In this regard, this study seeks not only to inform military and security professionals, defence policymakers and scholars, but also to serve as a foundation for future studies examining the complex security implications of EDTs in the context of terrorism.

Halil Sıddık AYHAN
Colonel (TUR A)
Director, COE-DAT

Acknowledgments

This volume aims to equip key decision-makers with a comprehensive understanding of the multifaceted challenges posed by terrorism and to enhance the defense capabilities of NATO Allies and Partners. The Centre of Excellence for Defence Against Terrorism (COE-DAT) plays a pivotal role in providing essential information support to member states and affiliated partners. By integrating relevant topics into ongoing discussions, COE-DAT has established itself as an internationally recognized authority in the field of terrorism studies. It functions as NATO's principal hub for research, education, and collaboration within the global counter-terrorism community. Supporting the publication of new agenda items, such as the intersection of Emerging Disruptive Technologies (EDTs) and terrorism, is a crucial aspect of its mission.

This edited volume, entitled "Emerging Disruptive Technologies and Terrorism," comprises ten scholarly articles designed to investigate how these technologies are reshaping the operational capabilities of terrorist organizations.

I would like to acknowledge that this scholarly work represents the culmination of a rigorous team effort. The process, which commenced at the beginning of the year, was facilitated by Colonels Tamas Kender and Sekan Karagöz from COE-DAT. Their unwavering dedication and insightful contributions were instrumental in the successful assembly of this volume.

I extend my profound gratitude to Colonel Halil Sıddık AYHAN, Director and Turkish Senior National Representative of the COE-DAT, as well as Chief of Staff Ahmet Erol, for their thorough review of the articles and their invaluable critiques. Their support and engagement provided a significant opportunity for enhancing the quality of this work.

Furthermore, I would like to express my sincere appreciation to the authors, whose expertise and diligence made this publication possible. Within a condensed timeframe, they produced comprehensive articles that reflect their extensive knowledge and expertise. Their timely cooperation during the editing process ensured the work was completed within the anticipated schedule.

Special recognition is due to Stephen Harley for his meticulous reviewing and editing of the articles. His efforts greatly enhanced the clarity and accessibility of the texts.

In conclusion, I would like to convey my heartfelt gratitude to the readers. In the absence of engaged readership and constructive evaluations, the purpose of writing and disseminating academic works becomes diminished in contemporary society. I sincerely hope this volume reaches a broad audience and makes a meaningful contribution to the discourse on terrorism and emerging technologies.

John CHRISTIANSON
Colonel (USAF)
Deputy Director, COE-DAT

DISCLAIMER

The edited book is a product of the Centre of Excellence-Defence Against Terrorism (COE-DAT). It is produced for NATO, NATO member countries, NATO partners, related private and public institutions and related individuals. It does NOT represent the opinions or policies of NATO, COE-DAT or the framework and sponsoring nations of COE-DAT. The views and terminology presented in the book are those of the authors.

Contributors

Project Manager & Editor

Mitat Çelikpala is an academic in the field of International Relations, currently serving as a Professor and the Vice Rector at Kadir Has University in Istanbul. His educational journey began with a bachelor's degree from Middle East Technical University in Ankara, where he graduated in 1992. He obtained a Master's degree from Hacettepe University in 1996 and a PhD from the Department of International Relations at Bilkent University in 2002.

Prof. Çelikpala's academic focus encompasses graduate and undergraduate curricula, addressing critical themes such as Eurasian security, energy security, critical infrastructure protection, and Turkish foreign and domestic policy. He has been a member of the International Relations Council of Turkey since 2004 and was the Managing Editor of the Journal of International Relations: Academic Journal.

His prior appointments attest to his expertise in security studies and policy formulation. He served as an academic advisor to NATO's Centre of Excellence for Defense Against Terrorism in Ankara from 2009 to 2012, concentrating on regional security dynamics and critical infrastructure protection. Additionally, he served as a board member of the Strategic Research and Study Center (SAREM) under the Turkish General Staff from 2005 to 2011. He served as Academic Adviser to the Center for Strategic Research (SAM) at the Turkish Foreign Ministry from 2002 to 2010. His academic affiliations include that of a Senior Associate Member at St Antony's College, University of Oxford, during the 2005-2006 academic year.

Prof. Çelikpala has made significant contributions to scholarly discourses in various esteemed academic journals, including Middle Eastern Studies, Energy Security, the International Journal of Turkish Studies, Insight Turkey, and the Journal of Southeast European and Black Sea Studies, enhancing the understanding of regional and international security issues. His extensive work reflects a robust engagement with the challenges of contemporary international relations and security studies.

Author Biographies[1]

Özgün Erler Bayır is a Professor of International Relations at Istanbul University. She is an expert in European studies, diplomacy, digital diplomacy, space policy, digitalization, foreign policy analysis, new forms of diplomacy, disinformation, and science diplomacy. She has extensive experience in international research project management and coordination, curriculum development, and integrating digital skills

[1] The authors are listed in alphabetical order by their last names.

and technology into international relations education. Her Ph.D. dissertation, completed in 2011, is titled “Dilemma between Atlanticism and Europeanization in Poland’s Foreign Policy.” She implemented the Jean Monnet Module at Istanbul University titled “Future of the EU: Security, Economy, and Transatlantic Relationship” (2020–2023). She coordinated the Erasmus+ KA220-HED project “Digital Diplomacy: Building the Common Future with Technology” (DD-TECH) between 2022 and 2025. In addition, she served as the project coordinator for two NATO Public Diplomacy Division Grants in 2022 and 2023. She is also the Project Manager of the TÜBİTAK 3005–Support Program for Innovative Solutions in Social Sciences project titled “Reconciling Social Sciences and Space: Shaping the Future with an Interdisciplinary Perspective on the New Space Ecosystem” (2022–2024). Currently, she is conducting a Jean Monnet Module titled “Challenges and Opportunities for the Future of Europe” (2023–2026). She is the principal investigator of another public diplomacy project funded by the U.S. Embassy in Türkiye, titled “Make Information True Again (MITA): Reinforcing Democratic Values to Foster U.S.–Turkey Relations” (2022–2024). She has also been a project researcher and lecturer in the Jean Monnet Module “EU-GlobalDigi: EU as a Global Digital Actor,” coordinated by the University of Bucharest, Romania (2024–2027). She recently completed a project under NATO’s Science for Peace and Security (SPS) Programme titled “The Evolution of Space for Security and Prosperity: Risks, Defence, and Cooperation,” in partnership with the International Space University, France. Professor Bayır has published numerous articles on international relations and authored two books. Her first book, “Dilemma between Atlanticism and Europeanization in Poland’s Foreign Policy,” was published in 2012, and her second, “New-New Diplomacy,” in 2023. She serves as an executive member of the Istanbul University Board of Science and Research Policies and the Executive Committee of the Istanbul University Research Council for the Development and Management of International Research Projects. Since February 2025, she has also been the Chair of the Ethics Committee for Social and Human Sciences Research at Istanbul University

Seray Baykal has a PhD degree in International Relations. She graduated from Bilkent University, International Relations department in 2017 and obtained her master’s degree from Istanbul University, International Relations department in 2019. She successfully defended her dissertation titled “Applicability of Science Diplomacy and Commitments of Paris Agreement in Realist Theory: Turkey Case”. She successfully completed her doctorate in 2024 with a dissertation titled “The Impact of Changes in Public Diplomacy Activities in the Digital Age on Turkish Foreign Policy.” She specializes in diplomacy, science diplomacy, public diplomacy, space diplomacy, digital diplomacy, and foreign policy analysis. She has been working at different research projects as researcher including Jean Monnet Module, “Challenges and Opportunities for the Future of Europe”, Erasmus+ KA2 Cooperation Partnership

Project, “Digital Diplomacy: Building the Common Feature with Technology”, TUBITAK Research Project, “Reconciling Social Sciences and Space: Shaping the Future with an Interdisciplinary Perspective to the New Space Ecosystem and NATO Public Diplomacy Division's Co-Sponsorship Grants Program Projects, “Learn2Unite: Simulation-based learning against NATO’s Emerging Challenges” in 2023 and “You then NATO: Youth Vision for the Future of Turkey-NATO Relations” in 2022. Recently, she worked as a member of the organizing committee for the project titled “The Evolution of Space for Security and Prosperity: Risks, Defense, and Cooperation,” funded by the NATO Science for Peace and Security (SPS) Programme - Advanced Research Workshop in 2025. She is currently a postdoctoral researcher at Istanbul University

Ambassador Mehmet Fatih Ceylan is a retired career Turkish diplomat who served at the Turkish Ministry of Foreign Affairs for almost 40 years, from 1979 to 2019. Ambassador (R) Ceylan holds a B.A. from the Faculty of Political Science at Ankara University. Following his university education, he attended post-graduate studies at Rutgers/Princeton Universities in the U.S. He received his master’s degree (M.A.) in international relations in 1982.

During his tenure at the Foreign Ministry (MFA), which he joined in 1979, he served at different Turkish missions abroad. He was assigned to the Turkish Embassy in Islamabad/Pakistan, in 1983 as the Second Secretary when there was a war in Afghanistan waged by the Afghan insurgents against the Soviet forces. His assignment in Pakistan enabled him to gain a comprehensive understanding of the issues prevalent in the Subcontinent at the time.

His next assignment was in Deventer/the Netherlands, in 1985 as the Consul at the Turkish Consulate General. During his three-year tenure in the Netherlands, he was able to follow Dutch policies on different aspects of European issues and social inclinations among the Turkish community residing in the Netherlands. Toward the end of the Cold War, he became the Chief of Section at the NATO Department at the Foreign Ministry in Ankara. In 1990, he was appointed to the Turkish Delegation to NATO, first as First Secretary and later as Defence Councilor of the Turkish Delegation. In his assignment at NATO, he witnessed the demise of the Warsaw Pact and the Soviet Union as well as the reunification of Germany. He was also responsible for following the activities of the Western European Union when it was activated in 1992. He served five years at the Turkish Delegation to NATO between 1990-1995. His NATO assignment during those years coincided with the evolving European Security and Defence Identity, gaining traction following the Maastricht Summit in 1991.

Ambassador Ceylan was the Turkish Consul General in Düsseldorf/Germany, between 1997 and 2000. That assignment had added to his perspective on European issues, with a particular focus on Germany's approach to various European matters.

In 2000, he was assigned to the Turkish Delegation to WEU as the Deputy Permanent Representative, later to be followed by his tenure at the Turkish Mission to the EU as Deputy Chief of Mission responsible for the EU's Common Foreign and Security Policy (CFSP)/European Security and Defence Policy (ESDP). After serving at the MFA's Department of International Security Affairs (NATO and the EU) as the Head of Department (2002-2005), he became Deputy Director General at the same Department before he was appointed as the Turkish Ambassador to Khartoum/Sudan between 2006-2009.

Back in Ankara between 2009-2013 he first became Director General in charge of ex-Soviet countries, including the Caucasus and Central Asia, for one year and was promoted to Deputy Undersecretary (Junior Deputy Foreign Minister) responsible with a vast array of files covering, inter alia, international security and defence (UN, NATO, OSCE, EU) matters extending to Far Eastern Affairs and the former Soviet geography.

Ambassador Ceylan's last assignment abroad was at NATO between 2013 and 2018 as the Turkish Permanent Representative during an extremely volatile period in international affairs.

Ambassador Ceylan retired from the MFA in 2019 after a forty-year career.

He spent a total of more than twenty years of his career on security and defense matters, focusing on NATO and the EU's security and defense files.

Following his retirement, Ambassador Ceylan was elected President of the Ankara Policy Center (APC) in 2022, a well-reputed think tank in Ankara that brings together retired Turkish Ambassadors, renowned Turkish academics, and journalists.

Sıtkı Egeli, Associate Professor, is a military and security studies analyst at Izmir University of Economics. He earned degrees from Bosphorus University (B.A.), the University of Chicago (A.M.), and Bilkent University (Ph.D.). From 1991 to 1999, he served at Turkey's Undersecretariat for Defence Industries (SSM), advancing to Director of Foreign Affairs. Between 1994 and 1999, he was a Board Member of TUSAŞ - Turkish Aircraft Industries, Inc. In 1994, he graduated from the NATO Defence College (Course-83). From 2000 to 2015, he served as Vice President of an international consulting firm specializing in defence and aerospace industries. He has published numerous books, book chapters, and articles on topics including the proliferation of WMD and delivery systems, air and missile defense, air power, arms and export controls, the defense industry, the militarization of space, and emerging disruptive technologies.

Major General (Retired) Paul Hurmuz. Paul Hurmuz's military career began in 1983 in a SIGINT and Electronic Warfare Unit, where he held various positions, including Head of the COMINT Department. After attending the Staff College between 1990 and 1992, he was appointed as a Battalion Commander before joining the Romanian Military Intelligence Directorate (MID) in 1993. He was later appointed to Defence and Diplomacy positions in Ankara (Türkiye) and London (UK). As Defence Attaché in the UK, he represented Romania in various capacities during operations in Iraq, Afghanistan, and the Balkans.

Before joining the Brussels NATO HQ in September 2013, he served as the Head of Plan, Policy, and International Cooperation in the Romanian MID. He was promoted to the rank of Brigadier General on 1st December 2013. Paul HURMUZ assumed the Deputy Director position of the Intelligence Division in the NATO International Military Staff at a critical time for the Alliance, facing great challenges from both the Eastern and Southern flanks. He was also responsible as the Chair of the Military Intelligence Committee (Working Level), the Senior Military Coordinator for Joint Intelligence, Surveillance and Reconnaissance (JISR), and the Chair of the NATO Geospatial Board (NGB). In his role as the NATO Senior Military Coordinator for JISR, he ensured senior-level, cross-functional coordination across the International Military Staff, Strategic Commands, and NATO Agencies for this high-visibility project and was instrumental in achieving the Initial Operational Capability for NATO JISR.

On 2nd September 2016, at the end of his NATO tour, he was appointed Deputy of the State Secretary and Chief of the Defence Policy and Planning Department of the Romanian Ministry of National Defence. On 1st December 2016, he was promoted to Major General. He retired in August 2017 after serving 34 years in the military.

Since January 2023, he has been a Senior Associate Expert at the New Strategy Center, a prominent think tank organization in Bucharest, Romania.

Ambassador (R) Tacan İldem, who is the Chairman of the Istanbul-based think tank EDAM, Centre for Economics and Foreign Policy Studies, is a veteran Turkish diplomat. During his long career, spanning from 1978 to 2021, he held various senior positions, including NATO Assistant Secretary General. He was a member of the NATO Independent Experts Group, commissioned by the Heads of State and Government, which presented a report entitled "NATO 2030: United for a New Era." This report served as input to NATO's latest Strategic Concept. He served as the Turkish Ambassador to the Netherlands and Permanent Representative to NATO and the OSCE. He also served as Director General for International Security Affairs at the Ministry of Foreign Affairs, Chief of Cabinet, Principal Foreign Policy Advisor, and Spokesperson of the President of the Republic. His postings abroad also include the Turkish Permanent Representation to NATO in Brussels and Turkish Embassies in

Washington, D.C., Athens, and New Delhi. Ambassador İldem is a graduate of Ankara University Faculty of Political Science. He is a recipient of the decoration of Grand Officer of the Order of the Star of Italian Solidarity and the Medal of Gratitude of Albania.

Krešimir Mamić is the Head of Counter Terrorism Service of the Ministry of Interior of the Republic of Croatia. He is a national representative in all relevant working groups and platforms on Counter-Terrorism issues within the European Commission, the Council of the European Union, Europol, Interpol, the UN, the Council of Europe, and other organizations. Additionally, he is the author of numerous scientific articles and books on topics including Criminal Law, Counterterrorism, and National Security. He also teaches as a guest lecturer at the Faculty of Criminal Investigation and Public Safety of the Ministry of the Interior, as well as at the War School of the Croatian Ministry of Defence.

Robert Mikac, PhD., is an Associate Professor at the Faculty of Political Science, University of Zagreb. He also teaches at the Croatian Military Academy "Dr. Franjo Tuđman". He specializes and has scientific interest in the field of security studies, specifically in the areas of strategic management, crisis management and recovery, civil protection, migration, and critical infrastructure protection. He has expertise in Afghanistan and counterinsurgency operation themes. Prior to his academic career, he worked in the Armed Forces of the Republic of Croatia, Civil Protection, and the Police. He has extensive experience spanning operational to strategic levels, both nationally and internationally, in matters related to international operations and project management. As an author and co-author, he has published seven books (in Croatian, English, and Macedonian) and around fifty scientific articles.

Dr. Aleksander Olech is the Head of International Cooperation at Defence24 Group and Editor-in-Chief of Defence24.com as well as Visiting Lecturer at the Baltic Defence College. He lectures at national and international universities, serves as a NATO associate, and is an analyst and publicist. Previously, he served as Deputy Director of the Department at the Ministry of Foreign Affairs. In recent years, he has closely cooperated with NATO ENSEC COE, NATO StratCom, NATO CCD COE, and NATO COE DAT. A graduate of the European Academy of Diplomacy and the University of War Studies, his research focuses on French-Russian relations, security challenges in Africa, and NATO's security policy.

Dr. Zeynep Sütalan holds a PhD in International Relations from the Middle East Technical University. From 2005 to 2011, she served as a concept specialist at the Centre of Excellence Defence Against Terrorism (COE-DAT). She has delivered lectures on terrorism at COE-DAT and at the Partnership for Peace Training Center in Ankara. Her research interests include terrorism, counterterrorism, gender and terrorism, as well as the history, politics, and economics of the Middle East. Between

2018 and 2022, she was an adjunct lecturer in the Department of International Relations at Atılım University. From 2019 to 2023, she served as the academic advisor for COE-DAT's Workshop Series on Gender in Terrorism and Counterterrorism. Dr. Sütalan continues to collaborate closely with COE-DAT, contributing through lectures, research projects, and education and training activities.

Prof. Dr. Acad. Ashok Vaseashta received a Ph.D. from the Virginia Polytechnic Institute and State University, Blacksburg, VA, in 1990, followed by Kobe's post-doctoral fellowship. He was awarded an Honoris Causa doctorate from Riga Technical University, Honorary membership of the Academy of Sciences of Moldova, membership of the Academy of Sciences of Georgia, membership of the Euro Mediterranean Academy of Arts and Sciences, and a Gold Medal for his leadership in Nanotechnology from the National Polytechnic University of Armenia. Currently, he serves as the Executive Director of Strategic Research at the International Clean Water Institute in Virginia, USA. He served as a Professor at Virginia Tech and Marshall University, Director of Research at the Institute for Advanced Sciences Convergence and International Clean Water Institute for Norwich University Applied Research Institutes, Vice-Provost (Rector) for Research in South Carolina, and Executive Director and Chair of the Institutional Review Board at a State University in New Jersey. He held visiting positions as a Professor at the Riga Technical University, Latvia; the 3 Nano-SAE Research Center, University of Bucharest, Romania; Transylvania University of Brasov, Romania; a member of CIRET, France; and a scientist at the Weizmann Institute of Science, Israel. He served the U.S. Department of State in two rotations as a strategic S&T advisor in the Bureau of International Security and Nonproliferation (ISN), Office of Weapons of Mass Destruction and Terrorism. He served as NATO project director (NPD) for eight activities funded under NATO's Science for Peace and Security program. Inspired by nature and guided by societal necessities, he strives for technological innovations to address the global challenges of the 21st century. He specializes in dual-use research to identify embedded hybrid threats, using research tools such as foresight, heuristics, artificial intelligence, and complexity science. His research interests include chemical-biological sensors, nanotechnology, environmental/ecotoxicology science, critical infrastructure protection, and the environmental impact of micro- and nano-plastics, all utilizing the nexus of advanced technological solution platforms. He is a Fulbright Specialist through 2026 and serves as a research fellow at the Center for Disruptive Technologies and Future Warfare in the Institute for National Strategic Studies at the National Defense University. He is the author/editor of 27 books and has published over 400 articles in scientific journals, book chapters, and conferences. He serves on the editorial boards of several international journals and is an active member of various professional organizations.

INTRODUCTION

Mitat Çelikpala

Emerging disruptive technologies (EDTs) represent innovative advancements that increasingly permeate various facets of contemporary life, ranging from electronic devices such as smartphones and computers to everyday activities, including grocery shopping and banking. These technologies are effecting significant transformations in organizational and industrial operations while concurrently exerting profound influences on security paradigms. As dual-use technologies, EDTs present a spectrum of risks and opportunities that affect a diverse array of stakeholders, including corporations, governments, and international organizations. Their expanding influence impacts all societal domains and necessitates the reevaluation of security strategies, which must now address new threats posed by both state and non-state actors within military and civilian contexts.

NATO is especially affected by the dynamics of EDTs, which significantly shape operational strategies and strategic planning among its member states and allies. The introduction of innovative technologies presents new opportunities for NATO's military forces, enhancing their effectiveness, resilience, cost efficiency, and sustainability while simultaneously addressing immediate capability shortfalls and achieving defined objectives. Nevertheless, these technologies also introduce new vulnerabilities stemming from threats by both state and non-state actors, in turn targeting both military and civilian targets. To leverage these opportunities while mitigating the risks associated with EDTs, NATO has engaged in collaborative efforts with member states to develop responsible, innovative, and agile policies regarding these technologies. Moreover, NATO is actively facilitating the acceleration of the adoption and integration of new technological innovations among its Allies. By fostering partnerships with relevant stakeholders in academia and the private sector, NATO aims to sustain its technological superiority and military preeminence, thereby reinforcing its capacity to deter aggression and protect Allied nations.

In December 2019, NATO leaders established an Emerging and Disruptive Technology Implementation Roadmap, delineating seven pivotal areas: data, artificial intelligence (AI) and autonomy, quantum technologies, biotechnology and human enhancement technologies, hypersonic technologies, and space. This roadmap aims to provide a framework for NATO's initiatives in these critical technological domains, facilitating member nations' assessments of the implications of such technologies for deterrence, defense, and capability development. In July 2020, the Secretary General appointed the inaugural NATO Advisory Group on Emerging and Disruptive Technologies, composed of 12 external experts from the private sector and academia, representing the diverse nations within the Alliance. This group is tasked with offering strategic guidance to NATO on the adoption of innovative technologies, while also addressing interconnected aspects of education, financing, and the overall innovation ecosystem.

NATO Defence Ministers endorsed the first-ever strategy, 'Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies' in February 2021. This framework serves as NATO's overarching strategy to instruct its relationship with EDTs, bifurcating its focus into two principal domains: fostering a coherent approach to the development and adoption of dual-use technologies – approaches that cater to both commercial markets and defense applications – to

enhance the Alliance's technological edge; and establishing a forum for Allies to fortify their defenses against the exploitative use of EDTs by adversarial entities, while also safeguarding their own technological innovations and ecosystems from interference and manipulation. These strategic objectives are fundamental to maintaining NATO's strategic effectiveness and dominance.

Currently, following the footsteps of previous efforts, NATO's innovation activities concentrate on nine priority technology areas: Artificial Intelligence (AI); Autonomous Systems (AS); quantum technologies; biotechnology and human enhancement; space; hypersonic systems; novel materials and manufacturing; energy and propulsion; and next-generation communications networks. The Alliance is formulating specific plans for each of these crucial technology domains. These strategies are essential for laying the groundwork necessary for NATO to accelerate responsible innovation and the swift adoption of modern technologies, thereby enhancing decision-making processes and guiding transatlantic innovation for defense and security, in alignment with Allied values, norms, and international law.

At the 2021 Brussels Summit, Allied Leaders agreed to establish the Defence Innovation Accelerator for the North Atlantic (DIANA). This initiative aims to enhance transatlantic cooperation on critical technologies, promote interoperability, and leverage civilian innovation by engaging with academia and the private sector. Launched in 2022, DIANA collaborates with leading researchers and entrepreneurs, from early-stage start-ups to more established companies, to tackle pressing defense and security challenges through dual-use technologies. DIANA operates by conducting competitive industry challenges. Each challenge targets a significant defence or security issue, inviting innovators to develop advanced, dual-use technologies as solutions. Participants selected for DIANA's programs receive non-dilutive grants—investment capital that does not require them to give up equity or ownership of their companies.

Furthermore, they benefit from access to over 20 accelerator sites and more than 180 testing centers across multiple countries within the Alliance. Participants also connect with a network of mentors, including scientists, engineers, industry experts, end-users, and government procurement specialists, as well as a community of trusted investors. Lastly, DIANA offers pathways to market opportunities both within NATO and among its Allies.

At the 2021 Brussels Summit, NATO leaders also reached an agreement to establish the NATO Innovation Fund. The NATO Innovation Fund stands as the world's first multi-sovereign venture capital fund, comprising 24 NATO Allies as Limited Partners: Belgium, Bulgaria, Czechia, Denmark, Estonia, Finland, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Türkiye, and the United Kingdom. The fund makes direct investments in start-ups located within any of these 24 participating Allied countries and engages in indirect investments in deep-tech funds that have a transatlantic impact. The Fund is a €1 billion venture capital initiative designed to make strategic investments in start-ups developing dual-use emerging and disruptive technologies essential for Allied security. Many deep-tech start-ups struggle to secure sufficient funding due to the lengthy time-to-market timelines and the significant capital intensity of their research endeavors. The NATO Innovation Fund addresses this challenge by positioning itself as a patient investor

with a 15-year run time, which is more suited to the prolonged timelines that deep-tech start-ups often require.

The strategic concept adopted by NATO during the June 2022 Madrid Summit delineates the primary challenges confronting the Alliance and articulates the approach NATO will employ to address them. It acknowledges that EDTs present both substantial opportunities and inherent risks, fundamentally altering the nature of conflict and acquiring increased strategic significance as vital arenas of global competition. Consequently, the Allies reached a consensus in the Strategic Concept to promote innovation and augment investments in EDTs, thereby sustaining NATO's interoperability and military advantage. Member states will collaborate to adopt and integrate new technologies, work alongside the private sector, protect their innovation ecosystems, establish standards, and commit to principles of responsible usage that reflect the democratic values and human rights upheld by the Alliance.

There is a strong consensus that NATO must prioritize innovation and increase investments in emerging technologies to maintain military interoperability and superiority. NATO characterizes EDTs as advanced innovations that can fundamentally transform warfare and reshape international security. These technologies have the potential to disrupt conventional military operations, shift the geopolitical balance of power, and introduce new strategic challenges for member nations. As a result, NATO emphasizes the importance of comprehensively understanding and proactively adapting to these advancements to maintain both thematic and strategic superiority, as well as to fulfill its collective defense obligations.

To achieve these objectives, NATO collaborates with a diverse array of stakeholders, including public and private sectors, academic institutions, and civil society organizations. This collaboration aims to promote technological innovation, establish international standards for the responsible usage of emerging technologies, and maintain a competitive edge through ongoing research and development. Acknowledging the strategic imperative of keeping pace with technological changes beyond the Alliance, Allied Leaders endorsed NATO's Rapid Adoption Action Plan at the 2025 NATO Summit in The Hague. This initiative aims to significantly accelerate the adoption and integration of new technological products into Allied armed forces, with a target timeframe of 24 months or less. The plan outlines shared objectives and best practices that enhance adoption procedures, allocate resources, and embrace calculated risks, all of which are supported by NATO.

The initiative will empower Allies to expedite their national processes for procuring and integrating new technologies into their armed forces swiftly. It will also facilitate the testing of emerging technologies and mitigate investment risks by establishing NATO-approved standards that foster trust and confidence. Furthermore, it will ensure that defense industry and innovation stakeholders are aligned with NATO's defense priorities and can effectively coordinate their activities to meet the military needs of the Alliance as a whole.

NATO has created various organizations to address EDTs, such as the NATO Data and AI Review Board, the NATO Innovation Board, the Transatlantic Quantum Community (TQC), the Digital Policy Committee, the Conference of National Armaments Directors, the Science and Technology Organization, and the NATO Communications and Information Agency, among others. These strategies and official entities highlight NATO's strong commitment to EDTs, which is closely linked to collaboration with partners across the public and private sectors, academia, and civil

society. Given that many defense applications of EDTs are developed in partnership with the private sector, engaging with industry – particularly start-ups – remains crucial. The North Atlantic Council has hosted several technology-focused sessions that facilitate interactions between Permanent Representatives and executives who are spearheading technological innovations.

Therefore, NATO is undertaking a comprehensive review of its strategies and organizational structures to effectively address both traditional and emerging threats posed by state and non-state actors. This evaluation is vital for ensuring that member states are fully equipped to navigate the complexities of an increasingly dynamic global landscape. In this context, countering terrorism has become a primary focus for NATO and is integral to its operational agenda. The Alliance recognizes that the nature of terrorism is changing, with extremist organizations increasingly exploiting new technologies and social dynamics to advance their agendas. By viewing these extremist threats as opportunities for innovation, NATO underscores the importance of adopting a proactive and multifaceted approach to counterterrorism. This involves enhancing collaboration among member nations, sharing intelligence, and developing strategies that integrate both military and non-military resources to achieve common objectives.

Moreover, NATO is committed to fostering a collaborative environment where shared experiences and best practices can be leveraged to bolster collective security. This fresh perspective in the fight against terrorism is essential not only for neutralizing current threats but also for preventing the emergence of new ones in the future.

Terrorist organizations are increasingly harnessing these EDTs to facilitate their activities in three broad ways: radicalization and recruitment, enhancing operational planning and training, and implementing strategic initiatives, including remote attacks. EDTs provide a new framework for expanding radicalization initiatives, considerably improving the ability of extremist groups to engage with a diverse range of audiences across multiple countries and regions. These groups not only capitalize on cultural and social dynamics to reach potential recruits but also enhance their ability to establish, develop, and sustain social connections. This interconnectedness amplifies their influence and creates pathways for the recruitment of new adherents to their ideology. Consequently, these non-state actors can effectively exploit such technologies to spread misinformation, incite violence, and cultivate virtual ideological and social communities. This not only allows them to promote their extremist views but also fosters an environment where like-minded individuals can connect, share ideas, and reinforce their beliefs, further solidifying their online presence and influence. Through these methods, radicalizers can manipulate public perception and recruit individuals who may otherwise be resistant to their ideologies.

EDTs also offer new ways to plot and train for acts of terrorism. Terrorist groups are likely to be more prepared due to their time planning, preparing, and training in blending augmented and virtual reality. Furthermore, the increasing realism and accessibility of first-person shooter games—particularly those that permit users to create custom environments and scenarios—may contribute to desensitizing individuals to violence. This exposure could lead to a concerning normalization of aggressive behavior, potentially resulting in real-life attacks and violent acts. As these technologies continue to evolve, the implications for security and counter-terrorism efforts become increasingly complex. In response, first responders can combat these

threats by understanding how technological innovations can empower terrorist tactics and by implementing effective countermeasures.

So, terrorists and non-state actors may exploit EDTs to develop innovative attack methodologies. These technologies create new possibilities for executing remote attacks, which could result in high-profile incidents. Furthermore, artificial intelligence (AI), particularly when integrated with machine learning, can assist terrorists in identifying new targets. This capability enables faster decision-making and facilitates efficient adaptation of operational strategies. AI has the potential to significantly enhance both the efficiency and lethality of drone-based attacks.

In conclusion, the intersection of EDTs and terrorism has attracted considerable attention. This volume, Emerging Disruptive Technologies and Terrorism, has been developed under the auspices of COE DAT, one of NATO's prestigious centers of excellence, and examines how these emerging technologies are transforming the capabilities of terrorist organizations. This transformation complicates the efforts of investigators and responders to mitigate these threats. As mentioned above, terrorists may utilize these technologies for various purposes, including enhancing radicalization and recruitment efforts, improving the planning, preparation, and execution of attacks, and adopting new remote methods for conducting assaults. Given the urgency of these challenges, first responders and policymakers must understand how technological advancements can empower terrorist tactics, techniques, and procedures (TTPs). This understanding will enable the implementation of informed countermeasures. To facilitate this dialogue, the following ten articles may prove valuable.

The article by Ambassador (Retired) Mehmet Fatih Ceylan, EDTs, Terrorism and Counterterrorism in a Multi-Domain Context, seeks to elucidate the intricate connections between EDTs and the domains of terrorism and counterterrorism strategies. The author posits that EDTs serve as foundational elements, elaborating on the nuanced analyses presented by various scholars regarding the implications of these technologies in the context of terrorism and counterterrorism initiatives.

To evaluate NATO's evolving perspective, Ambassador Ceylan delineates four critical domains: the physical domain, the cyber domain (encompassing both digital and quantum aspects), the biological domain, and the chemical, radiological, and nuclear (CRN) domains, alongside cognitive considerations. These domains were selected because they currently inform and shape strategic frameworks within a multi-domain operational context adopted by prominent international and regional organizations. The author acknowledges that as EDTs continue to evolve, future assessments may necessitate the identification of additional domains to provide a more comprehensive understanding of their implications.

Ambassador Ceylan highlights a significant contemporary challenge: the potential exploitation of EDTs by terrorist organizations. As the scope of EDTs expands and becomes increasingly sophisticated, protecting against, preventing, mitigating, and deterring their use by terrorist entities has become increasingly complex. This dynamic threat landscape represents an ongoing work in progress, wherein advancements in technology correlate with an increase in the magnitude of disruptions and shocks to the security of states and their citizens.

In the context of defense, there has been a discernible shift toward a non-linear approach that integrates various operational domains—namely, land, air, sea, cyber, and space—into a singular, cohesive structure. This transformation has necessitated

adaptations in the policies, procedures, governance, decision-making processes, doctrines, operational priorities, and science and technology efforts of international and regional organizations, including NATO and the EU.

The ongoing exponential proliferation of EDTs, which present unique opportunities for terrorist organizations, necessitates that relevant entities operate within a multi-domain framework. This interconnectedness is particularly salient, as the convergence of various components of EDTs implies that a terrorist attack leveraging an EDT in one domain could yield a cascading effect across others, thereby causing significant damage within both physical and virtual realms. For instance, a substantial cyberattack on critical infrastructure could inflict considerable costs on societal cohesion and profoundly disrupt routine societal functions.

Moreover, the execution of a disinformation campaign by a terrorist group has the potential to incite social unrest and compromise the resilience of governments and societal structures under siege. Concrete instances of terrorist actions across diverse EDT domains illustrate that the transnational, cross-sectoral, and intersectional nature of contemporary existential risks and threats underscores the necessity of adopting a comprehensive perspective for effective prevention, mitigation, deterrence, defense, and counterterrorism against the exploitation of EDTs.

Ambassador Ceylan concludes by asserting that the contemporary nature of terrorism has transcended the confines of the physical domain, extending into the virtual realm and merging both spheres with grave implications for governmental and societal structures. Considering this emergent phenomenon, counterterrorism strategies at all levels of governance must embrace an integrated architectural framework that encompasses all four EDT domains. Such a plan should be predicated upon a multidisciplinary, multi-stakeholder, and cross-domain approach, aimed at anticipating threats and coordinating responses effectively. This holistic framework requires vigilance, resilience, interoperability, and adaptability, which are supported by the inherent capabilities of EDTs.

Professor Ashok Vaseashta, in his extensive article Human Factors in Terrorism: Countering the Dual-Use of Emerging Disruptive Technologies, critically examines the dual-use nature of EDTs. The accelerated development of these technologies is fundamentally transforming critical sectors, including precision healthcare, defense, cybersecurity, and international security frameworks. However, the inherent dual-use characteristic – wherein these technologies may be employed for both beneficial and malicious purposes – raises formidable concerns regarding their potential exploitation by adversaries and terrorist organizations. Notably, military and civilian critical infrastructure represent prime targets for global aggressors due to their essential roles in various operational contexts.

While such innovations possess considerable potential for generating positive societal outcomes, their misuse can significantly augment the capabilities of non-state actors, thereby intensifying the risks associated with terrorism and violent extremism. Human factors – including cognitive biases, behavioral tendencies, the exploitation of technology, and organizational vulnerabilities – play a pivotal role in how terrorists leverage EDTs. As emerging technologies such as artificial intelligence, biotechnology, 3D printing, quantum computing, and autonomous systems continue to advance at an unprecedented pace, their dual-use potential - encompassing both beneficial and harmful applications – raises critical concerns in the field of counterterrorism.

This paper rigorously explores the human factors that present challenges in addressing malicious intent within counterterrorism efforts and examines the deployment, governance, and ethical oversight of these technologies when repurposed for security objectives. By analyzing numerous case studies and interdisciplinary literature, he elucidates significant gaps in training, accountability, and communication that must be rectified to ensure resilience against misuse. Furthermore, the paper proposes a comprehensive framework aimed at mitigating the risks associated with the dual-use dilemma, emphasizing the necessity of international cooperation, regulatory oversight, and proactive countermeasures.

Addressing the human factors related to EDTs necessitates the implementation of interdisciplinary strategies that involve adapting technology, applying complexity science, utilizing algorithmic control in machine learning, and supporting policymakers and intelligence agencies. This approach is intended to avert the inadvertent contribution to terrorism by these innovations. Effective risk management and counterterrorism strategies must duly consider the evolving nature of these technologies and counter their potential to empower malicious actors in unprecedented ways.

Professor Vaseashta concludes his discussion with a series of policy recommendations aimed at promoting human-centric, ethically informed, and globally cooperative approaches to mitigating the risks associated with dual-use technologies in the security domain. His principal recommendation advocates for the establishment of a proactive, interdisciplinary framework for policymaking—one that anticipates intentional misuse, mitigates unintended consequences, and embeds human-centered ethical safeguards throughout the innovation lifecycle.

He posits that both government agencies and private developers should embrace human-centered design principles throughout all stages of technological development. This encompasses the inclusion of end-users and affected communities in both the design and testing processes, prioritizing transparency, explainability, and accountability in system architecture, and incorporating fallback and override mechanisms to maintain human oversight. Furthermore, he emphasizes the need for governments to establish independent oversight bodies responsible for regulating dual-use technologies across various sectors. Additionally, he emphasizes that public trust is crucial for the legitimacy of security technologies. States and developers should disseminate non-sensitive information concerning the objectives, capabilities, and limitations of deployed tools, thereby facilitating democratic oversight and input, particularly in surveillance-related policies. Supporting independent research and journalism that critically examines dual-use practices is equally essential. While transparency can mitigate the risks of public backlash, misinformation, and erosion of democratic accountability, it also presents a double-edged sword, as adversaries may exploit such transparency and accountability for their own purposes.

In conclusion, the risks associated with dual-use technologies are inherent to emerging innovations and can often be exacerbated by the human factors that influence their development and deployment. Although no solution can be deemed entirely foolproof, a strategic approach founded on ethical considerations, targeted education, robust policy frameworks, and a proactive security posture can substantially diminish the likelihood of misuse and enhance resilience against adversarial exploitation.

In their scholarly article, “Terrorist Threats Emanating from Cyberspace: Disinformation, Radicalization, and Recruitment,” Professors Robert Mikac and Krešimir Mamić address pivotal research questions concerning the use of disinformation by terrorist and criminal organizations within the digital landscape. Their inquiry focuses on (1) how these groups leverage disinformation to facilitate radicalization and recruitment, (2) the principal platforms and tools they employ to disseminate propaganda and attract new adherents online, and (3) the implications of Artificial Intelligence and Deepfake technologies in the proliferation of disinformation and the enhancement of propaganda efforts.

Professors Mikac and Mamić characterize cyberspace as a transformative domain that profoundly impacts contemporary society, offering a multitude of advantages that render it an indispensable component of modern existence. As a global connector, cyberspace transcends geographical barriers, enabling instantaneous communication across continents. This connectivity engenders unprecedented collaboration in scientific research, business, and education, thereby accelerating the processes of innovation and knowledge dissemination. Nevertheless, the authors caution that alongside these myriad benefits, cyberspace harbors significant challenges that necessitate vigilant scrutiny. The rapid dissemination of disinformation and misinformation poses a critical concern, as the propagation of false narratives has the potential to erode trust, manipulate public sentiment, and lead to tangible harm in the physical world. The expansive and interconnected nature of cyberspace, while presenting abundant opportunities, is also systematically exploited by a diverse array of actors engaging in detrimental and illicit activities. This spectrum of malicious entities encompasses nation-states involved in espionage, infrastructure disruption, and political interference, multinational corporations engaging in data exploitation and unethical surveillance practices, and intelligence communities that, while typically operating within legal frameworks, may employ cyber capabilities in covert operations that challenge ethical boundaries. Moreover, terrorist organizations wield the digital realm for propaganda dissemination, recruitment, and attack planning. Organized crime syndicates exploit cyberspace through the use of ransomware, fraud, and data theft. Individual hackers and hacktivists, propelled by motivations ranging from financial gain to political activism, further complicate the threat landscape by engaging in unauthorized access, data breaches, and service disruptions. The pervasive presence of these varied actors underscores the urgent necessity for robust cybersecurity measures and international collaborative efforts to safeguard the digital frontier.

In their comprehensive analysis, the authors focus on how terrorists, primarily, and organized criminal groups, secondarily, utilize cyberspace to achieve their strategic objectives. They examine the sophisticated methodologies employed by these groups to leverage digital platforms for various illicit activities, and the authors specifically investigate the strategies employed by terrorists to disseminate disinformation, thereby manipulating public opinion and instilling fear. Furthermore, they analyze the methods used by terrorists to cultivate radicalization, drawing individuals into extremist ideologies and preparing them for violent actions.

In concluding their analysis, Professors Mikac and Mamić emphasize the intricate and evolving role of cyberspace in the operational activities of terrorist and organized crime groups, with a particular focus on the European context. They assert that the convergence of disinformation, radicalization, and recruitment in cyberspace has emerged as a defining characteristic of contemporary terrorism and organized

crime, particularly within the European Union. Disinformation is framed not merely as a byproduct but as a deliberate and strategic tool used to sway public opinion, promote radicalization, and recruit new adherents. Terrorist and criminal organizations adeptly exploit both mainstream and encrypted digital platforms to disseminate propaganda, coordinate their activities, and create echo chambers that reinforce extremist ideologies. The advent of artificial intelligence and deepfake technologies has further exacerbated these threats, facilitating the rapid and large-scale dissemination of sophisticated disinformation and propaganda. To address these multifaceted challenges, a comprehensive approach is imperative, one that integrates technological solutions, robust regulatory frameworks, international cooperation, and enhanced digital literacy initiatives. By cultivating an understanding of the tactics and tools employed by nefarious actors in cyberspace, policymakers and law enforcement agencies can develop more effective strategies to counter the evolving threats posed by disinformation, radicalization, and recruitment in the digital age.

In his article Terror-AI-sm: The Future of Artificial Intelligence in the Hands of Terrorists, Dr. Aleksander Olech addresses terrorism as a significant challenge to international security. He emphasizes the escalating capabilities of artificial intelligence (AI) and the adaptive nature of terrorist threats, elucidating the intricate relationship between technological advancements and associated security risks. Dr. Olech asserts that there is a notable trend in which terrorist organizations are increasingly harnessing AI for purposes such as propaganda dissemination, cyberattacks, and physical assaults through autonomous combat systems. This trend engenders transformative operational capabilities, fundamentally altering the landscape of asymmetric warfare.

The convergence of AI and terrorism is no longer speculative; it is becoming an immediate reality. As AI systems become increasingly accessible, autonomous, and sophisticated, the potential for their misuse by terrorists presents a formidable concern. AI has emerged as an indispensable tool for terrorist organizations, significantly enhancing their capabilities in communication, planning, targeting, and systemic disruption. This development signifies a profound shift in the dynamics of asymmetric conflict. Historically, terrorism has evolved in tandem with technological advancements; however, the integration of AI may represent an unprecedented transition, reallocating power from state institutions to individual actors on a scale never seen before. Dr. Olech emphasizes the crucial need for a comprehensive understanding of how emerging technologies can be exploited and the mechanisms by which global systems can respond to these evolving threats. He introduces the term ‘Terror-AI-sm’ as a conceptual framework that encapsulates the pressing necessity of comprehending the future of AI under the influence of terrorist actors.

Dr. Olech posits that AI functions as both a multiplier of existing terrorist capacities and a gateway to entirely novel forms of asymmetric conflict. ‘Terror-AI-sm’ serves not merely as an academic construct; it is a critical lens through which to analyze the forthcoming decade of global security challenges. The potential deployment of AI in warfare presents both tantalizing opportunities and grave risks. Although AI can replicate the efficiency of seasoned military personnel, it inherently lacks a moral compass. Consequently, AI-driven weaponry may not adhere to the same ethical constraints that human combatants encounter, which could lead to the adoption of significantly more aggressive tactics. Terrorist organizations, already responsible for extensive civilian and military casualties, would likely exploit such tools to escalate violence. For these entities, AI is simply a novel means to pursue

longstanding ideological objectives – free from the restrictions of morality or proportionality – analogous to the operations of autonomous machines. In this context, AI becomes an instrument designed to maximize destruction while minimizing operational losses.

Moreover, drones may serve pivotal roles in propaganda efforts, showcasing advancements in technology. Driven by their ideological fervor, terrorist groups can be expected to exploit all available means, including both weaponry and drones, to target military and civilian infrastructures indiscriminately, irrespective of AI's role in their operations. The adoption of such emergent tools by violent extremists has transcended the defensive capabilities currently available to state actors, establishing a contemporary 'sword-and-shield' dynamic. The widespread availability of drones – utilized in conflict zones such as Ukraine and spurred by a highly competitive market – affords non-state actors notable air power that is challenging to regulate comprehensively.

In conclusion, to address effectively the threats posed by the prospective weaponization of AI by terrorist organizations, Dr. Olech advocates for coordinated international action. The future of 'Terror-AI-sm' will be determined by the interplay between innovation and regulation, offense and defense, and openness and control. As terrorism evolves at an unprecedented pace, the imperative for decisive, coordinated international action that unites governments, industry leaders, and civil society is more urgent than ever. Absent such concerted efforts, the gap between the potential for harm and the means of prevention will only widen. In this rapidly changing landscape, the critical question is not whether terrorists will weaponize AI, but rather how prepared the global community will be when they inevitably do. The phenomenon of terrorism – like technology is now more globalized than ever.

Ambassador (Ret.) Tacan İldem provides a comprehensive analysis of the intersection between social media and terrorism in his article, "Social Media and the Shadow of Terrorism: Impacts, Risks, and the Way Forward." Leveraging his substantial expertise in diplomacy and security, he delineates the urgent concerns that emerge at the nexus of extremism and digital technologies. The proliferation of social media has given rise to a range of complex and significant risks, including the emergence of cyberterrorism and the dissemination of misinformation. While these platforms possess the capacity to foster connections and facilitate dialogue among individuals and institutions, they simultaneously harbor a more sinister potential: the rapid radicalization of individuals.

Ambassador İldem contends that the risks associated with social media extend beyond the proliferation of harmful content. The underlying algorithms that dictate social media interactions, the anonymity afforded to users, and the incessant flow of information collectively contribute to the virality of extremist narratives. This interplay enables radical content to reach susceptible individuals across diverse geographical and cultural landscapes, significantly influencing their beliefs and subsequent actions in alarming ways. To effectively mitigate the spread of extremist ideologies online, Ambassador İldem advocates for a multifaceted approach. He emphasizes the importance of robust public-private partnerships, which should involve collaboration among governmental entities, technology firms, and civil society organizations.

Furthermore, he accentuates the importance of developing well-designed policy frameworks that can adapt to the rapidly evolving digital environment. Investing in digital literacy programs is crucial, as these initiatives equip individuals with the

analytical skills necessary to evaluate information and distinguish between fact and fiction critically. Additionally, promoting credible counter-narratives is essential; these narratives should form an integral part of a proactive communication strategy that resonates with diverse audiences, thereby showcasing alternative perspectives.

As the digital realm increasingly intersects with our physical existence, Ambassador İldem emphasizes that the challenge of preventing the misuse of social media extends beyond mere technical issues. It has emerged as a pivotal concern for global security and the maintenance of democratic governance. He notes that achieving a balance between the imperative of safeguarding fundamental rights, such as freedom of expression, and the necessity of preventing the exploitation of social media platforms presents a formidable challenge. Efforts aimed at curtailing harmful threats must be meticulously crafted to avoid infringing upon the rights and liberties that underpin democratic societies.

Moreover, he identifies the intertwined relationship between social media and terrorist networks as one of the most pressing threats in the contemporary landscape. Terrorist organizations have evolved beyond simply disseminating propaganda; they now embed themselves within social media platforms, transforming these virtual spaces into nodes for recruitment, coordination, and instilling fear. Ambassador İldem effectively illustrates that the digital landscape constitutes not merely a novel battlefield but a complex and dynamic ecosystem where various factors – propaganda, recruitment, psychological warfare, cybercrime, and hybrid attacks – mutually reinforce and exacerbate one another, presenting significant challenges when confronted holistically.

The advent of sophisticated technologies – including Deepfakes, encrypted messaging, algorithmic manipulation, and advanced disinformation tactics – has outpaced traditional detection and prevention measures. This reality necessitates that responses from governments, technology companies, and civil society organizations remain proactive and comprehensive rather than reactive and fragmented. As new challenges continually emerge, particularly within the encrypted and hard-to-monitor areas of the Internet, additional hurdles arise for those endeavoring to counteract extremist narratives and activities.

In his concluding remarks, Ambassador İldem posits that the objective is unequivocal: to ensure safety while concurrently safeguarding fundamental rights such as freedom of speech, access to information, and privacy. Striking this balance poses a considerable challenge, as formulating policies that reconcile these often-competing priorities is both vital and intricate. He emphasizes the significance of fostering robust public-private partnerships, implementing responsible governance of online platforms, and promoting initiatives that enhance digital literacy. Furthermore, supporting authentic counter-narratives is imperative to engage diverse communities meaningfully and to clearly distinguish between veracity and falsehood. Efforts to curtail the misuse of digital platforms must not come at the expense of democratic values and fundamental freedoms. It is also essential that security and counterterrorism strategies function in concert; their synergistic efforts must aim to prevent attacks while simultaneously bolstering societal resilience against the psychological tactics deployed by extremist entities.

Dr. Zeynep Sütalan’s article, The Role of Digital Ecosystems in the Evolution of Terrorist Strategy of Radicalization and Recruitment, undertakes a comprehensive analysis of how open digital ecosystems function as platforms that facilitate

radicalization by design. In contrast, closed digital systems can promote radicalization by fostering a sense of trust and legitimacy. Dr. Sütalan characterizes open digital ecosystems by their high visibility, mass engagement, and algorithmically curated content. Platforms such as YouTube, TikTok, Instagram, and X (formerly Twitter) shape user experiences through automated recommendations that prioritize engagement metrics.

Terrorist actors capitalize on this structure to foster environments of ambient radicalization, wherein individuals are passively and insidiously exposed to extremist narratives. Conversely, closed digital ecosystems rely on encrypted, small-scale, trust-based communication. Platforms, including WhatsApp, Signal, and private Telegram groups, offer end-to-end encryption, low discoverability, and enhanced user control, which render them particularly conducive to relational radicalization. In such frameworks, recruitment is achieved through personal connections, hereditary networks, or peer affiliations. These micro-networks often exist within diaspora communities, religious congregations, or cultural associations, where shared identities and grievances create fertile ground for ideological persuasion and influence. Unlike open ecosystems, where exposure is indirect, closed systems depend fundamentally on the deliberate establishment of trust.

Dr. Sütalan asserts that the digital environment has emerged as a pivotal arena for contemporary terrorist radicalization and recruitment. Terrorist organizations strategically exploit both open and closed digital ecosystems, each fulfilling distinct yet complementary roles within the radicalization continuum. Open platforms, such as YouTube, Twitter/X, or TikTok, provide expansive outreach, algorithmic amplification, and low barriers to entry for individuals who may only possess a peripheral interest in extremist ideologies. Through viral content, memes, and influencer-driven engagement tactics, these platforms normalize extremist discourses, reduce psychological barriers to entry, and serve as gateways to more insular communities.

In contrast, closed digital ecosystems – including Telegram, encrypted forums, and the dark web – create controlled environments where radicalization can intensify, and recruitment can be formalized. Within these secure spaces, terrorists can insulate their followers from external scrutiny, reinforce their ideological commitment, and coordinate operational or logistical planning under the safeguard of anonymity and encryption. Consequently, open and closed ecosystems should not be perceived as mutually exclusive entities but rather as interdependent stages within a dynamic radicalization pathway.

The critical analysis of this exploitation yields several important implications. First, it enables scholars and policymakers to map the trajectories of individuals across digital spaces, from initial exposure and indoctrination to mobilization and action. Such mapping is essential; without it, counter-radicalization strategies risk treating platforms in isolation, thereby overlooking the interconnected nature of extremist ecosystems. Second, recognizing these dynamics highlights the methods by which extremists manipulate algorithmic recommendation systems, digital affordances, and social engineering tactics to maximize their audience reach and retention. Third, this analytical framework enables the anticipation of adaptive strategies, as terrorist groups swiftly migrate to new platforms or modify their digital presence in response to regulatory and security interventions.

The ramifications for policy formulation are profound. By elucidating the complementary functions of both open and closed platforms, governments and

international organizations can develop targeted and differentiated interventions that effectively address the needs of diverse populations. Strategies for open platforms should focus on content moderation, algorithmic transparency, and the dissemination of counter-narratives that disrupt recruitment at its nascent stages. Conversely, closed ecosystems require intelligence-led approaches, including lawful access mechanisms, digital infiltration, and international collaboration to penetrate and monitor highly secure environments. Most crucially, effective policy must also address the cross-platform continuum, ensuring that interventions do not inadvertently displace terrorist activities from one platform to another without destabilizing the broader ecosystem.

In summary, the systematized analysis and recognition of how terrorists exploit digital ecosystems is imperative for the development of effective policy frameworks. Such analysis enables the development of holistic, adaptive, and rights-conscious approaches that can both prevent radicalization at its origins and disrupt its consolidation within secure environments. Absent this recognition, counterterrorism strategies risk remaining fragmented and reactive, thereby leaving critical vulnerabilities that extremists are well-positioned to exploit.

In his article The Future of Counterterrorism for the Intelligence and Security Agencies in the Age of Emerging and Disruptive Technology, Major General (Retired) Paul Hurmuz provides a comprehensive analysis of the contemporary landscape and prospective developments in counterterrorism and intelligence operations, particularly considering the transformative influences of EDTs. He critically examines the mechanisms through which Intelligence and Security Agencies (ISAs) can adeptly re-evaluate their strategic intelligence priorities while concurrently embracing technological innovations, all without compromising their core missions and ongoing operational efficacy.

General Hurmuz systematically explores the ramifications of EDTs on ISAs, placing particular emphasis on the transformative potential of AI in reconfiguring intelligence operations. He articulates that, despite the myriad advantages conferred by technological advancements—including improved data analysis capabilities and enhanced operational efficiency—ISAs encounter substantial challenges associated with these technologies. As both state and non-state adversaries increasingly adopt and exploit novel tools, Hurmuz underscores the imperative for ISAs to remain cognizant of and proactive in addressing the complexities that arise within this multifaceted technological paradigm.

A significant focus of General Hurmuz's discourse centres on the erratic and unpredictable impacts of EDTs on societal structures, including their propensity to engender terrorism. He posits that ISAs must cultivate a nuanced comprehension of the innovative capabilities possessed by both state and non-state actors, particularly on how these entities are adept at synthesizing various technological instruments to exploit specific vulnerabilities inherent in societal frameworks. This necessitates an acute awareness that the availability of new technologies – particularly those characterized by accessibility, affordability, user-friendliness, portability, concealability, and effectiveness – will likely result in rapid adoption and adaptation by Violent Extremist Organizations (VEOs).

General Hurmuz identifies several emerging technologies that possess the potential to augment the operational reach and effectiveness of terrorist organizations. For instance, the proliferation of commercial drones introduces new modalities for surveillance and targeted interventions, while advancements in cyber weaponry

facilitate unauthorized incursions into critical infrastructure. Furthermore, innovations in 3D printing enable the swift fabrication of weaponry and associated tools, thereby amplifying the destructive capacity of VEOs. The democratization of access to previously restricted dual-use technologies, facilitated by AI, further empowers these groups, enabling them to harness sophisticated resources that could significantly enhance their operational capabilities. Within this context, Hurmuz elucidates the myriad ways in which terrorists may exploit software, including reverse engineering open-source military applications, leveraging leaked battlefield technologies, and repurposing drone control software and AI-enhanced targeting systems to further their objectives.

In navigating the challenges posed by a landscape characterized by Volatility, Uncertainty, Complexity, and Ambiguity (VUCA), General Hurmuz contends that ISAs must fundamentally reevaluate their operational strategies, technological frameworks, and methodological approaches. The diffusion of EDTs among both state and non-state actors engenders a novel asymmetry in warfare, wherein success increasingly hinges on 'innovation power' – the ability to rapidly invent, adapt, and deploy cutting-edge technologies in a manner that outpaces adversaries. Technologies such as high-performance computing, cloud computing solutions, advanced sensor systems, AI, and data analytics possess transformative potential for critical intelligence missions and processes in the near term. Moreover, he notes that advances in domains such as space-based intelligence collection, quantum computing, robotics, nanotechnology, and synthetic biology present ISAs with new avenues to enhance their operational capabilities and effectiveness. Nevertheless, Hurmuz acknowledges that harnessing these advanced capabilities raises complex legal and ethical considerations. He emphasizes the pronounced public expectation that ISAs will conduct operations that prioritize the safeguarding of citizens' rights and freedoms. The expansive scope of surveillance, data collection, and targeting necessitates the establishment of appropriate policy and legal frameworks, which are essential to mitigate civilian casualties, enhance accountability and oversight, and ensure compliance with international legal principles and treaties. As ISAs navigate these multifaceted challenges, they must adopt a balanced approach that harmonizes the embrace of technological advancements with the upholding of fundamental rights and liberties of the populations they serve.

Professors Özgün Erler Bayır and Seray Baykal explore novel and understudied themes in their article, "Cyber Diplomacy in the Space Age: Fostering the Responsible Use of Space for Global Security." This scholarly work investigates the role of cyber diplomacy in addressing cybersecurity threats, specifically those targeting national digital infrastructures and space-based systems. Furthermore, it examines how EDTs, when combined with the responsible use of space, can be leveraged for the greater good. The authors underscore the potential of diplomatic initiatives to transform disruptive forces into opportunities that promote global peace and security.

As space technologies become increasingly integrated into global communications, navigation, and defense frameworks, they are concurrently subjected to rising cyber threats, which introduce novel security challenges. Satellites and other forms of space infrastructure are indispensable to contemporary life, thereby necessitating their robust protection within the cybersecurity landscape. In this regard, cyber diplomacy emerges as a critical instrument for fostering international collaboration, nurturing trust among nations, and establishing normative frameworks

for managing cybersecurity risks associated with space technologies. Additionally, cyber diplomacy provides a structured approach for mitigating risks, thereby ensuring that space technologies are utilized responsibly and securely.

The concept of 'responsible use of space' encompasses not only the benefits derived from space technologies but also the imperative to prevent space pollution and ensure sustainability. It emphasizes the need to leverage technological advancements – particularly in space – to address humanity's collective global challenges. Thus, the responsible use of space extends beyond environmental preservation; it encompasses the strategic application of space technologies for the standard good and international security. Attaining this goal necessitates effective diplomatic engagement within the cyber domain.

The authors argue that the practice of cyber diplomacy necessitates a coherent set of regulatory frameworks at both the national and international organizational levels. Presently, however, the efficacy of cyber diplomacy is constrained by significant deficiencies in current legal frameworks, international agreements, and the absence of a universally accepted set of norms. Such limitations impede the effectiveness of cyber diplomacy, which is often perceived not as a catalyst for human-centered, norms-based solutions but as a challenge that exacerbates existing issues. Nevertheless, this challenge can be reframed as a strategic opportunity. By leveraging space technologies, there exists the potential to develop innovative solutions to global security challenges more efficiently and effectively, provided that existing obstacles are duly addressed. The establishment of international norms, along with mechanisms to ensure compliance through enforceable measures at the organizational level, would substantially enhance the efficacy of cyber diplomacy, thereby facilitating the responsible use of space while transforming the potential adverse effects of technological advancement into constructive outcomes.

In conclusion, the authors argue for the establishment of a more concrete and rules-based nexus between diplomacy, science, and technology. Ensuring secure and reliable engagement, particularly within digital domains and cyberspace, is vital for augmenting the capacity and agency of both state and non-state actors. Moreover, with recent advancements in technology and the emergence of new infrastructures linked to space, the responsible use of space has gained even greater significance.

Historically, space endeavors were predominantly characterized by missile development, armament, and significant state-led investments. In contrast, the emerging paradigm of 'New Space' has diversified the landscape, with private enterprises and the commercial sector assuming pivotal roles alongside state actors, all while associated costs have decreased markedly. This evolution not only presents risks but also substantial opportunities. Ultimately, the collective responsibility lies with both state and non-state actors, underscoring the importance of aligning their objectives and coordinating efforts within this evolving context.

In a thorough examination, Professor Sıtkı Egeli delineates the transformative impact of uncrewed vehicles – commonly referred to as uncrewed or uninhabited vehicles – on contemporary warfare in his article, "Innovative Tools Available to Non-State Actors: Aerial Drones and Unmanned Systems at Sea and on Land." Egeli's discourse elucidates how a diverse array of actors, including lone wolves, terrorist organizations, and organized crime syndicates, have increasingly integrated drones into their hybrid warfare methodologies. This paradigm shift has fundamentally altered the perceptions of threats and security priorities for states worldwide.

Professor Egeli initiates his analysis by scrutinizing the modalities through which non-state actors employ drones, accentuating the tactical advantages these devices confer in combat scenarios. He asserts that access to drone technology has empowered these actors to undertake sophisticated operations that were historically the prerogative of state militaries. This empowerment not only redefines the contours of conflict but also engenders novel challenges for national security. Subsequently, he pivots to an examination of the responses elicited from state actors striving to mitigate the risks associated with the burgeoning prevalence of UAVs. The article furnishes a comprehensive overview of contemporary defensive measures and technologies being deployed by states to counter the drone threat, including missile defense systems, electronic warfare strategies, and counter-drone technologies designed to detect, disrupt, and neutralize UAVs. Professor Egeli discusses the growing significance of these initiatives across various domains, encompassing maritime, underwater, and terrestrial environments.

In his analysis, Professor Egeli concludes that technological advancements in uncrewed vehicles have frequently been appropriated and operationalized by non-state actors before being integrated into military contexts by conventional national forces. He notes that non-state entities have harnessed operationally relevant UAVs, First-Person View (FPV) drones, and one-way attack uncrewed sea vehicles (OWA-USVs) ahead of state actors, thus affording them a substantial tactical advantage in numerous conflict scenarios.

The research reveals a critical disparity: new forms of uncrewed vehicles and advanced technologies have disproportionately benefited non-state actors over state actors. A notable exception to this trend is the deployment of larger UAVs by state forces, which have proven pivotal in counterinsurgency and counterterrorism operations. These sizable UAVs, capable of conducting intelligence, surveillance, and reconnaissance (ISR) operations, have facilitated state actors in executing surgical strikes and targeted kill operations with enhanced precision. Nonetheless, the 2010s and 2020s have heralded a significant shift in the accessibility of drone technology, marking a democratization of these tools. Non-state actors can now procure smaller, less technologically sophisticated, yet highly effective uncrewed vehicles at a fraction of the cost of conventional military platforms. The proliferation of operationally viable OWA and FPV drones has recalibrated the tactical equilibrium, favoring non-state adversaries and compelling state security forces to adopt a more reactive stance. These economically advantageous and readily accessible systems, when employed with ingenuity and judicious targeting strategies, are capable of inflicting substantial and disproportionate damage on state forces.

Professor Egeli contends that as long as states fail to adapt their air defense architectures effectively to counter the drone threat, they will persistently encounter substantial challenges from technologically astute non-state actors. The increasing accessibility and affordability of drone-related hardware and operational know-how exacerbate this dilemma. Ultimately, Professor Egeli posits that uncrewed vehicles are not merely a transient phenomenon but are fundamentally reshaping the dynamics of conflict engagement between state and non-state actors. In the absence of an emergent wave of technological advancements capable of neutralizing the advantages currently possessed by non-state actors, the drone threat may persist and escalate. Furthermore, ongoing innovations, including the development of AI-enabled drone swarms, autonomous navigation capabilities, and enhanced target recognition technologies, portend a challenging future in which the threats posed by uncrewed

vehicles to state actors continue to intensify. Given these realities, it is imperative for policymakers and security agencies to familiarize themselves with this evolving paradigm and to prepare robustly for the complexities and challenges it presents.

In the concluding article of the collection, The Potential Use of Emerging Disruptive Technologies by Non-State Actors in the Energy Domain, Professor Mitat Çelikpala examines the role and significance of EDTs within the energy sector, with particular emphasis on their potential application by non-state actors. The energy sector is characterized by extensive interconnections with critical industries and a strong focus on technology and innovation, making it a frequent recipient of EDTs.

Private companies, both domestic and international, play a vital role in this sector, serving as both owners and operators. This involvement presents substantial opportunities and inherent risks linked to technological advancements. Consequently, EDTs are pivotal tools for transforming fundamental energy infrastructures, thereby revolutionizing methodologies related to energy generation, distribution, and consumption. Considering global challenges such as climate change and the finite nature of fossil fuel reserves, these technological innovations offer a strategic pathway towards establishing a more sustainable and resilient energy future. From this perspective, EDTs play a crucial role in the ongoing transition from dependence on fossil fuels to a renewable and clean energy foundation.

The dynamic interaction between EDTs and critical energy infrastructures is essential for the development of a secure and sustainable energy paradigm. By embracing innovation while effectively managing associated challenges, stakeholders can cultivate an energy landscape that is more resilient, efficient, and accessible. The integration of these technologies not only enhances the performance of existing systems but also lays the groundwork for a transformative energy ecosystem that can meet the needs of a growing global population while simultaneously safeguarding environmental integrity.

Moreover, the intersection of terrorism and EDTs poses a significant threat to global security, particularly concerning critical energy infrastructure. As the energy sector rapidly adopts innovative technologies, it inadvertently creates new vulnerabilities that malicious actors may exploit. A comprehensive understanding of this relationship is crucial for devising robust defense and protection mechanisms to prevent potential attacks that could disrupt energy production, distribution, and consumption.

Professor Çelikpala seeks to address several pertinent questions: What specific measures can stakeholders implement to enhance cybersecurity in energy infrastructure? How can organizations effectively balance the innovation of energy technologies with the necessity for security? What role do international collaborations play in addressing the security implications associated with emerging energy technologies?

In addressing these, it is imperative to recognize that EDTs embody not only a wave of innovation but also intricate challenges in the ongoing struggle against terrorism. Technologies such as artificial intelligence, blockchain, and advanced surveillance systems offer substantial benefits; however, they concurrently introduce new vulnerabilities that nefarious actors may exploit. This evolving landscape requires a thorough reevaluation of existing strategies and methodologies to counter these threats effectively.

The transformation of the energy sector through EDTs introduces numerous vulnerabilities that terrorist organizations could potentially exploit. An increasing reliance on digital systems, smart grids, and the Internet of Things (IoT) devices in energy production and distribution has rendered critical energy infrastructures more susceptible to both physical threats and cyberattacks. To mitigate these evolving risks, it is essential for stakeholders – including governmental agencies, private sector entities, and international organizations – to engage in vigilant monitoring, innovative problem-solving, and robust inter-sectoral collaboration.

By prioritizing security measures and fostering resilience within the energy sector, stakeholders can establish more effective defenses against potential terrorist actions. Such efforts necessitate investment in advanced cybersecurity protocols, conducting thorough and regular risk assessments, and ensuring that energy infrastructure is fortified against both physical and cyber threats. These proactive measures not only safeguard essential services, such as electricity and fuel supply, but also promote broader societal stability by maintaining public trust in critical systems.

In conclusion, the intersection of terrorism and EDTs poses considerable challenges to global security, particularly regarding the integrity of critical energy infrastructure. As the energy sector increasingly incorporates innovations such as renewable energy sources, artificial intelligence, and automation, it inadvertently creates new vulnerabilities that malicious actors may exploit. A nuanced understanding of this relationship is essential for developing effective strategies to prevent potential attacks that could disrupt energy production, distribution, and consumption. Furthermore, stakeholders must remain informed about the latest technological advancements and their implications for security in the energy domain.

CHAPTER 1

EDTS AND TERRORISM AND COUNTERTERRORISM IN A MULTI-DOMAIN CONTEXT

Mehmet Fatih Ceylan

I. INTRODUCTION

Terrorism has been and still is one of the main sources of threats that challenges peace, security, stability and well-being of the international community.

It has so far manifested itself in different forms throughout history spanning from the use of explosives, assault weapons, guerilla warfare, hijackings, kidnappings, stabbings, money extortion, hit-and-run attacks, sabotage, armed attacks against governmental and societal entities to the exploitation of dual-use technologies, Improvised Explosive Devices (IED), use of different vehicles for attacks (i.e. vehicular terrorism), lone-wolf operations, suicide bombings, disinformation/misinformation campaigns, hybrid warfare, and finally the exploitation of Emerging and Disruptive Technologies (EDTs hereafter) for terrorist operations.

During the Cold War period, that is, in a bipolar world order, both blocs strove to have the technological edge for maintaining supremacy, and kept technological advancements confined to the maximum extent to defence-military domains. The urge to jealously keep them from public channels and to imply strict measures for their protection was robust and rigid. Such an institutional context impeded the diffusion of such novel technologies to adversaries, thus limiting the access of those non-governmental actors, including terrorist groups, to them. Such a restrictive framework of security did not stop the non-governmental entities with malign intentions from breaching measures of protection, nor of their spying activities to reach the level of know-how to produce such capabilities.

By the end of the Cold War terrorism had been identified as one of the main asymmetrical threats to deal with in addition to weapons of mass destruction (WMD), ballistic missiles, disruptions of access to energy and vital resources, organized crime, mass movement (i.e., irregular migration), regional conflicts, failed states etc.

These new risks and threats had driven the main strategy documents of both NATO and the EU in the immediate aftermath of the Cold War period. The greatest perceived threat for NATO was the probability of WMDs falling into the wrong hands,

especially terrorists. As a strong countermeasure, NATO became the frontrunner in advancing arms control, disarmament, and non-proliferation initiatives. (1) (2) (3)

With the end of the Cold War, the majority of Western state actors and international/regional organisations gave traction to globalisation based on a 'rules-based liberal order'. This new global order had indeed brought about expansion in economic-commercial ties, strengthened connectivity among different regions and continents, and accelerated the process of the trickling down of technology, both conventional and emerging.

The global spiral of technological advancements has proven beneficial for both state and non-state actors. However, the more democratization, privatization, and commercialization of technology has taken place, the more the risks and threats for governments and societies have emerged.

It is under such a largely under-regulated and under-governed context that EDTs such as artificial intelligence (AI), unmanned systems, quantum computing, bio- and nano-technology, advanced cyber capabilities, and space technologies have started to take 'the driving seat'. These new and emerging technologies have blurred the line between war and peace and the distinction between reality and fiction. They have been instrumental in weakening the resilience of governments and societies, making them vulnerable to shocks and disruptions in all domains of life. Almost all of them could be used either for improving the quality and productivity of states and societies or for inflicting heavy damage to the well-being of the international community, organizations, and citizens on a global scale. In that sense, if left unchecked, the EDTs, particularly when employed simultaneously in a multi-domain space, could be defined as 'EDTs of Mass Destruction' under these new circumstances.

Given the increasingly diffuse nature of the threat landscape, it has thus become essential to take the evolution of the policies, doctrines, practices and procedures NATO has implemented over years.

During the Cold War the Alliance had maintained its deterrence and defence throughout three main operational domains: land, sea, and air. The defence and reinforcement plans focused primarily on intra-domain specificities against different contingencies without denial of the importance of joint operations that tie together different forces. In the main, the linear concept of operations (Air-Land battle) was in fashion. (4)

The post-Cold War period caused a shift toward a more integrated, notably non-linear way of conducting deterrence and defence. This shift manifested itself in the Combined and Joint Task Forces (CJTF) concept adopted in 1994 at the Brussels Summit. The Concept was designed as a multinational (combined) and multi-service (land, air, sea) task force to operate in unison during a battle with the commensurate Command and Control (C2) structures. It has evolved into initially NATO Response Force (NRF) followed by Very High Readiness Joint Task Force (VJTF) as a module within NRF against the backdrop of an increased threat to the Euro-Atlantic security by Russia's aggressive posture in Ukraine. (5) (6) (7) (8)

The underlying premise of CJTF was to add different modules of forces depending on the evolving circumstances of the battle theatre. In that framework, the strong inclination toward a network-centric structure became prevalent. Hence the journey toward Multi-Domain Operations (MDO), bringing together a network-and data-centric approaches, thus culminating in an overall Network of Networks structure in a digitised era. (9)

One of the underlying premises of MDO is to converge effects across all domains – air, land, maritime, space, and cyberspace – to surpass those of adversaries in competition and conflict. MDO is, in a way, reliant on a variable geometric structure, including conventional as well as non-conventional assets and capabilities (i.e. the modalities of EDTs).

NATO adopted primarily a capability-based (both conventional and nuclear) approach for deterrence and defence during the Cold War period with an intelligence informed understanding against the only source of threat (i.e., the Warsaw Pact), and following the Cold War shifted to capability- and effects-based structures and forces with more emphasis on effects of potential MDOs accompanied by comparatively modest Levels of Ambition (LOA) it set for itself. Given the recent flow of events, which upended the global security landscape, the adoption of novel ways to perform MDOs alongside the continuum of capability-threat-effects-intelligence-based and EDT-enabled structures and forces became inevitable. This holistic model should be applicable to counter the two main threats, that is, Russia and terrorism, defined by the latest Strategic Concept, as well as other sources of risks the Alliance faces.

The overall model adopted by the Alliance, which also inspires the EU's efforts in the security and defence fields, brings MDOs into sharp focus the priority that should be attached to an EDT-enabled MDO construct.

Insofar as EDTs and terrorism and counter-terrorism in a multi-domain context are concerned, the taxonomy used in this analysis will comprise physical, cyber (digital and quantum), biological, chemical, radiological, nuclear (BCRN), and cognitive domains. These four fundamental domains of EDTs have been selected due to the fact that they presently represent disruptive technological innovations that shape and inform strategies under a multi-domain operational framework adopted by the leading international and regional organizations. As EDTs further develop, it is highly likely that future analyses will have to define additional domains within a broader picture.

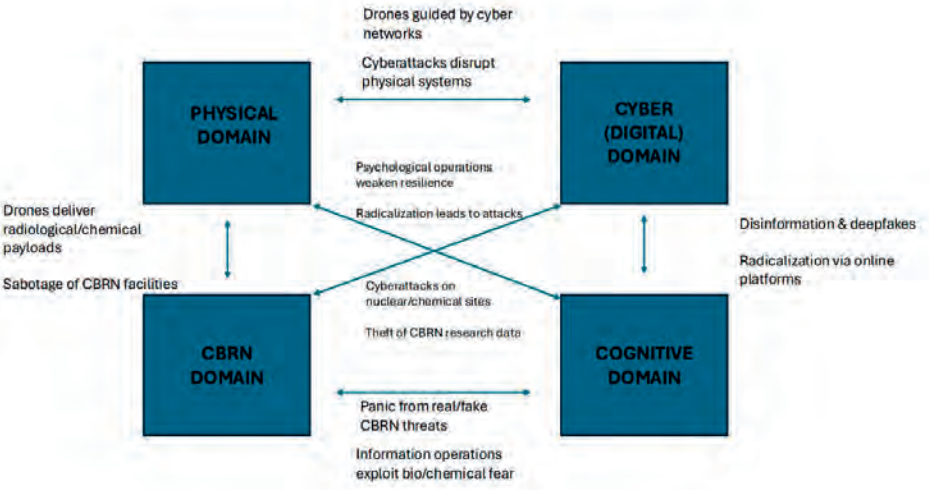


Figure 1: Multi-Domain Context

The purpose of this chapter is to provide an overall frame for the linkages between EDTs and terrorism/counter-terrorism efforts and initiatives. For this reason, it should be seen as a scene-setter, since in the subsequent chapters, detailed analyses will be elaborated by different analysts on diverse aspects of the implications of EDTs as they relate to the subject of terrorism and counterterrorism.

II. THE PHYSICAL DOMAIN

Physical terror attacks against critical assets and infrastructure have so far been the most notorious trademark of terrorism. They can be committed in the form of bombings, hijackings, suicide attempts against political and industrial figures, kidnappings, illegal arms and drug smuggling, extortion or money laundering for malicious intent etc. Those terror related activities and how to counter them were well documented in a flurry of policy documents adopted by the UN, OSCE, the EU and NATO.

Key institutional frameworks such as the UN Global Counter-Terrorism Strategy (2006), the OSCE Consolidated Framework for the Fight Against Terrorism (2012), NATO's Defense Against Terrorism Programme of Work (DAT POW), Council of Europe Counter-Terrorism Strategy (2018) (10) , the EU Counter-Terrorism Strategy (2020) and UN80 Reforms to United Nations Counter-Terrorism Activities Report (2025) (11) offer comprehensive guidance for countering traditional physical threats, with an emphasis on multilateral coordination, critical infrastructure protection and technological adaptation.

There already exists an accumulated body of knowledge on policy, governance, regulations and procedures to prevent, protect, deter, mitigate and defend against the conventional forms of terrorism, such as physical attacks, at the national, regional, and

international level. The UN's Global Counter-Terrorism Strategy (2006) built around four pillars, ranging from addressing conditions conducive to terrorism to ensuring human rights and the rule of law provides a comprehensive framework. Notably, the Compendium of Good Practices on the Protection of Critical Infrastructure Against Terrorist Attacks (2018) outlines mechanisms such as hybrid governance models (voluntary and mandated), the role of the Counter-Terrorism Committee, and threat assessments involving both the physical and virtual domains. In parallel, the OSCE's Consolidated Framework for the Fight Against Terrorism (2012) and the Bucharest Plan of Action (2001) emphasize multidimensional responses to terrorism across its politico-military, economic, and human dimensions. These documents promote cooperation among national authorities, regional partners, and public-private stakeholders in securing critical infrastructure against conventional threats. OSCE efforts particularly highlight cross-sectoral engagement and the co-development of early warning, conflict prevention, and democratic institution-building in counter-terrorism efforts. (12) (13) (14) (15)

In the context of NATO's initiatives, the Defence Against Terrorism Programme of Work (DAT POW), shaped in the aftermath of 9/11 and subsequent operations in Afghanistan, provides operational guidance and training to prevent and respond to conventional terrorist threats, including attacks on infrastructure, transport, energy grids and financial systems. NATO's 2022 Strategic Concept reaffirms terrorism as a core threat, urging members to integrate counter-terrorism into defense capacity building and resilience initiatives. (16) (17)

The EU, for its part, through its Counter-Terrorism Strategy (2005) and the Security Union Strategy (2020), has operationalized prevention, protection, pursuit, and response as four foundational pillars. Under 'protection', the EU focuses on minimizing vulnerabilities in critical infrastructure, reinforcing CBRN preparedness, and preventing the misuse of explosive precursors. These efforts are supported by Europol and dedicated task forces. Together, these institutional frameworks reflect an institutionalized and cooperative approach toward conventional counter-terrorism and infrastructure protection at all levels. Moreover, the EU Strategic Compass (EUSC) for Security and Defence adopted in 2022 reinforces the EU's ambition to become a more assertive and capable security actor, particularly in an environment shaped by hybrid threats, terrorism, and EDTs. It underscores the need to enhance the EU's awareness, resilience, and readiness in the face of increasingly complex threats, including terrorists' resort to dual-use and emerging technologies such as drones, cyber tools and AI. The EUSC also calls for the development of a rapid deployment capacity, enhanced cyber defence coordination, and greater investment in innovation and digital technologies to protect critical infrastructure and European citizens. Importantly, the Strategic Compass aligns with NATO's multi-domain defense orientation while emphasizing the EU-specific tools such as the European Defense Fund, Permanent Structured Cooperation (PESCO), and the EU Innovation Hub for Internal Security to counter both conventional and technologically sophisticated forms of terrorism. (18) (19) (20) (21)

While NATO remains the primary actor in collective deterrence and defense and military-focused counter-terrorism operations, the EU has emerged as a key normative and regulatory power, especially in developing detailed civilian protection frameworks and resilience-building strategies. The two institutions operate in a

complementary manner, with NATO focusing on operational capabilities and military deterrence, and the EU emphasizing legal frameworks, cross-sectoral coordination and technological innovation, including internal security.

AI-enabled unmanned and autonomous systems at the disposal of terrorist groups on land, at sea, and in the air represents a grave challenge for national, regional and international actors. Recent assessments by the U.S. Defense Intelligence Agency indicate that non-state actors continue to explore AI-based systems and unmanned aerial capabilities to strike high-value targets. These groups are increasingly capable of integrating advanced commercial technologies with asymmetric tactics to circumvent conventional defenses and exploit societal vulnerabilities. Use of cyber and hybrid warfare by terrorists further compounds the current threat spectrum. For instance, in 2017, Daesh deployed modified commercial drones in over 300 documented attacks in Iraq and Syria, including kamikaze-style strikes and intelligence-gathering operations using quadcopters with improvised explosive devices (IEDs). The UN Security Council's 2022 Report on Emerging Terrorist Threats noted a "dramatic rise" in the accessibility of unmanned systems and autonomous navigation technologies among non-state actors, especially in conflict zones with porous borders. (22) (23) (24)

Uncrewed Aerial Systems (UAS), commonly known as drones, have been flagged by the UN Security Council Counter-Terrorism Committee as a primary terrorist threat. These systems are attractive to non-state actors because they are affordable, easy to acquire from civilian markets or dark-web vendors, and capable of carrying payloads for reconnaissance, sabotage, or lethal operations including small arms and improvised explosives. By 2024, the drone market was estimated at nearly USD 43 billion, and around 65 non-state actors were assessed to have operational UAS capabilities, underscoring both their accessibility and the urgency of comprehensive regulation and counter-measures. (25)

In the cyber domain, Europol's 2024 Terrorism Situation and Trend (TE-SAT) Report highlights that terrorist-affiliated groups increasingly exploit cyber tools for disinformation campaigns, digital radicalisation, and the probing of critical infrastructure. Europol documented a 55% increase in cyber-attacks by Ideologically Motivated Violent Extremists (IMVEs) between 2022 and 2023. Hybrid threats are also proliferating. The 2023 NATO-EU Task Force on the Resilience of Critical Infrastructure has warned that state-backed and independent terrorist groups could combine cyberattacks with physical sabotage to create cascading failure effects, particularly in the energy, transport, and digital infrastructure sectors. (26) (27)

Dual use products commercially available around the globe that could be modified for terror attacks is a particular area of concern for policy makers, defence planners and security institutions responsible for counter-terrorism efforts. As documented in recent studies, dual-use technologies are often sourced from unregulated markets, including online platforms. These tools can be repurposed for reconnaissance, targeting, or payload delivery, enabling terrorist groups to wage effective asymmetric attacks without state support. (28)

Terror groups can carry out ISR (intelligence, surveillance and reconnaissance) activities in a covert or overt manner on targets they intend to inflict damage. Use of

drones for ISR purposes are routinely used in the Middle East by Hezbollah, the PKK, the PYD-YPG, and the Yemeni Houthis. The PKK, for instance, has been using Iranian origin kamikaze drones of its own and staging drone attacks against Turkish forces and military bases. Recent assessments indicate that terrorist organizations are increasingly adopting commercial drone technology, not only for reconnaissance but also for offensive operations. The growing availability of modular drone components and payload adapters allows groups to convert civilian drones into weaponized platforms with minimal technical expertise. The use of drone swarms and first-person view (FPV) drones has further demonstrated how asymmetric actors leverage accessible technologies to conduct precision attacks at low cost while evading traditional air defenses. (29) (30)

EDTs such as robotics and unmanned systems, particularly drones with autonomous capabilities, enable terror groups to amplify the effect of their acts with a low-cost, commercially available technology, but at a very high cost for target nations and their critical assets. The challenge posed by the use of drones multiplies particularly in the case of drones with different types of weapons. If combined with conventional physical methods of terror, the use of weaponized autonomous drones further amplifies the impact of physical and psychological damage caused to the state and nation targeted by terror groups. Drones were first used by a Japanese cult Aum Shinrikyo in 1995 to deliver sarin attack in the Tokyo underground. Daesh had formed the necessary bureaucratic network in its ranks, namely the 'Unmanned Aircraft of the Mujahideen' to organise drone attacks on Iraqi troops in Mosul in 2017. It was able to fly seventy drones in a day, halting Iraqi forces' operations. It also employed drones against US Special Operations Forces in Iraq and Syria. (31) (32) (33) (34) (35) (36)

Easily procured drones have become a powerful tool for terrorists to use against military forces or civilian targets. Their weaponized versions have morphed into flying IEDs, thus necessitating taking counter measures against their use.

One of the biggest challenges for defense planners and military-security authorities could be drone swarms to be used for terror purposes against multiple targets simultaneously. Daesh had already proven its ability to use drones ('killer bees') flying together against the military troops deployed in Iraq and Syria. It is highly likely that such terrorist groups would draw the necessary conclusions from the effective and frequent use of First Person View (FPV) drones by Ukrainian forces and the recent drone swarm attacks by Ukraine on the Russian strategic facilities and assets. The war between Israel and Iran that started in June 2025 has witnessed the intensive use of sophisticated drones by both states to target critical infrastructure in both countries. Although terrorist groups, for the time being at least, do not possess such highly advanced drones for employment against population centres and the critical infrastructure of a targeted country, they may be drawing the necessary lessons for themselves to inflict high-cost damage to their perceived adversaries in the future. The implications could be even more serious if EDTs intersect with the potential sabotage of nuclear infrastructure. As recent global security reports have emphasized, terrorist threats involving EDTs can extend to scenarios such as remote sabotage of nuclear command-and-control systems or interference with critical safety mechanisms. (37) (38)

Given the current trends in the proliferation of drone technology and its use in daily life, counter-drone measures are becoming more important than ever, particularly for the military and security forces of many countries. From a military perspective, use of surface-to-air attack assets, electronic warfare, the employment of aerial assets to shoot down identified or unidentified UASs, laser-guided systems against drones are commonly used in the battlefield in Ukraine, Russia, Israel and Iran. The operational code of conduct against drones used by terrorist groups is, in the main, the same as those implemented in different theatres of conflict.

Another challenge in terms of combating terrorism is the potential use of driverless, autonomous vehicles by terrorist organisations. This could be the next level of "vehicular terrorism" targeting populations and high value centres for a nation. The current absence of attacks by autonomous vehicles cannot be taken for granted in counter-terrorism efforts. So far terrorist groups have either used vehicles with drivers that they have detonated in their attacks against military forces or facilities or rammed through crowds in different cities to spread fear and panic. Notable examples include the 2016 Nice truck attack, where a 19-tonne cargo truck was deliberately driven into a crowd celebrating Bastille Day, killing 86 people and injuring hundreds; and the 2017 Barcelona attack, in which a van was used to ram pedestrians along Las Ramblas, leaving 16 people dead and more than 130 injured. In that sense, they are already familiar with techniques and tactics in implementing terror acts with vehicles. They might as well leverage autonomous vehicles of different sorts in committing terror acts against their identified military and civilian targets. It would, therefore, be in the direct interest of states and non-state entities that invest in autonomous vehicles technology to introduce measures in the design of such territorial systems to prevent their use for malign purposes. (39) (40)

Autonomous or Remotely Controlled Maritime Uncrewed Systems (MUS) could also be included in the toolbox of terrorist networks against targets in the maritime domain. The EU and NATO have embarked upon investment and research into multinational MUS projects to protect maritime infrastructure against adversaries. (41) (42)

The successful employment of such systems by Ukraine against Russia in the Black Sea to destroy Russia's critical assets of the Black Sea fleet and its headquarters could set a precedent for terrorist groups to plot attacks against maritime infrastructure, including undersea cables and oil rigs. It would, therefore, be prudent for competent state and non-state institutions to put effective measures in place against such a contingency before it is late.

III. THE CYBER (DIGITAL-QUANTUM) DOMAIN

The exponential expansion in the cyber domain, including its propensity to diversify the interconnectedness of a variety of public and private sectors, is one of the trademarks of recent ties.

Combining dual-use technologies with widely accessible reach and on a global scale and the ever-increasing digitisation spreading throughout the world, it is evident that terrorist groups are on watch to leverage the cyber (digital-quantum) space for malicious intents such as launching attacks both in physical and virtual realms. The

cyber domain has thus become a subject for not only geostrategic competition among states, but an open space for terrorist organisations in which they can organize their activities with more efficiency and accuracy on lower costs.

Recent policy briefs underline that the 'hybridisation' of cyber operations now integrates misinformation, ransomware and attacks against critical infrastructure as parallel strategies. According to NATO and private-sector assessments, digital resilience is no longer limited to traditional cybersecurity, but encompasses safeguarding public trust, countering information manipulation, and ensuring the integrity of democratic processes under persistent hybrid threats. (43)

Artificial intelligence (AI) is a powerful tool for terrorist groups to disseminate disinformation, to prepare deepfakes with a view to manipulating the public, to recruit and radicalize targeted segments of societies, to preplan their malicious activities such as by using Augmented Reality (AR), and to increase the effect of their attempts and attacks. In the words of Kristan J. Wheaton, for instance:

> "Terrorists will likely use AR to travel to and inside foreign countries to meet with collaborators in impactful, quasi-physical ways without documentation…AR can also help terrorists to plan operations remotely by digitally monitoring locations and even potentially executing events (through the recruited in foreign countries or theaters of conflicts-author) while avoiding physical surveillance."

AR could, therefore, be a mixture of the physical and virtual domains to inflict damage to citizens or infrastructure without traces and with a lower cost for terrorists. (44)

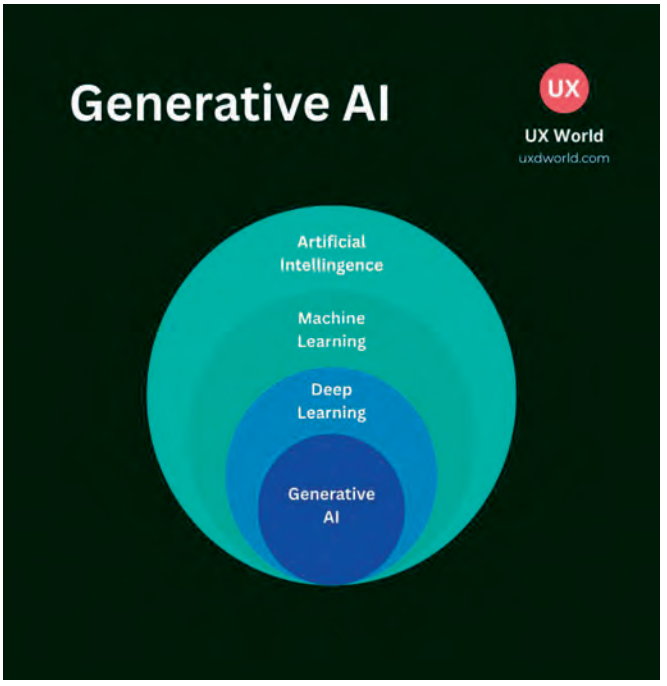


Figure 2: Generative AI diagram by UX World, uxdworld.com

There currently exist different types of AI such as Narrow AI, General AI, and Super AI, each with different subsets for specific tasks. Each of these AI categories may lend themselves to be misused by terrorist organizations. (45)

In recent field research, it was observed that terrorist organizations are leveraging generative AI to automate the production of propaganda materials and tailor messaging to specific demographic profiles. This shift enables the creation of multilingual audio-visual content designed for maximum emotional impact without requiring human translators or editing teams raising the risk of refined disinformation campaigns that can rapidly adapt to local social contexts. In this regard, digital deception networks (DDNs), powered by AI and capable of spreading disinformation at scale, posing a parallel threat. Terrorist groups can deploy these tools to manipulate public perception after an attack, mislead security forces and coordinate operations across borders while remaining digitally concealed. (46) (47)

Underneath AI there is also the growing capacity and capability of Machine Learning and Deep Learning which benefit from very wide data sets all over the world in different languages (Large Language Models). Internet of Things (IOT) and Big Data are two major sources that feed Machine and Deep Learning algorithms. At the heart of these capabilities lie artificial neural networks (ANNs), which are computational models inspired by the structure and functions of the human brain. Neural networks enable AI systems to identify patterns, classify inputs, and make predictions across massive datasets. In the context of terrorism, this means that malicious actors can

exploit neural networks to automate target recognition, enhance data-driven propaganda strategies, or develop deepfake content with unprecedented realism when combined with generative models like GANs (Generative Adversarial Networks). These networks serve as a key infrastructure behind many modern AI applications, amplifying both the potential benefits and risks of AI tools. Neural networks are the foundation of many AI systems exploited for malicious purposes. These systems can identify, categorise and adapt to new data inputs with minimal human oversight, thereby granting terror groups unprecedented autonomy in planning and decision-making. (48) (49)

Human-Machine Learning/Interaction (HML) serve different purposes in facilitating daily lives across different strands of activity such as facial recognition, social media optimization, healthcare, financial accuracy, predictive analytics etc. may offer opportunities for terrorist organisations to increase the effects of their activities even before they occur. The downside of HML could be the potential it may offer for those groups, state or non-state, with malign intentions. (50)

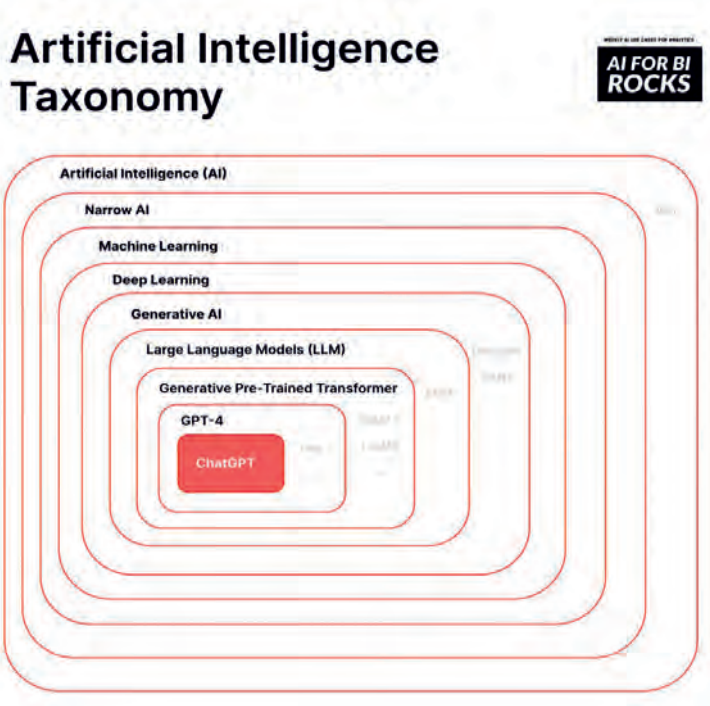


Figure 3: Artificial Intelligence Taxonomy by Tobias Zwingmann. Originally published with AI For BI Rocks.

They exploit cyber-attacks in a highly digitalized ‘network of networks’ either on their own or deniably sponsored by rogue states. Behind such sinister groups (such as hacker groups) there are strong indicators of intelligence agencies aiming to manipulate adversaries by exploiting social media, using deepfakes, penetrating electoral systems run by electronic means etc.

The alleged interference of Russia in the 2016 U.S. presidential elections is a solid case in point. It seems that Russian and Chinese hackers continue to use cyber-attacks to build their own narrative directed against foreign states and societies. (51) (52)

The Stuxnet malware was reportedly used by the U.S. and Israel against the Natanz nuclear facility as a decisive cyber weapon in 2009. The Colonial Pipeline ransomware attack executed by a group of hackers called DarkSide in 2021 was another example of disruption of the operation of critical infrastructure, this time in the U.S. More recently Israel used its cyber-attack capability against the Hezbollah leadership by detonating pagers and walkie-talkies used by supporters of Hezbollah in 2024. (53) (54) (55)

Directed Energy Weapons (DEW), including but not limited to High Energy Lasers (HELs) and High-Power Microwaves (HPMs), could also be a serious cause for concern if they are used by terrorists at comparatively lower costs to inflict damage either on humans, military capabilities or vulnerable infrastructures. The notorious 'Havana Syndrome', for instance, that had stricken serving diplomats in Havana, Moscow and Beijing since 2016 is attributed by a number of analysts to microwave weapons. Such weapons cause brain injuries and symptoms such as:

> "…Dizziness, loss of balance, nausea and headaches…The impact on some of the victims has been debilitating and long-lasting."

If such weapons that directly affect humans are used in combination with other means of DEW by terrorists in the future, the damage that would transpire both for states and societies could be beyond imagination. (56) (57) (58)

DEWs and HPMs, however, are also capabilities that may be designed as counter weapons against potential terror groups in possession of such capabilities. The EU has started to play an important role in tapping into the potential offered by DEWs with a forward-looking approach. The U.K. has recently launched an ambitious program to use High-Power Microwave Weapon against drone swarms and tested the system for battlefield and homeland defense. This capability could become a powerful deterrent against potential terror attacks with such directed energy weapons. (59) (60) (61)

In sum, attacks against digital networks by using cyber capabilities have become a commonplace for non-state entities intent upon causing shocks and disruptions to states and societies. Cyber-attacks are at the same time 'safe havens' for stealing sensitive data, causing disruptions to critical infrastructure, and have the potential to inflict heavy damage, including in the physical domain, to a plethora of actors. They are transnational in nature and an influential multiplier in the hands of terrorist groups.

One final capability of convenience for terrorist groups is expanding quantum computing that widens the scope of end-to-end encryption methods. This is another area where terrorist entities could hide themselves electronically, avoid tracking and/or detection by military-security institutions, communicate with each other in a safe manner, create their own social platforms, recruit citizens for their cause, and procure

their lethal material through illegal web (DarkWeb) markets. The potential presented by quantum technologies to terrorist groups cannot be underestimated since this is an area which attracts investment by public and private institutions, quite a number of which are accessible to terrorist organisations.

The Dark Web, as an encrypted space of the internet not indexed by conventional search engines, has become an essential enabler for terrorist organizations and cybercriminal networks alike. It facilitates the anonymous exchange of illicit goods, malware, stolen data and false documents, as well as weapons, including CBRN-related materials and ransomware software. Research highlights that terrorist groups use Dark Web marketplaces not only to procure technological tools but also to share manuals on cyberattack methodologies, coordinate operational logistics, and even crowdsource funding through cryptocurrencies, while also further reducing their digital footprint and avoiding financial surveillance. Terrorist groups also use AI-enhanced anonymisation tools to evade detection, automate phishing attacks, and conduct complex fraud schemes to fund their operations. (62) (63)

The development of Quantum Key Distribution (QKD) and post-quantum cryptographic techniques significantly enhances the ability to conceal communications beyond the capacity of conventional monitoring systems. For example, QKD enables the transmission of encryption keys with theoretically unbreakable security, making interception or decryption by state surveillance tools virtually impossible. Moreover, quantum-enhanced machine learning systems may assist terrorist cells in analysing patterns of state behaviour, evading surveillance algorithms, or coordinating decentralized operations more efficiently. The concern grows further considering the fact that various civilian research institutions and tech firms are conducting open-access quantum research, which can be exploited by malicious non-state actors operating in permissive or unregulated environments. As these technologies move from laboratory to application, the asymmetric risk they pose will likely increase, especially if proper international governance and access control mechanisms are not enforced. (64)

The cyber/digital space is one of the best examples of EDTs bringing together different domains under the same rubric of virtual capacity that could be exploited by terrorists to pursue their agenda vis-à-vis both public and private sectors. There also exists an intersection between cyber and physical domains in practice. That is well proven by what has happened so far in real world events. This domain is a solid case, *par excellence*, for building an integrated multi-domain framework both by public and private sectors. To this effect, EDTs are also a powerful means to prevent, protect, deter, mitigate and defeat terrorist groups, if used in a coordinated and cooperative manner, within an overall structure at the national and international levels.

IV. THE CHEMICAL, BIOLOGICAL, RADIOLOGICAL AND NUCLEAR (CBRN) DOMAIN

Since the end of the Cold War one of the main sources of asymmetric threats has been the use of CBRN capabilities both by state and non-state actors with malicious intent. This challenge has now become more perilous owing to the potential use of EDTs and the wider space offered by dual use technologies in the new millennium.

Resort to biological agents (i.e., pathogens) is not a new phenomenon. In addition to earlier use of chemical and biological agents the international community had witnessed a series of attacks both by state and non-state actors in the last three decades: an attack that took place in Oregon/U.S. in 1984 made use of salmonella; the use of toxic material delivered by air to the Japanese Parliament; and the biological attack to the Tokyo metro station in 1995 by the Aum Shinrikyo cult; the delivery of anthrax letters to media outlets and senators in the U.S.A immediately after the 9/11 terror attacks; a series of chemical attacks by the Syrian regime against insurgents in Syria starting in 2013; the poisoning of ex-Russian spy Sergei Skripal and his daughter by the Russian intelligence agency with the nerve agent Novichok in 2018 in the U.K.; and the attempts by Al Qaida to manufacture bioweapons since 1998 are just a few examples of how state agencies and terror groups seek to leverage such lethal capabilities that would inflict unprecedented damage to societies. As such, bio-and-chemo-terror threats have become concrete manifestations of terrorism at an increasing scale that states and societies have to be prepared to deal with. (65) (66) (67) (68) (69)

EDTs could be designed by terror groups to acquire more elements of biotechnology, including synthetic biology and genome editing. The more these novel bio- and chemo-technologies become accessible, the more the risk that terror groups could develop ways to redesign pathogens or develop toxins for deadly use. The prospect in the future that the use of such technologies has the potential to cause disruption in supply chains of food and water cannot be mitigated against unless strict measures are put in place by governments and resilience of societies is enhanced by a whole-of-society approach. (70) (71)

Another serious hazard that should be addressed is the use of radiological materials or sufficient amounts of enriched uranium by terrorist organisations to produce ‘dirty bombs’, which could be defined as radioactive isotopes that can be spread widely with or without high explosives by a radiological dispersion device (RDD). A radiological accident (not a terror attack) in Goiânia/Brazil in 1987 and 1988 that caused many civilian casualties clearly demonstrated the potential deadly impact of a terrorist attack if a dirty bomb was to be used by these groups against the population or critical infrastructure. (72)

The increasing threat of CBRN capabilities prepared the grounds for NATO to adopt the CBRN Defence Policy in 2009. NATO recognised the threat emanating from the potential use of CBRN materials for terror purposes by non-state actors to the extent that:

> “…They are known to both seek access to more sophisticated CBRN materials and WMD, as well as to attempt to weaponize toxic industrial chemicals and other materials that may be easier to acquire. Moreover, scientific and technological innovation continues to reduce the barriers to acquiring or developing advanced and diverse CBRN materials and means of delivery. Consequently, the risk of CBRN use or proliferation by non-state actors is likely to continue to grow.” (73)

To reinforce its CBRN Defence Policy, the Alliance further adopted its first International Strategy on Biotechnology and Human Enhancement

Technologies in 2024. It thus developed a set of core principles and counter measures against risks that AI-enabled technologies in particular could provide for terror groups to benefit from diverse bio and human enhancement technologies to create panic, fear and disruption to security at large. (74)

NATO's CBRN Defence Policy and its strategy on Biotechnology and Human Enhancement Technologies (BHET) make it abundantly clear that a multi-domain approach to cover its five operational domains is essential in combatting terrorism that seeks to misuse EDTs for sinister purposes. It also demonstrates the need for international and regional cooperation, including NATO's partners, in upholding the principles and commitments adopted by the UN at the international level as well as within the Alliance and the competent regional organisations such as the EU.

In line with this, the United Nations' key conventions, such as the Biological Weapons Convention (BWC, 1972), the Chemical Weapons Convention (CWC, 1997), and the International Convention for the Suppression of Acts of Nuclear Terrorism (2005), form the global legal framework against the misuse of CBRN materials by both state and non-state actors. These conventions oblige member states to prohibit the development, acquisition, transfer and use of biological, chemical, and radiological weapons, while also enhancing cooperation in detection, prevention, and response measures. On the European Union's side, the EU CBRN Action Plan (2009) and the subsequent EU Security Union Strategy (2020–2025) stress the need for strengthening detection capabilities, protecting critical infrastructure, managing hazardous materials, and improving preparedness against CBRN threats. (75) (76) (77) (78) (79)

In terms of counter-measures, both NATO and its partners promote a multi-layered defensive posture including CBRN detection and identification systems, decontamination units, medical countermeasures such as stockpiling antidotes and vaccines, rapid response teams, and public health resilience measures. Moreover, investment in AI-enabled surveillance systems, sensor networks, and bio-detection platforms has become a growing component of counter-CBRN strategies in the era of EDTs. (80)

Figure 4: NATO's Principles and Commitments for CBRN Defence, *https://www.nato.int/cps/fr/natohq/official_texts_197768.htm?selectedLocale=en*

V. THE COGNITIVE DOMAIN

Attempts by terrorist organisations to utilize the cognitive domain have increased in parallel with the panoply of EDTs spreading through the sinews of social life. This domain brings together different segments of EDTs such as AI, cyber, Augmented Reality, and quantum technologies. Academic analyses further caution that advancements in neurotechnology and AI-integrated brain-computer interfaces may allow for manipulation of human cognition beyond traditional influence operations. Such technologies could be weaponized to induce cognitive fatigue, exploit psychological vulnerabilities, and disrupt decision-making processes among targeted groups or populations. In crisis situations, misinformation and disinformation campaigns not only destabilize institutions but also exacerbate panic behaviours among civilian populations. Understanding how misinformation spreads during emergencies, including terror-related cyberattacks, has become essential for both crisis response planning and counter-terrorism strategies focused on the cognitive domain. (81) (82)

The main purposes of terrorist groups are to disseminate fake news, fuel hate speech, launch disinformation/misinformation campaigns against the targeted state or public, spread conspiracy theories to undermine the resilience of societies and create distrust and anxiety among populations/communities, and shape human perceptions and behaviours to be more amenable to their cause.

The Cognitive Domain, when ‘weaponised’ virtually, is an influential tool at the disposal of terrorists amongst modern types of warfare such as cyber and hybrid warfare. Thus, cognitive warfare is an inseparable part of cyber and hybrid modes of malicious activities that is prone to serving the interests of not only violent extremist groups and terrorist organisations, but also members of organized crime, human and

drug traffickers, cross border public opinion manipulators, money launderers etc. It is, therefore, an indispensable interface that ties together both the physical and virtual contexts.

Different layers of AI capabilities, for instance, could be designed by such groups to recruit, radicalise and mobilize militants and sympathizers anywhere and everywhere without huge costs. It is, in many cases, a low cost/high impact asset for malign purposes. (83)

The Cognitive Domain is a rich space for terrorists, among others, to launch psychological operations (PSYOPS), to initiate social engineering with ast view to creating a conducive environment for spreading propaganda, and to exploit vulnerabilities within a state or a society through online disinformation campaigns (i.e. via social media) and reinforced by deepfakes. The EU Agency for Cyber Security (ENISA) Report of 2024, for example, demonstrates the increasing trend in the use of deepfakes/fake news by extremist groups in the EU and non-EU countries. The EU's Horizon research programs have identified cognitive warfare as a strategic challenge requiring cross-sectoral solutions. Projects under Horizon Europe focus on countering the weaponization of information, strengthening societal resilience against disinformation, and enhancing capabilities to detect manipulation in a digital information ecosystem that is increasingly exploited by violent extremist groups. In parallel, NATO has increasingly prioritised the cognitive domain within its EDT agenda. The NATO Innovation Fund and the Defense Innovation Accelerator for the North Atlantic (DIANA) explicitly includes cognitive security among their focus areas. NATO's Science and Technology Organization (STO) has also initiated research into the impacts of neuro-technologies, cognitive warfare and behavioural manipulation, examining how adversaries may exploit vulnerabilities in public perception and decision-making. Furthermore, the NATO Strategic Communications Centre of Excellence (STRATCOM COE) continues to deliver detailed analysis of influence operations, disinformation and psychological manipulation as core elements of hybrid and cognitive warfare, supporting member states in improving resilience against such threats. (84) (85) (86) (87)

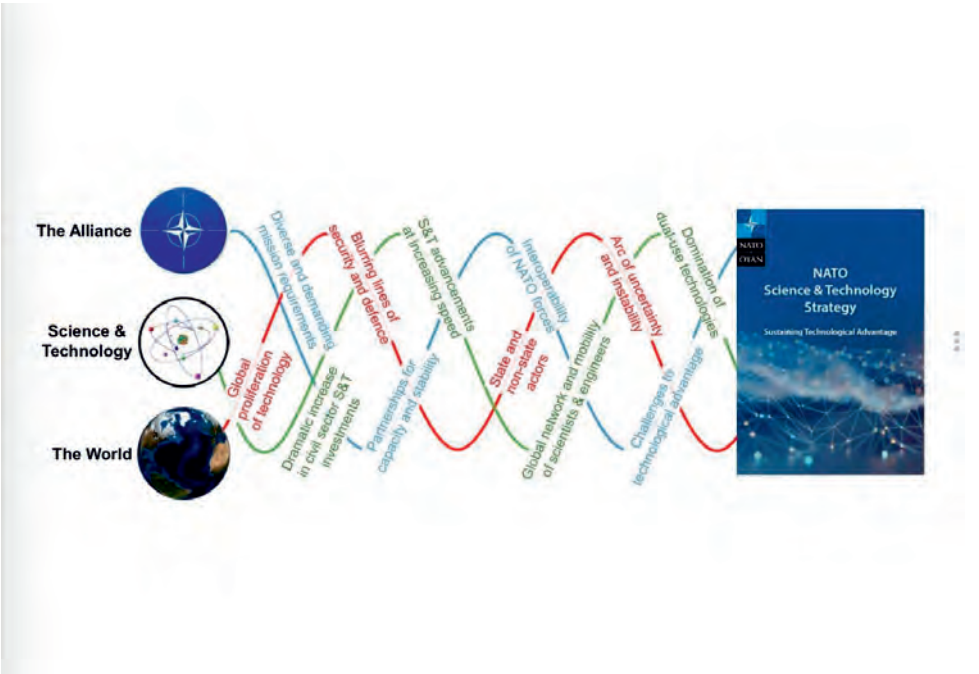


Figure 5: NATO Science & Technology Strategy,

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_07/20181107_180727-ST-strategy-eng.pdf

It would not be surprising to see extremist/terrorist groups to probe the capabilities offered by machine learning and human-computer interfaces: in sum, neuro-technologies to run their attempts in waging cognitive warfare. By 'taming' machines, distorting Large Language Models, and following progress in human-machine interfaces, they can enhance their initiatives to recruit more, to radicalize particularly the susceptible communities, and augment human capacity to cause serious devastation to states and societies.

Another technology posing a significant risk in the cognitive and physical domains is 3D printing, which has become an accessible tool for terrorist organizations. The ability to produce weapon components, firearms parts, explosive devices, and even drone frames using commercially available 3D printers significantly reduce logistical constraints for these groups. Academic research and security agency reports highlight how terrorist actors exploit open-source designs shared across encrypted platforms or the Dark Web to manufacture undetectable weapons and bypass traditional arms control mechanisms. The combination of 3D printing with AI-generated blueprints further accelerates this risk, allowing malicious actors to innovate low-cost, yet high-impact capabilities without relying on conventional supply chains. (88) (89)

Neuroscience, however, tends to strengthen the capacity of competent authorities for early warning of terrorist attacks, identifying behavioural manners *a priori* pre-empting their lethal and non-lethal attacks, and widening the horizon of counter-terrorism initiatives and projects. Thus, neuro-technologies, once turned into enablers for predicting, preventing, monitoring and detecting the ways in which terrorists operate, would be extremely useful enablers for counter-terrorism authorities. It is mainly for this reason that an effective, integrated and result-oriented framework for cooperation between public and private sectors is indispensable in maintaining technological superiority not only against state actors, but also against non-state actors with violent and malign intents and behaviors. This, in turn, necessitates continuous building of counter-terrorism efforts at the international level (the UN), and regional organisations such as NATO, the EU, and OSCE. (90) (91) (92)

VI. CONCLUSION

A challenge faced today by humanity is the use and misuse of EDTs by terrorist groups. This is an evolving threat landscape and a work in progress. In that sense, as the level of technology increases, so is the magnitude of shocks and disruptions to the security of nations and their citizens.

Following the Cold War, the world has seen unprecedented globalisation of many walks of life, increased connectivity across different sectors of governmental and societal structures, expanding commercial and trade ties among the members of the international community, and the emergence of new and disruptive technologies that could be used for benign or malign purposes.

Different forms of technologies such as AI, quantum computing, bio and nano capabilities, cyber, robotics, unmanned systems, blockchains, cloud technologies, the Internet of Things etc. have radically widened the scope of EDTs with ramifications for their use – or abuse – by terrorist organisations. The more expanded and sophisticated the scope of EDTs, the more difficult it has become to protect, prevent, mitigate and defend against and deter their use by terrorist entities. Moreover, the accelerating convergence of civilian and military technological innovation has fundamentally altered modern conflict dynamics. Technologies that were once confined to state militaries such as unmanned systems, AI-driven targeting, or quantum encryption are now increasingly accessible to non-state actors, enabling them to wage asymmetric warfare with capabilities previously limited to nation-states. (93)

The increasing role of the private sector in producing such technologies and their dual-use nature has complicated efforts to fight terrorism. Thus, the scope and nature of terrorism has also been privatized, commercialized and globalized. Added to this already complex situation the geostrategic/geopolitical competition among major powers has penetrated the technological realm, thus further compounding counter-terrorism efforts.

In defence there has been a clear trajectory to bring together operational domains (land, air, sea, cyber, and space) under an integrated structure. This required international and regional organisations such as NATO and the EU to adapt their policies, procedures, governance, decision-making processes, doctrines, operational and logistical priorities, exercises, efforts in science and technology, and decision-

making systems. In sum, all relevant organisations have inevitably started to operate in a multi-domain context given the ongoing exponential expansion of EDTs that offer opportunities for terrorist organisations.

Under present circumstances, notably, the high level of integration/intersection between different components of EDTs, a terror attack with an EDT in one domain could create a domino effect in other domains of EDT, thus inflicting damage both in physical and virtual domains. A serious cyber-attack against critical infrastructure, for instance, would result in intolerable costs for the well-being of societies and exact a heavy toll on societal life. A disinformation campaign run by a terrorist organisation in any country would stir social unrest and disrupt the resilience of those governments and societies under attack.

Concrete examples of terrorist attacks across different EDT domains make it abundantly clear that because of the transnational, cross sectoral, and intersectional nature of modern existential risks and threats, a bird's eye view is essential in preventing, mitigating, deterring, defending and fighting against terrorists exploiting EDTs as multipliers to evade tracking, monitoring and detection by competent governmental and private institutions.

EDTs, however, are at the same time a ‘double-edged sword’ that could be leveraged in the fight against terrorism. AI, quantum computing, AI-enabled Intelligence, Surveillance and Reconnaissance (ISR) capabilities, counter drone technologies comprising Directed Energy Weapons, the online surveillance and monitoring of Big Data complemented by predictive analyses to disrupt potential terror planning, training and operationalising, systems like NATO’s DEXTER and DIANA projects, the EU Innovation Hub for Internal Security, the EU CBRN Centers of Excellence and the Horizon Europe Program are all designed to enhance the role of EDTs across different technological domains to fight terrorism. (94)

Any organisation, no matter how equipped it may be, cannot combat terrorism alone without cooperating with its counterparts and partners. This is also applicable to states combatting terrorism as the most direct asymmetric threat for international security and populations throughout the world.

EDTs could be powerful force multipliers for competent authorities in tracking and detecting terrorists’ behaviour patterns, movements, and plans for attacks. They would be used to take efficient and actionable decisions in fighting terrorism. Nevertheless, their very existence cannot ensure a foolproof path to defeat terrorism., They are not, therefore, precursors for remaining complacent in the ever-lasting fight against different forms and manifestations of terrorism.

The nature of modern terrorism has already transcended the physical domain and extended into the virtual domain, thus bringing the two together with potentially dire consequences for both governmental and societal structures and resilience. It is mainly for this new phenomenon that counter-terrorism endeavours at all levels of governance necessitate an integrated architecture which should encompass all four domains of EDTs elaborated above. They should be predicated upon a multidisciplinary, multi stakeholder, cross domain enterprise with a view to anticipating threats and coordinating responses accordingly. Such a holistic framework demands

vigilance, resilience, interoperability, and adaptability supported by capabilities inherent in EDTs.

Footnotes (APA References)

(1) NATO. (1991, November 8). The Alliance's new strategic concept. https://www.nato.int/cps/en/natohq/official_texts_23847.htm

(2) Council of the European Union. (2003, December 12). A secure Europe in a better world: European security strategy. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/reports/76255.pdf

(3) NATO. (2023, February 27). Weapons of mass destruction. https://www.nato.int/cps/en/natohq/topics_50325.htm

(4) NATO Allied Command Transformation. (2025, May 2). Multi-domain operations and digital transformation: Enabling converged effects in the modern battlespace. https://www.act.nato.int/article/mdo-dt-enabling-converging-effects/

(5) Ibid

(6) NATO. (1999). Press info – The Combined Joint Task Forces concept. https://www.nato.int/docu/comm/1999/9904-wsh/pres-eng/16cjtf.pdf

(7) NATO. (2025). NATO response force (2002–2024). https://www.nato.int/cps/en/natohq/topics_49755.htm

(8) Global Security. (2019). Spearhead force: Very high readiness joint task force (VJTF). https://www.globalsecurity.org/military/world/int/vjtf.htm

(9) United Nations. (2006, September 8). The United Nations global counter-terrorism strategy (A/RES/60/288). https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy

(10) Council of Europe. (2018, July 4). *Council of Europe counter-terrorism strategy (2018–2022).* Council of Europe. https://policehumanrightsresources.org/content/uploads/2024/02/Council-of-Europe-Counter-Terrorism-Strategy-2018-20221.pdf

(11) Saul, B. (2025, August). *UN80 reforms to United Nations counter-terrorism activities: Strengthening human rights, gender equality, the rule of law and prevention* (Briefing note). United Nations. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/activities/sr-ct-un80-reforms-august-2025.pdf

(12) United Nations. (2006, September 8). The United Nations global counter-terrorism strategy (A/RES/60/288). https://www.un.org/counterterrorism/un-global-counter-terrorism-strategy

(13) United Nations Security Council. (2018). Compendium of good practices on the protection of critical infrastructure against terrorist attacks. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf

(14) Organization for Security and Co-operation in Europe. (2012). OSCE consolidated framework for the fight against terrorism (PC.DEC/1063). https://www.osce.org/pc/98008

(15) OSCE. (2001). The Bucharest plan of action for combating terrorism. https://www.osce.org/files/f/documents/3/b/42524.pdf

(16) NATO. (n.d.). Defense against terrorism programme of work (DAT POW). https://www.nato.int/cps/en/natolive/topics_50313.htm

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

(18) Council of the European Union. (2005). EU counter-terrorism strategy (14469/4/05 REV 4). https://data.consilium.europa.eu/doc/document/ST-14469-2005-REV-4/en/pdf

(19) European Commission. (2020, July). EU security union strategy. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en

(20) Ibid

(21) European Union External Action. (2022, March). A strategic compass for security and defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

(22) Defense Intelligence Agency. (2025, March 7). Statement for the record: Worldwide threat assessment. https://armedservices.house.gov/uploadedfiles/2025_dia_statement_for_the_record.pdf

(23) United Nations Security Council. (2019, July 31). Eighth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security (S/2019/612). https://undocs.org/en/S/2019/612

(24) United Nations Security Council. (2022). Emerging threats: Use of emerging technologies by terrorist groups. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/new_delhi_-_statement_by_uncted.pdf

(25) Vision of Humanity. (2023, September 11). Preventing terrorists from using emerging technologies. https://www.visionofhumanity.org/preventing-terrorists-from-using-emerging-technologies/

(26) Europol. (2024). European Union terrorism situation and trend report 2024 (EU TE-SAT). https://www.europol.europa.eu/publication-events/main-reports/european-union-terrorism-situation-and-trend-report-2024-eu-te-sat

(27) NATO–EU Task Force. (2023). Final assessment report on the resilience of critical infrastructure in Europe. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf

(28) Calcara, A. (2023, March 3). One step back, two steps forward: The EU, NATO and emerging and disruptive technologies (CSDS Policy Brief 07/2023). https://www.brussels-school.be/sites/default/files/CSDS%20Policy%20brief_2307_0.pdf

(29) Soylu, R., & Kemal, L. (2024, March 22). Has the PKK acquired kamikaze drones to hit Turkish aircraft? Middle East Eye. https://www.middleeasteye.net/news/turkey-pkk-acquired-kamikaze-drones-aircraft

(30) Rassler, D. (2016, October). Remotely piloted innovation: Terrorism, drones and supportive technology. Combating Terrorism Center at West Point. https://ctc.westpoint.edu/wp-content/uploads/2016/10/Drones-Report.pdf

(31) Ibid

(32) Archambault, E., & Veilleux-Lepage, Y. (2020). Drone imagery in Islamic State propaganda: Flying like a state. International Affairs, 96(4), 955–973. https://doi.org/10.1093/ia/iiaa014

(33) Veilleux-Lepage, Y., & Archambault, E. (2022, December). A comparative study of non-state violent drone use in the Middle East. ICCT Report.

https://icct.nl/sites/default/files/2022-12/Drones%20in%20the%20Middle%20East%20-%20Full%20Report%20Final%20-%20Ready%20to%20Publish.pdf

(34) The Washington Post. (2017, February 21). Use of weaponized drones by ISIS spurs terrorism fears. https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html

(35) Larter, D. B. (2017, May 16). SOCOM commander: Armed ISIS drones were 2016's 'most daunting problem'. Defense News. https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/

(36) Gibbons-Neff, T. (2017, June 14). ISIS drones are attacking U.S. troops and disrupting airstrikes in Raqqa, officials say. The Washington Post. https://www.washingtonpost.com/news/checkpoint/wp/2017/06/14/isis-drones-are-attacking-u-s-troops-and-disrupting-airstrikes-in-raqqa-officials-say/

(37) Dahlgren, M., & MacKenzie, L. (2025, June 4). Ukraine's drone swarms are destroying Russian nuclear bombers. What happens now? Center for Strategic & International Studies. https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now

(38) Jaworek, P., Melamed, M., Rusten, L., & Andreasen, S. (2025, April). Navigating disruption in the global nuclear order: Managing risks and shaping a new way forward. Nuclear Threat Initiative. https://www.nti.org/analysis/articles/navigating-disruption-in-the-global-nuclear-order-managing-risks-and-shaping-a-new-way-forward/

(39) BBC News. (2016, July 19). Nice attack: What we know about the Bastille Day killings. https://www.bbc.com/news/world-europe-36801671

(40) Dallison, P. (2017, August 17). Barcelona attack: What we know so far. Politico EU. https://www.politico.eu/article/barcelona-attack-what-we-know-so-far/

(41) European Defence Agency. (2022). Best practice guide for unmanned maritime systems handling, operations, design and regulations. https://eda.europa.eu/docs/default-source/documents/eda_ums-bpg-edition-2022_public.pdf

(42) NATO. (2020, November). Maritime unmanned systems (MUS): Factsheet. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/11/pdf/2011-factheet-mus.pdf

(43) Foreign Policy Analytics, & Microsoft. (2025, June). Advancing NATO's digital resilience: Insight brief. https://fpanalytics.foreignpolicy.com/2025/06/17/nato-digital-resilience/

(44) Sim, S., Hartunian, E., & Milas, P. J. (Eds.). (2024). Emerging technologies and terrorism: An American perspective. US Army War College Press. https://press.armywarcollege.edu/monographs/967

(45) American University. (2025). Types of AI. https://subjectguides.library.american.edu/c.php?g=1410777&p=10447758

(46) Liang, C. S. (2022, March 17). Emerging technologies and terrorism. Vision of Humanity. https://www.visionofhumanity.org/emerging-technologies-and-terrorists/

(47) Feldstein, S. (Ed.). (2025). Digital deception: Disinformation, DDNs, and democratic resilience. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Feldstein_DDN_final-2026.pdf

(48) United Nations Interregional Crime and Justice Research Institute (UNICRI), & United Nations Counter-Terrorism Centre (UNCCT). (2021). The malicious use of artificial intelligence for terrorist purposes. https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf

(49) Valle-Cruz, D., García-Contreras, R., & Gil-Garcia, J. R. (2024). Exploring the negative impacts of artificial intelligence in government: The dark side of intelligent algorithms and cognitive machines. International Review of Administrative Sciences, 90 (2), 353–368. https://doi.org/10.1177/00208523231187051

(50) Puscas, I. (2022). Human–machine interfaces in autonomous weapon systems: Considerations for human control. United Nations Institute for Disarmament Research. https://unidir.org/files/2022-07/UNIDIR_Human-Machine%20Interfaces.pdf

(51) Harding, L. (2016, December 16). What we know about Russia's interference in the US election. The Guardian. https://www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election

(52) Romero, A. (2025, January 8). Report: China hackers steal palace, Philippine military data. The Philippine Star. https://www.philstar.com/headlines/2025/01/08/2412630/report-china-hackers-steal-palace-philippine-military-data

(53) Mishra, S. (2024, September 21). How CIA, Mossad used a computer virus to dismantle Iran's nuclear program. NDTV. https://www.ndtv.com/world-news/israel-iran-hezbollah-stuxnet-how-cia-mossad-developed-a-digital-weapon-to-target-iran-nuclear-site-6614789

(54) Mittal, M. (2024). Colonial pipeline cyberattack drives urgent reforms in cybersecurity and critical infrastructure resilience. International Journal of Oil, Gas and Coal Engineering, 12(5), 106–119. https://doi.org/10.11648/j.ogce.20241205.11

(55) Murphy, M., & Tidy, J. (2024, September 20). What we know about the Hezbollah device explosions. BBC News. https://www.bbc.com/news/articles/cz04m913m49o

(56) Regenstein, L. (2024, April 1). Havana syndrome: The history behind the mystery. Foreign Policy Research Institute. https://www.fpri.org/article/2024/04/havana-syndrome-the-history-behind-the-mystery/

(57) Borger, J. (2021, May 2). Havana syndrome: NSA officer's case hints at microwave attacks since 90s. The Guardian. https://www.theguardian.com/world/2021/may/02/havana-syndrome-nsa-officer-microwave-attacks-since-90s

(58) Sodders, L., & Smith, B. (2024, September 20). Focused on the threat: Directed energy weapons. Space Systems Command. https://www.ssc.spaceforce.mil/newsroom/article-display/article/3913339/focused-on-the-threat-directed-energy-weapons-part-3-of-6

(59) Spencer, J., & Carafano, J. (2004, August 2). The use of directed-energy weapons to protect critical infrastructure. The Heritage Foundation. https://www.heritage.org/defense/report/the-use-directed-energy-weapons-protect-critical-infrastructure

(60) Kremidas-Courtney, C. (2025, June 4). Directed energy weapons and the future of European defence. European Policy Centre. https://epc-web-

s3.s3.amazonaws.com/uploads/ckeditor/2025/06/04/directed-energy-weapons-ckc-4-june-2025.pdf

(61) Newdick, T. (2025, April 17). British high-power microwave weapon successfully tested against drone swarms. The War Zone. https://www.twz.com/news-features/british-high-power-microwave-weapon-successfully-tested-against-drone-swarms

(62) United Nations Interregional Crime and Justice Research Institute (UNICRI), & United Nations Office of Counter-Terrorism (UNOCT). (2024). Beneath the surface: Terrorist and violent extremist use of the dark web and cybercrime as a service for cyber-attacks. https://unicri.org/sites/default/files/2024-07/DW_BtS.pdf

(63) Ünver, A. (2023, August). The role of technology: New methods of information manipulation and disinformation. EDAM. https://edam.org.tr/en/cyber-governance-digital-democracy/the-role-of-technology-new-methods-of-information-manipulation-and-disinformation

(64) Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-quantum cryptography (1st ed.). Springer. https://doi.org/10.1007/978-3-540-88702-7

(65) Riedel, S. (2004). Biological warfare and bioterrorism: A historical review. Baylor University Medical Center Proceedings, 17(4), 400–406. https://doi.org/10.1080/08998280.2004.11928002

(66) Juling, D. (2023). Future bioterror and biowarfare threats for NATO's armed forces until 2030. Journal of Advanced Military Studies, 14(1), 82–102. https://doi.org/10.21140/mcuj.20231401005

(67) Sever, B.& Kelly, R. (2024). Anthrax letter attacks. EBSCO Research Starters: Science. https://www.ebsco.com/research-starters/science/anthrax-letter-attacks

(68) Lombardo, C. (2019, February 17). More than 300 chemical attacks launched during Syrian civil war, study says. NPR. https://www.npr.org/2019/02/17/695545252/more-than-300-chemical-attacks-launched-during-syrian-civil-war-study-says

(69) BBC. (2024, December 2). Ex-spy Skripal was a ‘sitting duck’, inquiry told. BBC News. https://www.bbc.com/news/articles/cj6z2d7xnnro

(70) National Human Genome Research Institute. (2025). Synthetic biology. Genome.gov. https://www.genome.gov/about-genomics/policy-issues/Synthetic-Biology

(71) Mackby, J. (2006). Strategic study on bioterrorism. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/061016_bioterrorism.pdf

(72) Zimmerman, P. D., & Loeb, C. (2004, January). Dirty bombs: The threat revisited. Defense Horizons, (38), 1–11. Center for Technology and National Security Policy, National Defense University. https://ndupress.ndu.edu/Portals/68/Documents/defensehorizon/DH-038.pdf

(73) NATO. (2022, March 24). NATO’s chemical, biological, radiological and nuclear (CBRN) defence policy. https://www.nato.int/cps/en/natohq/official_texts_197768.htm.

(74) NATO. (2024, April 12). Summary of NATO’s biotechnology and human enhancement technologies strategy. https://www.nato.int/cps/en/natohq/official_texts_224669.htm

(75) United Nations Office for Disarmament Affairs. (1972). Convention on the prohibition of the development, production and stockpiling of bacteriological

(biological) and toxin weapons and on their destruction (BWC). https://disarmament.unoda.org/bwc/

(76) Organisation for the Prohibition of Chemical Weapons. (1997). Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction (CWC). https://www.opcw.org/chemical-weapons-convention

(77) United Nations. (2005). International convention for the suppression of acts of nuclear terrorism. https://treaties.un.org/doc/Treaties/2005/04/20050413%2004-41%20PM/Ch_XVIII_15p.pdf

(78) European Commission. (2009). EU CBRN action plan. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0273

(79) European Commission. (2020, July 24). EU security union strategy 2020–2025. https://home-affairs.ec.europa.eu/pages/page/security-union-strategy-2020-2025_en

(80) NATO. (2022). NATO CBRN defence policy. https://www.nato.int/cps/en/natohq/official_texts_197768.htm

(81) Robinson, M. (2025). The establishment of an international AI agency: An applied solution to global AI governance. International Affairs, 101(4), 1483–1497. https://doi.org/10.1093/ia/iiaf105

(82) Ünver, A. (2017). Crisis networks and emergency behavior: Digital technologies and non-state political actor engagement. Cyberpolitik Journal, 2(3). www.cyberpolitikjournal.org

(83) Gandhi, M. (2024, January). Terrorism, extremism, disinformation and artificial intelligence: A primer for policy practitioners. Institute for Strategic Dialogue. https://www.isdglobal.org/wp-content/uploads/2024/01/Terrorism-extremism-disinformation-and-artificial-intelligence_A-primer-for-policy-practitioners.pdf

(84) Balkan, E., & Ünver, A. (2023, September). Combating disinformation: The policy framework. EDAM. https://edam.org.tr/en/cyber-governance-digital-democracy/dezenformasyonla-mucadele-politika-cercevesi

(85) European Union Agency for Cybersecurity (ENISA). (2024, March). Foresight cybersecurity threats for 2030 – Update. https://www.enisa.europa.eu/sites/default/files/2024-11/Foresight%20Cybersecurity%20Threats%20for%202030-Update-fullreport_en_0.pdf

(86) European Commission. (2025). Developing a better understanding of information suppression by state authorities as an example of foreign information manipulation and interference. Horizon Europe Programme (HORIZON-CL2-2023-DEMOCRACY-01-02). https://cordis.europa.eu/programme/id/HORIZON_HORIZON-CL2-2023-DEMOCRACY-01-02

(87) NATO. (2025). Defence ministers endorse NATO science & technology strategy. https://www.sto.nato.int/Lists/STONewsArchive/displaynewsitem.aspx?ID=793&ContentTypeId=0x010058AEAF164323DB46A46F391B932BA019

(88) Gilbert, F., & Russo, I. (2024). Mind-reading in AI and neurotechnology: Evaluating claims, hype, and ethical implications for neurorights. AI and Ethics, 4(3), 855–872. https://doi.org/10.1007/s43681-024-00514-6

(89) Veilleux-Lepage, Y. (2024). Printing terror: An empirical overview of the use of 3D-printed firearms by right-wing extremists. CTC Sentinel, 17(6), 1–10.

https://ctc.westpoint.edu/printing-terror-an-empirical-overview-of-the-use-of-3d-printed-firearms-by-right-wing-extremists/

(90) Shafi, N. (2021). The neuroscience of terrorism: A neuroscientific approach to understanding cognitive-behavioral traits of violent extremists. The New School Psychology Bulletin, 18(1). https://www.nspb.net/index.php/nspb/article/view/470

(91) Wall, C. (2025). The ghost in the machine: Counter-terrorism in the age of artificial intelligence. Studies in Conflict & Terrorism, 14(1), 1–27. https://doi.org/10.1080/1057610X.2025.2475850

(92) Husna, S. (2020). Into the mind of terrorist & violent-extremist: A neuroscience perspective & review on radicalisation. Advances in Social Science, Education and Humanities Research, 452.

(93) Wallace, D., & Reeves, S. (2013). Non-state armed groups and technology: The humanitarian tragedy at our doorstep? University of Miami National Security and Law of Armed Conflict Journal, 3(Summer), 26–45.

(94) NATO. (2025). Defence Innovation Accelerator for the North Atlantic (DIANA). https://www.nato.int/cps/en/natohq/topics_216199.htm

CHAPTER 2

HUMAN FACTORS IN TERRORISM: COUNTERING DUAL-USE OF EMERGING DISRUPTIVE TECHNOLOGIES

Ashok Vaseashta[234]

Abstract: The accelerated advancement of Emerging Disruptive Technologies (EDTs)—such as artificial intelligence (AI), quantum computing, biotechnology, and autonomous systems—is reshaping critical sectors ranging from precision healthcare to defense, cybersecurity, and international security frameworks. However, the dual-use nature of these recent technologies – where they serve both beneficial and malicious purposes – has raised significant concerns about their potential exploitation by adversaries and terrorist groups, since military and civilian Critical Infrastructure (CIS) stand out as prime targets for global aggressors due to their critical role in operations. While these innovations offer immense potential for positive societal advancements, their misuse can amplify the capabilities of non-state actors, leading to increased risks of terrorism and violent extremism. Human factors, including cognitive biases, behavioral tendencies, technology exploitation, and organizational vulnerabilities, play a crucial role in terrorists' exploitation of EDTs. As emerging technologies such as AI, biotechnology, 3D printing, quantum computing, and autonomous systems advance rapidly, their dual-use potential - beneficial and harmful – raises profound concerns in the counterterrorism context. This paper examines the human factors that present the challenges posed by malicious intent in counterterrorism efforts, as well as in the deployment, governance and ethical oversight of these technologies when repurposed for security. By drawing on several case studies and interdisciplinary literature, we identify key gaps in training, accountability, and communication that must be bridged to ensure resilience against misuse. Furthermore, the paper proposes a comprehensive framework for mitigating the risks associated with the dual-use dilemma, emphasizing the importance of international cooperation, regulatory oversight, and proactive countermeasures. Addressing the human factors in the context of EDTs requires interdisciplinary strategies involving technology adaptation, complexity science, algorithmic control for Machine Learning (ML) and support from policymakers, as well as intelligence agencies to ensure that such innovations do not inadvertently contribute to terrorism. Effective risk management and counterterrorism strategies must account for the evolving nature of these technologies and counter their potential to empower malicious actors in unprecedented ways. The study concludes with policy recommendations to

[2] International Clean Water Institute, Office of Strategic Research, Manassas, VA, 20112 USA[0000-0002-5649-0067]
[3] Ghitu IEEN, Technical University of Moldova, and Academy of Sciences, Chisinau, MOLDOVA
[4] Institutul de Cercetare al Universităţii din Bucureşti, Magurele, ROMANIA Corresponding author: Email: prof.vaseashta@ieee.org

support human-centric, ethically guided, and globally cooperative approaches to mitigate the risks associated with dual-use technologies in the security domain.

Keywords: dual-use, Emerging Disruptive Technologies, Artificial intelligence, behaviors, security

Introduction

The rapid evolution of emerging disruptive technologies (EDT) – ranging from Artificial Intelligence (AI), biotechnology, autonomous systems, 3D printing, smart materials, neuromorphic processors, to quantum computing—has introduced transformative capabilities with broad societal impacts. Notwithstanding the tactical advantages of these technologies, therein also lies the complex challenge of dual use, i.e., the potential for these technologies to be harnessed for adversarial or malicious purposes[5]. In general, technologies developed for beneficial purposes often possess a latent risk that such capabilities can be misappropriated for malicious use[6]. The dual-use nature of EDT thus presents a significant challenge in the modern counterterrorism landscape, and this dual-use dilemma is more pressing in counterterrorism, where innovations that enable predictive intelligence, real-time surveillance, or even disease propagation can also be weaponized by state and non-state actors. When confronted with increasingly sophisticated terrorist threats, national security institutions are now adopting these technologies to enhance situational awareness, improve Intelligence, Surveillance, and response (ISR), and preempt violent actions[7] from both non-kinetic and kinetic force platforms.

Fundamentally, understanding the human factors – psychological, social, cognitive, and organizational – that influence behavior, mindset, and strategies is crucial in crafting effective mitigation strategies and policy, as well as for proportionate responses[8]. Paradoxically, advanced technologies that are engineered for defense are also weaponized by adversaries. While human factors in deployment are routinely assessed, the more pressing concerns stem from the underlying influences – cognitive, cultural, ethical and institutional – that guide their development and governance[9]. These concerns are embedded in the broader sociotechnical systems that govern technology's lifecycle, from development to oversight. Stakeholders such as engineers, intelligence analysts, policymakers, and the public contribute varied cognitive biases, cultural norms, ethical frameworks, and institutional logics that collectively shape how these tools are implemented and regulated.

This chapter explores the intersection of human factors and the dual-use potential of EDTs in the context of terrorism. It critically examines how human behavior, decision-making, psychology and organizational dynamics influence both

[5] Vaseashta, A. (2025). Intrinsic and Existential Risks Associated with Emerging Security Threats from Dual-Use Technologies. In: Rocha, Á., Vaseashta, A. (eds) Developments and Advances in Defense and Security. MICRADS 2024. Smart Innovation, Systems and Technologies, vol 423. Springer, Singapore. https://doi.org/10.1007/978-981-96-0235-3_11

[6] Vaseashta, A. (2023). "Existential Risks Associated with Dual-Use Technologies" in Intersections, Reinforcements, Cascades: Proceedings of the 2023 Stanford Existential Risks Conference. The Stanford Existential Risks Initiative. Stanford Digital Repository. Available at https://purl.stanford.edu/zy474yf0050. https://doi.org/10.25740/zy474yf0050.

[7] Vaseashta, A. et al. (2025). Hybrid Threats, Risks, and Vulnerabilities—Critical Infrastructure Resilience Solutions Toolkit for Cross-Sectoral Applications. In: Radu, D., Hukić, M., Vaseashta, A. (eds) Countering Hybrid Threats Against Critical Infrastructures. ICSIMAT 2024. NATO Science for Peace and Security Series B: Physics and Biophysics. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-2304-4_2

[8] Aven, T., & Renn, O. (2010). Risk Management and Governance: Concepts, Guidelines and Applications. Springer

[9] Vaseashta, A., (2022), Nexus of Advanced Technology Platforms for Strengthening Cyber-Defense Capabilities, pg. 14-31, Vol. 155: Practical Applications of Advanced Technologies for Enhancing Security and Defense Capabilities: Perspectives and Challenges for the Western Balkans. DOI: 10.3233/NHSDP220003

the exploitation of and defense against these technologies. Strategies for countering the malicious repurposing of these technologies are proposed, emphasizing multidisciplinary approaches, policy frameworks, and ethical design. It is further argued that understanding and addressing these human factors is essential to the responsible and effective use of emerging technologies in counterterrorism contexts. While much of the current discourse emphasizes technical capabilities and regulatory controls, relatively little attention has been paid to the psychological, organizational, and ethical dimensions that shape how technologies are interpreted, implemented, and potentially misused. The integration of human-centered analysis into the dual-use conversation is not only a matter of ethics – it is a matter of strategic necessity. Through a multidisciplinary lens, this paper explores the interplay between human behavior and dual-use technologies in counterterrorism settings. Drawing on recent case studies and theoretical frameworks from psychology, political science, ethics, and security studies, key risk areas are identified, and governance strategies are proposed that prioritize human accountability, transparency, and ethical foresight. The overall objective is to contribute to a more resilient and morally coherent approach to technological innovation in high-stakes security environments.

1. Threat Landscape of Dual-Use Technologies

Dual-use technologies are systems, tools, or platforms that can be utilized for both civilian and military purposes, as well as for peaceful and harmful purposes. The term was initially used in the context of nuclear materials, followed by its latent use in synthetic biology. The ever-increasing landscape of technological innovations and widespread use of information technology (IT) and the internet has provided numerous capabilities, as well as challenges. The scope of the term “dual use” now includes not only the military but also commercial and innovation space. An overview of dual-use technologies, including basic sciences, technologies, EDTs, and transformative engines in innovation and commercial spaces, is shown in Fig. 1.

Figure 1: An overview of Dual-use technologies (reproduced with permission).[10]

In counterterrorism, the dual-use nature is particularly critical since the same AI systems that are used for border security can be repurposed for mass surveillance, and the Unmanned Aerial Vehicles (UAVs), also known as drones, are designed for reconnaissance but which can be weaponized for targeted strikes. Also, a virus-modifying biotechnology intended for vaccine research might be co-opted by non-state actors to develop biological threats, such as gain-of-function research[11,12] to make specific pathogens more virulent. The distinction between 'intended' and 'unintended' use is often blurred due to technical flexibility and competing ethical, political, and institutional priorities. The ambiguity surrounding intent, ownership, and control complicates both legal oversight and moral accountability. It also assigns a premium on preemptive governance, requiring stakeholders to assess potential misuse scenarios before technologies are operationalized. Without the benefit of such foresight, the rapid advancement of tools like AI, synthetic biology or cyber-physical systems capabilities may outpace our ability to contain their consequences.

Emerging disruptive technologies hold tremendous promise for enhancing national security, particularly in counterterrorism. These technologies offer unparalleled proactive defense capabilities through data analytics, predictive surveillance, real-time decision-making, and integrated forensics and threat detection.

[10] Vaseashta, A. (2025). Existential Risks with Dual-Use Technologies Across Nano, Cyber, and CBRN Domains. In: Petkov, P., Achour, M.E., Popov, C. (eds) Nanotechnological Advances in Environmental, Cyber and CBRN Security. NATO Science for Peace and Security Series B: Physics and Biophysics. Springer, Dordrecht. https://doi.org/10.1007/978-94-024-2316-7_1

[11] Casadevall A, Fang FC, Imperiale MJ. The Epistemic Value of Gain of Function Experiments. mSphere. 2024 Jan 30;9(1):e0071423. doi: 10.1128/msphere.00714-23.

[12] Baldwin, J., Noorali, S., & Vaseashta, A. (2023). Biology and Behavior of Severe Acute Respiratory Syndrome Coronavirus Contagion with Emphasis on Treatment Strategies, Risk Assessment, and Resilience. COVID, 3(9), 1259-1303. https://doi.org/10.3390/covid3090089

For instance, Artificial Intelligence (AI) can filter through vast volumes of data to identify behavioral patterns indicative of terrorist planning. Autonomous drones can conduct surveillance or even engage targets in hazardous environments without risking human lives. Similarly, by leveraging advanced biosurveillance, precision bioinformatics, and convergent AI-enabled threat detection, uncertainty can be transformed into actionable insights, such as the rapid detection of bioweapon agents or the development of countermeasures against engineered pathogens.

However, EDT potential comes with significant risks. The very features that make these technologies effective tools for counterterrorism also make them susceptible to misuse by bad and non-state actors. While it is beneficial in identifying suspects using detection, classification, recognition, and identification (DCRI) technologies, the identification technology research, such as facial recognition systems, can be exploited by authoritarian regimes for mass surveillance or social control, exposing biases, vulnerabilities, performance issues, and creating a general sense of lack of accountability. Additionally, AI-generated algorithms can be repurposed to generate sophisticated misinformation campaigns using deep-fake content, thus introducing confusion and distrust. Furthermore, developments in synthetic biology raise the complexity of bioweapons, such as custom-designed viruses being weaponized and released into civilian populations. Biothreats propitiate significant challenges due to delayed responses, attributional ambiguity, proliferation asymmetry, and lack of robust enforcement mechanisms.

This duality, i.e., the capacity to protect and to harm, makes these technologies particularly challenging to regulate. What makes the issue even more complex is the speed at which these innovations have advanced, often outpacing the development of legal frameworks, ethical guidelines and international agreements. Verification protocols remain insufficient, and without cohesive governance, deterrence strategies are ineffective. In particular, the ethical and legal policies governing and guiding the development, testing, and use of biotechnologies and bioagents are not uniform internationally, and such variation in standards and practices can establish varying constraints, thus exacerbating dual-use potential. The line between beneficial use and weaponization is increasingly blurred, especially in the ‘grey zone’ of cyber and bio threats, due to a lack of attribution and minimal regulation. Moreover, the globalized nature of research and development in these fields complicates efforts to enforce oversight. Technologies developed in open, civilian labs can be appropriated or reverse-engineered by malicious actors. Cloud-based AI services, 3D printing of drone components, and open-source genomic data further weaken the traditional boundaries between military and civilian domains. While harnessing the positive applications of these technologies in counterterrorism is essential, anticipating and mitigating the pathways through which they could be misused is equally critical. This requires not just technical solutions but also an integrated understanding of the human dynamics and systemic vulnerabilities that enable misuse—an understanding that will be explored in the following sections.

2.1. Characteristics of Dual-Use Technologies

Dual-use technologies possess the potential for both civilian and military applications. Key characteristics include ease of accessibility, scalability, stealth nature, and high impact potential with minimum technical knowledge or training. Certain technologies, such as AI-driven surveillance, Clustered Regularly Inter-

Spaced Palindromic Repeats (CRISPR) based gene editing[13], and drone swarms exemplify tools that can be weaponized with minimal technical expertise[14]. Furthermore, intentionality is difficult to quantify; hence, assessing whether a technology, originally intended to benefit, will be deployed for harmful purposes at any stage of its implementation is challenging. Dual-use threats often stem from an asymmetry in technological expectations: the offensive application of dual-use technologies may rely on minimal technical capabilities, whereas effective countermeasures typically require advanced, resource-intensive solutions. Addressing this asymmetry, therefore, necessitates a comprehensive understanding of the human factors – such as intent, behavior, and contextual decision-making – that influence the development and deployment of appropriate mitigation strategies.

2.2. Emerging Disruptive Technologies

Emerging Disruptive Technologies (EDTs) are innovations that significantly alter or replace existing systems, industries, or ways of life. EDTs start at the margins but rapidly advance to reshape markets and societies, and their disruption lies in their potential to significantly alter the surroundings, often faster than regulatory, economic, or social systems can adapt. EDTs are typically driven by breakthroughs in science, engineering or data with nonlinear impacts, meaning their effects can grow exponentially. These technologies tend to span multiple industries and disciplines in response to market and societal shifts. EDT has significant potential benefits but also poses a dual-use challenge. Several examples are listed below and illustrated in Fig. 2. With substantial progress in technological platforms, EDTs, and other transformative technologies, these innovations have the potential to alter the course of innovation, serving as inflection points that can reshape global systems. They can make existing business models obsolete and require significant societal adaptation. Understanding and anticipating their development is crucial for strategic planning across business, government, and society.

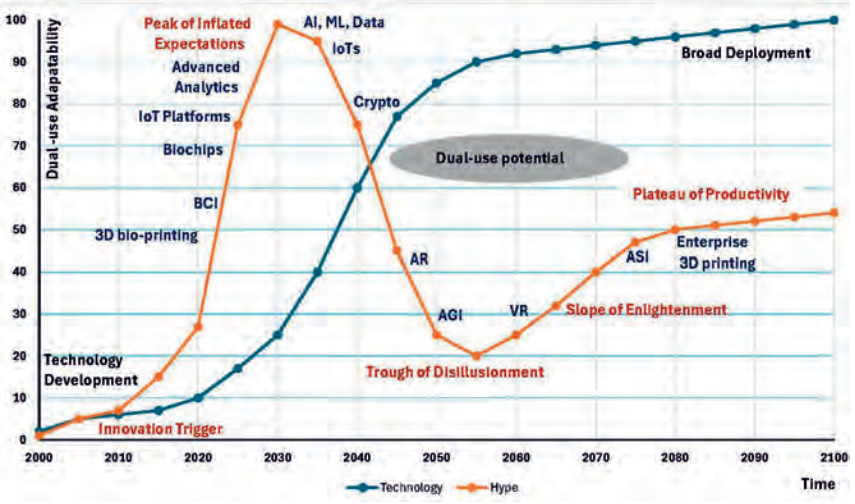


Figure 2: Diagram of Dual-Use Potential in Emerging Disruptive Technologies.

[13] Redman M, King A, Watson C, King D. What is CRISPR/Cas9? Arch Dis Child Educ Pract. Ed. 2016 Aug;101(4):213-5. doi: 10.1136/archdischild-2016-310459. Epub 2016 Apr 8. PMID: 27059283; PMCID: PMC4975809.
[14] National Research Council. (2004). Biotechnology Research in an Age of Terrorism. National Academies Press

Some of the key EDTs with dual-use potential include AI and Machine Learning (ML), which have the potential to transform automation, decision-making, and human-machine interaction. However, they also have dual-use potential, including autonomous targeting, deepfakes, and predictive policing. Yet another dual-use technology is on the horizon with the rise of Artificial General Intelligence (AGI)[15], which has the potential to revolutionize medicine, combat climate change, and unravel complex problems previously deemed intractable through synergistic coalescence of multiple disciplines. However, the AGI could also deceive, replicate, and operate beyond human control, even with the "human-in-loop" paradigm. Scaling laws in ML and Deep Learning (DL), unprecedented R&D funding, and competitive pressure have brought AGI to the edge of a technological transformation that rivals the discovery of fire or the splitting of the atom. Quantum computing is yet another aspect that promises exponential increases in processing power for specific tasks; however, cryptographic disruption and quantum sensing are among its dual-use applications. Synthetic biology, biotechnology, and genetic engineering are revolutionizing healthcare, agriculture, and human enhancement; however, pathogen engineering, genetically modified organisms, and CRISPR-based gene editing present significant moral and ethical concerns. Autonomous Systems have redefined logistics, warfare, and mobility, yet Lethal Autonomous Weapons (LAWs), unmanned aerial vehicles (UAVs), and their use in illegal drug trafficking present a significant dual-use challenge. Other EDTs with dual-use potential include Cyber-Physical Systems, the Electromagnetic Spectrum, Neuromorphic microprocessors, Blockchain and Decentralized Systems, Advanced Materials and Nanotechnology, and Extended Reality-Augmented Reality (ER/AR)/ Virtual Reality (VR)/ mixed reality (MR): some of these are described, within the scope of this article, in more detail later in this paper.

3. Human Factors Exploitation of Technology By Terrorists

While technological innovation often dominates the discourse around dual-use systems, human intentions, judgment, behavior and organizational context ultimately dictate how these tools are applied. Understanding these human factors is crucial for anticipating both the intended and unintended consequences of utilizing emerging technologies in counterterrorism operations.

3.1. Human Factors in Technology Development

Human factors refer to behavior, cognitive limitations, decision-making processes, and socio-technical interactions that influence how technologies are created, adopted, and potentially exploited. In dual-use scenarios, these considerations have become especially critical in anticipating misuse, minimizing operator error, and embedding safeguards throughout the system lifecycle. Incorporating human factors into a dual-use context helps identify vulnerabilities, improve interface design to reduce misinterpretation or unintended activation, and inform protocols for ethical use, risk mitigation, and resilience. Furthermore, behavioral and organizational insights can further assist in detecting insider threats, reinforcing accountability, and guiding training strategies to promote responsible innovation. Given the complexity and unpredictability of EDTs, human-centered designs have become not only a matter of efficiency or safety but a strategic imperative to ensure that technological advances do not become instruments of harm. Some specific examples are listed below.

[15] https://futurism.com/artificial-superintelligence-agi-2027-goertzel, accessed June 24, 2025

Cognitive Biases in Decision-Making

One of the most influential yet often overlooked aspects of technology use in security settings is the presence of cognitive biases. Analysts and decision-makers may fall prey to confirmation bias, selectively interpreting data to support preexisting notions about potential threats. Optimism bias can lead developers to underestimate the potential for misuse, especially when driven by confidence in their technology's security or a designated intent, undermining risk assessments and leading to vulnerabilities or unintended consequences. Automation bias refers to the tendency to overly trust machine-generated outputs, which can be particularly hazardous in high-stakes environments, such as predictive surveillance, proactive threat deterrence, or autonomous targeting, where any singular error can result in life-or-death consequences.

Risk Perception and Threat Prioritization

Risk is not assessed in isolation; even algorithmic, AI-enabled assessment systems are subject to human-influenced parameters – shaped by cultural doctrine, operational experience, and affective biases – affecting both data interpretation and decision-making processes. Security professionals and policymakers may view the same technology through different lenses, depending on whether their focus is on short-term operational effectiveness or long-term societal impact. For example, a predictive surveillance algorithm might be perceived as a breakthrough in crime prevention but may also be perceived as a tool for racial profiling by civil rights advocates. Such misalignment in risk perception among stakeholders can hinder coordination and lead to further ethical 'blind spots'.

Cultural and Institutional Influences

The organizational culture within which a technology is developed or deployed plays a substantial role in shaping its function. Military institutions often emphasize efficiency and control, potentially prioritizing functionality over ethical nuance. Academic and research institutions may focus on openness and discovery, which can inadvertently facilitate unintended dual-use risks. In the private tech sector, the drive for innovation and market leadership may overshadow considerations of long-term societal impact. These contrasting institutional values affect how technologies are designed, evaluated, and operationalized.

Communication Gaps and Interdisciplinary Silos

A recurring problem in the dual-use landscape is the communication gap between technologists, policymakers, and security practitioners. Developers may not comprehensively realize the operational context in which their technologies are used, while security agencies, focused on their mission, may inadvertently overlook the technical aspect to identify hidden vulnerabilities. These silos can lead to poor implementation, misuse, or failure to foresee second-order effects. Bridging these gaps requires sustained dialogue, shared ethical training, and the establishment of interdisciplinary teams that can collectively assess both technical performance and broader implications.

Accordingly, human factors are central—not ancillary—to the dual-use technology paradigm, as they fundamentally shape the interpretation, deployment, and mitigation of associated risks. It is critical to explore the intersection of these human dimensions with ethical and legal considerations, particularly in contexts where transparency, accountability, and civil liberties are at stake.

3.2. Cognitive Drivers and Radicalization

Cognitive drivers refer to the underlying psychological, emotional, and informational processes that influence human perception, reasoning, belief formation, and decision-making[16]. These cognitive mechanisms are central to understanding how individuals or groups may become radicalized and motivated to exploit such technologies for extremist or malicious ends. Radicalized actors increasingly view EDTs as instruments of asymmetric leverage and tactical advantage. Cognitive biases – such as optimism bias, dehumanization, and in-group/out-group dynamics – facilitate moral disengagement, lowering psychological barriers to the indiscriminate and weaponized use of these advanced technologies by terrorist entities[17]. Accordingly, cognitive drivers and radicalization are not merely sociopolitical issues—they are fundamental to understanding and shaping the human-technology interface in ways that promote security, resilience, and ethical responsibility.

3.3. Organizational Behavior of Terrorist Networks

Terrorist networks, although often decentralized and covert, exhibit complex organizational behaviors that mirror those of legitimate institutions in their capacity to adapt, innovate, and leverage emerging technologies[18]. Decentralized terrorist cells exhibit traits similar to those of agile startups with rapid prototyping, opportunistic learning, and tech adoption capabilities. The organizational culture within these groups often rewards innovation, facilitating the prospects of tech repurposing[19]. The diffusion of dual-use technologies further accelerates this innovation cycle. Open-source platforms, global supply chains and unrestricted dissemination of scientific information provide terrorist actors with unprecedented access to tools that can be adapted for asymmetric warfare, cyberterrorism, or mass disruption. Organizational behavior within these groups is often characterized by a pragmatic blend of ideology and technocratic acumen, where innovation is not just tolerated but incentivized. Understanding these behaviors is essential for developing countermeasures. Intelligence and security frameworks must evolve to monitor not only individual actors but also patterns of innovation, recruitment, training, and operational doctrine within these organizations. Behavioral surveillance metrics, including shifts in procurement behavior, resource prioritization and the emergence of ideological narratives around technology, may function as critical early indicators of dual-use technology misuse.

3.4. Psychological Profiles of Tech-Savvy Terrorists

The emergence of tech-savvy terrorists signals a significant evolution in modern threat dynamics. From a counter-terrorism perspective, profiling their psychological and cognitive characteristics is essential for anticipating behaviors and shaping tailored interventions. These individuals often possess advanced technical knowledge and digital fluency and leverage their expertise to repurpose AI, cyber tools, drones, or synthetic biology for asymmetric attacks, cyberterrorism and ideological disruption. Tech-savvy terrorists often exhibit high openness to experience, technical proficiency and moral disengagement. Understanding these traits helps in

[16] Wolfowicz M, Litmanovitz Y, Weisburd D, Hasisi B. Cognitive and behavioral radicalization: A systematic review of the putative risk and protective factors. Campbell Syst Rev. 2021 Jul 20;17(3):e1174. doi: 10.1002/cl2.1174. PMID: 37133261; PMCID: PMC10121227.

[17] Bandura, A. (1999). Moral disengagement in the perpetration of inhumanities. Personality and Social Psychology Review, 3(3), 193–209.

[18] Helfstein, S. (2009). Governance of Terror: New Institutionalism and the Evolution of Terrorist Organizations. Public Administration Review, 69(4), 727–739. http://www.jstor.org/stable/27697917

[19] Cronin, A. K. (2015). ISIS is not a terrorist group. Foreign Affairs, 94(2), 87–98.

profiling and intercepting potential threats[20]. Common psychological traits may include narcissism linked to perceived intellectual superiority, moral disengagement that justifies technological harm as necessary or righteous, and a utilitarian mindset that prioritizes effectiveness over ethical boundaries. Coupled with a strong sense of grievance, whether political, ideological or personal, these individuals may channel their technical skills into developing sophisticated attack vectors using dual-use technologies to hide their innate intent. Fundamentally, their motivations are not always rooted in traditional extremist ideologies, as their ideologies are driven by anti-establishment sentiments, techno-anarchism or even transhumanist visions distorted by radical interpretations. This complexity underscores the need for early identification and intervention strategies that are both multidisciplinary and strategic, requiring close collaboration among behavioral scientists, cybersecurity specialists, intelligence analysts, and technologists. Hence, one can conclude that the 'human element' is not a variable to be minimized—it is a central driver of outcomes.

4. Human Factors in Counterterrorism

Human factors encompass how individuals and groups engage with technologies, operational settings, and decision-making systems. Within the security domain, dual-use threats, particularly terrorism, are often defined by asymmetrical strategies, the opportunistic exploitation of emerging technologies, and inherent unpredictability. In this complex environment, integrating human factors into counterterrorism strategies is crucial for ensuring effective, adaptable, and ethical responses[2122]. From counterterrorism perspectives, this includes an understanding of the behaviors, cognitive biases, situational awareness, stress responses, communication patterns, and training needs of those involved in prevention, detection, and response efforts. In general, human factors research serves as the foundation for the development of behavioral surveillance techniques, threat recognition systems, and early warning indicators, all grounded in psychological and social analysis. These insights are crucial for identifying radicalization trajectories, insider threats, or misuse of accessible technologies. Incorporating human factors into counterterrorism within the dual-use domain extends beyond technical solutions alone. It requires a systemic, multidisciplinary approach that accounts for the capabilities and limitations of both adversaries and defenders. Ultimately, human-centered design and operational insight become strategic assets, strengthening situational awareness, minimizing errors, and promoting ethical and sustainable security in a world where emerging technologies continuously reshape the threat landscape, thereby enhancing security and resilience.

Counterterrorism professionals are tasked with processing large volumes of information under high-stress conditions. Key human factors – such as cognitive load management, situational awareness, and bias mitigation – directly impact mission effectiveness.[23]. Additionally, immersive simulation environments, leveraging Virtual and Augmented Reality (VR/AR), can significantly enhance training by simulating complex threat scenarios in controlled settings. Human-centric design ensures that technologies augment rather than overload users[24]. Furthermore, effective

[20] Post, J. M. (2005). The mind of the terrorist: The psychology of terrorism from the IRA to al-Qaeda. Palgrave Macmillan.
[21] Warnes, R., Human Factors in Effective Counterterrorism , Routledge, Miami, USA. ISBN 9781032451602.
[22] Hubbard EM. Hostile intent and counter terrorism: human factors theory and application. Ergonomics. 2016 Apr;59(4):612-3. doi: 10.1080/00140139.2015.1097056.
[23] Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors, 37(1), 32–64.
[24] Salas, E., et al. (2002). Simulation-based training: A review and needs assessment. Human Factors, 44(4), 103–118.

counterterrorism operations demand interdisciplinary collaboration among cybersecurity experts, behavioral analysts and psychologists, AI ethicists and military strategists. Building an adaptive learning culture is essential to anticipate evolving threats and respond decisively[25]. Figure 3 illustrates a flowchart of the Human-Centered Dual-Use Identification and Safeguards Development Training framework."

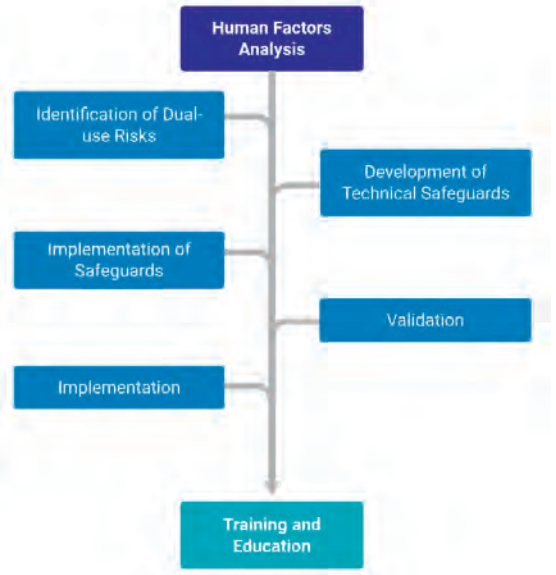


Figure 3: Flowchart of Human-Centered dual-use identification and safeguards development Training

5. Case Studies of Dual-Use Misappropriation

To illustrate the complex interplay of human, ethical and legal dimensions in the dual-use of EDTs, this section presents selected real-world case studies. Due to the sensitive nature of the topic, details are intentionally limited to highlight both the opportunities and risks of applying advanced tools in counterterrorism, while avoiding disclosure of any specific TTPs that adversaries could exploit.

5.1. Deepfake Propaganda Campaigns

In 2020, a deepfake video allegedly showed a Western political leader making inflammatory remarks that circulated extremist forums, inciting civil unrest. The video was created using open-source deepfake tools, demonstrating how generative AI can be co-opted for terrorist propaganda[26]. In 2022, a deepfake video surfaced showing Ukrainian President Volodymyr Zelensky allegedly calling for surrender to Russian forces. Although the video was crude and quickly debunked, it exemplifies the potential for deepfake-driven psychological operations (PSYOPs) by state or non-state actors to weaken resistance or erode trust. There are also instances of such deepfake videos being used for election interference. Equally, terrorist groups could

[25] Senge, P. M. (1990). The Fifth Discipline: The Art & Practice of The Learning Organization. Doubleday.
[26] Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1819.

create deepfake videos of respected religious or cultural figures endorsing their ideology. This could manipulate vulnerable populations and aid in online radicalization efforts. Terrorists could release deepfake content that mimics another group or nation (known as 'false flag operations'), claiming responsibility for an attack, triggering misattribution, political conflict or retaliation.

5.2. DIY Biohacking for Bioterrorism

The 2018 case of a biohacker in Germany, who attempted to modify *E. coli* to produce a toxin, underscores the risks of democratized biotechnology. Though stopped by authorities, the case revealed lapses in oversight and the psychological profiling of individuals engaging in DIY bioterrorism[27]. With the DIYBIO toolkits, organizations such as the International Genetically Engineered Machine (iGEM)[28], using interactive programs such as BioBrick[29] can generate DNA sequences to produce complex biological systems via modularization. Additionally, research centers, such as the Synthetic Biology Research Center (SynBERC)[30], and the Engineering Biology Research Consortium (EBRC) has been developing "desired" biological components and assembling them into integrated systems. Put broadly, synthetic biology is the intentional modification of cells, organisms, colonies, or major sub-systems thereof; however, the keyword is 'intentional'. The aforementioned platforms offer academic forums for designing biological systems that utilize living cells. Despite their academic potential, the major drawback of these otherwise 'academic social interest groups' is the action of special interest groups with potentially 'not so social' intentions, with the potential of crafting artificial biological agents that evade detection or countermeasures.

Since the ratification of the Biological Weapons Convention (BWC) in 1972 – which established a foundational legal framework for prohibiting the development, production, and stockpiling of biological and toxin weapons – synthetic biology has emerged as a critical next frontier for biosecurity governance. This domain is digitally driven, globally interconnected, and increasingly decentralized, expanding both its beneficial applications and its dual-use risks. The evolving threat landscape is marked by attributional ambiguity, delayed detection capabilities, and limited deterrence—factors that strain traditional defense postures. As such, a robust security framework must prioritize anticipatory governance, international norms for responsible innovation, real-time threat monitoring and operationally credible deterrence mechanisms. This requires coordinated efforts across national security, public health, intelligence and scientific communities.

5.3. Drone-Based Attacks

In 2016, Daesh deployed modified commercial drones (e.g., DJI Phantom, fixed-wing models) to drop small explosives on opponents in Iraq. In 2018, two explosive-laden DJI Matrice 600 drones were used in an attempted attack on President Nicolás Maduro during a military parade in Venezuela. Since 2019, Yemen's Houthi rebels have used Iranian drone technology in attacks on Saudi infrastructure. The Russia-Ukraine and Middle East conflicts have been primarily conducted using

[27] Esvelt, K. M., & Carlson, J. (2019). The responsibility of synthetic biologists to anticipate biosecurity threats. eLife, 8, e43955.
[28] https://www.igem.org/ Accessed: June 24, 2025.
[29] Sleight SC, Bartley BA, Lieviant JA, Sauro HM. In-Fusion BioBrick assembly and re-engineering. Nucleic Acids Res. 2010 May;38(8):2624-36. doi: 10.1093/nar/gkq179. Epub 2010 Apr 12. PMID: 20385581; PMCID: PMC2860134.
[30] https://ebrc.org/synberc/ Accessed June 24, 2025

drones and have changed the battlefield dynamics. At the US southern border, while border agents use drones to monitor illegal border crossings, the Mexican cartels, particularly Jalisco New Generation Cartel (CJNG), have deployed drones fitted with explosives in conflicts with rival groups and police, and also to smuggle drugs and guns across the border. These adaptations reflect both technical knowledge and creativity by operatives with access to open-source schematics and consumer-grade technology[31].

5.4. Artificial Intelligence

While the world operates with artificial narrow intelligence (ANI), world leaders are forming working groups to address the dual-use aspects of artificial general intelligence (AGI). Industry leaders predict that AGI may emerge within the next five years: some might say sooner. Demis Hassabis of Google DeepMind, Dario Amodei of Anthropic, and Sam Altman of OpenAI are not speculating – they are building to get there first. Private companies, startups, and even rogue actors may soon hold this power. Furthermore, while the potential benefits are extraordinary, the risks are existential. The consensus is that 'we should not fear intelligence. We should fear leaving it unguided.' However, even with guardrails in place, rogue developers and even state actors are unlikely to follow any guidelines. From a tactical standpoint, adversarial use of AI with autonomous weapon systems and decision-making will pose a significant challenge.

Autonomous weapon systems (AWS), including loitering munitions and AI-enabled drones, are increasingly being tested and deployed in conflict zones with counterterrorism elements. In 2020, a United Nations report suggested that an autonomous drone may have operated independently to engage a target in Libya—a potentially historic first. Such systems offer operational advantages as UAVs can execute reconnaissance, logistics, and strike missions with minimal human-in-the-loop exposure, with speed, reach, and risk reduction for personnel. However, they raise serious questions about delegating lethal decision-making to machines. Critics argue that without human oversight, UAVs and AWS may lack the capacity to distinguish between combatants and civilians, or to accurately interpret intent and distinguish between surrender and other actions. Perhaps, one of the critical aspects is human–machine teaming through cognitive interoperability to ensure that human users retain situational awareness, command authority, and moral authority. This challenges the principles of proportionality and discrimination under international humanitarian law. The case of UAVs and AWS reflects one of the most ethically charged dimensions of dual-use technologies, where technological autonomy threatens to outpace human moral and legal judgment. These case studies demonstrate that while EDTs can significantly bolster counterterrorism efforts, they also introduce profound ethical, operational, and governance challenges.

5.5. AI and Facial Recognition in Urban Counterterrorism

Recently, many cities have adopted and deployed AI-powered facial recognition systems as part of their security infrastructure[32]. These systems are used to identify individuals in real-time, especially at airport screening, monitor high-risk locations, and analyze behavioral patterns. In some cases, facial recognition has successfully aided in the apprehension of known terrorists or the prevention of planned

[31] Gettinger, D. (2017). Drone Databook. Center for the Study of the Drone at Bard College.
[32] https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition Accessed June 24 2025.

attacks. However, these technologies have also faced intense backlash due to concerns over mass surveillance, racial bias, and false positives. Investigations have shown that facial recognition systems are less accurate for people with darker skin tones and women, raising issues of algorithmic discrimination. In the UK and the US, civil rights organizations have challenged the legality of such surveillance, leading to temporary bans or stricter oversight in several jurisdictions. This case exemplifies how the implementation of AI in public security must contend not only with technical efficacy but also with societal values such as fairness, transparency, and trust.

5.6. Biosecurity During Pandemics

The COVID-19 pandemic highlighted the dual-use nature of biotechnology in stark terms. Technologies such as CRISPR, mRNA vaccine platforms, and synthetic biology, while central to global public health responses, have also revealed vulnerabilities in biosecurity. The same tools that enabled the rapid development of vaccines could, in theory, be used to engineer pathogens with enhanced transmissibility or resistance to treatment. Security agencies worldwide began reassessing their readiness for bioterrorism, acknowledging that non-state actors or rogue states could exploit these technologies for malicious purposes. The pandemic also reignited debates about research oversight, gain-of-function experiments, and the sharing of genomic data, particularly when such data can be used to design both cures and weapons. This case highlights the urgent need for dual-use risk assessment in the life sciences. It underscores the importance of interdisciplinary cooperation among bioengineers, public health experts, and national security institutions.

5.7. Emerging Platforms

Emerging technologies such as quantum computing, hypersonics, space systems, and smart materials offer transformative capabilities, but also introduce significant security challenges. Within the scope of this paper, particular attention must be given to the risk vectors associated with microelectronics. A documented case study involving compromised components in a Chinese-manufactured solar power plant highlights the operational fragility of the global microelectronics supply chain[33]. These components, often synthesized using smart materials, are reportedly capable of bypassing firewalls, transmitting data covertly, and even initiating unauthorized system shutdowns. This incident underscores the dual-use nature and critical vulnerability of microelectronic systems that underpin mission-relevant functions, often in ways that are neither transparent nor controllable. The insertion of ‘compromised’ components into existing electronic infrastructure effectively constitutes a latent 'kill switch.' In a conflict scenario, activation of such embedded systems could trigger blackouts, disrupt grid synchronization, and compromise operational continuity across defense-critical installations. As AI-enabled platforms increasingly depend on layered data architectures and autonomous decision loops, any compromise to hardware integrity risks collapsing the entire command-and-control structure. This is not a vulnerability that can be addressed solely by software patches—it requires end-to-end command oversight of the microelectronics pipeline, coupled with battlefield-grade validation and assurance for every critical system component.

6. Human Factors and Tech Misuse: Counterstrategies, Ethics and Mitigation

[33] https://itecsonline.com/post/hidden-threat-rogue-communication-devices

The deployment of dual-use technologies in counterterrorism efforts occurs at the intersection of ethics, law, and security. While these tools offer powerful advantages in detecting and neutralizing threats, they also raise difficult questions about accountability, privacy, due process, and ethical limits. These dilemmas are not abstract; they directly impact how societies balance the imperatives of security with the protection of human rights. To frame this discourse, several relevant aspects are discussed below.

6.1. Ethics-by-Design Technological Frameworks

Embedding ethical constraints and fail-safe strategies into the design phase of EDTs is quintessential. Ethics-by-Design (EbD) frameworks aim to embed ethical principles directly into the architecture, development and deployment processes of emerging technologies. This proactive approach is crucial for minimizing misuse and ensuring responsible innovation. For dual-use technologies such as synthetic biology, AI, drones or quantum computing, the risks of unintended proliferation or malicious repurposing are significant. EbD frameworks serve as ethical guardrails, reinforcing security, transparency and resilience without stifling innovation. The intended output aligns technological capabilities with international norms and human rights, facilitates compliance with export control, arms control treaties and biosecurity standards, as well as enabling anticipatory governance in high-stakes domains, such as lethal autonomous systems or gene-editing tools.

6.2. Behavioral Surveillance and Anomaly Detection

Advanced surveillance technologies, including facial recognition, biometric tracking and predictive analytics, can vastly enhance situational awareness in counterterrorism contexts[34]. However, their use also presents significant risks of overreach, particularly when applied in ways that infringe on civil liberties. Governments and organizations utilize behavioral analytics to identify early signs of radicalization, insider threats, or cyber breaches by monitoring communications, access patterns, and physical movement using machine learning. These systems integrate behavioral psychology with computational models[35]. Predictive algorithms that forecast potential terrorist activity based on behavioral or demographic data can lead to discriminatory profiling, false positives and the stigmatization of entire communities. Authoritarian regimes may use behavioral surveillance to suppress dissent, profile populations and exert social control. Similarly, poorly designed anomaly detection systems can lead to reinforcing systemic discrimination or violating civil liberties. Several technological platforms, such as AI-driven pattern recognition, identify outliers in digital activity. Biometric and physiological monitoring tracks gait, facial expressions or heart rate to detect stress or deception, while Contextual Awareness Systems (CAS) fuse multiple data streams to interpret situational norms. In liberal democracies, such practices strain the relationship between citizens and the state and may even fuel the very radicalization they seek to prevent. Striking a balance between effective surveillance and the protection of rights such as privacy, free expression, and due process is one of the most contentious ethical issues in this space.

6.3. Policy and Regulatory Interventions

[34] https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/behavioral-analytics/ accessed Jun 24, 2025.
[35] Brantingham, P. J., Valasik, M., & Mohler, G. O. (2018). Does predictive policing lead to biased arrests? Results from a randomized controlled trial. Statistics and Public Policy, 5(1), 1–6.

The international legal landscape governing dual-use technologies is fragmented and underdeveloped. While some frameworks, such as the Biological Weapons Convention (BWC) or the Wassenaar Arrangement[36] on export controls offer partial guidance to regulate dual-use technologies; however, they are not equipped to handle the speed and scale of current technological innovation. Many dual-use technologies, such as AI-driven cyber tools or synthetic biology platforms, fall into legal grey areas where jurisdiction, enforcement and attribution are unclear. Additionally, norms around acceptable state behavior in cyberspace, biotechnology and autonomous weapons remain contested among nations. Without consensus, states may engage in a technological arms race or exploit legal loopholes, increasing the risk of escalation, misuse or accidental harm. Multilateral dialogue and updated legal instruments are urgently needed to provide a shared ethical and legal foundation. These ethical and legal challenges are not just constraints to innovation—they are essential guardrails that define the legitimacy and sustainability of technological use in counterterrorism. However, enforcement is uneven, requiring international harmonization[37]. For AGI, some work has already begun. In 2023, seventy parliaments pledged cooperation on AGI governance. The Organization for Economic Co-operation and Development (OECD) is developing capability indicators, and the European Union's AI Act 2.0 lays the groundwork for a regional foundation. Efforts are underway to harmonize governance under a global platform that encompasses every nation, i.e., the United Nations (UN). Efforts are underway to request that the UN convene a special session of the General Assembly dedicated to AGI governance. However, these are scattered efforts, and a highly coordinated framework is needed, without which the AGI may evolve more rapidly than the systems intended to guide it.

6.4. Community Engagement and Deradicalization

Community engagement and deradicalization are critical, human-centered strategies that, when ethically augmented by technology, can counter the misuse of dual-use innovations. A successful approach requires balancing trust-building and rights-respecting interventions with technological sophistication to reduce radicalization drivers while preserving democratic values. Programs such as the UK's Prevent strategy incorporate social workers, psychologists and community leaders to reduce radicalization. These human-centered strategies address the roots of ideological extremism[38]. Other strategies, such as prevention through engagement to create early-warning ecosystems that detect and disrupt pathways to extremism, and deradicalization support by using data-informed psychosocial strategies to work with former extremists to reintegrate them into society, can reduce the pool of actors likely to weaponize dual-use technology. While these strategies are effective, there are unintended consequences if misused, such as the tools spreading extremist ideology or being used as tools of state propaganda. Additionally, community-based tech interventions risk alienation if perceived as coercive or intrusive, undermining trust.

6.5. Accountability and Transparency in Automated Systems

As counterterrorism increasingly relies on ML and autonomous decision-making systems, the issue of accountability becomes deeply embedded and complex. When an AI-powered surveillance tool misidentifies a target or an autonomous drone

[36] https://www.wassenaar.org/ Accessed June 24, 2025.
[37] Moodie, M. (2016). Controlling dual-use research: The experience of the Australia Group. Nonproliferation Review, 23(3-4), 369–384.
[38] Neumann, P. R. (2013). The Trouble with Radicalization. International Affairs, 89(4), 873–893.

causes civilian harm, it is often unclear who is responsible – the developer, the remote pilot in control (RPIC), the satellites for misidentifying the target, the algorithm or the state. This diffusion of responsibility challenges traditional legal and moral frameworks, underscoring the need for transparent system design and clear chains of accountability. Moreover, many of these technologies operate as 'black boxes', offering little visibility into how decisions are reached. This opacity undermines trust, particularly when decisions affect individual liberties or have life-and-death consequences. Ethical design principles, such as explainability, auditability and 'human-in-the-loop' control, must be embedded into systems from the outset, rather than being added as afterthoughts.

7. Governance and Oversight Mechanisms

Effective governance of dual-use technologies requires a multidimensional approach that addresses the unique risks these tools present while preserving their legitimate and beneficial applications. Current oversight mechanisms, while helpful, are often fragmented, slow to adapt, and inconsistently enforced across jurisdictions. Governance and oversight have become more complex due to human factors, such as the intentionality of those involved in dual-use technologies. This section assesses existing frameworks and proposes guidance grounded in ethical foresight, interdisciplinary collaboration and international cooperation.

7.1. Limitations of Existing Frameworks

Several international treaties and agreements form a foundational framework for managing the security risks associated with dual-use technologies. The Wassenaar Arrangement on export controls provides a mechanism for regulating the transfer of certain military and dual-use goods and technologies. The Biological Weapons Convention prohibits the development and use of biological weapons, including those that could arise from synthetic biology or genetic engineering. Similarly, the Geneva Conventions and associated protocols govern the conduct of war, including the use of technologies in armed conflict. However, these instruments frequently lack the agility and scope required to address the challenges posed by rapidly advancing technologies. They tend to be reactive rather than proactive, limited in scope and lack enforcement power. Furthermore, existing mechanisms provide limited and sometimes no coverage of Emerging Disruptive Technologies, leaving critical oversight gaps. Moreover, state actors interpret and implement these agreements differently, creating loopholes and inconsistencies. Finally, these frameworks lack mechanisms to integrate human factors into both risk assessment and the mitigation of dual-use threats.

7.2. The Role of Institutional Review and Ethics Boards

In civilian and academic contexts, ethics review boards and institutional oversight committees play a crucial role in evaluating dual-use risks, particularly in biotechnology and data science. However, these mechanisms are often absent in security or corporate R&D settings, where secrecy, speed, and competitive advantage are prioritized. Creating standardized dual-use review processes across sectors could help identify potential red flags early in the development process. To be effective, such review boards must include not just technical experts but also ethicists, legal scholars, human rights advocates and members of affected communities. This multidisciplinary composition ensures that ethical considerations are integrated into design, deployment, and policy from the beginning, not as an addendum or afterthought.

7.3. National Policies and Cross-Sectoral Regulations

Governments play a pivotal role in establishing the legal, ethical, and strategic parameters for the development and deployment of emerging disruptive technologies. Nevertheless, many national regulatory frameworks remain fragmented or underdeveloped, particularly in addressing the complex challenges posed by dual-use technologies. Few countries have adopted comprehensive policies that encompass the full spectrum of EDTs, and even fewer explicitly incorporate human factors into their governance models. To close these critical gaps, national strategies must evolve to include mandatory ethical and security impact assessments for high-risk technologies, enforce transparency and accountability in public-private technology contracts, and institutionalize dual-use awareness training for scientists, engineers, and security professionals. Furthermore, fostering participatory governance through public engagement initiatives and inclusive forums like the AI Action Summit in Paris, which convened global leaders, technologists, academics, civil society actors and artists, can build societal trust and legitimacy. These measures are essential to cultivating a culture of responsible innovation while ensuring that emerging technologies are governed in a manner that is secure, ethical, and aligned with democratic values.

7.4. The Need for International Cooperation

As technological innovation transcends national borders, effective governance requires an equally global and collaborative framework[39]. Without sustained international cooperation, unilateral or inconsistent regulatory approaches will inevitably create exploitable gaps – opportunities that malicious actors can leverage to bypass oversight. A coordinated global strategy must include the modernization of international legal frameworks to explicitly address EDTs, such as AI, autonomous systems, UAVs, smart and functional materials, and biotechnology. It should also prioritize the creation of multilateral forums dedicated to dual-use ethics and governance, engagement of human factors, the exchange of best practices, the development of globally recognized ethical standards, and the promotion of regulatory interoperability among national oversight bodies. Such collaboration is critical to ensuring that emerging technologies are deployed not only for effective counterterrorism but also in ways that uphold legitimacy, ethical integrity and long-term sustainability. As the dual-use dilemma intensifies, governance systems must evolve in both scope and sophistication to reflect the complexity and transboundary nature of the technologies they aim to regulate.

8. Policy Recommendations

The dual-use nature of EDTs necessitates a proactive, interdisciplinary approach to policymaking—one that can anticipate intentional misuse, mitigate unintended consequences, and embed human-centered ethical safeguards throughout the innovation lifecycle. Drawing on insights from the preceding discussion, the following policy recommendations aim to enhance the responsible development and deployment of dual-use technologies in counterterrorism contexts.

Government agencies and private developers should adopt human-centered design principles of technological development. This includes involving end-users and

[39] Vaseashta, A., (2022), Applying Resilience to Hybrid Threats in Infrastructure, Digital, and Social Domains Using Multi-sectoral, Multidisciplinary, and Whole-of-Government Approach. Pp. 42-59. Vol. 61: Building Cyber Resilience against Hybrid Threats. DOI: 10.3233/NICSP220017

affected communities in the design and testing process, prioritizing transparency, explainability and accountability in system architecture, and designing for fallback and override mechanisms to maintain human oversight. Human-centered design helps align technological functionality with societal values, ensuring tools are practical without compromising rights or ethical standards. Additionally, all security-related technologies should undergo dual-use risk assessments prior to deployment, considering the potential for misuse or repurposing by malicious actors, societal and ethical impacts of failure or misapplication, and systemic risks stemming from reliance on automation or opaque algorithms. Such assessments should be iterative, adapting as technologies evolve, and involve a diverse range of experts, including ethicists, social scientists and representatives from civil society. In contrast, the misuse of technologies stems from human factors; however, risks can be effectively mitigated through human-centered design frameworks that integrate core security principles and advanced technological safeguards to shift the paradigm from a reactive posture to proactive preparedness.

Governments should establish independent oversight bodies responsible for regulating dual-use technologies across various sectors. These agencies must set safety and ethical standards, monitor compliance across industry and public institutions, and provide certification or licensing for high-risk technologies. To further the outcome, these bodies should be empowered to conduct audits, issue moratoriums on unsafe tools, and facilitate cross-sector dialogue. Furthermore, it is necessary to promote ethics and security literacy among technologists, as well as tech literacy among policymakers and security personnel, through dual-use ethics modules in STEM and intelligence curricula, cross-disciplinary fellowships or exchange programs, and continuing education requirements for professionals in high-value fields. Education is a long-term investment in cultural change – an essential component of responsible innovation. From an adversarial perspective, intentionality is often indeterminate: however, mitigating the misuse of dual-use technologies requires a multifaceted approach, emphasizing education, ethical training, regulatory guidance, and moratoria on unsafe or unvalidated tools. At the global level, the international community should update treaties and norms to address the dual-use potential of emerging technologies explicitly. By creating an international code of conduct for dual-use technologies, it is possible to promote diplomatic mechanisms to de-escalate technological arms races. International cooperation ensures that technological progress does not outpace the legal and ethical infrastructure needed to manage it responsibly.

Finally, public trust is vital for the legitimacy of security technologies. States and developers should publish non-sensitive information on the goals, capabilities and limitations of deployed tools to enable democratic oversight and input, particularly in surveillance-related policies, and support independent research and journalism that scrutinizes dual-use practices. Transparency reduces the risk of public backlash, misinformation, and the erosion of democratic accountability. However, it is a double-edged sword since adversaries are likely to misuse such transparency and accountability.

9. Conclusion and Path Forward

The dual-use nature of Emerging Disruptive Technologies presents a defining challenge for the future of counterterrorism and global security. These technologies – ranging from AI and biotechnology to autonomous systems – are not inherently

predetermined as good or evil. Instead, their impact is shaped by human intent, institutional culture, governance frameworks and societal values. Addressing the human factors involved in the dual-use of EDTs is pivotal in modern counterterrorism efforts. This paper has explored the promise of a multidisciplinary and human-centered approach. These tools enable faster threat detection, more precise interventions and enhanced intelligence capabilities, as they strike a balance between innovation and precautionary measures, which will be crucial to ensuring that technological advancements do not outpace our capacity to manage their risks. Nevertheless, the perils are equally profound. Misuse, overreach, and ethical neglect can undermine civil liberties, exacerbate global instability and erode public trust in democratic institutions. At the heart of this tension lie human factors, viz., the cognitive biases that shape decisions, the organizational pressures that influence design, and the ethical blind spots that go unnoticed until harm is done. These human dimensions are not just soft considerations – they are central determinants of whether technology becomes a force multiplier for purposes both good and bad. Navigating this landscape requires a new kind of leadership – one that is anticipatory, interdisciplinary and grounded in ethics. It requires building systems of governance that are as agile and intelligent as the technologies they regulate. It also demands cultivating a culture of accountability, where innovation is aligned with the public good, and where the right questions are asked before the wrong tools are deployed. Ultimately, the goal is not to resist or restrict technological progress, but to steward it wisely. By embedding ethical foresight and human-centered values into the development and use of dual-use technologies, we can shape a future where security and liberty reinforce each other, rather than threaten one another. The future directions and emerging challenges of human factors in dual-use technologies encompass the primary challenges that may arise from the convergence of technologies, which increase overall risk exponentially. Addressing these challenges requires interdisciplinary forecasting and scenario planning[40]. These challenges also present unique opportunities to develop robust frameworks and systems that strengthen security posture and enhance deterrence. This includes advancing intelligence and surveillance capabilities, establishing alliance-driven norms, implementing cognitive deterrence and strategic messaging programs, formulating innovation-informed deterrence postures, and modernizing dual-use risk assessment protocols by engaging the human factors paradigm. Governments must institutionalize these practices to remain ahead of potential misuse[41]. Human-centric AI tools in Counterterrorism play a vital role; hence, such tools must be interpretable, trustworthy and enhance rather than replace human oversight. The human-centric AI should promote transparency and accountability in counterterrorism applications[42]. Lastly, anticipatory governance must encompass horizon scanning, participatory foresight and adaptive regulations for managing the evolving dual-use risks and opportunities.

In conclusion, dual-use risks are intrinsic to emerging innovations, often amplified by the human factors that shape their development and deployment. While no solution is foolproof, a strategic approach grounded in ethics, targeted education, robust policy frameworks and a proactive security posture can significantly reduce the likelihood of misuse and enhance resilience against adversarial exploitation.

[40] Garreau, J. (2005). Radical Evolution. Doubleday.
[41] Guston, D. H. (2014). Understanding 'anticipatory governance'. Social Studies of Science, 44(2), 218–242.
[42] Rahwan, I. (2018). Society-in-the-loop: Programming the algorithmic social contract. Ethics and Information Technology, 20(1), 5–14

CHAPTER 3

TERRORIST THREATS EMANATING FROM CYBERSPACE: DISINFORMATION, RADICALIZATION AND RECRUITMENT

Robert Mikac

Krešimir Mamić

Some scientists believe that the term 'cyberspace' was first used by William Gibson in his science fiction works in a short story, 'Burning Chrome,' in 1982, and reused later in his celebrated novel, *Neuromancer*, in 1984.[43] Gibson also proposed a definition:

"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data. Like city lights, receding..."[44]

Since then, cyberspace has materialized from an idea and has become an indispensable part of numerous processes and activities in the modern world for the most diverse spectrum of actors. Indeed, a vast number of actors now utilize cyberspace for their various needs and goals, and the subsequent focus will be on exploring how some of these actors (terrorists and organized criminal groups) exploit cyberspace for illegal purposes.

Introduction

Cyberspace has profoundly transformed our world, offering a myriad of benefits that make it an indispensable part of modern life. It serves as a global connector, bridging geographical distances and enabling instantaneous communication across continents. This connectivity fosters unprecedented collaboration in scientific

[43] Pym, D. J. (2021) The Orgins of Cyberspace. In: Cornish, P. (ed) *The Oxford Handbook of Cyber Security* (page 11). Oxford: Oxford University Press.

[44] Gibson, W. (1984) *Neuromancer* (page 51). New York City: Ace Books.

research, business and education, accelerating innovation and knowledge sharing. Cyberspace also democratizes access to information, providing vast online libraries, educational resources and news outlets that empower individuals worldwide. For businesses, it opens up global markets, facilitates e-commerce and streamlines operations, driving economic growth. Furthermore, it offers a rich tapestry of entertainment, social interaction and creative expression, allowing individuals to connect with like-minded communities and pursue their passions. In essence, cyberspace has become the backbone of our interconnected society, enabling progress and enriching countless aspects of human experience.

Despite its many advantages, cyberspace presents significant challenges that demand careful attention. The rapid spread of disinformation and misinformation is a major concern, as false narratives can erode trust, manipulate public opinion, and even incite real-world harm. The sheer number and diversity of online platforms make it incredibly difficult to monitor and regulate content effectively, creating fertile ground for harmful activities. Moreover, the increasing sophistication of artificial intelligence (AI) and deepfake technologies poses a grave threat. These tools can be misused to create highly convincing fake images, audio, and videos, leading to identity theft, reputational damage, and the spread of propaganda. The anonymous nature of much of the internet also facilitates cybercrime, online harassment, and the exploitation of vulnerable individuals. Addressing these complex issues requires a multi-faceted approach involving technological solutions, robust regulatory frameworks, international cooperation, and enhanced digital literacy among users.

The vast and interconnected nature of cyberspace, while offering immense opportunities, is unfortunately exploited by a wide array of actors for negative and illegal activities. This spectrum of malicious entities ranges from nation-states engaging in espionage, infrastructure disruption and political interference, to multinational corporations involved in data exploitation and unethical surveillance. Intelligence communities, while often operating under legal frameworks, can also leverage cyber capabilities for covert operations that blur ethical lines. Beyond these powerful entities, terrorist organizations utilize the digital realm for propaganda, recruitment and planning attacks, while organized crime syndicates profit from ransomware, fraud and data theft. Finally, individual hackers and hacktivists, driven by diverse motivations from financial gain to political protest, contribute to the complex threat landscape through unauthorized access, data breaches and service disruptions. The pervasive presence of these varied actors underscores the constant need for robust cybersecurity measures and international cooperation to safeguard the digital frontier.

This analysis will focus on examining how terrorists primarily, and organized criminal groups secondarily, exploit cyberspace to achieve their objectives. We will

delve into their sophisticated use of digital platforms for a range of illicit activities. Specifically, we will explore their strategies for spreading disinformation to manipulate public opinion and incite fear. The analysis will also cover their methods for fostering radicalization, drawing individuals into extremist ideologies and preparing them for violent acts. Furthermore, we will investigate how these groups leverage the internet for recruitment, identifying and grooming new members, often across international borders, to expand their networks and capabilities. Understanding these tactics is crucial for developing effective countermeasures against evolving threats in the digital realm.

Terrorist organizations are increasingly exploiting cyberspace for the purposes of disinformation, radicalization, and recruitment. Sophisticated tools such as artificial intelligence, deepfakes, and the Internet of Things (IoT) are being weaponized by these groups to enhance their operational capabilities. Detecting and preventing cyber-based terrorist activities presents a more complex challenge than traditional forms of terrorism due to the inherently global nature of the internet and the prevalent use of encryption technologies.

Furthermore, terrorist entities are exhibiting a growing tendency to collaborate with organized crime groups to achieve their objectives, with cyberspace serving as a particularly advantageous domain for these illicit partnerships. The Europol EU Terrorism Situation and Trend Report (TE-SAT) 2024 highlights the extensive use of social media platforms and encrypted communication channels by terrorist groups for disseminating propaganda, facilitating radicalization processes, and recruiting new members. The report specifically underscores the impact of global events, such as conflicts in the Middle East, on the mobilization of individuals through disinformation campaigns.[45] Concurrently, the Europol EU Serious and Organized Crime Threat Assessment 2025 (EU-SOCTA) identifies cyber threats as a critical instrument for organized crime, encompassing the spread of false information aimed at societal destabilization and the generation of funds to finance terrorist activities.[46] Notably, both the TE-SAT and EU-SOCTA reports establish a nexus between terrorists and organized criminal networks through their shared utilization of advanced technologies, overlapping operational networks and the common factor of online radicalization.[47]

---

[45] Europol (2024) European Union Terrorism Situation and Trend Report (EU TE-SAT). Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf [Accessed May 15, 2025].

[46] Europol (2025) EU Serious and Organised Crime Threat Assessment 2025 (EU-SOCTA). Available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf [Accessed May 15, 2025].

[47] When researching the phenomena of terrorism, organized crime, and the broader context of security threats within the European Union, two key Europol documents – the Terrorism Situation and Trend Report (TE-SAT) and the Serious and and Organised Crime Threat Assessment (EU-SOCTA) – stand out as exceptionally relevant and methodologically reliable sources. Their particular value stems from the fact that they are the result of intensive, multi-year analytical work by multidisciplinary teams of experts operating within Europol, who have access to the most comprehensive dataset (often including classified information that is not available to the public or other researchers) on security threats across the entire European Union.

In this analysis, we have chosen to investigate how terrorists and organized crime groups utilize cyberspace. This focus is driven by the increasing convergence of these two actor groups, both of whom extensively leverage the digital domain. By examining them together, we aim to gain a broader and more comprehensive understanding of the activities they undertake in cyberspace. Furthermore, it is important to highlight that the geographical scope of this research is predominantly centered on the European Union / European region, though it selectively draws upon extra-EU examples to enrich the investigation and discourse. As authors, our extensive involvement in and familiarity with developments in this area allow us to provide in-depth insights, including those gained through operational work on the topics under investigation. We believe these insights will be valuable for other researchers and future studies.

The central aim of our research is to analyze the ways in which these two increasingly interconnected groupings – terrorists and organized criminals, whose boundaries can often be blurred – leverage cyberspace for disinformation, radicalization, and recruitment. Through this investigation, we intend to address the following key research questions:

- How do terrorist and criminal groups leverage disinformation in cyberspace to facilitate radicalization and recruitment?
- What are the primary platforms and tools exploited by terrorist and criminal groups to disseminate propaganda and recruit new members online?
- What roles do artificial intelligence and deepfake technologies play in the proliferation of disinformation and terrorist and criminal group propaganda?

The Nexus of Disinformation, Radicalization and Recruitment

Disinformation, radicalization, and recruitment are interconnected processes that terrorist and criminal groups often use to expand their influence, attract new members, and destabilize society. Today, the internet and social media play a crucial role in these processes, enabling the rapid and anonymous spread of extremist narratives and the manipulation of vulnerable individuals.

Alexander Meleagrou-Hitchens, Audrey Alexander, and Nick Kaderbhai in their 2017 work extensively analyzed the impact of digital communications on the processes of radicalization and recruitment within extremist groups. A particular emphasis is placed on the role of the internet and social media in spreading ideologies and recruiting new members. Authors generally agree that while the internet significantly facilitates and catalyzes terrorist organizations and their networks, it is not

a standalone radicalizing agent. Despite varied analyses, there is a consensus that the virtual realm largely complements, rather than replaces, real-world interactions.[48]

In the same year, Paul Gill and his associates conducted a study of 223 convicted terrorists based in the United Kingdom, examining the extent and purpose of their internet use. The authors concluded that the internet serves as an important resource for information, communication and support for terrorists, particularly for those planning sophisticated attacks or who are part of larger networks. It is crucial to note that the internet is largely a facilitative tool that provides greater opportunities for violent radicalization and attack planning. Nevertheless, radicalization and attack planning are not solely dependent on the internet; a portion of these activities also take place in the offline world. Regarding internet usage, certain differences were observed that depend on the terrorists' needs and capabilities – those who require specific knowledge or communication with others are more likely to use the internet for that purpose. Online platforms offer new opportunities for offenders who are limited by their offline environment or the scope of their plans. Gill and his associates found significant differences in how terrorists use these platforms, depending on their targeting strategies, ideologies, network structures and their propensity for online learning and communication. A strong link was found between the selection of more difficult targets and the use of online learning. Similarly, technically complex attacks, such as those involving IEDs, were associated with more extensive online searching than simpler attacks. Lone actors, who lack a team's collective skills, also showed a greater need for online learning. Additionally, in the United Kingdom, extreme-right-wing offenders were more likely than those with terrorist ideologies exploiting religion to use online resources for learning and communication.[49] This paper provides a quantitative insight into the internet's role in terrorist activities and confirms that the internet is essential for the radicalization, learning and the recruitment of terrorists.

Ruslana Grosu and Vasile Bubuioc highlight how the internet and social media have become key tools for the spread of disinformation, propaganda and targeted recruitment by terrorist organizations such as Al-Qaeda and Daesh. Terrorists use the online space as a form of psychological warfare, combining elements of fear, ideological manipulation and appealing narratives to influence vulnerable groups, especially young people. Through anonymity, global reach, and a lack of regulation, social media enable the creation of virtual communities where potential recruits are attracted, screened, and molded in accordance with extremist ideology. Authors emphasizes that disinformation – intentionally distorted and emotionally charged

[48] Meleagrou-Hitchens, A., Alexander, A., & Kaderbhai, N. (2017) The impact of digital communications technology on radicalization and recruitment. International Affairs, Volume 93, Issue 5, pages 1233-1249. Available at: https://doi.org/10.1093/ia/iiy173 [Accessed May 17, 2025].

[49] Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017) Terrorist use of the Internet by the numbers: Quantifying behaviors, patterns, and processes. Criminology & Public Policy, Volume 16, Issue 1, pages 99-117. Available at: https://doi.org/10.1111/1745-9133.12249 [Accessed May 18, 2025].

messages – is a central tool in the radicalization process, as it fosters feelings of injustice, isolation, and a moral obligation to act. Recruitment increasingly occurs through a personalized approach, utilizing multimedia content – from music and video games to infantile animations – thereby subtly infiltrating radical ideology into the daily digital lives of young people. The key objective of these tactics is to create a sense of belonging and purpose in individuals experiencing an existential or identity crisis, enabling terrorist organizations to 'translate' disinformation into real action and recruitment.[50]

In the digital environment, disinformation plays a crucial role in the process of radicalization and recruitment because it erodes trust in traditional sources of information and encourages the adoption of alternative, extremist narratives. Joe Whittaker emphasizes how disinformation often acts as a bridge between moderate views and radical ideologies, especially when targeting vulnerable individuals already exposed to social frustrations or identity insecurity. Online platforms enable the rapid dissemination of such content, thereby facilitating the creation of 'echo chambers' where users increasingly consume content that confirms extreme beliefs, while simultaneously losing contact with alternative viewpoints. Thus, disinformation does not appear merely as a byproduct of extremism, but as an active tool in the recruitment process, particularly when skillfully integrated into appealing narratives and visual content.[51]

In the TE-SAT 2024 report, the growing interconnection between disinformation, radicalization and recruitment is highlighted, particularly in the context of religiously motivated or right-wing extremism. The report emphasizes that online spaces, especially social media and encrypted messaging platforms, have become critical environments for spreading extremist narratives and manipulating perceptions. Disinformation is systematically used to distort facts, fuel grievances and create a sense of crisis or injustice, which provides fertile ground for radicalization. Echo chambers and algorithm-driven content foster insular communities where extremist ideologies can flourish unchecked. Recruitment efforts are increasingly personalized, with actors targeting vulnerable individuals using tailored messages and misinformation.[52] Special attention should be paid to the recruitment of young people. As the report indicates, in 2023, young adults and minors were actively involved in planning attacks, producing terrorist propaganda and inciting violence. This active engagement of young individuals in terrorism and violent extremism represents a

[50] Grosu, R., & Bubuioc, V. (2018) The role of internet and social media in recruitment in certain Islamic terrorist organizations. Cases of Al Qaeda and Daesh. Central and Eastern European eDem and eGov Days, pages 179-188. Available at: DOI:10.24989/ocg.v325.15 [Accessed May 18, 2025].

[51] Whittaker, J. (2022) Online radicalization: What we know. European Commission, Radicalization Awareness Network. Available at: https://home-affairs.ec.europa.eu/system/files/2023-11/RAN-online-radicalisation_en.pdf [Accessed May 19, 2025].

[52] Europol (2024) European Union Terrorism Situation and Trend Report (pages 5-10).

general trend across the entire ideological spectrum and is a growing concern related to their potential exploitation by terrorist groups. In several investigations, some of those arrested were found to have been in online contact with each other, spending time on the same channels and messaging groups. Through these platforms, they accessed propaganda, training materials and other resources that could be used to plan and carry out an attack. Many of these self-radicalized individuals were not sponsored by any particular group but were instead embedded within virtual online communities of like-minded individuals who sought to take action in real life.[53]

In the EU-SOCTA 2025 report, the online domain is described as an "essential, omnipresent aspect of daily life," and its role in fostering serious and organized crime is highlighted, including the spread of disinformation that facilitates radicalization and recruitment. Criminal and extremist networks manipulate information online to create distrust, polarize societies and attract new recruits. The digital environment enables the rapid and large-scale dissemination of propaganda and falsehoods, thereby accelerating the radicalization cycle.[54] Disinformation campaigns are used as part of broader hybrid activities – ranging from the aftermath of the COVID-19 pandemic to the Russian war of aggression against Ukraine and the ongoing conflicts in the Middle East, as well as economic and political tensions (e.g., China, Iran, North Korea).[55] Furthermore, in terms of radicalization, a variety of criminal groups leverage digital platforms to normalize acts of extreme cruelty, extort victims, share child sexual abuse material and radicalize individuals into violent extremism.[56] Regarding recruitment, it is directed toward various segments of society, but for the purpose of this analysis, we place a special focus on young people. The report states that the criminal exploitation of young perpetrators has increasingly become a tactic used by criminal networks to avoid detection, capture, prosecution and punishment. Recruitment methods are evolving to include tailored language and online channels that align with youth culture. As these young recruits often lack knowledge of the broader criminal network and have reduced legal exposure, they serve as low-risk assets for criminal networks.[57]

Both reports emphasize how disinformation is used as a tool for radicalization and recruitment, especially of young people. TE-SAT 2024 highlights how propaganda messages and conspiracy theories are spread through online communities, utilizing visual content, music and short videos for faster emotional identification with the message. EU-SOCTA 2025 further connects hybrid threats and criminal networks that

[53] Ibid (page 8).
[54] Europol (2025) EU Serious and Organised Crime Threat Assessment 2025 (page 6).
[55] Ibid (page 14).
[56] Ibid (page 47).
[57] Ibid (page 23).

use disinformation to undermine democratic processes and create societal polarization.

Exploiting Digital Platforms: Tools and Tactics of Propaganda

Gonda Yumitro and associates emphasize that terrorists increasingly exploit digital platforms – especially mainstream social media like Facebook, Twitter, YouTube, Telegram, and encrypted forums – as vital tools and tactics of propaganda. They highlight how extremist groups misuse these channels to disseminate radical ideologies, recruit new members, indoctrinate followers, fundraise, coordinate logistics, and broadcast real-time updates and graphic content to maximize psychological impact and global reach. By leveraging the affordances of these platforms, terrorist organizations such as Daesh and Al-Qaeda have constructed powerful, visually compelling narratives that resonate with tech-savvy audiences and facilitate cyberterrorism, compelling governments to develop enhanced monitoring, counter-speech and technical solutions to thwart these digital threats.[58]

Moustafa Ayad analyzed around 450 social networks pages and accounts related to promotion of the Daesh terrorist organization and found that most of those accounts were run by young users, mostly minors and that content was in most cases tailored to radicalize young populations[59]. Online youth radicalization is still one of the biggest challenges for security services around the world. According to Adrian Shtuni, Daesh's digital operations in 2025 remain a key pillar of its strategy to maintain global influence, project power, and advance its ideological and operational goals. The organization effectively exploits social media platforms and encrypted messaging tools to disseminate propaganda, and to radicalize and recruit supporters, particularly targeting younger demographics who are both most active online and vulnerable to radicalization.[60] According to Shtuni, young individuals are active online but, in most cases, due to their age, are unknown to security and counter terrorism services.

Andrea Di Nicola argues that today's organized crime groups exploit digital platforms not only for operational purposes but also as powerful tools and tactics of propaganda. Through tailored content on social media, these groups shape narratives, normalize their activities, and recruit new members. They harness the blurred boundaries between online and offline spheres, orchestrating coordinated campaigns – often utilizing bots – to amplify influence, spread disinformation, and enhance their

[58] Yumitro, G., Febriani, R., Roziqin, A., & Indraningtyas, A. (2023) Bibliometric analysis of international publication trends on social media and terrorism by using the Scopus database. Frontiers in Communication. Volume 8. Available at: https://doi.org/10.3389/fcomm.2023.1140461 [Accessed May 21, 2025].

[59] Ayad, M., (2025) Teenage Terrorists and the Digital Ecosystem of the Daesh, CTC Sentinel, Combat Terrorist Center at West Point, Volume 18, Issue 2, Pages: 1-8

[60] Shtuni, A., (2025) The Deash in 2025: an Evolving Threat Facing a Waning Global Response, International Centre for Counter-Terrorism, Available at: https://icct.nl/publication/islamic-state-2025-evolving-threat-facing-waning-global-response, published 11 July 2025 [Accessed June 11, 2025].

public perception, effectively converting digital networks into recruitment and image-management ecosystems.[61]

Mariam Nouh, Jason R. C. Nurse, and Michael Goldsmith, in their research, thoroughly investigated how the Internet, and particularly online social networks, have fundamentally altered the methods by which terrorist and extremist groups exert influence and radicalize individuals. Their analysis revealed a distinct mode of operation: these groups initially expose a broad audience to extremist material on open online platforms. Following this initial exposure, they systematically migrate interested individuals to less public or more exclusive online platforms for more intensive and targeted radicalization.[62] Their study, which notably leveraged Twitter as a primary platform for analysis, provided crucial insights into this multi-stage process. Open platforms like Twitter serve as vital initial points of contact due to their wide reach and public accessibility, allowing extremist content to be disseminated broadly and organically to potential recruits. Once individuals show interest or engage with this content, they are then directed to more private, encrypted or niche online spaces.

Adam Badawy and Emilio Ferrara also utilized Twitter as their research platform, employing a dataset of over 1.9 million messages posted by approximately 25,000 Daesh members. Their research explores how Daesh makes use of social media to spread its propaganda and to recruit militants from the Arab world and across the globe. By distinguishing between violence-driven, theological, and sectarian content, their work traces the connection between online rhetoric and key events on the ground.[63] The study's findings are significant as they yield new important insights about how social media is used by radical militant groups to target the Arab-speaking world and reveal important patterns in their propaganda efforts.

TE-SAT 2024 details the sophisticated use of digital platforms by terrorist and extremist groups for propaganda purposes. These actors leverage a range of online tools to maximize reach and impact. Social media, encrypted messaging apps, and video-sharing platforms are used to disseminate ideological content, operational instructions, and calls to action. Propaganda is often multi-modal (text, video, memes) and tailored to specific audiences, increasing its effectiveness. Extremist groups exploit trending topics and mainstream platforms to insert their narratives into broader public discourse.[64] The use of digital platforms by terrorist and extremist groups for propaganda purposes was found in the case of two right-wing terrorist attacks foiled

[61] Di Nicola, A. (2022) towards digital organized crime and digital sociology of organized crime. Trends in Organized Crime. Volume 8. Available at: https://doi.org/10.1007/s12117-022-09457-y [Accessed May 22, 2025].

[62] Nouh, M., Nurse, J. R. C., & Goldsmith, M. (2019) Understanding the Radical Mind: Identifying Signals to Detect Extremist Content on Twitter. 17th IEEE International Conference on Intelligence and Security Informatics. Available at: https://doi.org/10.1109/ISI.2019.8823548 [Accessed May 21, 2025].

[63] Badawy, A., & Ferrara, E. (2017) The Rise of Jihadist Propaganda on Social Networks. Journal of Computational Social Science. Available at: https://doi.org/10.1007/s42001-018-0015-z [Accessed May 22, 2025].

[64] Europol (2024) European Union Terrorism Situation and Trend Report (pages 7-10).

in France and Luxembourg in 2023. It was determined that young right-wing terrorists and violent extremists are taking on a more active role as creators of propaganda, recruiters, and organizers of attacks, as well as engaging in active incitement.[65] During the same year, various propaganda activities by terrorist groups exploiting religion in Sweden, Denmark and the Netherlands were also recorded.[66]

The EU-SOCTA 2025 report underlines that the digital space is now the main ecosystem for many forms of organized crime, including the dissemination of propaganda. Criminal networks use social media, dark web forums and encrypted channels for propaganda, recruitment, and operational coordination. These platforms enable anonymity, rapid communication and global reach, making them ideal for spreading criminal and extremist messages.[67] Criminal groups, in contrast to terrorist organizations, tend to use digital platforms less for propaganda purposes. According to the report, these platforms and various digital tools are leveraged for a wide range of illegal activities. These activities include money laundering through blockchain technology, cyberattacks (such as disabling digital security measures on various systems to enable a subsequent physical break-in), and the dissemination of propaganda about their own activities, aimed at normalizing acts of extreme cruelty, as previously mentioned.

Both reports state that digital platforms are a key tool for terrorist propaganda and criminal activities. The use of End-to-End Encrypted (E2EE) communication applications, social media, the dark web, and specialized forums enables anonymous advertising of illegal services, recruitment, and the dissemination of ideologies. TE-SAT cites examples of minors actively participating in the creation and spread of online propaganda, exploiting social media to disseminate extremist content.

The Emerging Threat: AI, Deepfakes, and the Spread of Disinformation

In *AI Deception: A Survey of Examples, Risks, and Potential Solutions*, a group of authors highlight the growing threat of AI in the hands of malicious actors, including terrorists and criminal organizations. The authors detail how AI can be used to create convincing deepfake videos, generate targeted disinformation campaigns and manipulate public opinion. The article emphasizes that AI-driven deception is increasingly being leveraged to radicalize individuals, recruit new members, and destabilize societies.[68] The research is significant because it provides a comprehensive overview of the risks and outlines potential solutions, stressing the

[65] Ibid (page 33).

[66] Ibid (page 26).

[67] Europol (2025) EU Serious and Organised Crime Threat Assessment 2025 (page 18).

[68] Park, P. S., Goldstein, S., O'Gara, A., Chen, M., & Hendrycks, D. (2024) AI deception: A survey of examples, risks, and potential solutions. Patterns. Available at: https://doi.org/10.1016/j.patter.2024.100988 [Accessed May 27, 2025].

urgent need for robust detection tools and policy interventions to mitigate these threats.

Jacob Ware and Ella Busch explores how far-right extremist groups are adopting deepfake technology to incite political violence, undermine trust in democratic institutions, and recruit new members. The authors explain that deepfakes – synthetic media generated by AI – are used to create highly realistic but fake video content, which can be deployed to spread disinformation, manipulate narratives and radicalize vulnerable individuals.[69] The research is important because it identifies a new and evolving threat vector for extremism and calls for policy responses, public awareness and countermeasures to address the challenges posed by deepfakes.

Shlomit Wagman points to the dangers of AI development, stating that AI has potential "in developing unconventional weapons and cyber threats. The technology is increasingly used to identify and exploit security vulnerabilities in defense systems, corporate networks and critical infrastructure. By automating cyber reconnaissance and penetration testing, AI enables adversarial actors to execute highly adaptive, autonomous cyberattacks at speeds far beyond human capabilities. These attacks could potentially disable military communications, manipulate satellite systems or disrupt power grids, posing direct threats to national security. Beyond cyber threats, AI lowers barriers for the development of nuclear and bioweapons, automated hacking tools and AI-optimized malware, allowing hostile nations and terrorist groups to build unconventional weapons with minimal resources".[70]

TE-SAT 2024 identifies artificial intelligence and deepfake technology as emerging threats that significantly enhance the capabilities of extremist and terrorist actors. AI-driven tools can automate the creation and dissemination of propaganda, making it more difficult to detect and counter. Furthermore, deepfakes and synthetic media are used to fabricate events, impersonate individuals, and undermine trust in information sources. The increasing sophistication and accessibility of these technologies pose new challenges for law enforcement and counter-terrorism efforts.[71] Deepfake technology is being utilized by terrorists for spreading disinformation, creating propaganda and forging false identities. The technology's ability to manipulate real-time videos raises significant concerns that it could be exploited to trigger widespread social panic or to simulate terrorist attacks. For instance, right-wing extremists have already used AI-generated propaganda materials and deepfake

[69] Ware, J., & Busch, E. (2023) The Weaponization of Deepfakes: Digital Deception on the Far-Right. The International Centre for Counter-Terrorism (ICCT). Available at: https://icct.nl/publication/weaponization-deepfakes-digital-deception-far-right [Accessed May 28, 2025].

[70] Wagman, S. (2025) Weaponized AI: A New Era of Threats and How We Can Counter It. Harvard Kennedy School, Ash Center for Democratic Governance and Innovation. Available at: https://ash.harvard.edu/articles/weaponized-ai-a-new-era-of-threats/ [Accessed May 29, 2025].

[71] Europol (2024) European Union Terrorism Situation and Trend Report (pages 6-10).

content to disseminate racist or antisemitic messages. Furthermore, deepfake technology facilitates the creation of counterfeit identities and the management of automated bots for group communication.[72] This technology represents a growing threat as it can be leveraged to produce highly convincing false narratives and to destabilize society.

The EU-SOCTA 2025 report discusses how emerging technologies, particularly AI, accelerate the evolution of organized crime. AI and related technologies expand the speed, scale and sophistication of criminal operations, including the spread of disinformation and the creation of deepfakes. These innovations complicate detection, attribution and prevention efforts, thereby requiring new strategies and tools for law enforcement.[73]

“AI and other new technologies are fundamentally reshaping the serious and organized crime landscape in two main ways: as a catalyst for crime, and as a driver for criminal efficiency.”[74]

Furthermore, criminal networks are increasingly leveraging advanced, user-friendly AI systems, such as Large Language Models (LLMs) and Generative AI (GenAI), to facilitate a wide spectrum of crimes. These tools, which drastically lower the barriers to entry for digital crime, enable criminals to create sophisticated malware, target victims globally and produce realistic synthetic media (deepfakes) for fraud, extortion and identity theft. Easily accessible and not requiring specific technical skills, these tools amplify the threat of fraud, including the proliferation of child sexual abuse material (CSAM). Furthermore, the emergence of blockchain technology and cryptocurrencies has enabled criminals to efficiently laundering money and make payments, with their use expanding into traditional forms of crime like drug trafficking. New methods have also emerged for stealing cryptocurrencies and resources (known as cryptojacking).[75]

Artificial intelligence and deepfake technologies are dramatically changing the criminal landscape. EU-SOCTA 2025 reports that AI enables the automatic generation of disinformation, voice cloning, the creation of false identities, and sophisticated scams, while TE-SAT 2024 warns of the use of generative AI and LLMs for spreading racist and extremist content in the form of deepfakes. Furthermore, there is growing concern about the possibility of using deepfakes in real-time, for example, for terrorist purposes via livestreaming.

Response of European Union bodies

[72] Ibid (pages 6-10).

[73] Europol (2025) EU Serious and Organised Crime Threat Assessment 2025 (pages 6-21).

[74] Ibid (page 21).

[75] Ibid (page 21).

Before discussion, it should be noted that large internet companies recognized the vulnerabilities of their platforms and stand together with European Commission and other stakeholders to implement preventive measures, to avoid misuse of their platforms for radicalization and terrorist propaganda.

First step was made by European Commission in December 2015 when EC launched *EU Internet Forum* (EUIF) as a high level discussion forum on misuse of internet for terrorist purposes. According to official web page[76] of EUIF, main action of EUIF is to reduce accessibility of terrorist content online and to increase the volume of effective alternative narratives.

EUIF brings together EU Agencies and Institutions as well as big internet companies such as Amazon, Automattic, DailyMotion, Discord, Dropbox, Meta, MistralAI, Google, Internet Archive, Just Paste.it, Mega, Microsoft, Snap, Soundcloud, Telegram, Twitter, Twitch, Yubo, TikTok, Roblox and Zoom.

Main EUIF activities are discussions on implementation of the technical solutions for prevention of misuse of digital platforms for terrorist purposes.

Large internet companies also established an NGO called *Global Internet Forum to Counter Terrorism* (GIFCT) with the role of technical discussions on the prevention of exploiting digital platforms for terrorist purposes. Since 2017 and establishment of the GIFCT, companies have worked together to enhance their capacities and capabilities for identification of terrorist content on their platforms.

One of the results of discussions on EUIF was creation of *EU Internet Referral Unit* (EU IRU) in European Counter Terrorism Center (ECTC) of Europol. According to Europol[77], main task of EU IRU is to support competent EU authorities with strategic and operational analysis, to identify terrorist content online and to share information with relevant partners, to detect and request removal of internet content and to support referral procedures in close cooperation with the industry. Many EU Member States established Internet Referral Units in their respective Counter Terrorism Authorities. Role of national IRU is to identify terrorism and extremism related content from national point of view, to monitor radicalization online, to work on prevention of misuse of internet and digital platforms for terrorism purposes and to cooperate with EU IRU of Europol and other IRU units in Member States.

Regarding legal framework for addressing of the terrorist content in virtual space, most important legislation is *Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on Addressing Dissemination of Terrorist Content Online* (TCO Regulation). TCO Regulation obliges Hosting Service

[76] EU Internet Forum web: https://home-affairs.ec.europa.eu/networks/european-union-internet-forum_en [Accessed May 30, 2025].

[77] EU IRU web: https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru [Accessed May 30, 2025].

Providers (HSP's) to react on removal orders sent by the competent authority of the Member State and to remove terrorist content from their platform within a period of one hour.

One more important piece of EU legislation in this area is *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC* or so-called Digital Services Act (DSA). According to European Commission, DSA regulates online intermediaries and platforms such as marketplaces, social networks, content-sharing platforms, app stores, and online travel and accommodation platforms. Its main goal is to prevent illegal and harmful activities online and the spread of disinformation. It ensures user safety, protects fundamental rights, and creates a fair and open online platform environment[78]. The DSA introduces a range of measures, including transparency requirements for content moderation, risk assessments of algorithmic systems, mandatory mechanisms for user redress, and significant oversight provisions. It also empowers national regulators, known as Digital Services Coordinators, and the European Commission to monitor and enforce compliance. By focusing on systemic risks, the Act distinguishes itself from earlier piecemeal regulations and aims to create a sustainable and rights-oriented digital ecosystem[79].

The aforementioned actions and legal frameworks are only a part of efforts at the EU and international level for addressing of the issue of misuse of virtual and digital technologies for terrorist purposes, but represent readiness of the main internet platforms and companies as well as EU Agencies and Institutions to tackle this phenomenon.

Discussion and Conclusion

The analysis presented in this document underscores the complex and evolving role of cyberspace in the activities of terrorist and organized crime groups, with a particular focus on the European context. The following discussion addresses the central research questions:

1. How do terrorist and criminal groups leverage disinformation in cyberspace to facilitate radicalization and recruitment?

Disinformation in cyberspace has become a central tool for radicalization and recruitment by terrorist groups, while also representing a significant segment of the activities of criminal organizations. Online platforms enable the rapid and anonymous spread of extremist narratives, which are often emotionally charged and tailored to exploit vulnerabilities such as age, feelings of injustice, isolation or identity crises.

[78] European Commission, The Digital Services Act, https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en [Accessed August 23, 2025].
[79] Peter, H. (2025). The EU's Digital Services Act: A New Era of Platform Regulation.

Disinformation erodes trust in traditional sources of information and encourages the adoption of alternative, extremist worldviews and narratives. New forms of extremism raised during COVID-19 pandemic, such as Violent Anti-System Extremism (VASE) were fueled by disinformation and conspiracy theories. By distorting facts and fueling grievances, disinformation fosters a sense of crisis or injustice, which is essential for transforming moderate individuals into radicalized actors. The process is further amplified by the creation of online echo chambers, where users are exposed only to content that reinforces extremist beliefs, thereby accelerating the radicalization cycle. As noted earlier, disinformation is not merely a byproduct but an active instrument in the recruitment process, especially when integrated into compelling narratives and visual content.

2. What are the primary platforms and tools exploited by terrorist and criminal groups to disseminate propaganda and recruit new members online?

Terrorist and criminal groups exploit a wide array of digital platforms and tools to disseminate propaganda and recruit new members. Mainstream social media platforms such as Facebook, Twitter (now X), YouTube and Telegram are frequently used due to their global reach and ease of access. These platforms allow for the rapid dissemination of propaganda, coordination of activities, and the creation of virtual communities where potential recruits are identified, screened, and indoctrinated. They use end-to-end encrypted (E2EE) communication applications, specialized forums, AI, deepfakes, and IoT technologies as tools. On the other hand, large internet companies have developed resources for the identification and removal of terrorist and extremist content on their platforms. Encrypted messaging apps and forums are especially valuable for secure communication and the exchange of operational information. Some terrorist organizations and criminal groups have even established cooperation with individuals for the development of specialized communication apps for their activities. The research highlights the fact that extremist groups also use multimedia content – including music, video games, and animations – to subtly infiltrate radical ideologies into the daily digital lives of young people. The anonymity, global reach, and lack of regulation in these digital environments make them particularly advantageous for terrorist activities.

3. What roles do artificial intelligence and deepfake technologies play in the proliferation of disinformation and terrorist and criminal groups propaganda?

Artificial intelligence and deepfake technologies are increasingly being weaponized by terrorist and criminal groups to enhance the effectiveness of disinformation and propaganda. These technologies enable the creation of highly realistic fake images, audio and videos, which can be used to impersonate public figures, fabricate events and manipulate public perception. AI-driven tools can automate the production and dissemination of propaganda, allowing for large-scale

and targeted campaigns that are difficult to detect and counter. Deepfakes, in particular, pose a significant threat as they can be used to spread false narratives, incite violence and undermine trust in institutions. Our findings emphasize that the increasing sophistication of these technologies presents a grave challenge for law enforcement and policymakers, necessitating advanced detection methods and robust regulatory frameworks.

In conclusion we need to underline that the convergence of disinformation, radicalization, and recruitment in cyberspace has become a defining feature of contemporary terrorism and organized crime, especially within the European Union. Disinformation is not only a byproduct, but a deliberate and strategic tool used to manipulate public opinion, foster radicalization, and recruit new members. Terrorist and criminal groups exploit the affordances of mainstream and encrypted digital platforms to disseminate propaganda, coordinate activities, and create echo chambers that reinforce extremist ideologies. The advent of AI and deepfake technologies has further amplified these threats, enabling the rapid and large-scale proliferation of sophisticated disinformation and propaganda.

Addressing these challenges requires a multi-faceted approach that combines technological solutions, robust regulatory frameworks, international cooperation and enhanced digital literacy. By understanding the tactics and tools employed by malicious actors in cyberspace, policymakers and law enforcement agencies can develop more effective strategies to counter the evolving threats posed by disinformation, radicalization, and recruitment in the digital age.

CHAPTER 4

TERROR-AI-SM THE FUTURE OF ARTIFICIAL INTELLIGENCE IN THE HANDS OF TERRORISTS

Dr. Aleksander Olech

Introduction

Terrorism remains one of the major challenges to international security. The past decade has witnessed a rapid convergence of two forces with profound implications for global stability: the accelerating capabilities of artificial intelligence and the persistent, adaptive threat of terrorism. What was once the realm of science fiction — autonomous machines making battlefield decisions, synthetic media manipulating public opinion — is now technically feasible and increasingly accessible to non-state actors. This convergence is already reshaping the threat landscape, compelling governments and international institutions to reconsider and adapt their counterterrorism frameworks in order to address the realities of an era where terrorism and cutting-edge technology are inextricably linked.

Artificial Intelligence (AI) is an interdisciplinary domain typically considered a subset of computer science that focuses on models and systems performing functions commonly linked to human intelligence, including reasoning and learning. It has become one of the most groundbreaking achievements of the past decade, facilitating speech recognition, language translation, data analysis and autonomous decision-making. Primarily founded on machine learning methodologies that assimilate extensive datasets to enhance pattern recognition and forecasting, AI's applications now encompass medical diagnostics, autonomous vehicles, fraud detection, and real-time interpretation, all propelled by increasing computational power, abundant digital data, and open-source frameworks that expedite development timelines and reduce expenses. Generative AI represents a significant advancement capable of producing text, images, audio, and other synthetic data based on basic prompts. Its ability to replicate intricate human behaviors and generate customized outputs enhances commercial prospects — from media production to design — and security applications, aiding in areas such as intelligence analysis and counter-terrorism. However, it also prompts urgent concerns regarding bias, privacy, intellectual property rights, and the necessity for stringent governance to ensure the technology aligns with societal interests[80].

[80] C. Anthony Pfaff, "Introduction: Terrorism and Artificial Intelligence", in *The Weaponization of AI: The Next Stage of Terrorism and Warfare*, ed. C. Anthony Pfaff (Centre of Excellence Defence Against Terrorism, 2025), 8. "Violent Extremists' Use of Generative Artificial Intelligence", First Responder Toolbox, Joint Counterterrorism Assessment Team (NCTC, DHS, FBI), May 6 2024, accessed: June 01, 2025,

Terrorism is the unlawful use or threatened use of force or violence against individuals or property with the intent to instill fear, exert pressure on governments or societies, or gain political, religious, or ideological objectives[81]. It remains the foremost asymmetric threat to global security: agile networks exploit porous borders, conflict zones and weak governance to recruit, finance, and carry out attacks, increasingly using commercial and military technologies — including cyber tools and other emerging "disruptive" capabilities — to magnify their reach and lethality. Historically associated with bombings, kidnappings, mass shootings, or suicide attacks, terrorism has evolved alongside technological progress[82]. Today, terrorists are increasingly turning to advanced tools such as artificial intelligence, which can be exploited for propaganda, cyberattacks, and physical assaults using autonomous combat systems, opening new dimensions of operational capability[83].

At first glance, terrorism and Artificial Intelligence may appear to be completely disparate phenomena. Terrorism is generally linked to traditional assaults executed with rudimentary, 'low-tech' techniques such as improvised explosive devices, small arms, or hijackings, frequently conducted by non-state actors in conflict-affected regions. Artificial intelligence, on the other hand, represents technological advancement — an intricate and swiftly developing domain that is transforming contemporary society, encompassing areas such as healthcare, finance, transportation and security systems.

As AI systems become more accessible, autonomous and proficient, the potential for their exploitation by terrorist organizations appears to be a growing concern. The convergence of these ostensibly disparate domains presents intricate ethical, strategic and technological challenges. It contests current security paradigms and prompts a pressing inquiry: what will happen when future technologies are wielded by individuals with malicious intent? This question highlights the significance of continuous research in this domain, especially regarding the future of Artificial Intelligence in the hands of terrorists – 'Terror-AI-sm' –emphasizeing the need to understand how emerging technologies can be weaponized and how global systems can address these evolving threats.

One of the first examples of the misuse of AI-like technology took place in Iraq and Syria between 2016 and 2018, when Daesh programmed basic drone flight paths to attack enemy fighters and drop grenades.[84] These were crude systems, but they foreshadowed the future use of such capabilities in terrorist activities. The same period

https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/151s_First_Responders_Toolbox-Violent_Extremists_Use_of_Generative_Artificial_Intelligence.pdf.
Vladimir Voronkov and Antonia Marie De Meo, "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes", 2021, accessed: June 01, 2025, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.
Clarisa Nelu, "Exploitation of Generative AI by Terrorist Groups", International Centre for Counter-Terrorism, June 10, 2024, accessed: June 01, 2025, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[81] Allied Joint Doctrine, Edition F, Version 1, NATO Standardization Office, December 2022, accessed: June 04, 2025, https://www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_%281%29_2437.pdf.

[82] Brundage, Miles et al., "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", arXiv:1802.07228, February 2018, 26–27, accessed: June 04, 2025, https://arxiv.org/pdf/1802.07228.

[83] NATO's policy guidelines on counter-terrorism, official text, July 10, 2024, accessed: June 04, 2025, https://www.nato.int/cps/fr/natohq/official_texts_228154.htm.

[84] Kerry Chávez, Dr. Ori Swed, "Off the Shelf: The Violent Non-state Actor Drone Threat", Air University, 2019, accessed: June 04, 2025, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-34_Issue-3/F-Chavez_Swed.pdf..

also brought bots, flooding Twitter with recruitment propaganda, marking an early form of large-scale algorithmic manipulation[85].

Artificial Intelligence has quickly become a key tool used by terrorists. Its ability to improve communication, planning, targeting and disrupting systems makes it a transformative force in asymmetric warfare. Although terrorism has always evolved alongside technological developments, AI could represent a qualitative leap, transferring power from state structures to non-state actors and even individuals on an unprecedented scale[86].

Given the clandestine nature of terrorist operations and the high level of confidentiality around intelligence concerning their capabilities, the scope of this study is necessarily constrained to open-source information, verified media reports, academic publications, and official institutional statements. No classified, operationally sensitive, or unverifiable data has been used. This limitation inevitably restricts the level of technical detail regarding specific tools, networks, and operational procedures employed by terrorist organizations, particularly in the context of AI integration. As a result, the analysis focuses on documented cases, credible threat assessments, and observable trends, acknowledging that the actual scale, sophistication, and innovation of the use of AI by terrorists may exceed what is publicly available.

The author gratefully acknowledges the invaluable contributions of experts and practitioners whose insights, guidance, and critical perspectives have significantly enriched the quality and depth of this study[87].

Contemporary Threat Landscape & Policy Context

Artificial-intelligence systems — ranging from large language models to autonomous robotics — are contributing to rapid advances in automation, analysis and creative production, which can, however, also be exploited by violent extremists. Readily available generators such as GPT can draft polished manifestos, social-media posts, or different language propaganda, while AI-driven chatbots and recommendation engines can scrape profiles, tailor radicalizing messages, and flood feeds with convincing disinformation that is harder for outsiders to debunk or trace. By reducing costs, expanding reach, and personalizing delivery, these tools amplify extremist recruitment and shield it from detection.

The continuous increase in the number of new online services and the decline in content moderation have significantly expanded the volume of propaganda. The use of generative AI and emerging technologies for the creation and dissemination of propaganda and hate speech has attained unprecedented levels. A sustained fascination with weaponry and explosives resulted in several incidents, alongside a growing prevalence of 3D-printed firearms[88].

---

[85] J. M. Berger, Jonathon Morgan, "The ISIS Twitter Census", Brookings Institution, 2015, accessed: June 04, 2025, https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf..

[86] Melissa De Witte, "The Ethics of Autonomous Weapons", Stanford University, May 21, 2019, accessed: June 04, 2025, https://news.stanford.edu/stories/2019/05/ethics-autonomous-weapons..

[87] The author expresses sincere gratitude to Dr. Sarah Lohmann, Dr. Heather S. Gregg, and Dr. Damian Szlachter for their valuable input and guidance, as well as to the Defence24.com team — A. Wojciechowska, J. Smoleń, K. Kremiec, M. Grochalska, and N. Matiaszczyk — for their research support. The contributions of other professionals, whose names remain undisclosed due to the sensitive nature of their roles, were also essential in shaping this work.

[88] European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT), Publications Office of the European Union, Luxembourg, 2025, accessed: August 01, 2025, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf.

Terrorist organizations have traditionally relied on inexpensive, low-tech methods such as improvised explosives, knives, or vehicle attacks to spread fear and cause harm. However, the growing accessibility and power of artificial intelligence mark a turning point. AI is not only a powerful and transformative tool, but also one that is increasingly available to non-state actors and difficult to regulate effectively. This makes it particularly attractive to terrorist groups looking for new ways to operate and exert influence. As highlighted in the UNCCT Annual Report 2020:

> "this initiative aims to explore the risk-benefit duality of this technology, to inform Member States, industry and academia on the potential of the malicious use of AI by terrorist groups and individuals."[89]

This statement emphasizes that the threat is no longer hypothetical.

Extremist actors are likely to exploit AI, raising urgent questions about how, when, and to what extent it will be weaponized in future acts of terrorism.

In response to these growing threats, international regulatory bodies have begun to take action. In December 2024, the OSCE convened a global summit in Rome focused on the misuse of Artificial Intelligence by terrorist organizations. Lawmakers and experts discussed regulatory models, data governance, and defensive mechanisms. The summit called for the implementation of AI-specific counterterrorism protocols, including early detection systems for AI-generated propaganda and biometric surveillance of networks planning attacks with AI tools[90]. However, the implementation of these measures still lags behind the scale and speed of the threat. This gap highlights the urgent need for deeper international cooperation, coordinated regulatory frameworks, and the sharing of technological capabilities to effectively counter the evolving misuse of AI by terrorist actors.

The growing importance of artificial intelligence in terrorism reflects a broader transformation in the nature of modern conflict and operations across multiple domains. Where armies or explosives were once required, today even a single image uploaded to a free social media platform can have destabilizing effects. As generative AI models continue to evolve, and real-time control over drones, vehicles, and deepfakes becomes more accessible, the barriers to conducting large-scale terrorist operations are steadily decreasing. Strategic, legal, and ethical frameworks to respond to these developments remain a major challenge for security policymakers at local, regional, and global levels, particularly as militaries themselves are investing in AI for defense purposes[91].

It is therefore essential to constantly monitor and reassess the evolving capabilities of terrorist actors to stay ahead of emerging threats. In this regard, scientific research exploring the intersection of new technologies, such as AI, and global security challenges, including terrorism, is vital. So too is the role of international alliances and cooperation, including NATO and its specialized centers such as the NATO Centre of Excellence Defence Against Terrorism (COE-DAT). In such a rapidly

---

[89] UNCCT Annual Report 2020, United Nations Counter-Terrorism Centre (UNCCT), New York: United Nations Office of Counter-Terrorism, 2021, 156.

[90] Fourth Parliamentary Policy Dialogue on countering the use of artificial intelligence and new technologies for terrorist purposes, Rome Summit Report, December 05, 2024, accessed: July 01, 2025, https://www.oscepa.org/en/documents/ad-hoc-committees-and-working-groups/ad-hoc-committee-on-countering-terrorism/5183-fourth-parliamentary-policy-dialogue-outcome-document-5-december-2024/file.

[91] Aleksander Olech, Alan Lis, "Technology and terrorism: Artificial Intelligence in the time of contemporary terrorist threats", Institute of New Europe, Warsaw, 2021.

shifting landscape, awareness and knowledge of these threats are essential for building effective, long-term resilience.

Terrorists and AI development

Rapid technological advances are creating new opportunities for terrorist organizations to achieve their goals. One of them is the use of Artificial Intelligence. At present, the use of these solutions is primarily based on disinformation operations, spreading propaganda, increasing recruitment opportunities, and obtaining funding. These activities are common, regardless of the profile of the organization. AI is used by terrorist groups exploiting religion, such as the Daesh, its predecessor Al-Qaeda, the neo-Nazi group The Base,[92] and other far-right groups. Overall, the use of the state-of-the-art technologies, including AI, cannot be attributed to the single ideology of any selected terrorist group.

Terrorist and extremist groups are increasingly exploiting generative AI technologies for propaganda, recruitment, and operational guidance. In early 2023, pro-al-Qaeda networks released AI-generated posters and videos supporting the struggle in Gaza, targeting international audiences with multilingual content[93]. Later that year, Daesh and I State Khorasan Province (ISKP) shared encrypted bulletins and guides on how to use AI tools like ChatGPT for propaganda, reconnaissance prompts, and secure communication[94]. Simultaneously, neo-Nazi and white supremacist groups in the West have begun training or fine-tuning language models to produce hate speech, bomb-making manuals, and AI-generated extremist imagery[95]. In the UK, authorities documented a case in which an individual was reportedly radicalized through repeated interaction with an AI-based chatbot, highlighting how extremist actors could repurpose these tools as "virtual recruiters"[96].

A 2025 UN-backed analysis warned that terrorist groups may eventually use AI to weaponize autonomous systems, such as self-driving cars, as tools for remote, high-casualty attacks[97]. In the mid-2010s, groups such as Daesh were among the first users of digital tools, exploiting social media algorithms to radicalize their followers and utilizing commercial drones to drop Improvised Explosive Devices (IEDs)[98]. Although they were not based on AI technology, they revealed their readiness to use

[92] Ben Makuch, "How terrorist groups are leveraging AI to recruit and finance their operations", theguardian.com (website), accessed: July 26, 2025, https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence.

[93] "Early terrorist experimentation with generative artificial intelligence services": *pro-al-Qaeda use of AI-generated posters and imagery*, Tech Against Terrorism, accessed: August 06, 2025, https://techagainstterrorism.org/hubfs/Tech%20Against%20Terrorism%20Briefing%20-%20Early%20terrorist%20experimentation%20with%20generative%20artificial%20intelligence%20services.pdf

[94] "Here's how violent extremists are exploiting generative AI tools", Wired (website), accessed: August 06, 2025, https://www.wired.com/story/generative-ai-terrorism-content.
"Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts", The Soufan Center, accessed: August 06, 2025, https://thesoufancenter.org/intelbrief-2024-october-3/.

[95] "Neo-Nazis are all-in on AI", Wired (website), accessed: August 06, 2025, https://www.wired.com/story/neo-nazis-are-all-in-on-ai.

[96] Jonathan Hall KC, "Terrorists could exploit AI chatbots to spread hate and hatch plots, terrorism tsar warns", The Scottish Sun (website), accessed: August 06, 2025, https://www.thescottishsun.co.uk/news/15086176/terrorist-bot-plot-tsar-chatbot-ai-artificial-intelligence.

[97] "Terrorists could turn driverless cars into slaughterbots, UN warns", The Times (website), accessed: August 06, 2025, https://www.thetimes.com/uk/technology-uk/article/terrorists-could-turn-driverless-cars-into-slaughterbots-un-warns-t7wzx977d.

[98] Joby Warrick, "Use of weaponized drones by ISIS spurs terrorism fears", The Washington Post (website), February 21, 2017, accessed: July 14, 2025, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.

existing technologies for terrorist purposes[99]. At the time, many experts believed that AI would remain out of reach due to its high cost and complexity. This assumption has proven to be wrong[100].

Currently, extremist groups are utilizing generative AI tools to produce deepfake propaganda, translate radical content into various languages, and automatically generate bomb-making instructions or violent manifestos. A 2024 report by the International Centre for Counter-Terrorism indicates that terrorist organizations are utilizing AI-generated content to enhance the dissemination, targeting, and legitimacy of their communications, especially through personalized and localized recruitment materials[101]. The trajectory indicates that AI is no longer a remote threat, but a swiftly advancing instrument already being weaponized in the information sphere.

A concise discussion of additive manufacturing appears later in this chapter, adjacent to the analysis of Unmanned Aerial Vehicles (UAVs), to consolidate physical and kinetic threats in one place.

Spreading disinformation and propaganda using artificial intelligence

Disinformation remains one of the key tools used by terrorist organizations and extremist groups, enabling them to shape narratives, undermine the authority of institutions, and influence public opinion at home and abroad. In recent years, its effectiveness has increased significantly thanks to the use of new technologies, including AI-based tools[102]. AI enables the rapid creation and modification of propaganda content, including video, audio, and graphic materials that are difficult to distinguish from authentic ones. This facilitates the conduct of influence campaigns on a global scale, while minimizing the risk of identifying the source of the message.

The greatest threat posed by the use of artificial intelligence in disinformation is the ability to instantly create and mass distribute content, while making it difficult to identify its source[103]. A single user with a powerful graphics processor and an open-source AI model can now generate realistic fake videos, simulate the voices of famous people, or automate large-scale phishing campaigns. These capabilities are already a reality and have been demonstrated repeatedly in disinformation campaigns and cyberattack simulations.

AI also enables the rapid preparation of propaganda content in multiple formats and languages. Among others, text chatbots (e.g., ChatGPT, Bing Chat, Google Gemini), image and video generators (Midjourney, DALL-E, Stable Diffusion), and voice generators (e.g., Microsoft VALL-E) are used[104]. When combined with text-to-speech tools, this makes it possible to create audio-visual materials that are difficult to

[99] Charlie Winter, "Documenting the Virtual 'Caliphate'.", Quilliam Foundation, October 2015, accessed: July 14, 2025, https://core.ac.uk/download/pdf/30670971.pdf.
[100] P.W. Singer & Emerson T. Brooking, "LikeWar: The Weaponization of Social Media." (Houghton Mifflin Harcourt, June 2019, accessed: July 14, 2025, https://www.researchgate.net/publication/335149861_Like_War_-_The_Weaponization_of_Social_Media_by_P_W_Singer_and_Emerson_T_Brooking.
[101] Clarisa Nelu, "Exploitation of Generative AI by Terrorist Groups", ICCT, June 10, 2024, accessed: June 19, 2025, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.
[102] Renske van der Veer, "Terrorism in the Age of Technology | Strategic Monitor 2019-2020," www.clingendael.org, 2019, accessed: August 4, 2025, https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology/.
[103] Siegel Michael, Zeijlemaker Sander, Baxi Vidit, Raajah Sharavanan, "Rethinking the Cybersecurity Arms Race", MIT Sloan, Massachusetts Institute of Technology, April 10, 2025, accessed: August 4, 2025, https://cams.mit.edu/wp-content/uploads/Safe-CAMS-MIT-Article-Final-4-7-2025-Working-Paper.pdf.
[104] Clarisa Neru, "Exploitation of Generative AI by Terrorist Groups", accessed: July 26, 2025, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

distinguish from authentic ones[105], which can be precisely tailored to selected audiences and distributed on a global scale. Today, automated systems are capable of writing, translating, and disseminating radical content much faster than any team of humans[106].

Contemporary extremist groups and terrorist organizations are adapting AI technologies for propaganda, recruitment, and disinformation purposes[107]. Platforms such as Telegram and Gab publish deepfakes[108] depicting fabricated sermons by imams or clerics who have never actually delivered them [109]. In Q3 2024, Facebook took action against 14.9 million pieces of terrorist content — almost twice as many as in the previous quarter[110].

During the war in Gaza, pro-Palestinian online networks and accounts linked to H supporters used generative AI to create fake images of wounded children and satirical visuals of IDF soldiers in diapers (#IsraeliDiaperForce), aiming to undermine the authority of the Israeli army and ridicule their opponent[111]. The Daesh used AI[112] to generate bomb-making instructions using everyday items, create propaganda videos called 'News Harvest', and publish video bulletins read by virtual avatars[113]. In 2024, following the attack on Crocus City Hall in Moscow, ISKP released a video styled as a television news report, featuring AI-generated presenters[114].

In addition to armed conflicts, AI is also used in the context of terrorist attacks in Western Europe. After the attacks in Paris and Nice[115] manipulated images and videos appeared on social media, allegedly documenting further attacks or depicting the perpetrators in staged situations[116]. Such content, enriched with extremist narratives, can quickly cause social panic, increase the sense of threat, and reinforce the propaganda message coming from the organizations responsible for the attacks or their sympathizers.

Yet another important element concerns deepfakes that are synthetic media created using AI and deep learning to manipulate real data and produce false images or videos. This technology can be used maliciously, for example, by generating fake videos of politicians or celebrities to spread panic or discredit them. While detecting

---

[105] Vladimir Voronkov and Antonia Marie De Meo, Algorithms And Terrorism: The Malicious Use Of Artificial Intelligence For Terrorist Purposes, 2021, accessed: June 01, 2025, https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf

[106] The Guardian, op. cit.

[107]The Guardian. (2025). *AI Propaganda and Extremism,* https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence, accessed: August 04, 2025

[108] Vladimir Voronkov and Antonia Marie De Meo, "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes", 2021, accessed: June 01, 2025, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

[109] "Synthetic Media in Far-Right Messaging", EU DisinfoLab. (2025), accessed: August 04, 2025, https://www.disinfo.eu/disinfo-update-24-06-2025.

[110] "Actioned terrorism content items on Facebook worldwide from 4th quarter 2017 to 3rd quarter 2024" Statista, 2024, accessed: August 04, 2025, https://www.statista.com/statistics/1013864/facebook-terrorist-propaganda-removal-quarter/.

[111] Ibidem.

[112] Ben Makuch, "How terrorist groups are leveraging AI to recruit and finance their operations", theguardian.com (website), accessed: July 26, 2025, https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence.

[113] "Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts", The Soufan Center, accessed: July 27, 2025, https://thesoufancenter.org/intelbrief-2024-october-3/.

[114] Ibidem.

[115] "Attack in Nice: Photos of fake victims and fake suspects flood networks", FRANCE 24 Observers (2016), accessed: August 12, 2025, https://observers.france24.com/en/20160715-attack-nice-fake-victims-suspects-social-networks.

[116] Vladimir Voronkov and Antonia Marie De Meo, "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes", 2021, accessed: June 01, 2025, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

deepfakes is difficult, certain clues can help, such as unnatural facial movements, mismatched lip-syncing, odd blinking patterns, and errors in skin texture, lighting, or blurry backgrounds[117]. As AI advances, the line between real and fake may blur, making it harder for people to tell what is true.

This technology makes it possible, among other things, to impersonate well-known individuals or media institutions. Daesh has used this type of tool, which, as shown in a report by the Institute for Strategic Dialogue, prepared a media campaign based on fabricated video materials. Eight recordings were made —in different languages — styled to resemble material from well-known news stations such as CNN and Al Jazeera. One of the videos referred to the tragic attack on Crocus City Hall in Moscow in March 2024. Daesh claimed responsibility for the attack, and the fabricated material was intended to undermine the official narrative of the Russian authorities, who were trying to blame Ukraine[118].

Memetic warfare is playing an increasingly important role in the propaganda activities of terrorist organizations, with social media platforms such as TikTok, Instagram, and X becoming battlefields where memes in the form of images and short videos are the main weapons[119]. Generative AI makes it possible to flood this space with large amounts of consistent, visually appealing content that, thanks to recommendation algorithms, can quickly reach millions of recipients.

Memetic warfare conducted in this way is part of a broader, emerging concept known as AI struggle, in which terrorist organizations use artificial intelligence tools for propaganda purposes. Starting in 2023, both Al-Qaeda and Daesh began using audio deepfakes to imitate the voices of selected well-known figures. Propaganda videos featured popular characters from cartoons and TV series, such as SpongeBob and Rick and Morty, as well as major YouTubers, such as PewDiePie and MrBeast, singing religious battle songs, often reaching hundreds of thousands of views[120].

This content was deliberately targeted at the youngest audience, cleverly smuggling extremist messages under the guise of mainstream culture. It is worth mentioning that these films appeared on the wave of popularity of similar humorous materials, depicting, for example, US presidents talking while playing games such as Minecraft or CS:GO.

This fact demonstrates not only terrorist groups' high level of awareness of current Western trends, but also their ability to exploit Western pop culture for their own propaganda purposes — a process that could further facilitate and intensify the development of artificial intelligence.

AI materials are used not only to ridicule the enemy, but also to escalate social tensions and inspire supporters to take action. Their effectiveness is particularly high

---

[117] András József Uveges, "Terrorist Use of Artificial Intelligence-Driven Social Media", in *The Weaponization of AI: The Next Stage of Terrorism and Warfare*, ed. C. Anthony Pfaff, (Centre of Excellence Defence Against Terrorism, 2025), 46–47.

[118] Daniel L. Byman, Chongyang Gao, Chris Meserole, and V.S. Subrahmanian, "Deepfakes and International Conflict", The Brookings Institution, 1-4.
David Gilbert, "ISIS Created Fake CNN and Al Jazeera Broadcasts", Wired (website), accessed: August 06, 2025, https://www.wired.com/story/isis-created-fake-cnn-and-al-jazeera-broadcasts/.

[119] Sam Stockwell, "Propaganda by Meme," Centre for Emerging Technology and Security, 2024, accessed: August 06, 2025, https://cetas.turing.ac.uk/publications/propaganda-meme.

[120] Daniel Siegel, "AI Jihad: Deciphering Hamas, Al-Qaeda and Islamic State's Generative AI Digital Arsenal", GNET, February 19, 2024, accessed: June 14, 2025, https://gnet-research.org/2024/02/19/ai-jihad-deciphering-hamas-al-qaeda-and-islamic-states-generative-ai-digital-arsenal/.

in crisis situations, when recipients are looking for simple and quick explanations and the possibilities for verifying information are limited[121]. In such conditions, AI becomes a tool for influencing social reactions in real time, which can have a direct impact on public safety and decision-making process.

The development of generative technologies has significantly increased the pace and scale of disinformation campaigns conducted by non-state actors, including terrorist groups[122]. The ability to quickly create personalized, multilingual content and distribute it on a massive scale allows terrorist organizations to more effectively influence various audiences, both at the local and international levels. As a result, disinformation becomes not only an element of propaganda, but also a tool for destabilization and psychological pressure. Effective countermeasures require a combination of technological, intelligence, and legislative measures to limit the enemy's ability to use the information space as a battlefield.

The use of AI chatbots in terrorist recruitment

The development of artificial intelligence has enabled terrorist organizations to implement new forms of recruiting supporters. One of the most rapidly developing methods is interactive recruitment using chatbots, which can conduct conversations in a manner that is almost indistinguishable from that of a human being. This allows the process to be carried out around the clock, regardless of location, leaving recruiters anonymous and less vulnerable to detection. Combined with the ability to analyze behavior and personalize messages, this technology becomes an effective tool for psychological influence.

In the recruitment process, AI often acts as a bot that initiates a conversation with a potential candidate. The bot asks and answers basic questions, establishes contact, and tries to build initial trust. At a later stage, a human may join the conversation, taking the initiative and conducting a more in-depth interaction. The use of Large Language Models (LLMs), such as ChatGPT, makes it possible to create a conversation experience resembling contact with a real person, which increases terrorists' ability to build an emotional relationship with the recipient. Intensive interactions make it possible to reach so-called ‘lone wolves’ — people who are socially isolated and more susceptible to radicalization[123].

Recruitment chatbots provide advantages over traditional forms of contact. They are available 24 hours a day, can conduct hundreds of conversations simultaneously, and operate without geographical restrictions. They also minimize the risk for recruiters, who do not have to meet candidates in person. With the development of artificial intelligence capabilities in recognizing behavioral patterns and adapting communication, bots can dynamically change the tone, content, and form of conversation, increasing the effectiveness of recruitment[124].

This technology is no longer a hypothetical threat. Platforms such as Character.ai enable the creation of personalized chatbots, which were used for

[121] Daniel Siegel, “AI Jihad: Deciphering Hamas, Al-Qaeda and Islamic State’s Generative AI Digital Arsenal”, GNET, February 19, 2024, accessed: June 14, 2025, https://gnet-research.org/2024/02/19/ai-jihad-deciphering-hamas-al-qaeda-and-islamic-states-generative-ai-digital-arsenal/.

[122] “Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts”, The Soufan Center, accessed: August 08, 2025, https://thesoufancenter.org/intelbrief-2024-october-3/.

[123] Clarisa Neru, “Exploitation of Generative AI by Terrorist Groups”, accessed: July 26, 2025, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[124] James Paterson, “How Extremists Are Manipulating AI Chatbots” Lowy Institute,” Lowyinstitute.org, 2025, accessed: July 26, 2025, https://www.lowyinstitute.org/the-interpreter/how-extremists-are-manipulating-ai-chatbots.

recruitment purposes in 2024[125]. Jonathan Hall KC, an independent reviewer of counterterrorism legislation in the UK, pointed to cases of bots praising the activities of the Daesh, declaring "total dedication and devotion" to the organization, and impersonating its leaders. Such tools may in the future be used not only to recruit young men affected by loneliness[126], but also to identify and recruit individuals holding positions in state institutions who could sabotage counterterrorism efforts or facilitate attacks.

In addition to advanced chatbots, there are also simple bots that have been operating on the Internet for years, promoting extremist content. Their activities include automated posting, liking, commenting, and sharing. They often act as moderators in groups on platforms such as Telegram, shaping the narrative and strengthening the sense of community among recipients. According to research, they are a permanent feature of the religious internet ecosystem, sustaining the activity and cohesion of online communities[127].

Artificial intelligence can facilitate and accelerate the radicalization process. Chatbots, combining personalized messaging with unlimited reach and low risk for operators, may become one of the main recruitment tools for terrorist organizations in the future[128]. Combined with simple bots supporting online propaganda, they create an ecosystem of digital radicalization tools operating on an unprecedented scale.

New and Supplementary Applications of AI in Terrorism

While the most visible uses of artificial intelligence by terrorist organizations involve propaganda, recruitment, and cyber operations, the potential for AI misuse extends far beyond these domains. Several new applications — often functioning on the fringes of existing counterterrorism discourse — demonstrate how AI can reinforce operational resilience, expand attack vectors, and enhance the strategic flexibility of violent non-state actors. The following section discusses four supplementary areas where AI technologies could be integrated into terrorist activities: financial innovation, cyber-enabled disruption, autonomous weapons systems, and advanced language models for operational planning.

Terrorist organizations are increasingly using artificial intelligence to diversify their sources of funding, combining it with cryptocurrency technologies. Using deepfakes, they can bypass 'Know Your Customer' (KYC) verification procedures, which require the account holder to be present during a live video call, enabling them to set up fake accounts and facilitating the transfer of funds for operational purposes. AI also supports cryptocurrency trading through bots that analyze price patterns and trends, generating forecasts with confidence levels, which facilitates more profitable transactions and increased profits[129].

---

[125] Robert Mendick, "New Terror Laws Needed to Tackle Rise of the Radicalising AI Chatbots", The Telegraph (website), 2024, accessed: June 24, 2025, https://www.telegraph.co.uk/news/2024/01/01/terrorism-new-laws-ai-chatbots-new-group-violent-extremists/?ICID=continue_without_subscribing_reg_first.

[126] Sanna Karoliina Tirkkonen, Ruth Rebecca Tietjen, "Loneliness and Radicalization", Philosophy & Social Criticism, April 16, 2025, accessed: July 26, 2025, https://journals.sagepub.com/doi/10.1177/01914537251334550.

127 Abdullah Alrhmoun, Charlie Winter, János Kertész, "Automating Terror: The Role and Impact of Telegram Bots in the Islamic State's Online Ecosystem", in Terrorism and Political Violence, 36(4), February 7, 2023,1–16.

128 Asha Hemrajani, "The Use of AI in Terrorism", RSIS, August 2024, accessed: July 29, 2025, https://rsis.edu.sg/rsis-publication/rsis/the-use-of-ai-in-terrorism/.

129 Asha Hemrajani, "The Use of AI in Terrorism", RSIS, August 2024, accessed: July 29, 2025, https://www.rsis.edu.sg/wp-content/uploads/2024/08/CO24124.pdf.

Terrorists also utilize AI technology to carry out attacks in cyberspace, increasing the effectiveness and difficulty of detecting their activities. At the turn of 2016 and 2017, DAESH carried out a series of Distributed Denial-of-Service (DDoS) attacks targeting military, economic, and educational infrastructure, with the aim of crippling computer systems through massive connection requests[130]. Currently, the threat also includes the use of malicious software, such as malware and ransomware, to obtain databases or extort ransoms, with AI making it possible to create code that is even more difficult to detect. This technology also facilitates the generation of realistic phishing messages and vishing, i.e., telephone scams using synthetic voices[131].

Advanced language models are growing in importance as a means of providing operational support for terrorists, enabling them to plan, analyze, and refine attack scenarios[132]. Uncensored models that can provide answers without ethical restrictions or security mechanisms pose a particular threat[133]. In the hands of extremists, they can provide detailed instructions on how to obtain, manufacture, or improve weapons, locate security gaps, and predict the response of security services, as well as increase the precision and autonomy of combat systems, including drones and ballistic missiles.

One of the most disturbing applications of artificial intelligence in the context of terrorism is its potential use in autonomous combat systems, such as drones and vehicles capable of autonomous target recognition and attack. Thanks to machine learning algorithms, drones can analyze images in real time, identify military targets, and carry out precision strikes without human intervention. This technology is already being used in the war in Ukraine (including the Russian Lancet-3 and Ukrainian FPV drones with autonomous capabilities).

In the hands of terrorists, such devices could be programmed to independently attack a selected person, group of people, or critical infrastructure facility using facial or silhouette recognition. The threat also includes autonomous vehicle traps, which could independently reach their target and detonate explosives, eliminating the need for suicide bombers[134]. Although there is no confirmed evidence, there have been reports of Daesh working on such solutions[135]. In its June 2025 report, the UN also warns of the possibility of terrorists taking over autonomous cars and turning them into 'killer robots' controlled with minimal supervision, which would allow them to carry out multiple attacks without any losses among their own fighters[136].

These additional applications of AI, spanning finance, cyberspace, autonomous weapons, and strategic planning, underscore the technology's adaptability and the

---

[130] UK Home Office, *"The Islamic State in Iraq and Syria (ISIS): Security challenges and responses"*, December 2016–January 2017, accessed: June 01, 2025, https://assets.publishing.service.gov.uk/media/5d430bafed915d09dac9bb05/580_The_Islamic_State_in_Iraq.pdf.

[131] Vladimir Voronkov and Antonia Marie De Meo, "Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes", 2021, accessed: June 01, 2025, https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf.

[132] "*The Weaponization of Artificial Intelligence: The Next Stage of Terrorism and Warfare"*, ed. C. Anthony. Pfaff, (Centre of Excellence Defence Against Terrorism, 2025).

[133] Fabio Urbina et al. (2024), "Dual Use of Artificial Intelligence-powered Drug Discovery", Nature Machine Intelligence, 4(3), accessed: June 04, 2025, https://www.researchgate.net/publication/359073288_Dual_use_of_artificial-intelligence-powered_drug_discovery.

[134] Kateryna Stepanenko, "The Battlefield AI Revolution Is Not Here Yet: The Status of Current Russian and Ukrainian AI Drone Efforts", June 02, 2025, ISW Press.

[135] Clarisa Neru, "Exploitation of Generative AI by Terrorist Groups", accessed: July 26, 2025, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[136] Graham Hope, "UN Warns of Terrorist Threat for Self-Driving Cars", Slaughterbots, IoT World Today, 2025, accessed: June 04, 2025, https://www.iotworldtoday.com/security/un-warns-of-terrorist-threat-for-self-driving-cars-slaughterbots.

diverse threat vectors it can enable. While some remain largely theoretical, the accelerating pace of AI innovation, combined with declining costs and increasing accessibility of tools, suggests they may soon transition from peripheral concerns to central challenges for counterterrorism.

Drones

Unmanned Aerial Vehicles (UAVs) have become an increasingly attractive asset for terrorist organizations due to their affordability, accessibility, and strategic versatility. The relatively low cost of manufacturing or acquiring commercial drones means that their loss during operations poses minimal logistical or financial burden, making them ideal for repeated use in asymmetric warfare. In recent years, prominent groups such as Daesh, Hezbollah, and the Houthi rebels have not only weaponized off-the-shelf drones but also begun efforts to harden them electronically and evade countermeasures. Moreover, advances in artificial intelligence have enabled non-state actors to experiment with drone swarming capabilities and partially autonomous flight, significantly increasing operational potential while reducing human risk. These tools lower the psychological and material costs of deployment, allowing terrorists to launch coordinated, long-range attacks on military, political, and economic targets beyond their immediate reach. The potential for AI to independently identify, track, and eliminate targets further shifts the tactical balance, offering not just a method of warfare but a new form of strategic disruption in global security[137].

The convergence of AI and drone technology introduces an alarming prospect: making advanced warfare capabilities available to everyone. As major powers such as the United States, China, and Russia continue to deploy AI-controlled UAVs on the battlefield, the technology inevitably becomes more vulnerable to proliferation through black markets, state sponsorship, or battlefield scavenging. Once acquired, AI-enabled drones offer anonymity, strategic reach, and the ability to launch synchronized attacks across multiple locations, stretching the response capacity of state security services. The use of AI also detaches the attacker from the physical battlefield, allowing operations to be conducted remotely and at a large scale, while masking attribution and hindering intelligence efforts. As these technologies mature and become more affordable, it becomes increasingly likely that the first high-profile AI-powered terrorist attack will not be a question of if, but when — marking a transformative shift in both the nature of terrorism and the future of counterterrorism strategy.

Recently, the deployment of drones has accelerated across many battlefields, becoming a natural extension of existing military tools. Continuous testing of new systems is expanding the combat potential of Unmanned Aerial Combat Vehicles (UACVs), especially in roles like evading or overcoming anti-aircraft defenses. AI-controlled, low-signature UAVs are increasingly viewed as essential assets, capable of misleading or destroying traditional air defense systems.

The war in Ukraine has vividly demonstrated the strategic value of drones in both offensive and defensive operations. Ukrainian forces have effectively used Turkish-made Bayraktar TB2 drones to strike high-value Russian targets, including mobile air defense systems and supply convoys, with precision and minimal exposure. On the other hand, Russia has launched waves of Iranian-made Shahed drones to

[137] Aleksander Olech, "Unmanned Aerial Vehicle – a Lethal Weapon of Tomorrow for Terrorists", in Nowa Polityka Wschodnia, 2022, No 1 (32), 44–60.

probe and saturate Ukraine's air defenses, exposing weaknesses and forcing constant adaptation. These actions demonstrate how UAVs are reshaping air defense doctrines, with drones used not just for reconnaissance or strikes but to drain and distract costly anti-aircraft systems. As seen in earlier conflicts, such as the one in Libya, where Turkish drones destroyed Russian-made Pantsir systems, the inability to counter drone threats underlines a growing need for improved, multi-layered air defense solutions. In light of these events, even well-equipped nations with robust air defenses, such as Saudi Arabia, have found themselves vulnerable to attacks, as evidenced by the Houthi drone strikes on oil infrastructure in 2019. The Ukrainian conflict serves as the most current and high-profile example of how drone warfare is no longer supplementary — it is central to the modern battlefield[138].

In recent years, terrorist organizations have rapidly adapted emerging drone and AI technologies, transforming once-innocuous commercial UAVs into deadly tools of asymmetric warfare. What began as basic reconnaissance missions over military zones in regions such as Israel, Iraq, and Pakistan has evolved into coordinated, semi-autonomous drone attacks capable of evading detection, swarming targets, and delivering explosives with alarming precision. The first known lethal drone attack attributed to a terrorist group took place in 2016, when Daesh used an explosive-laden commercial drone to kill some units[139]. This incident marked a significant shift, revealing that non-state actors could begin to narrow the technological gap with state militaries by weaponizing commercially available drone platforms. From improvised Styrofoam UAVs to large-scale drone attacks on critical infrastructure, as exemplified by the 2019 attack on Saudi Arabia's Abqaiq oil facility by Iran-backed Houthi rebels.,these developments point to a future in which AI-enabled drones may play a central role in both terrorist operations and counterterrorist responses. Although the use of fully autonomous drone swarms by terrorist organizations has not yet been confirmed, the rapid pace of technological advancement suggests that such capabilities may soon become accessible beyond state control. As drone technology becomes cheaper and more accessible, the line between state and non-state military capabilities continues to blur — raising urgent questions around global security, military doctrine, and the ethical boundaries of autonomous warfare[140].

Terrorist organizations may use artificial intelligence to carry out their attacks. At the moment, these activities are fragmented — these groups have not yet mastered fully autonomous control of unmanned aerial vehicles, but it is only a matter of time before they acquire it.

Until now, drones have been used to gather intelligence on military bases and weapons, as well as to carry out attacks against state and non-state entities[141]. The use of these technologies gives terrorists an advantage, as they are relatively cheap and require minimal training. The functionality of a drone enhanced by AI would reduce the need for human resources, but it requires know-how and specialists, which results in the requirement for adequate funding and often the support of sponsor states. Only

---

[138] Aleksander Olech, "Unmanned Aerial Vehicle – a Lethal Weapon of Tomorrow for Terrorists", in Nowa Polityka Wschodnia, 2022, No 1 (32), 44–60.

[139] Michael S. Schmidt and Eric Schmitt, "ISIS Used an Armed Drone to Kill Two Kurdish Fighters", *The New York Times*, October 11, 2016, accessed: June 01, 2025, https://www.nytimes.com/2016/10/12/world/middleeast/isis-drones.html

[140] Aleksander Olech, "Unmanned Aerial Vehicle – a Lethal Weapon of Tomorrow for Terrorists", in Nowa Polityka Wschodnia, 2022, No 1 (32),44–60.

[141] Alan Lis i Aleksander Olech, "Wykorzystanie nowych technologii przez terrorystów na przykładzie dronów i deep fake'ów, Wiedza Obronna 2021"*, Vol. 275 No. 2.*

the largest organizations, such as al-Qaeda, Daesh, Hezbollah, the Taliban, the PKK, PIJ, Kata'ib Hezbollah, Lashkar-e-Tayyiba, and Boko Haram have such capabilities[142].

In the future, the acquisition of AI-controlled weapons would increase the capabilities of terrorists and break down geographical barriers, enabling them to carry out attacks in other countries. Drones could also reduce the number of suicide bombers. Between 2024 and 2025, European intelligence services uncovered a network linked to Hezbollah that was smuggling drone parts from Spain, France, and Germany to Lebanon[143].

The progressive integration of artificial intelligence with Unmanned Aerial Vehicle technology is not only changing the way warfare is conducted, but also redefining the potential threats posed by terrorist organizations. This trend, supported by the decreasing barrier to access to advanced technologies, indicates that in the future, the combat capabilities of extremist groups may approach those of states, requiring urgent action in the areas of law, technology control, and international cooperation.

3D printing and terrorist threats

Beyond AI-enabled UAVs, terrorists can also leverage additive manufacturing to circumvent arms controls and prototype components that enhance the lethality and survivability of their platforms. Over the past decade, the development of printed firearms has accelerated: their reliability and performance have improved, costs and technical barriers to home manufacture have plummeted, and blueprints now spread freely across global platforms, creating a decentralized, border-spanning ecosystem of weapon production. Although most designers, publishers, manufacturers and end-users employ this additive manufacturing technology lawfully or without violent intent, its 'democratization' nonetheless raises urgent, evidence-based concerns about political violence. Geographical and chronological data show a troubling rise in printed-firearm incidents across multiple regions, with their use shifting from niche hobbyist circles to extremist movements that treat such weapons as both practical tools and ideological symbols: by printing their own guns, they circumvent conventional legal and logistical hurdles, reinforce anti-government and libertarian narratives, and avoid regulated arms markets that are vulnerable to law-enforcement scrutiny.

This adaptability increases operational secrecy and complicates preventive measures, underscoring the need for continual monitoring, systematic documentation, advanced digital forensics, robust data collection and coordinated international cooperation. Law enforcement agencies are under the pressure to keep pace with these technological shifts, while legislators and global partners craft policies to curb the mounting risks as printed firearms become ever more embedded in criminal and extremist activity[144].

Additive Manufacturing (AM), commonly known as 3D printing, has evolved into a sophisticated, cost-effective, and readily available technology, whose application is

[142] Clarisa Neru, "Exploitation of Generative AI by Terrorist Groups", accessed: July 26, 2025, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

[143] "Spain, Germany Dismantle Network Supplying Drone Parts to Hezbollah in Lebanon", Defense Mirror. (2025), accessed: July 26, 2025 https://www.defensemirror.com/news/37314/Spain__Germany_Dismantle_Network_Supplying_Drone_Parts_to_Hezbollah_in_Lebanon.

[144] Yannick Veilleux-Lepage, "Printing Terror: An Empirical Overview of the Use of 3D-Printed Firearms by Right-Wing Extremists", CTC Sentinel 17, no. 6 (June 2024): 31–43, accessed: August 04, 2025, https://ctc.westpoint.edu/wp-content/uploads/2024/06/CTC-SENTINEL-062024_article-4.pdf.

rapidly increasing for both legitimate and illegitimate purposes. Recent advancements in materials science, Computer Aided Design (CAD), and artificial intelligence now permit users to print with an expanding variety of feedstocks, facilitating decentralized 'print-on-demand' production, swift prototyping, and customizable designs that could supplant segments of conventional manufacturing. As printers, materials, and software proliferate, supply chains may transition from global to local, necessitating a shift in interdiction from the seizure of physical goods to the regulation of digital blueprints, counterfeits, and inferior components which constitutes an urgent imperative considering that unverified Additive Manufactured components are already being incorporated into finished products and that the initial printed firearm (in 2013) posed a national security risk[145].

Revenues from commercial additive manufacturing are anticipated to increase by more than 24% annually until 2030, primarily within select high-value sectors. However, the same converging fields that propel growth — artificial intelligence, materials science, biology, chemistry, and nanotechnology — also exacerbate risks, including those associated with counterfeit products, illegal weaponry, and catastrophic product failures, thereby necessitating export controls and international collaboration to safeguard economic prosperity and public safety[146].

Emerging technologies foster innovation while simultaneously posing unprecedented security vulnerabilities. Additive manufacturing (3D printing) exemplifies the process in which objects are built layer by layer from plastics, metals, and other materials utilizing CAD files (computer-aided design files — digital blueprints for objects), and currently facilitates the production of items ranging from rockets and medical devices to humanitarian equipment. However, its dual-use characteristics provoke concern. In 2013, the organization Defense Distributed published online files for the 'Liberator', the inaugural nearly entirely 3D printed firearm, thereby demonstrating the concept. The threat materialized in 2019 when a far-right extremist employed a partially printed weapon during the Halle attack in Germany; analogous cases of 3D printed firearms have subsequently emerged in the UK, Spain, Ireland, Sweden and Finland. While terrorists primarily concentrate on 3D printed firearms, researchers caution that the same technology could facilitate their acquisition of weapons of mass destruction. Online DIY communities openly disseminate both theoretical and practical knowledge regarding 3D printing and bioprinting, while large language models make it easier to access dual-use scientific information[147].

3D printed firearms fall into three broad categories: fully printed weapons, excluding only the metal firing pin, which are often crude, single-use designs; hybrids, such as the FGC-9 priced at roughly $400, which combine inexpensive, unregulated hardware-store parts like tubes, springs, and bolts with printed components to match factory-made firearms in some tests; and completion kits, the most reliable but also the most expensive, merging printed pieces with factory-manufactured, pressure-bearing components that may require permits and are easier to trace. At the intersection of DIY (do-it-yourself) technology culture and gun enthusiasm, these weapons are embraced by hobbyists and right-wing extremists alike, serving both as

[145] Andy Greenberg, "Meet the 'Liberator': The World's First Fully 3D-Printed Gun", Wired (website), 6 May 2013, accessed: August 06, 2025, https://www.wired.com/2013/05/liberator-printed-gun/.
[146] Daniel M. Gerstein, Erin N. Leidy, "Emerging Technology and Risk Analysis: Additive Manufacturing", RAND Research, February 15, 2024, Accessed: July 23, 2024, https://www.rand.org/pubs/research_reports/RRA2984-1.html.
[147] Nicolò Miotto, "3D printing and WMD terrorism: a threat in the making?", accessed: August 04, 2025, https://europeanleadershipnetwork.org/commentary/3d-printing-and-wmd-terrorism-a-threat-in-the-making/.

a symbolic assertion of US Second Amendment rights and as a practical tool for bypassing import restrictions, enabling customization, and producing untraceable firearms even for prohibited purchasers. Their low marginal cost per unit increases the potential lethality accessible to malicious actors such as terrorists, while the generally legal sharing of CAD blueprints and instructional materials forces online platforms to balance legitimate engineering exchange with limiting extremist exploitation, using measures such as download restrictions, reduced algorithmic visibility, and collaboration with civil-society experts[148].

As for now, 3D-printed and other homemade weapons have not been found in the arsenals of most terrorist organizations, which continue to focus mainly on online propaganda and drones and are chiefly associated with right-wing terrorism; nevertheless, this poses a huge challenge. 3D-printed firearms have already been used in lethal attacks, uncovered in clandestine workshops, and linked to terrorism-related arrests, showing the technology is no longer theoretical. In order to mitigate the threat, law enforcement agencies must collaborate closely with industry to keep pace with technological developments. An international network of experts should keep authorities updated on new projects and methods, and a concise factsheet distilling key information and policy recommendations should be circulated to partners and decision-makers worldwide[149].

Conclusions

The convergence of artificial intelligence and terrorism is no longer a speculative threat but is becoming a reality. This study has shown how AI, once the domain of research labs and major corporations, is increasingly within reach of extremist actors. From automated propaganda and cyber warfare to the weaponization of drones and potential exploitation of autonomous systems, AI represents both a multiplier of existing terrorist capabilities and a gateway to entirely new forms of asymmetric conflict. As outlined throughout this work, the concept of “Terror-AI-sm” is not merely an academic construct — it is a lens through which to understand the coming decade of global security challenges.

Should terrorists gain access to AI-controlled weaponry, the threat to the international community will increase significantly. They will no longer be geographically limited, being able to strike across borders — even within the US or Europe. Recruitment may increase, reducing the need for suicide bombers by replacing them with drones. AI-supported hacking would simplify access to classified military information. Likely, their focus will shift toward the US and its allies, where AI is seen as a key military threat. If acquired, such technology could make these groups among the most innovative threats of the century. However, this remains less likely, as many states are hesitant to arm even their allies with advanced AI for fear of losing control.

The prospect of using AI in warfare is both tempting and alarming. While AI can quickly match a veteran soldier’s efficiency, it lacks a moral compass. AI weapons would not face the same inhibitions in combat decisions, leading to more extreme

[148] Kyle Dent, Yannick Veilleux-Lepage and Maria Zuppello, “Risks and Challenges in Online Communities for 3D-Printed Firearms Among Extremists and Terrorists”, GIFCT Red Team Working Group report, September 20, 2023, accessed: August 04, 2025, https://gifct.org/wp-content/uploads/2023/09/GIFCT-23WG-0823-3DPrinting-1.1.pdf.

[149] “Printing insecurity: Tackling the threat of 3D-Printed Guns in Europe”, Europol, (press release issued after the International Conference on 3D-Printed Firearms), May 27 2022, accessed: June 15, 2025, https://www.europol.europa.eu/media-press/newsroom/news/printing-insecurity-tackling-threat-of-3d-printed-guns-in-europe.

tactics. Terrorist groups, already responsible for mass civilian and institutional deaths, would eagerly use such tools to escalate violence. For them, AI is just a new method to pursue the same ideological goals — unrestricted by morality or proportionality — making them disturbingly similar to autonomous machines. AI becomes a tool to maximize destruction and minimize losses. Drones could also serve propaganda purposes, showcasing technological growth. Given their fanaticism, terrorists will continue to use any means — weapons or drones — to strike both military and civilian targets, regardless of whether AI is central to the mission.

Contemporary global terrorist threats mainly harness Artificial Intelligence that supports weaponized robots or missiles as well as clusters of killer drones. This narrative emerged a few years ago, indicating that terrorists may have a vastly greater array of options at their disposal because they may cooperate with some rogue states that will support them. The chance for terrorist organizations to gain access to Artificial Intelligence technology only increased due to the global competition surrounding it. Numerous articles, shows and films used on military training grounds and prepared by the relevant wealthy countries, highlight the efforts of individual powers to flaunt their achievements and solidify their lead in the AI competition. For most superpowers, AI-supported systems are imperative on the modern battlefield. This importance is only highlighted by the obstacles placed by China, Russia, or Iran on western intelligence agencies in securing and stealing research data, to ensure that they are not left behind in their race. Yet, growing interest will inevitably lead to further development and widespread usage of technology. Due to its potential spreading, terrorists will have a chance to operate weapons supported by AI. These events add up to a deeply concerning scenario which conceivably may also have to be confronted.

The adoption of emerging tools by violent extremists is surpassing the defensive capabilities of states in a contemporary ‘sword-and-shield’ dynamic: widely available drones — used on the battlefields of Ukraine and driven by an extremely competitive market — provide non-state actors with affordable airpower that is nearly impossible to regulate comprehensively; in contrast, the proliferation of 3D-printed firearms has been less extensive than anticipated due to the dominant presence of conventional small arms in conflict zones and the Global South, although this displacement effect still necessitates thorough examination. The most significant proliferation threat currently comes from modular, mainstream artificial intelligence ‘building blocks’ that can be illicitly obtained or provided by rogue states and swiftly weaponized for autonomous drones, bioengineering, extensive cyberattacks, or automated propaganda. Further challenges inevitably lie ahead.

The use of Artificial Intelligence by terrorist organizations is showing a clear upward history, providing them with a way to maximize damage while minimizing their own losses. So far, AI has been used mainly to create disinformation and propaganda content, conduct interactive recruitment, and raise funds, but with the development of technology, the implementation of autonomous drones, vehicles, and advanced cyberattack tools is becoming a reality. The barrier to entry for this type of activity is constantly decreasing thanks to the availability of open-source code, commercial plugins for generating images, sound, and text, and drones with facial recognition software that can be combined without costly research and development facilities. In addition, hostile states can provide terrorists with ready-made technology ‘packages’, and communities of technology enthusiasts can develop and share add-ons that integrate AI with commonly available equipment.

It is also increasingly emphasized that generative models are capable of writing polymorphic malware that mutates to avoid detection and learns from the effectiveness of subsequent attacks, which could become a particularly dangerous element in the arsenal of extremists[150]. Given the practice of terrorists appropriating technologies used by counterterrorism forces, close cooperation between governments and owners of key platforms, such as Meta and OpenAI, is necessary to develop joint strategies to counter these threats[151].

In order to effectively counter the threats posed by the potential use of artificial intelligence by terrorist organizations, coordinated action is necessary. Countries should develop clear legal regulations concerning AI technologies and autonomous systems and strengthen international cooperation in the control of dual-use technologies. At the same time, specialized security units capable of monitoring threats and responding quickly should be created. Institutional measures should be complemented by public education — developing digital literacy, critical thinking skills, and the ability to recognize disinformation are the foundation of a modern security system today.

In the coming years, the trajectory of AI will continue to redefine the parameters of security, sovereignty, and conflict. The same forces that drive innovation — open-source development, globalized markets, and decentralized knowledge sharing — also accelerate the diffusion of dangerous capabilities. Terrorist groups will not need to invent AI from scratch; they will adapt, modify, and repurpose what is already available, often faster than states are able to put appropriate legislation in place. In the past the cheapest way to carry out a terrorist attack was to have a knife or a gun. Today, extremists can use the Internet sitting in a safe place having only a connection to web.

The future of Terror-AI-sm will be shaped by the interplay between innovation and regulation, offense and defense, openness and control. Terrorism has a new version that is developing extremely rapidly. Without decisive, coordinated international action — uniting governments, industry leaders, and civil society — the gap between potentials threats and prevention will only widen. In such a landscape, the question is not whether terrorists will weaponize AI, but how prepared the global community will be when they do. Terrorism – like technology itself – is now more global than ever before. The choice before policymakers is stark: act now to close the window of opportunity for malicious actors, or face a future in which Artificial Intelligence becomes not only the tool for progress, but possibly the most sophisticated weapon of terror ever devised. Almost anyone who comes into contact with technology could be a potential victim of terrorist attacks, which jeopardize the majority of the world's population. Terror-AI-sm will continue to be a persistent challenge.

[150] Jean-Luc Marret, "New Tech, New Threats: Drones, 3D-Printed Guns, Artificial Intelligence and Violent Extremism", Note de la FRS no. 07/2025, Foundation for Strategic Research, May 15 2025, accessed: August 03, 2025, https://www.frstrategie.org/en/publications/notes/new-tech-new-threats-drones-3d-printed-guns-artificial-intelligence-and-violent-extremism-2025.

[151] Clarisa Neru, "Exploitation of Generative AI by Terrorist Groups", accessed: July 26, 2025, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

Bibliography

Books

1. Olech Aleksander, Lis Alan, “Technology and terrorism: Artificial Intelligence in the time of contemporary terrorist threats”, Institute of New Europe, Warsaw, 2021.

Reports, papers and articles

1. Alrhmoun Abdullah, Winter Charlie, Kertész János, “Automating Terror: The Role and Impact of Telegram Bots in the Islamic State’s Online Ecosystem”, in Terrorism and Political Violence, 36(4), February 7, 2023, 1–16.

2. Byman L. Daniel, Gao Chongyang, Meserole Chris, and Subrahmanian V.S, “Deepfakes And International Conflict”, The Brookings Institution, 1-4.

3. Dass Rueben, “3D-Printed Firearms and Terrorism: Trends and Analysis Pertinent to Far-Right Use” in Counter Terrorist Trends and Analyses 16, no. 3 (June 2024): 19–30, https://rsis.edu.sg/wp-content/uploads/2024/06/CTTA_June-2024.pdf.

4. Dent Kyle, Veilleux-Lepage Yannick and Zuppello Maria, “Risks and Challenges in Online Communities for 3D-Printed Firearms Among Extremists and Terrorists”, GIFCT Red Team Working Group report, September 20, 2023, https://gifct.org/wp-content/uploads/2023/09/GIFCT-23WG-0823-3DPrinting-1.1.pdf.

5. Early terrorist experimentation with generative artificial intelligence services: pro-al-Qaeda use of AI-generated posters and imagery, Tech Against Terrorism, https://techagainstterrorism.org/hubfs/Tech%20Against%20Terrorism%20Briefing%20%20Early%20terrorist%20experimentation%20with%20generative%20artificial%20intelligence%20services.pdf.

6. European Union Terrorism Situation and Trend Report 2025 (EU TE-SAT*)*, Publications Office of the European Union, Luxembourg, 2025, https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf.

7. Fourth Parliamentary Policy Dialogue on countering the use of artificial intelligence and new technologies for terrorist purposes, Rome Summit Report, December 05, 2024, https://www.oscepa.org/en/documents/ad-hoc-committees-and-working-groups/ad-hoc-committee-on-countering-terrorism/5183-fourth-parliamentary-policy-dialogue-outcome-document-5-december-2024/file.

8. Gerstein M. Daniel, Leidy N. Erin, “Emerging Technology and Risk Analysis: Additive Manufacturing”, RAND Research, February 15, 2024, https://www.rand.org/pubs/research_reports/RRA2984-1.html.

9. Nelu Clarisa, “Exploitation of Generative AI by Terrorist Groups”, International Centre for Counter-Terrorism, June 10, 2024, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

10. Olech Aleksander, “Unmanned Aerial Vehicle – a Lethal Weapon of Tomorrow for Terrorists”, in Nowa Polityka Wschodnia, 2022, No 1 (32), 44–60.

11. Pfaff Anthony C., “Introduction: Terrorism and Artificial Intelligence”, in *The Weaponization of AI: The Next Stage of Terrorism and Warfare*, ed. C. Anthony Pfaff (Centre of Excellence Defence Against Terrorism, 2025).

12. Siegel Michael, Zeijlemaker Sander, Baxi Vidit, Raajah Sharavanan, “Rethinking the Cybersecurity Arms Race”, MIT Sloan, Massachusetts Institute of Technology, April 10, 2025, https://cams.mit.edu/wp-content/uploads/Safe-CAMS-MIT-Article-Final-4-7-2025-Working-Paper.pdf.

13. Singer P.W. & Brooking T. Emerson, “LikeWar: The Weaponization of Social Media.” Houghton Mifflin Harcourt, June 2019, https://www.researchgate.net/publication/335149861_Like_War_-_The_Weaponization_of_Social_Media_by_P_W_Singer_and_Emerson_T_Brooking.

14. UNCCT Annual Report 2020, United Nations Counter-Terrorism Centre (UNCCT), New York: United Nations Office of Counter-Terrorism, 2021.

15. Urbina Fabio et al. (2024), “Dual Use of Artificial Intelligence-powered Drug Discovery”, Nature Machine Intelligence, 4(3), https://www.researchgate.net/publication/359073288_Dual_use_of_artificial-intelligence-powered_drug_discovery.

16. Uveges András József, “Terrorist Use of Artificial Intelligence-Driven Social Media”, in The Weaponization of AI: The Next Stage of Terrorism and Warfare, ed. C. Anthony Pfaff, (Centre of Excellence Defence Against Terrorism, 2025), 46–47.

17. Voronkov Vladimir and Marie De Meo Antonia, “Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes”, 2021, https://unicri.org/sites/default/files/2021-06/Malicious%20Use%20of%20AI%20-%20UNCCT-UNICRI%20Report_Web.pdf.

18. “Violent Extremists’ Use of Generative Artificial Intelligence”, First Responder Toolbox, Joint Counterterrorism Assessment Team (NCTC, DHS, FBI), May 6, 2024, https://www.dni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/151s_First_Responders_ToolboxViolent_Extremists_Use_of_Generative_Artificial_Intelligence.pdf.

19. Winter Charlie, “Documenting the Virtual ‘Caliphate’.”, Quilliam Foundation, October 2015, https://core.ac.uk/download/pdf/30670971.pdf.

Online sources

1. “Actioned terrorism content items on Facebook worldwide from 4th quarter 2017 to 3rd quarter 2024” Statista, 2024, https://www.statista.com/statistics/1013864/facebook-terrorist-propaganda-removal-quarter/.

2. “Attack in Nice: Photos of fake victims and fake suspects flood networks”, FRANCE 24 Observers (2016), https://observers.france24.com/en/20160715-attack-nice-fake-victims-suspects-social-networks.

3. Gilbert David, “ISIS Created Fake CNN and Al Jazeera Broadcasts”, Wired (website), https://www.wired.com/story/isis-created-fake-cnn-and-al-jazeera-broadcasts/.

4. Greenberg Andy, “Meet the ‘Liberator’: The World’s First Fully 3D-Printed Gun”, Wired (website), 6 May 2013, https://www.wired.com/2013/05/liberator-printed-gun/.

5. Hall KC Jonathan, “Terrorists could exploit AI chatbots to spread hate and hatch plots, terrorism tsar warns”, The Scottish Sun (website), https://www.thescottishsun.co.uk/news/15086176/terrorist-bot-plot-tsar-chatbot-ai-artificial-intelligence.

6. Hemrajani Asha, “The Use of AI in Terrorism”, RSIS, August 2024, https://rsis.edu.sg/rsis-publication/rsis/the-use-of-ai-in-terrorism/.

7. Here’s how violent extremists are exploiting generative AI tools, Wired (website), https://www.wired.com/story/generative-ai-terrorism-content.

8. Hope Graham, “UN Warns of Terrorist Threat for Self-Driving Cars”, Slaughterbots, IoT World Today, 2025, https://www.iotworldtoday.com/security/un-warns-of-terrorist-threat-for-self-driving-cars-slaughterbots.

9. Lis Alan i Olech Aleksander, “Wykorzystanie nowych technologii przez terrorystów na przykładzie dronów i deep fake’ów, Wiedza Obronna 2021”, Vol. 275 No. 2.

10. Makuch Ben, “How terrorist groups are leveraging AI to recruit and finance their operations”, theguardian.com (website), https://www.theguardian.com/world/2025/jul/08/terrorist-groups-artificial-intelligence.

11. Marret Jean-Luc, “New Tech, New Threats: Drones, 3D-Printed Guns, Artificial Intelligence and Violent Extremism”, Note de la FRS no. 07/2025, Foundation for Strategic Research, May 15 2025, https://www.frstrategie.org/en/publications/notes/new-tech-new-threats-drones-3d-printed-guns-artificial-intelligence-and-violent-extremism-2025.

12. Mendick Robert, “New Terror Laws Needed to Tackle Rise of the Radicalising AI Chatbots”, The Telegraph (website), 2024, https://www.telegraph.co.uk/news/2024/01/01/terrorism-new-laws-ai-chatbots-new-group-violent-extremists/?ICID=continue_without_subscribing_reg_first.

13. Miotto Nicolò, “3D printing and WMD terrorism: a threat in the making?”, https://europeanleadershipnetwork.org/commentary/3d-printing-and-wmd-terrorism-a-threat-in-the-making/.

14. Neo-Nazis are all-in on AI, Wired (website), https://www.wired.com/story/neo-nazis-are-all-in-on-ai.

15. Neru Clarisa, “Exploitation of Generative AI by Terrorist Groups”, https://icct.nl/publication/exploitation-generative-ai-terrorist-groups.

16. Paterson James, “How Extremists Are Manipulating AI Chatbots” Lowy Institute,” Lowyinstitute.org, 2025, https://www.lowyinstitute.org/the-interpreter/how-extremists-are-manipulating-ai-chatbots.

17. Pauwels Annelies and Herbach Merlina, “Buy It, Steal It, Print It: How Right-Wing Extremists in Europe Acquire Firearms and What To Do About It”, ICCT Policy Brief (International Centre for Counter-Terrorism), December 2024, 11, https://icct.nl/publication/buy-it-steal-it-print-it-how-right-wing-extremists-europe-acquire-firearms-and-what-do.

18. Renske van der Veer, “Terrorism in the Age of Technology | Strategic Monitor 2019-2020,” www.clingendael.org, 2019,

https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology/.

19. Stepanenko Kateryna, “The Battlefield AI Revolution Is Not Here Yet: The Status of Current Russian and Ukrainian AI Drone Efforts”, June 02, 2025, ISW Press.

20. Stockwell Sam, “Propaganda by Meme,” Centre for Emerging Technology and Security, 2024, https://cetas.turing.ac.uk/publications/propaganda-meme.

21. Terrorists could turn driverless cars into slaughterbots, UN warns, The Times (website), https://www.thetimes.com/uk/technology-uk/article/terrorists-could-turn-driverless-cars-into-slaughterbots-un-warns-t7wzx977d.

22. Terrorist Groups Looking to AI to Enhance Propaganda and Recruitment Efforts, The Soufan Center, https://thesoufancenter.org/intelbrief-2024-october-3/.

23. Tirkkonen Sanna Karoliina, Tietjen Ruth Rebecca, “Loneliness and Radicalization”, Philosophy & Social Criticism, April 16, 2025, https://journals.sagepub.com/doi/10.1177/01914537251334550.

24. Siegel Daniel, “AI Jihad: Deciphering Hamas, Al-Qaeda and Islamic State’s Generative AI Digital Arsenal”, GNET, February 19, 2024, https://gnet-research.org/2024/02/19/ai-jihad-deciphering-hamas-al-qaeda-and-islamic-states-generative-ai-digital-arsenal/.

25. Spain, Germany Dismantle Network Supplying Drone Parts to Hezbollah in Lebanon”, Defense Mirror (2025), https://www.defensemirror.com/news/37314/Spain__Germany_Dismantle_Network_Supplying_Drone_Parts_to_Hezbollah_in_Lebanon.

26. “Synthetic Media in Far-Right Messaging”, EU DisinfoLab. (2025), https://www.disinfo.eu/disinfo-update-24-06-2025.

27. Veilleux-Lepage Yannick, “Printing Terror: An Empirical Overview of the Use of 3D-Printed Firearms by Right-Wing Extremists”, CTC Sentinel 17, no. 6 (June 2024): 31–43, https://ctc.westpoint.edu/wp-content/uploads/2024/06/CTC-SENTINEL-062024_article-4.pdf.

28. Warrick Joby, “Use of weaponized drones by ISIS spurs terrorism fears”, The Washington Post (website), February 21, 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.

CHAPTER 5

SOCIAL MEDIA AND THE SHADOW OF TERRORISM: IMPACTS, RISKS, AND THE WAY FORWARD

Tacan İldem

I. Introduction

Over the two decades, social media has significantly transformed how we communicate, share information, research topics, follow the news, and present ourselves. It has become a space where the presence and activities of various actors, including those with malicious intentions such as terrorist groups, are noticeable. The combination of extremism and digital technology has introduced several significant risks, including cyberterrorism and information threats. (1)

I have witnessed firsthand in my previous capacities how these platforms can be both empowering and dangerous. On the one hand, they connect us; on the other, they can radicalize individuals in a shockingly short period. It is not solely the content; it is the algorithms, anonymity, and relentless flow of information that enable extreme narratives to go viral and influence minds across continents.

No matter how much effort is put in place, and despite all efforts and interventions at the platform level, challenges persist, particularly for niche platforms and encrypted networks. (2)

To effectively combat the online spread and appeal of extremism, we need stronger public-private partnerships, well-designed policy frameworks, greater investment in digital literacy, and the promotion of credible counter-narratives as part of a proactive communications strategy.

As the digital and physical spheres are increasingly intertwined, preventing the misuse of social media has become not just a technical concern but a pressing matter for global security and the health of democratic governance.

Striking the right balance between safeguarding fundamental individual rights, such as freedom of expression and preventing exploitation on social media has become an increasingly challenging task. But measures to curb malicious threats should in no way compromise individual rights and fundamental freedoms inherent in democratic governance.

II. The Role of Social Media in Terrorism

Terrorists have effectively exploited social media for four key related reasons:

1. Propaganda and the Dissemination of Ideology

According to Garth S. Jowett and Victoria O'Donnell (2018), propaganda is "the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour" to serve the propagandist's aims. In the 20th century, authoritarian regimes like Nazi Germany and the Soviet Union used centralised propaganda to enforce ideological conformity. Similar practices persist today, although propaganda is not limited to autocracies. In liberal democracies, despite legal safeguards and media diversity, these often manifest in subtler forms, such as framing, selective reporting, and manipulation through various means, including digital media. (3)

We are living through a digital revolution, an age where ideas can travel faster than we can think, wrapped in sleek, seductive packaging. Eli Pariser coined a term that has always stuck with the author: the 'filter bubble'. And it is real. Algorithms don't just show us what we like; they reinforce what we already believe. It is like a hall of mirrors; you think you're exploring, but you are just seeing more of yourself. (4)

It is deeply concerning how social media platforms, originally designed to promote dialogue and creativity, have become a fertile ground for propaganda and conflict. Sadly, the perpetrators speak our language, hijack our symbols, and manipulate our frustrations, while staying comfortably anonymous. (5) Without the oversight of traditional media controls, terrorists can rapidly spread large amounts of material with high precision and focus through social media.

Furthermore, today's propaganda heavily relies on visuals and emotional appeal, making it less about facts and more about feelings, which makes it a powerful tool in the fight for hearts and minds. In *Propaganda: The Formation of Men's Attitudes*, Jacques Ellul argues that pre-propaganda works by subtly embedding simplified messages within the cultural fabric, creating a psychological predisposition for the audience to accept more structured ideological narratives later. (6)

One of the most potent ways terrorists utilize social media is through their ability to create high-quality, emotionally impactful propaganda products and then disseminate them rapidly across digital networks. As Tufekci (2017) notes, networked platforms do not just broadcast messages; they allow engagement, remixing and amplification. Unlike traditional, top-down propaganda, today users can instantly share digital content, comment on it, reframe it, and re-circulate it, forming self-reinforcing echo chambers. In these spaces, radical ideas are disseminated, socially validated, and amplified, creating environments where recruitment and ideological commitment become more scalable and resilient to disruption. (7)

2. Recruitment and Mobilization

Terrorist groups exploit social media as a tool for recruitment and mobilization, enabling them to overcome geographic distance and physical constraints. The accessibility and reach of these platforms have allowed recruitment tactics to become significantly more advanced and targeted.

Platforms like Facebook, X (formerly Twitter), Instagram, and TikTok employ algorithms and data analytics to allow organizations to micro-target individuals based on their interests, demographics, and online behavior. Alongside political parties and other special interest groups, terrorist organizations have also exploited this level of

specificity to reach vulnerable individuals with customized messages. (Conway, 2017) (8)

As Neumann, P. R. (2013) states, posts, memes, video clips, endorsements and hashtags on social media can package stories in more forceful ways that align with users' identities, fears, or dreams. This emotive response transforms passive viewers into advocates or active participants. (9)

What is striking about social media-fueled mobilization is its speed. It is like watching a spark turn into a wildfire. In just hours, entire communities are galvanized, be it for good or evil. These platforms let people organize, rally, and act before institutions can even grasp what is happening. We have all seen protests shape overnight, movements launched from a single tweet, and disinformation campaigns go out of control while government institutions are still trying to catch up.

Movements propelled by hashtags, such as #BlackLivesMatter and #MeToo, demonstrate how online activism can extend beyond virtual spaces, shaping real-life developments, influencing societal conversations, and occasionally prompting policy changes. (10)

Social media breaks from traditional top-down communication, allowing any user, not just elites, to shape discourse through sharing and amplification. As Bennett and Segerberg (2012) note, this “connective action” encourages personal expression and validation, particularly amongst the youth, fostering deeper emotional engagement. (11)

While encrypted apps like Telegram and WhatsApp ensure privacy, platforms like Facebook and Instagram enable broader outreach and sustained emotional engagement, often targeting isolated or marginalized individuals, especially young people and diaspora members. (12)

Extremist recruitment has moved online in a way that is constant, quiet, and efficient. As Jytte Klausen noted, groups like Daesh now operate like marketing representatives, tracking responses and tailoring messages with precision. Platforms like Telegram and Discord host closed communities where radical ideologies grow and spread. (13)

It is, in short, a strategic communication method for recruiting terrorists that combines propaganda, psychological manipulation and networked outreach to facilitate real-world mobilisation through the virtual world. What is more worrying is the flexibility of these methods. Even as certain pieces of content are taken down, accounts are banned, or entire networks are disrupted, these groups often resurface under new names or migrate to other platforms, continuing to convey the same message. (14)

3. Preparations and Coordination

Beyond communication and propaganda, terrorists now use social media to plan and coordinate attacks. The ease of access and the ability to remain anonymous on these platforms offer a significant strategic advantage. Once initial contact is made, communication often transitions to encrypted services like Telegram, where operational details are discussed, responsibilities are delegated and information is

exchanged, frequently using tools such as disappearing messages to avoid surveillance. (15)

At the same time, content from social media that is open to the public, shared images, events, or personal updates that can be used by terrorist groups for surveillance and focusing on targets. Details offered in moments of carelessness can become a source of practical intelligence in the wrong hands. (16)

When logistics are planned digitally, such as for safe houses or weapon drops, the transportation of both is referred to as operational planning. Terrorist groups crowdfund local operational support in friendly online communities in war zones and failed states, blurring the line between propaganda and resources on the ground. (17)

Certain perpetrators remain in touch with coordinators through secure messaging services to plan synchronized assaults, whereas others opt to live-stream their actions on publicly accessible platforms. This real-time dissemination serves a dual purpose: to intensify the psychological impact and ensure widespread media attention. (18)

In addition, there are apps with built-in transactions, cryptocurrency wallets, and a direct connection to the Dark Web through browsers, where operations can become a true master of disguise in the cyber world. (19)(20)

Though high-impact attacks still need offline coordination, online activity in preparing for terror attacks has sharply increased. (21) The merging of platforms, which includes social media and messaging apps as well as file-sharing sites and Dark Web forums, has allowed terrorists to easily navigate between the open and closed parts of the online space. (22)

4. Psychological Warfare and The Enhancement of Fear

What strikes us is how violence is being turned into performance. Terrorists are not just committing acts; they are staging them for broadcast. Many of us will never forget seeing some of those livestreams, which were almost like choreographed performances, designed to go viral. The aim is not just destruction, it is to erode trust, instill fear, and pull society apart from within.

Terrorist groups now exploit digital imagery for psychological impact, using those in graphic form to provoke emotions and shape public discourse. The UN and other expert assessments note these broadcasts as tools of information warfare, aimed at radicalization, community destabilization, and undermining state authority. (23)(24)

Studies show that repeated exposure to violent media may result in heightened stress responses, including anxiety and symptoms consistent with Post-Traumatic Stress Disorder (PTSD), even amongst those not directly affected. For example, after the Boston Marathon bombing, people who watched over six hours of coverage reported more distress than some who were physically present at the scene. (25)

Emotionally charged, violent stories leave deeper memory traces with repeated exposure, especially harmful in polarized, conflict-ridden societies where algorithms amplify such content, deepening divisions and social fragmentation. This

highlights the urgent need for media literacy, scalable content moderation, trauma-informed discourse, and resilient digital spaces. (26)

Through decentralised networks and individual cells, terrorist groups can also localise content in a way that better resonates with local grievances, religious themes, or socio-political contexts, thereby strengthening the appeal of the content and its overall impact.

III. Cyberthreats Arising from This Intersection

Terrorism is evolving from bombs to bytes, blending shock tactics with digital precision and narrative control. This convergence heightens the psychological and social impact, while increasing vulnerability to new forms of cyberattack. Without taking serious action, we risk remaining reactive instead of being proactive. (27)

Terrorist cyber actors now use AI tools like deepfakes and synthetic imagery or audio to create realistic, deceptive content, such as fake statements by leaders, that can spark panic and erode trust in institutions. Their rapid spread across platforms makes early intervention increasingly difficult. (28)

On the fringes, terrorists exploit social media to gather personal data, analysing fears, belief systems, and group identities that can be weaponised for doxxing, intimidation, and blackmail. The strategic misuse of personal data contributes to an atmosphere of persistent anxiety, where individuals increasingly sense they are under constant observation and lack control over their digital footprints. (29)

At the same time, cryptocurrencies and online financial scams have emerged as critical enablers of terrorist financing. Extremist groups exploit social media platforms to circulate fundraising appeals tied to illegal activities and to conduct money laundering. Due to the decentralised architecture and semi-anonymous nature of these technologies, effective oversight remains elusive, weakening conventional counterterrorism financial tools and contributing to an expanding landscape of cyber vulnerabilities and psychological harm. (30)

IV. Disinformation Campaigns

In the digital era, disinformation has become a calculated and central component of operations conducted by both state and non-state actors as part of their hybrid tactics. Among the most skillful at deploying these tactics are terrorist organizations, no longer treating disinformation as incidental but rather as a foundational means to distort reality, influence public perception, and achieve strategic leverage. (31)

These campaigns often focus on several interrelated objectives:

- Creating Panic and Disorientation: In the immediate aftermath of attacks, fabricated or contradictory reports are circulated to heighten fear and confusion.
- Undermining Institutional Credibility: Targeted disinformation efforts work to delegitimise state institutions and diminish trust in public authorities, law enforcement, and media outlets.
- Deepening Social Divisions: By amplifying false narratives rooted in ethnic, religious, or political identities, such campaigns inflame polarisation and weaken societal unity.

- Facilitating Radicalisation: Propaganda frames acts of violence as noble or divinely sanctioned, appealing to ideological or religious sentiments to recruit followers.
- Saturating the Information Space: A pervasive flow of misleading content overwhelms fact-based messaging, making it harder for the public and institutions to distinguish truth from fiction, especially during crises. (32)

The tools of this disinformation enterprise include:

- ❖ Fake News: False reports created to mislead the public.
- ❖ Manipulated Media: Deceptive images and videos designed to stir emotions.
- ❖ Deepfakes: Realistic video forgeries can deceive viewers into believing what they see is genuine.
- ❖ Bot Armies and Troll Networks: Coordinated efforts to amplify specific messages, creating the illusion of widespread support or outrage.
- ❖ Impersonation: Disguised communications mimicking government or NGO sources to spread false alerts and conspiracy theories.
- ❖ Groups like Daesh and Al-Qaeda have effectively weaponized these strategies, often claiming responsibility for attacks or framing foreign interventions as 'crusades' to incite anger and attract recruits.
- ❖ The consequences of such disinformation efforts can be severe:
- ❖ Emergency Facilities Blockades: Critical services may be hindered in the chaos following an attack.
- ❖ Erosion of Democratic Discourse: Civil dialogue is undermined, leading to societal fragmentation.
- ❖ Judgment of Entire Communities: Disinformation can unjustly tarnish the reputation of entire communities.
- ❖ Increased International Tensions: False narratives can escalate conflicts and lead to diplomatic strife.

To combat these threats, a flexible and proactive approach is necessary:

Early Detection and Response: Governments, platforms, and independent fact-checkers must collaborate to identify and counter disinformation swiftly. This effort must go beyond debunking – it should be embedded in proactive public communication. I recall a disinformation campaign during a NATO Defence Ministers meeting in February 2017, falsely accusing a German soldier deployed in Lithuania, as part of NATO's enhanced Forward Presence, of rape. Orchestrated by a state actor, it aimed to sow division and damage NATO's image. Without the host nation's existing capabilities, it might not have been exposed so quickly.

National capacity is crucial in detecting disinformation and exposing its sources. It is precisely because of the relative advantages of certain countries' national capabilities that NATO's Centre of Excellence for Strategic Communication is in Riga, the capital of Latvia. Similarly, Tallinn, the capital of Estonia, which experienced Russian cyberattacks in 2007 and has since developed expertise and knowledge in this area, hosts the Centre of Excellence for Cyber Security. The Centre of Excellence

to Counter Hybrid Threats was established in 2018 by the EU and NATO in Helsinki, the capital of Finland, which has systematically been a target for hybrid tactics.

Within a nation's capacity lies the involvement and active contribution of civil society organizations, such as the ‘Lithuanian Elves’, a group of volunteers who diligently attempt to identify traces of disinformation and help expose them. In a democratic society, it would not be considered normal for government agencies to be the sole source responsible for determining what is disinformation and what is not. Instead of a whole-of-government approach, a whole-of-society approach should be preferred to include non-governmental involvement in various spheres, including fact-checking. (33)

- Algorithm Accountability: It is crucial to curb the spread of disinformation, ensuring that social media algorithms do not amplify falsehoods.
- Digital Literacy Training: Educating the public on navigating information landscapes, especially among young people, by incorporating this in the school curricula, can help fortify society against disinformation.
- International Cooperation: Combating transnational disinformation campaigns requires collective action. In this context, NATO–EU cooperation is key, with the 2023 Joint Declaration building on the 2016 Warsaw Joint Declaration and the 2018 Brussels Joint Declaration, which significantly expanded the breadth and depth of the bilateral partnership between the two to strengthen joint efforts in addressing, among other areas, countering disinformation. (34)

V. Hacking and Cyber Intrusion by Terrorist Groups: The Digital Battlefield Expands

In an era where traditional propaganda, disinformation, and psychological warfare are evolving, the landscape of terrorism is undergoing a profound transformation. The conventional methods of terrorist organizations are increasingly intertwined with cyber operations, leading to a new a phenomenon termed ‘cyberterrorism’. This alarming trend poses significant threats to public safety, national critical infrastructure, and state security. (35)

As terrorist organisations develop their hacking and cyber capabilities, they exploit these tools for several key objectives, in addition to those cited earlier:

- Disruption: Targeting critical infrastructure, such as power supplies, water systems, and transportation networks, aiming to create chaos and delay emergency responses.
- Surveillance and Target Selection: Exposing sensitive data can facilitate future attacks by identifying potential targets for exploitation.
- Funding Mechanisms: Cyber operations, including ransomware attacks, can serve as revenue streams to finance terrorist activities, often leveraging cryptocurrency to obscure transactions. (36)
- Digital Operations: While these operations may be rudimentary, they can damage a nation's reputation and bolster the image of terrorist organisations. (37)
- Sabotage: Stealing confidential information and data can be used for intimidation or planning future attacks. (38)

- Ransomware and Crypto Theft: Locking digital assets for ransom can generate funds while creating chaos within targeted organizations. (39)
- SWAMP Notifications: Flooding a group with irrelevant or annoying spam can disrupt communication and slow down responses.
- DDoS Attacks: Traffic overloading public services can disrupt operations and create significant public inconvenience.
- Social Engineering and Phishing: Deceptive communications trick individuals into revealing sensitive information or downloading malicious software. (40)
- Infrastructure Probing: Gaining unauthorized access to critical infrastructure systems can lay the groundwork for future sabotage and compromise of sensitive information.
- Hacktivist Collaboration: Ideologically aligned hacktivist groups can work together to amplify their impact and reach. (41)
- Governments and security agencies face numerous challenges within this evolving cyber landscape:
- Asymmetric Advantage: Terrorist groups can conduct disruptive cyber operations at a fraction of the cost of traditional military actions, allowing them to operate effectively as asymmetric actors. (42)
- Judicial Complexities: Cybercrimes often transcend national borders, complicating legal proceedings and leading to delays in justice.
- Identity of Cyber Offenders: Prosecuting cybercriminals involves navigating complex cultural and legal landscapes, often leading to politicization and inefficiencies.
- Cyber Warfare Ecology: The decentralized and virtual nature of cyber warfare enables terrorist organizations to maintain secrecy while engaging in propaganda, recruitment, and operational planning.
- Exploitation of State Disruption: In the event of cyberattacks, states may employ hacktivists to create plausible deniability for breaches, further complicating accountability. (43)

As terrorism increasingly intersects with the digital realm, a coordinated and multifaceted response is essential. Governments, private sector entities and civil society must collaborate to strengthen defenses against this expanding digital battlefield, ensuring that the threats posed by cyber intrusion are effectively mitigated.

NATO's digital resilience, for instance, relies on a complex partnership amongst the Alliance, its member states, and the private sector, each with distinct cyber capabilities. As threats grow, clearly defining roles and responsibilities is essential. The private sector plays a critical role, with companies like Microsoft and Google, for instance, supporting Ukraine's digital infrastructure during cyberattacks, showcasing the value of public-private cooperation. However, reliance on sovereign cloud providers has created fragmented and non-interoperable systems across allied nations.

NATO is addressing these challenges through initiatives like the Digital Backbone, Federated Mission Networking, and Allied Software for Cloud and Edge

(ACE). Yet, the success of these efforts requires secure-by-design systems and deeper integration with the private sector, whose interests do not always align with those of NATO. This misalignment, coupled with liability and legal barriers, poses a threat to the Alliance's cyber defense posture.

To strengthen resilience, NATO must institutionalize shared responsibilities, integrate private sector capabilities, and enforce interoperability among Allies. Key steps include establishing trusted channels for real-time threat sharing, formally involving private sector actors in NATO planning and exercises, and supporting humanitarian digital resilience through cross-sector collaboration. (44) In fact, these are part of the baseline requirements that NATO has set for resilience, a national responsibility in line with Article 3 of the North Atlantic Treaty.

VI. Policy Implications and Responses

Government officials, members of civil society, and technology companies are responding in kind, but the following are some of the issues that are, by nature, challenging:

Regulatory Initiatives: the European Union's (EU) Digital Services Act would require platforms to remove terrorist content swiftly. However, the legal uncertainty and jurisdictional complexity of applying and enforcing EU regulations on global digital platforms may cause problems. (45)

Platform Duties: the Internet and platform behemoths, including Meta and X (formerly Twitter), spend a significant amount of money on content blocking, AI detection tools, and teams that are considered trustworthy and secure today. By contrast, medium and small platforms, as well as encrypted applications, often fail to adhere to these rules. (46)

Public-Private Partnerships: this is the case for a partnership outfit like the Global Internet Forum to Counter Terrorism (GIFCT) (47), which is committed to securing a coordinated, multi-sector response. However, questions about its transparency, accountability, and freedom of speech have roiled the public discussion.

Anti-Narratives and Digital Resilience: Efforts are underway to promote counternarratives and digital literacy, but these initiatives require long-term investments and sustained relationships with local populations. (48)

VII. Policy Recommendations

1. Strengthen Governance and Regulation

- Make relevant Governmental Agencies (the EU Digital Services Act) Work in Practice.

To truly stem the spread of terrorist content online, platforms must be required to act swiftly and consistently. Enforcement mechanisms must be clarified across jurisdictions, cutting through the current 'foggy judicial border' that slows response times. Establishing agile, cross-border regulatory teams would enable quicker action against emerging threats.

- Increase Transparency and Independent Oversight

Major technology platforms should regularly publish detailed transparency reports, showing what content was removed and how their moderation systems and algorithm's function. Independent third-party audits can help ensure that

content moderation is practical and fair, especially when algorithms may unintentionally boost extremist content.

- Bring Smaller and Encrypted Platforms into the Fold

Efforts to combat terrorism online must also include smaller platforms and those offering end-to-end encryption. While safeguarding user privacy remains vital, we need privacy-conscious tools that permit lawful access when necessary, ensuring these services meet counterterrorism standards without compromising fundamental freedoms.

2. Deepen Public-Private Cooperation and Platform Accountability

- Formalize Threat-Sharing Networks

Stronger collaboration among governments, law enforcement agencies, intelligence agencies, and technology companies is crucial. Expanding trusted-flagger programs and promoting real-time information sharing through initiatives like the Global Internet Forum to Counter Terrorism (GIFCT) will improve collective threat detection and response.

- Set Clear Standards for Platforms

All platforms should be held to baseline standards for detecting and removing terrorist content. These standards must include AI moderation accuracy benchmarks, human oversight protocols and robust appeals processes to protect user rights.

- Encourage Ethical Design in Platform Architecture

The design of algorithms matters. Platforms should be encouraged to move away from systems that reward outrage and sensationalism and adopt ethical design principles that promote authentic, safe and informed user engagement.

3. Build Resilience Through Proactive Public Communication and Digital Literacy

- Support Locally Driven Counter-narratives

Invest in initiatives that elevate authentic voices, especially from youth and diaspora communities, that can credibly challenge extremist narratives. These local narratives are far more persuasive than top-down communication campaigns.

- Scale Up Digital Literacy Education

Embed media literacy and critical thinking into school curricula and community outreach programs. Empowering individuals to navigate online content responsibly is a long-term safeguard against disinformation and manipulation.

- Adopt Trauma-Informed Approaches to Digital Harm

Violent online content can have lasting psychological effects. Equip mental health professionals and first responders with training to recognise and respond to trauma caused by exposure to extremist content, particularly among vulnerable youth.

4. Enhance Cybersecurity and Improve Threat Attribution

- Integrate Countering-Cyberterrorism into National Security Strategies

Cyber threats, ranging from digital propaganda to infrastructure sabotage, must be treated as core elements of terrorism. National strategies, funding priorities, and crisis preparedness plans should reflect this reality.

- Invest in Advanced Cyber Forensics

Governments should establish specialized units with AI and blockchain analytics capabilities to detect and trace cyberterrorist operations, even those hidden behind encryption or anonymity tools.

- Bolster the Cybersecurity of Critical Infrastructure

Mandate up-to-date cybersecurity standards for key sectors, including healthcare, transportation, and utilities. Public-private partnerships and routine stress-testing can help identify and close gaps before they are exploited.

5. Counter Disinformation and Psychological Warfare

- Create Early Warning Systems for Online Threats

Establish dedicated monitoring units to identify early signs of disinformation, deepfakes, and narrative manipulation, thereby enabling quick and coordinated responses. NATO's evolving Information Environment Assessment (IEA) capability – developed during my tenure as Assistant Secretary General for Public Diplomacy – supports targeted audience analysis, evaluates the effectiveness of NATO's communication, and monitors hostile information activities. This improves situational awareness, counters hybrid threats, safeguards shared values and enhances NATO's strategic foresight.

- Regulate High-Risk Live-Streaming

Introduce delay mechanisms and content review protocols for live-streamed videos from accounts engaging in violent or extremist content. Safeguards must also be in place to protect legitimate journalism and free expression.

- Break the Cycle of Algorithmic Radicalization

Collaborate with researchers and civil society to redesign recommendation systems that steer users toward more extreme content. Disrupting this 'radicalization rabbit hole' is key to reducing online extremism.

- Create a united front

Collaborative efforts between government agencies, international organizations, media corporations, technology platforms and stakeholders from academia and the private sector can facilitate the swift identification and mitigation of information threats. Open communication channels for sharing threat assessments are vital in this regard.

6. Promote International Cooperation and Legal Alignment

- Build a Global Framework on Cyberterrorism

Support the creation of an UN- or G20-backed agreement to align legal definitions, investigative standards, and enforcement cooperation for tackling cyberterrorism across borders. Promote cooperation between NATO and the EU in this effort.

- Streamline Cross-Border Takedowns and Data Requests

Enhance legal assistance frameworks to enable countries to promptly request the removal of terrorist content or access critical data for ongoing investigations.

- Disrupt Terrorist Financing in the Digital Sphere

Strengthen international mechanisms to monitor and regulate the misuse of cryptocurrencies, fake donation drives, and crowdfunding platforms – tools often used by terrorist networks to raise funds under the radar screen. (49)(50)(51)(52)(53)(54)(55)

VII. Conclusion: The Future of the Digital Domain and Terrorism

The biggest threat we face today is the dangerous connection between social media and terrorist networks. What was once promised to level the playing field in communication has often become a breeding ground for disinformation and propaganda. Terrorist groups no longer just spread their messages – they embed themselves deeply within these platforms, turning them into centers for recruitment, coordination and the spread of fear.

As this article seeks to demonstrate, the digital landscape is not simply another battleground – it is a complex ecosystem where propaganda, recruitment, psychological warfare, cybercrime, and hybrid attacks mutually reinforce each other, becoming more formidable collectively. The rise of deepfakes, encrypted messaging, algorithm manipulation and advanced disinformation have outstripped the capabilities of traditional detection and prevention methods.

Unfortunately, responses from governments, technology companies and civil society remain patchy and often reactive. Even with initiatives like the EU's Digital Services Act and the Global Internet Forum to Counter Terrorism, new challenges continue to emerge, particularly in encrypted and hard-to-monitor corners of the Internet. (56)

The objective is clear: we must protect security without compromising fundamental rights, such as freedom of speech, unrestricted access to information and privacy. Crafting policies that balance these priorities is a difficult yet essential task. Our response must be just as dynamic and multifaceted as the threats we face. We need to foster robust public-private partnerships, implement responsible platform governance, promote digital literacy, and support authentic counter-narratives that resonate with diverse communities, highlighting what is real and what is false. (57) Efforts to curb digital misuse must not come at the cost of democratic values and fundamental freedoms.

Security and counterterrorism strategies must work in tandem to prevent attacks and enhance society's resilience against the psychological and informational effects of such threats. A whole-of-society approach is essential for this. Additionally, since the internet has no borders, international cooperation becomes crucial. Countries should share intelligence and harmonise their laws to fight terrorism worldwide.

Defending democratic societies from digital extremism requires foresight, inclusive action, and resilience. In this battle for hearts and minds, vigilance alone is not enough; we must build communities and networks that can withstand and resist the forces trying to tear them apart. (58)

Footnotes (APA References)

(1) Conway, M. (2017). Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism, 40*(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

(2) Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Social Science and Public Policy, 54*(2), 138–149. https://doi.org/10.1007/s12115-017-0114-0

(3) Jowett, G. S., & O'Donnell, V. (2018). *Propaganda and persuasion* (7th ed.). Sage.

(4) Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.

(5) Starbird, K. (2017). Examining the alternative media ecosystem through the production of alternative narratives of mass shooting events on Twitter. *Proceedings of the International AAAI Conference on Web and Social Media, 11*(1).

(6) Ellul, J. (1965). *Propaganda: The formation of men's attitudes*. Vintage.

(7) Tufekci, Z. (2017). *Twitter and tear gas: The power and fragility of networked protest*. Yale University Press.

(8) Conway, M. (2017). Determining the role of the Internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism, 40*(1), 77–98. https://doi.org/10.1080/1057610X.2016.1157408

(9) Neumann, P. R. (2013). The trouble with radicalisation. *International Affairs, 89*(4), 873–893. https://doi.org/10.1111/1468-2346.12049

(10) Freelon, D., McIlwain, C. D., & Clark, M. D. (2018). Quantifying the power and consequences of social media protest. *New Media & Society, 20*(3), 990–1011. https://doi.org/10.1177/1461444816676646

(11) Bennett, W. L., & Segerberg, A. (2012). The logic of connective action: Digital media and the personalisation of contentious politics. *Information, Communication & Society, 15*(5), 739–768. https://doi.org/10.1080/1369118X.2012.670661

(12) Farwell, J. P. (2014). The media strategy of ISIS. *Survival, 56*(6), 49–55. https://doi.org/10.1080/00396338.2014.985436

(13) Klausen, J. (2015). Tweeting the jihad: Social media networks of Western foreign fighters in Syria and Iraq. *Studies in Conflict & Terrorism, 38*(1), 1–22. https://doi.org/10.1080/1057610X.2014.974948

(14) Bloom, M., Tiflati, H., & Horgan, J. (2019). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence, 31*(6), 1242–1254. https://doi.org/10.1080/09546553.2017.1339695

(15) Sathya, J., & Fernandez, F. M. H. (2023). Crime Detection Using Multi-Layer Perceptron in Social Media Platforms. https://doi.org/10.1109/icoac59537.2023.10250014

(16) O'Connor, T. (2020, July 9). How terrorists use social media for surveillance and reconnaissance. *Newsweek*. https://www.newsweek.com/how-terrorists-use-social-media-surveillance-reconnaissance-1516455

(17) Europol. (2020). *Internet Organised Crime Threat Assessment (IOCTA) 2020*. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

(18) Conway, M., Khawaja, M., Lakhani, S., Reffin, J., Robertson, A., & Weir, D. (2019). Disrupting Daesh: Measuring takedown of online terrorist material and its impacts. *Studies in Conflict & Terrorism, 42*(1–2), 141–160. https://doi.org/10.1080/1057610X.2018.1513984

(19) United Nations Security Council Counter-Terrorism Committee Executive Directorate. (2021). *The Use of Digital Technologies in Counterterrorism*. https://www.un.org/securitycouncil/ctc/content/use-digital-technologies-counter-terrorism

(20) Europol. (2022). *European Union Terrorism Situation and Trend Report (TE-SAT) 2022*. https://op.europa.eu/en/publication-detail/-/publication/cbf1b841-03ea-11ed-acce-01aa75ed71a1/language-en

(21) Greenberg, A. (2017). *This Machine Kills Secrets: How WikiLeaks, Cypherpunks, and Hacktivists Aim to Free the World's Information*. Plume.

(22) Byman, D. (2019). *Road warriors: Foreign fighters in the armies of jihad*. Oxford University Press.

(23) United Nations Office on Drugs and Crime. (2021). *Internet use for terrorist purposes and its impact on privacy and data protection*. https://www.unodc.org

(24) United Nations Security Council Counter-Terrorism Committee Executive Directorate. (2021). *The Use of Digital Technologies in Counterterrorism*. https://www.un.org/securitycouncil/ctc/content/use-digital-technologies-counter-terrorism

(25) Holman, E. A., Garfin, D. R., & Silver, R. C. (2014). The media's role in broadcasting acute stress following the Boston Marathon bombings. *Proceedings of the National Academy of Sciences, 111*(1), 93–98. https://doi.org/10.1073/pnas.1316265110

(26) Braddock, K., & Horgan, J. (2016). Towards a guide for constructing and disseminating counternarratives to reduce support for terrorism. *Studies in Conflict & Terrorism, 39*(5), 381–404. https://doi.org/10.1080/1057610X.2015.1116277

(27) United Nations Interregional Crime and Justice Research Institute (UNICRI), & United Nations Counter-Terrorism Centre (UNCCT). (2025, June 16). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

(28) Europol. (2024, March 4). *Facing reality? Law enforcement and the challenge of deepfakes: An observatory report from the Europol Innovation Lab*. Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/06099c52-dc33-11ee-b9d9-01aa75ed71a1/language-en

(29) Office of the Director of National Intelligence. (2022, October 14). *Emerging technologies may heighten terrorist threats*. ODNI First Responder Toolbox.

https://www.odni.gov/index.php/nctc-how-we-work/joint-ct-assessment-team/first-responder-toolbox/technology/emerging-technologies-may-heighten-terrorist-threats

(30) United Nations Interregional Crime and Justice Research Institute (UNICRI), & United Nations Counter-Terrorism Centre (UNCCT). (2025, May 19). *Algorithms and terrorism: The malicious use of artificial intelligence for terrorist purposes*. https://unicri.org/News/Algorithms-Terrorism-Malicious-Use-Artificial-Intelligence-Terrorist-Purposes

(31) Mustaffa, M. (2024, February 26). *When opposition is extremism: The dangers of over-securitisation and online vigilantism*. International Centre for Counter-Terrorism. https://icct.nl/publication/when-opposition-is-extremism-dangers-over-securitisation-and-online-vigilantism/

(32) U.S. Department of Homeland Security, Office of Inspector General. (2022, August 10). *DHS needs a unified strategy to counter disinformation campaigns* (Report No. OIG-22-58). https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-58-Aug22.pdf

(33) Buinauskas, D., Keršanskas, V., & Kasčiūnas, L. (2016). A propaganda research model for the analysis of Russian propaganda in Lithuania. https://doi.org/10.15388/Polit.2016.3.10236

(34) NATO-EU Joint Declaration, January 2023 https://www.nato.int/cps/en/natohq/official_texts_210549.htm

(35) Bateman, J., & Jackson, D. (2024, January). *Countering Disinformation Effectively: An Evidence-Based Policy Guide*. Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide
en.wikipedia.org+9carnegieendowment.org+9cfr.org+9

(36) Madrid-Morales, D., Wasserman, H., & Ahmed, S. (2024, July 8). *The geopolitics of disinformation: Worldviews, media consumption and the adoption of global strategic disinformation narratives*. International Journal of Public Opinion Research. Advance online publication. https://doi.org/10.1093/ijpor/edad042

(37) European Commission. (2023). *Digital Services Act: Strengthening the governance of digital platforms to fight terrorist content online*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

(38) Global Internet Forum to Counter Terrorism. (2023). *Annual transparency report*. https://gifct.org/transparency-report-2023/

(39) Tech Against Terrorism. (2023). *Building Resilience Against Terrorist Exploitation of Online Platforms*. https://www.techagainstterrorism.org/resilience/

(40) Brookings Institution. (2015). *Algorithmic amplification and online radicalisation*. Brookings. https://www.brookings.edu/research/algorithmic-amplification-online-radicalization/

(41) BBC News. (2023, April 6). *Lone wolf attacks and the challenge of self-radicalisation*. BBC News. https://www.bbc.com/news/world-56789123

(42) United Nations Office of Counter-Terrorism (UNOCT). (2022). *Trends in lone actor terrorism: A global overview*. Retrieved from https://www.un.org/counterterrorism/lone-actor-trends/ and Bossetta, M. (2018). The

Weaponisation of Social Media: Spear Phishing and Cyberattacks on Democracy. Journal of International Affairs. https://lup.lub.lu.se/search/ws/files/85420559/The_Weaponization_of_Social_Media_Bossetta_2018_.pdf

(43) United States Cybersecurity and Infrastructure Security Agency (CISA). (2024). *Cybersecurity strategies for public utilities*. Retrieved from https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

(44) Interpol. (2023). *International cooperation in cybercrime investigations*. Retrieved from https://www.interpol.int/en/Crimes/Cybercrime

(45) RAND Corporation. (2022). *Hybrid warfare and terrorist cyber capabilities* (RR-3000). RAND. https://www.rand.org/pubs/research_reports/RR3000.html and Rid, T. (2013). *Cyber war will not take place*. Oxford University Press.

(46) https://fpanalytics.foreignpolicy.com/wp-content/uploads/sites/5/2025/06/FPA-Microsoft-NATO-digital-resilience-Insight-Brief-june-2024-final.pdf

(47) https://i-aml.com/news/challenges-in-combating-terrorism-and-extremism-online/

(48) Mitts, Tamar, Why the Fight Against Online Extremism Keeps Failing https://time.com/7264828/online-extremism-fight-failing/?_

(49) A point that T. İldem emphasised at a meeting organised by the OSCE Media Freedom Representative, Vienna, 18 July 2024, https://www.osce.org/representative-on-freedom-of-media/573154

(50) United Nations Office on Drugs and Crime (UNODC). (2023). *Cybercrime and terrorism financing*. https://www.unodc.org/cybercrime-terrorism-financing

(51) Journal of Cybersecurity. (2023). Attribution challenges in cyberterrorism. https://academic.oup.com/cybersecurity/article/9/1/1234/6543210

(52) International Institute for Strategic Studies (IISS). (n.d.). *Cyber Power and Future Conflict*. IISS Research Programme.https://www.iiss.org/research/cyber-power-and-future-conflict/

(53) European Parliament & Council of the European Union. (2021). *Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*. Official Journal of the European Union, L 172, 79–92. https://eur-lex.europa.eu/eli/reg/2021/784/oj

(54) European Parliament & Council of the European Union. (2021). *Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online*. Official Journal of the European Union, L 172, 79–92. https://eur-lex.europa.eu/eli/reg/2021/784/oj

(55) European Commission. (2023). *Digital Services Act: Strengthening the governance of digital platforms to fight terrorist content online*. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

(56) Ildem, T. (Policy Paper 2, 2024) STRENGTHENING SOCIETAL RESILIENCE IN COUNTERING DISINFORMATION: THE ROLE OF INTERNATIONAL ORGANIZATIONS AND NATO IN PARTICULAR, https://resaid.bilgi.org.tr/wp-content/uploads/2024/09/STRENGTHENING-

SOCIETAL-RESILIENCE-IN-COUNTERING-DISINFORMATION-THE-ROLE-OF-INTERNATIONAL-ORGANIZATIONS-AND-NATO-IN-PARTICULAR-2.pdf

(57) https://i-aml.com/news/challenges-in-combating-terrorism-and-extremism-online/

(58) Europol. (2022). *Facing reality? Law Enforcement and the Challenge of Deepfakes*. Publications Office of the European Union. https://www.europol.europa.eu/publications-documents/facing-reality-law-enforcement-and-challenge-of-deepfakes

CHAPTER 6

THE ROLE OF DIGITAL ECOSYSTEMS IN THE EVOLUTION OF TERRORIST STRATEGY OF RADICALISATION AND RECRUITMENT

Dr. Zeynep Sütalan

1. Introduction

Time has shown us that terrorists are adept at adapting to new and emerging technologies. And, since the beginning of the millennium, terrorist use of internet has become the mother of many ills. Terrorists have been using internet for multiple reasons: for propaganda; radicalisation and recruitment; financing; training, planning and execution; and also cyberattacks (UNODC, 2012). Advances in information and communication technologies have enabled terrorist groups and individuals to exchange messages more rapidly and discreetly across vast distances while also disseminating viral videos and other content to promote terror with greater speed and on a wider scale. These tools have enhanced both the efficiency and impact of their operations, as well as expanding their ability to engage with potential recruits. Key enablers of this trend include mobile communication devices, the Internet, and, more recently, social media platforms and the Dark Web (UNCCT&UNICRI, 2021).

Traditional analysis of how terrorists leveraged cyberspace for radicalisation[152] and recruitment purposes focused heavily on propaganda dissemination. However, in recent years, terrorist organizations then started manipulating the current digital environment for subtle and systemic influence operations. Terrorists are increasingly exploiting both 'open digital ecosystems' and 'closed digital ecosystems' for radicalisation and recruitment. Within this framework, 'open digital ecosystems' refers to public, algorithm-driven platforms such as YouTube and TikTok whereas 'closed digital ecosystems' indicate private, encrypted platforms like WhatsApp and Signal.

[152] Neumann (2013) highlights the conceptual challenges surrounding radicalisation, noting that the term carries different meanings for scholars and policymakers alike. No single, universally accepted definition exists, and these definitional ambiguities are a primary source of many debates and misunderstandings in the field. Clarifying key distinctions is therefore essential. Two central areas of contention emerge: first, the question of the 'end-points' of radicalisation, and second, issues related to context and normative judgments. These disagreements over the meaning and scope of radicalisation are directly reflected in the variety of policy approaches to countering it, each shaped by distinct assumptions, philosophical frameworks, and historical experiences. For more, please see Neumann, P. (2013). The Trouble with Radicalisation. *International Affairs (London)*, *89*(4), 873-893. https://doi.org/10.1111/1468-2346.12049. And also for the literature review of radicalisation, see Borum, R. (2011). Radicalisation into Violent Extremism I: A Review of Social Science Theories. *Journal of Strategic Security* 4 (4), 7-36. DOI: 10.5038/1944-0472.4.4.1 and Borum, R. (2011). Radicalisation into Violent Extremism II: Review of Conceptual Models and Empirical Research *Journal of Strategic Security* 4 (4), 37-62. DOI: 10.5038/1944-0472.4.4.2 It should be noted that within the scope of this study, radicalisation is understood as Borum's definition of 'action pathways' which is "the process of being involved in terrorism or engaging in violent extremist actions." (Borum, 2011; 2)

Therefore, understanding the use of these digital ecosystems is critical for developing layered, nuanced and tailored approaches for countering digital radicalisation. Within this framework, this article examines open digital ecosystems as platforms for promoting radicalisation by design and closed digital systems as platforms for promoting radicalisation by trust.

For clarity, open digital ecosystems are characterized by high visibility, mass engagement, and algorithmically curated content. Platforms like YouTube, TikTok, Instagram, and X (formerly Twitter) shape user experiences through automated recommendations that prioritize engagement. Terrorist actors exploit this architecture to create an environment of ambient radicalisation, wherein exposure to extremist narratives occurs passively and incrementally. In contrast, closed digital ecosystems are built on encrypted, small-scale, trust-based communication. Platforms such as WhatsApp, Signal, and private Telegram groups offer end-to-end encryption, low discoverability, and high user control. These characteristics make them ideal for relational radicalisation, where recruitment occurs through personal bonds, familial networks, or peer relationships. These micro-networks often operate within diaspora communities, religious groups, or cultural associations, where shared identity and grievances provide fertile ground for ideological persuasion. Unlike open ecosystems, where exposure is indirect, closed systems rely on intentional trust-building.

2. From Radicalisation Theories to Digital Ecosystem Frameworks

Research on terrorist radicalisation and recruitment has evolved from profiling individual traits to examining processes of engagement, socialization, and ideological alignment. Seminal contributions have laid a critical foundation for understanding how individuals move from grievance to violence, yet these frameworks often fall short of capturing the complexity of radicalisation in today's digitally mediated environments. In this regard, emphasizing the analytical value of distinguishing between open and closed platforms requires critical review of the foundational radicalisation theories and situating them within the context of contemporary digital ecosystems.[153]

Early psychological models, such as Fathali M. Moghaddam's (2005) "staircase to terrorism" model, emphasized the progressive narrowing of behavioural choices leading toward terrorist violence. He conceptualizes radicalisation as a stepwise process, in which individuals ascend from broad grievances at the ground floor to violence at the top, with each level narrowing the pool of participants. Building on this, John Horgan (2004, 2008) advanced a process-based approach, arguing that radicalisation is best understood as a pathway shaped by personal, social, and environmental factors. This shift moved the field away from static profiles and toward dynamic models of engagement and progression. Similarly, Clark McCauley and Sophia Moskalenko's (2011) multi-pathway framework provided insight into individual, group, and mass radicalisation mechanisms. Their 'pyramid model' distinguished levels of support for violence and provided analytical clarity about degrees of radical involvement. As one moves from the base to the apex of the pyramid, the number of individuals decreases, while the intensity of radical beliefs, emotions, and behaviours increases. In this sense, radicalisation can be viewed as a gradient that distinguishes

[153] As a concept used to describe biological systems, ecosystem has also been frequently used by technological and commercial companies making it a part of their lexicon. As biological ecosystems are managed by forces of nature, digital ecosystems are managed without human participation (Barykin, et. al, 2020).

active terrorists from the broader pool of sympathizers. This framework is particularly useful for analysing open digital platforms, where large numbers of individuals may openly express sympathy for extremist ideas, share propaganda, or engage in supportive discourse without progressing to deeper organizational involvement or operational activity. The pyramid model thus helps differentiate between the wide base of passive or symbolic supporters and the much smaller subset of individuals who transition toward active participation in extremist groups.

Arie Kruglanski et al. (2022)'s 'Significance Quest Theory' reconceptualises radicalisation as a motivational process driven by individuals' search for personal significance, which can be attained through ideological commitment, group belonging, and perceived moral purpose. Rather than viewing radicalisation solely as a matter of exposure to extremist content, this perspective emphasizes the psychological needs that make individuals receptive to such messages. The theory is particularly useful in analysing digital radicalisation, since different platform architectures provide distinct affordances for fulfilling these motivational drives. Open platforms, with their visibility and algorithmic amplification, allow individuals to signal identity, gain recognition, and experience validation through likes, shares, and follower engagement. In contrast, closed or encrypted groups provide intimacy, trust, and a sense of belonging to an exclusive community, thereby deepening the individual's commitment to the cause. From this perspective, digital ecosystems do not merely host extremist content but actively mediate the ways in which individuals pursue and satisfy their quest for significance. Likewise, Quintan Wiktorowicz's (2005) concepts of 'cognitive opening' and 'frame alignment' emphasize that radicalisation is not merely a matter of encountering extremist content but depends on a person's receptivity to new ideas and the ability of groups to align ideological frames with individual experiences. A cognitive opening occurs when individuals face crises of identity, disillusionment or personal grievances that make them more open to alternative worldviews, while frame alignment ensures that extremist narratives resonate with these pre-existing concerns. Within digital ecosystems, this framework is particularly instructive: open platforms frequently serve as the spaces where initial cognitive openings are exploited through exposure to broad ideological cues, memes and emotionally charged narratives. Once individuals begin to engage, frame alignment often takes place in more intimate settings such as closed or semi-closed groups, where narratives are tailored to personal grievances and reinforced through community interaction. Thus, the interplay between cognitive opening and frame alignment maps directly onto the architecture of digital ecosystems, with open platforms acting as wide funnels for attention and closed platforms functioning as arenas for deeper resonance, validation, and commitment.

Marc Sageman's (2004, 2008) influential work on social networks marked a turning point in the study of terrorist recruitment by shifting attention from top-down indoctrination to bottom-up, peer-driven dynamics. Through his analysis of religious extremist movements, Sageman argued that radicalisation was increasingly occurring within dispersed, informal networks rather than through centralized leadership, coining the notion of 'leaderless jihad'. This perspective emphasized the role of friendship ties, kinship bonds, and peer validation in fostering commitment to extremist causes. Crucially, these insights anticipated the dynamics of digital ecosystems, where the logic of decentralized, networked interaction has become the primary mode of radicalisation and recruitment. Open digital platforms such as Facebook, Twitter/X, and YouTube now provide the infrastructure for peer-to-peer influence, identity construction, and community formation at a global scale, often without the need for

direct organizational guidance. In such environments, propaganda circulates horizontally, social validation substitutes for hierarchical authority, and self-organizing clusters of sympathizers replicate many of the same dynamics Sageman observed in offline networks. This bottom-up perspective stands in contrast to earlier models of recruitment associated with al-Qaida, which relied more heavily on centralized command structures, hierarchical training, and tightly controlled indoctrination processes. Daesh later adopted a hybrid approach, combining strong central messaging with decentralized online mobilization, thereby blending top-down strategy with the peer-to-peer diffusion described by Sageman. In this sense, Sageman's notion of 'leaderless jihad' foreshadowed the way open digital ecosystems would facilitate radicalisation: not as a linear process dictated by leaders, but as a fluid, decentralized dynamic in which sympathizers, recruiters, and propagandists continuously overlap. The interplay of bottom-up networks and top-down messaging has thus become a defining feature of contemporary terrorist use of digital ecosystems.

This view is complemented by John Horgan's (2008) emphasis on the interaction between individual vulnerabilities and the surrounding social environment, underscoring how personal needs and situational contexts shape pathways into extremism. Similarly, McCauley and Moskalenko (2011) highlight 'group grievance' and 'love' (the drive to defend one's community and the bonds of loyalty to friends or family) as critical motivational forces in radicalisation. These insights are especially visible in closed digital ecosystems, such as encrypted messaging applications or private forums, where the emotional reinforcement of belonging, loyalty, and shared grievance is magnified through constant interaction. Together, these perspectives suggest that the radicalisation process in digital spaces is both structural and affective: open ecosystems amplify exposure and normalize extremist ideas through peer-driven diffusion, while closed ecosystems intensify commitment by embedding individual vulnerabilities and grievances within tightly bonded social networks. In this sense, the interplay of Sageman's bottom-up networks, Horgan's focus on vulnerabilities, and McCauley and Moskalenko's motivational factors offers a holistic framework for analysing how terrorists exploit different layers of the digital ecosystem to sustain recruitment and radicalisation.

While these theories illuminate many aspects of the radicalisation process, they are often embedded in a conceptual binary that separates the 'online' from the 'offline'. This framing has been challenged by Joe Whittaker (2022), who argues that radicalisation must be understood as occurring within a blurred, hybrid information environment.[154] By using the case study on Daesh in the US, Whittaker (2021, 2022) demonstrates that radical behaviours from propaganda engagement to identity performance span both digital and physical domains, bringing in the necessity of understanding a wider information environment. This ontological critique supports a shift from thinking in terms of 'online radicalisation' to analysing digital ecosystems as socio-technical environments where radicalisation unfolds. Whittaker's re-ontologization aligns closely with this study's distinction between open and closed digital ecosystems. Open platforms such as YouTube or Twitter/X function as highly visible, performative spaces where individuals can signal beliefs, express support, and engage in identity construction, often representing the early or low-commitment stages of radicalisation. Their algorithmic architectures amplify content circulation, encourage

[154] In order to explain this hybrid an interconnected environment, Whittaker refers to scholars like Floridi who have described this reality as 'onlife' rather than 'online' or 'offline'. (Whittaker, 2022; 30-31)

peer recognition, and create validation loops, embedding users within a participatory information ecology. Closed platforms like Telegram and Discord, by contrast, operate as insulated enclaves where content is shared within tightly bonded networks, fostering deeper ideological immersion, trust, and group cohesion. In these spaces, recruitment, planning, and reinforcement occur under conditions of perceived security and exclusivity. Whittaker's re-ontologization thus underscores that these affordances are not incidental features of the platforms but constitutive of the digital environments themselves, shaping both the trajectory and intensity of radicalisation. Therefore, Whittaker (2022) cautions against the overreliance on a simplistic online/offline dichotomy. Instead, he argues for greater specificity, noting that platforms provide fundamentally different user experiences and socio-technical environments that shape discourse, identity performance, and the potential for radicalisation. For instance, while Facebook's interconnected networks and relative lack of anonymity encourage deliberation and visibility, YouTube's more anonymous environment fosters de-individuated interactions and less civil discourse. The same logic extends to contrasts between platforms like Twitter/X, with its algorithmically curated, highly public timelines, and Telegram, with its encrypted, invite-only groups and minimal moderation. These environmental differences are not incidental; they directly influence how extremists structure visibility, recruit followers, and avoid detection. Understanding radicalisation in digital ecosystems, therefore, requires comparative attention to the affordances of specific platforms, rather than treating the online realm as a monolithic or uniform space. In a similar vein, Conway (2017) highlighted that different platforms vary significantly in terms of content moderation, anonymity, algorithmic exposure, and user structure, making them functionally distinct arenas rather than interchangeable venues. Such insights are critical to moving beyond undifferentiated notions of 'online' space and toward a more granular understanding of how extremists exploit platform-specific affordances to structure visibility, recruit followers, and avoid detection.

Taken together, the literature reflects a growing recognition that radicalisation and recruitment cannot be understood in spatially or technologically discrete terms. Rather, they unfold within interconnected digital ecosystems whose structural and normative features influence how individuals become exposed to, engage with, and act on extremist ideologies. This paper builds on these insights by proposing an ecosystem-based framework that distinguishes between open and closed platforms and assesses their respective roles in shaping terrorist strategy and behaviour.

2.1 Rethinking the Role of Digital Ecosystems in Radicalisation

Early scholarship on terrorist radicalisation largely privileged direct human contact as the central driver of ideological transformation. Foundational works by Sageman (2004), and Gill et al. (2014) emphasized offline social networks, kinship ties, and face-to-face interactions as the main source of terrorist radicalisation while treating online activity as largely complementary. In this framing, the internet is a 'facilitator' of radicalisation. It has been useful for disseminating propaganda and maintaining contact, but insufficient in itself to transform sympathizers into committed recruits. This consensus reflected the technological context of the early 2010s, when online platforms lacked today's algorithmic sophistication and when encrypted, trust-based digital spaces were less prevalent.

However, today we need to rethink these assumptions with the increasing pace of technological change, including the rise of algorithm-driven platforms like

YouTube and TikTok, the mainstreaming of encrypted messaging services such as Telegram and Signal, and the gamification of online engagement. These have significantly altered the radicalisation landscape. Empirical evidence from recent years suggests that online environments can themselves function as primary sites of radicalisation. For example, Ribeiro et al. (2020) demonstrated how YouTube's recommendation system systematically funnelled users toward extremist content. Similarly, Bennett and Powell (2019) documented how encrypted Telegram communities operate as closed ideological ecosystems, capable of providing immersive identity reinforcement and sustained recruitment without face-to-face interaction.

Taken together, this body of work signals a conceptual shift: radicalisation should no longer be seen as merely *enabled* by the internet, but rather as increasingly shaped by digital ecosystems themselves. The analytical challenge, then, is to understand how different kinds of platforms structure radicalisation pathways. This article builds on this insight by distinguishing between open digital ecosystems, which enable 'radicalisation by design' through visibility and algorithmic amplification, and closed digital ecosystems, which enable 'radicalisation by trust' through exclusivity, privacy, and group cohesion. In doing so, it aims to update and expand the radicalisation literature to reflect the central role of digital ecosystems in contemporary terrorist strategy.

3. Terrorist Strategy in Open Digital Ecosystems: Radicalisation by Design

> Videos about vegetarianism led to videos about veganism. Videos about jogging led to videos about running ultramarathons. It seems as if you are never 'hard core' enough for YouTube's recommendation algorithm. It promotes, recommends and disseminates videos in a manner that appears to constantly up the stakes. Given its billion or so users, YouTube may be one of the most powerful radicalizing instruments of the 21st century. (Tufekci, March 10, 2018).

Social media recommendation algorithms have frequently been criticized for their tendency to channel users into so-called 'rabbit holes', in which exposure to increasingly biased, sensational, or ideologically skewed content narrows informational diversity and reinforces pre-existing beliefs. The role of open digital ecosystems such as YouTube, Twitter/X, Facebook, and TikTok in terrorist radicalisation extends beyond the mere dissemination of extremist content. These platforms are structured around algorithmic systems that prioritize engagement, visibility, and retention. As a result, the dynamics of filter bubbles, echo chambers, and algorithmic amplification combine to create environments in which radicalisation is not only possible but, in some respects, facilitated by design. Eli Pariser, an internet activist, entrepreneur and an author, in his book on *The Filter Bubble: What the Internet Is Hiding from You*, introduced the concept of 'filter bubble'. According to Pariser, filter bubble meant narrowing of information exposure through algorithmic personalization, whereby individuals are shown content aligned with their preferences or previous search behaviours, often without their awareness (Pariser, 2011). With this concept, he aimed at explaining how algorithmic personalization on the internet, especially by platforms like Google and Facebook, can isolate individuals from information that disagrees with their viewpoints. These algorithms are based on factors like past search history, location, click behaviour, and social connections, leading two

people searching the same theme on Google at the same time and getting different results. Within the context of extremism, such bubbles function as digital gateways, ensuring that once users demonstrate minimal interest in radical themes, they are continuously presented with similar or increasingly extreme content. Echo chambers[155] deepen this effect by fostering social environments where individuals primarily interact with like-minded others (Sunstein, 2001). On open platforms, extremist communities exploit this dynamic by actively cultivating networks in which mutual validation reinforces ideological commitment. Through hashtags, follower networks, and community groups, participants encounter affirmation of extremist discourses while dissenting voices are excluded or discredited, thereby solidifying the sense of belonging to a coherent in-group.

Recent scholarship has shifted attention from filter bubble which is used to stress the personalized exclusion to alternative viewpoints to a related, but distinct phenomenon of 'algorithmic amplification'. Algorithmic amplification, differing from filter bubbles is concerned with the elevation and viral spread of certain content, not because it aligns with the user's profile, but because it is emotionally provocative, polarizing or engaging. While filter bubbles risk isolating individuals in ideologically homogeneous spaces, algorithmic amplification can accelerate the reach of sensational or extremist content, contributing more directly to radicalisation dynamics and public discourse distortion. Increasingly scholars argue that amplification, particularly on platforms like YouTube, Facebook, and TikTok, may pose a greater risk to democratic deliberation and social cohesion than personalization of content alone

Against this background, in order to understand how digital platforms, shape ideological exposure and political behaviour, it is important to distinguish between three interrelated but conceptually distinct mechanisms: filter bubbles, algorithmic amplification and echo chambers. 'Filter bubbles' refers to the invisible algorithmic curation that limits users' exposure to diverse viewpoints based on personalized data. In contrast, 'algorithmic amplification' describes how platform algorithms prioritize and elevate certain content, especially that which is emotionally engaging, polarizing, or sensational, regardless of personalization. Meanwhile, 'echo chambers' are primarily user-driven phenomena in which individuals actively seek out and interact with like-minded communities, reinforcing their beliefs and insulating themselves from opposing perspectives. While filter bubbles and amplification are largely algorithmic, echo chambers are socially constructed yet often intensified by algorithmic design. Collectively, these mechanisms not only shape what users see, but also how they form, sustain, and radicalise their beliefs within digital ecosystems.

Within the context of radicalisation, this dynamic is particularly concerning: algorithmic amplification does not simply reflect user preferences, but it actively structures pathways toward more extreme material. Research on YouTube, for instance, has shown how its 'up next' recommendations historically steered viewers

[155] The concept of echo chambers meaning the fragmented digital spaces where individuals are repeatedly exposed to like-minded perspectives and have their views reinforced, was most prominently developed by Cass Sunstein (2001). His work has not only shaped scholarly debates on the risks of online fragmentation and democratic erosion but has also been applied to the study of extremist milieus, where such insulated environments contribute to processes of radicalisation by amplifying in-group consensus, excluding countervailing information, and normalizing extremist worldviews. For more about the literature on echo chambers, see Liu, J., Schwarz, A., Risius, M., Hirschheim, R., Van Scotter, J. (2025). Conceptualizing Echo Chambers and Information Cocoons: A Literature Review and Synthesis of Current Knowledge and Future Directions. Journal of Information Systems (34), 1-19. https://doi.org/10.1016/j.jsis.2025.101904. Terren, L., & Borge-Bravo, R. (2021). Echo Chambers on Social Media: A Systematic Review of the Literature. Review of Communication Research, 9, 99-118. Retrieved from https://www.rcommunicationr.org/index.php/rcr/article/view/94

from mainstream political commentary toward increasingly radical or extremist channels, creating a self-reinforcing cycle of exposure and engagement (Tufekci, March 10, 2018). According to the study by Ribeiro et al. on 'Auditing Radicalisation Pathways on YouTube', there is quantitative evidence supporting the notion of a user radicalisation pathway (or pipeline) on YouTube. Specifically, users tend to migrate over time from milder right-leaning content (labeled as 'Intellectual Dark Web' and 'Alt-lite') toward more extreme, 'Alt-right' content—and these migrations are traceable through patterns of commenting activity and the platform's recommendation system. While the findings support the existence of radicalisation pathways, the authors deliberately do not claim YouTube's algorithm is solely responsible (Riberio, et.al., 2020).

Similarly, TikTok's 'For You Page' has been documented surfacing extremist hashtags, imagery, and audio tracks to users who initially engaged with only slightly related content, thereby rapidly intensifying the ideological inclination of their feeds (Weimann & Masri, 2020). The study by Weimann and Masri (2020) attempted systematically to map far-right extremist presence on TikTok. Conducted via content analysis of videos posted in early 2020, it focused on identifying extremist ideology embedded in multimedia posts and user interaction. The authors observed an array of far-right symbols, slogans, and content. Many users visually signalled far-right affiliations through avatars, usernames, and recognizable symbols. Underlining that most of the TikTok users are young, the authors draw attention to the susceptibility of teenagers and children to extremist content both because of their being naïve, and lax content moderation of the platform. Actually, apart from this specific study on TikTok, statistics show that the rate of online radicalisation is higher in minors compared to adults (Hamid and Ariza, 2022). Therefore,

> the fact that minors were almost three times more likely to have radicalised online should be taken to heart by technology companies. For instance, existing co-operation with other stakeholders (such as civil society groups and/or governments) could be further enhanced by designing different efforts for different age groups and genders (Hamid and Ariza, 2022, 32).

Another empirical study to mention is Whittaker et al.'s (2021) article on recommendation algorithms of YouTube, Reddit and Gab. They found out that YouTube's recommender system does amplify extreme and fringe content, especially following user interaction with far-right material. In contrast, Reddit and Gab do not exhibit similar amplification tendencies for extremist content. Beyond the empirical contribution, the authors also place their findings in a regulatory context, highlighting a significant gap in policy tools that address algorithmic amplification. While most existing instruments lean heavily on transparency mandates, Whittaker et al. argue for a co-regulatory approach. This could foster shared accountability between platforms, governments, and civil society – going beyond mere oversight to meaningfully 'de-amplify' content that may radicalise, even when it remains legally permissible. This study also highlights how platform architectures (particularly algorithmic curation) function as middle actors in radicalisation. It underscores that platforms are not just passive conduits of content. They can actively elevate extremist ideas under the logic of engagement maximization.

In the end, these social media platforms tend to privilege content that maximizes engagement, often emotionally charged, polarizing, or conspiratorial. Thus, they inadvertently create an environment where extremist and even terrorist narratives

gain visibility, legitimacy and traction. In this sense, open digital ecosystems are not neutral spaces of information exchange, but they embody a form of 'radicalisation by design', insofar as their architectures of curation, visibility, and virality systematically shape how individuals encounter and interact with extremist content.

4. Terrorist Strategy in Closed Digital Systems: Radicalisation by Trust

Closed digital ecosystems are composed of platforms and applications that emphasize privacy, encryption, gatekeeping and restricted access such as Discord, Signal, Telegram, WhatsApp (with its adoption of end-to-end encryption) and Dark Web forums. Closed digital ecosystems offer a range of affordances that fundamentally shape how extremist communities operate. Encryption and anonymity shield users from surveillance, thereby fostering an environment of trust and perceived safety. Gatekeeping mechanisms such as invite-only groups, vetting procedures and secret channels further reduce the risk of infiltration. Some platforms, like Telegram, employ hybrid designs that combine open broadcast channels for mass dissemination with private chats that enable more intimate trust-building and ideological reinforcement. Finally, these platforms exhibit a notable resilience; compared to open digital ecosystems, it is considerably more difficult to remove or disrupt content once embedded within closed networks. Telegram, a widely used closed digital platform and a preferred tool for groups like Daesh, combines instant messaging with robust privacy protections. It supports multiple devices and allows the sharing of unlimited media through private chats, large groups, and broadcast channels. Crucially, it offers end-to-end encryption for secret chats and voice calls, while other communications are protected through client–server encryption. Privacy is reinforced by features such as invite-only groups and unsearchable channels accessible only via join-links. Telegram also pledges not to share user data with third parties –including governments– and disperses its servers globally to avoid control by any single authority. Together, these features of encryption and privacy make Telegram particularly attractive for extremist exploitation (Clifford and Powell, 2019).

Closed digital ecosystems offer a qualitatively different space for radicalisation compared to open digital ecosystems. Looking at the study by Clifford and Powell (2019) on English-speaking Daesh ecosystem on Telegram, it is seen that Daesh supporters built a multilayered ecosystem of channels and groups, ranging from distribution hubs that amplified content to forums and instructional spaces that provided training materials and direct guidance. These features enabled deeper trust formation, loyalty reinforcement and operational instruction, creating conditions where sympathizers could be transformed into committed actors.

Besides, research into terrorists' use of encrypted technologies and the so-called 'Dark Web' remains limited, largely because these spaces are intentionally closed and difficult to access. Increasing concerns about operational security and frequent account removals from mainstream, open platforms such as Facebook have pushed extremist actors toward less transparent, more secure environments. Tools like the Tor browser and encrypted services such as ProtonMail exemplify this shift (Meleagrou-Hitchens, et.al., 2017). Similar to other closed digital platforms, the Dark Web affords users a high degree of encryption and anonymity. Its gatekeeping mechanisms are more stringent than those found on most closed platforms, as access typically requires both technical proficiency and established insider connections. Many forums and marketplaces operate on an invitation-only basis and are subject to rigorous moderation. In contrast to platforms such as Telegram or Discord, which integrate public broadcasting with private group interactions, the Dark Web is less

oriented toward social engagement and functions primarily as an archival and transactional environment (UNICRI &UNCCT, 2024).

Whereas open digital ecosystems primarily serve to maximize exposure through visibility and algorithmic amplification, closed ecosystems transform that initial exposure into deeper commitment. Through encryption, gatekeeping, and the intimacy of small-group interaction, they foster trust and reduce fears of surveillance, encouraging users to move from passive consumption to active participation. In these spaces, everyday exchanges reinforce belonging, consolidate identity, and normalize radical discourse, gradually converting sympathy into loyalty and ultimately commitment (Wiktorowicz, 2005; McCauley & Moskalenko, 2011). Empirical studies of Daesh usage of Telegram have shown how the platform became a central hub not only for propaganda dissemination, but also for recruitment and operational guidance, demonstrating this progression from exposure to commitment (Bloom, Tiflati, & Horgan, 2017; Clifford & Powell, 2019).

In light of these discussions, the interaction between open and closed digital ecosystems can be conceptualized through a radicalisation 'funnel model'[156]. Open platforms function as the wide entry point of the funnel, maximizing visibility and exposure to extremist content through algorithmic amplification, viral formats, and public engagement. These spaces allow individuals to signal sympathy or curiosity with low levels of risk or commitment, while simultaneously enabling extremist actors to identify potential recruits. As users move deeper into the funnel, closed platforms provide the narrower, more insulated stages where exposure is transformed into trust and belonging. Here, encryption, gatekeeping, and small-group intimacy reduce the fear of surveillance, reinforce ideological commitment, and encourage behavioural loyalty. In this way, open ecosystems act as amplifiers of reach, while closed ecosystems act as breeding places of commitment, together forming a mutually reinforcing architecture of radicalisation.

5. Conclusion

The digital environment has become a central arena for contemporary terrorist radicalisation and recruitment. Terrorist groups strategically exploit both open and closed digital ecosystems, each serving distinct but complementary purposes in the radicalisation pipeline. Open platforms such as YouTube, Twitter/X, or TikTok provide expansive reach, algorithmic amplification, and low-threshold entry points for individuals who may only have a peripheral interest in extremist narratives. Through viral content, memes and influencer-like engagement strategies, these platforms normalize extremist discourses, lower psychological barriers to entry, and serve as gateways to more insular communities.

In contrast, closed digital ecosystems including Telegram, encrypted forums, and the Dark Web facilitate controlled environments where radicalisation can deepen and recruitment can be formalized. Within these spaces, terrorists can insulate followers from external critique, reinforce ideological commitment, and coordinate operational or logistical planning under the protection of anonymity and encryption. Thus, open and closed ecosystems should not be seen as discrete environments but rather as interdependent stages in a dynamic radicalisation path.

[156] Gerwehr and Daly's (2006) RAND report on al-Qaeda's recruitment strategies identified the 'funnel model' as one of the key frameworks for understanding how individuals progress from broad exposure to deeper involvement. The present conceptualization of radicalisation across open and closed digital ecosystems builds on this insight, adapting the funnel metaphor to account for the distinct affordances of contemporary online environments.

Analysing this exploitation is critical for several reasons. First, it allows scholars and policymakers to understand the movement of individuals across digital spaces, from exposure to indoctrination to mobilization. Without such mapping, counter-radicalisation strategies risk treating platforms in isolation, thereby overlooking the connective nature of extremist ecosystems. Second, recognizing these dynamics highlights how algorithmic recommendation systems, digital affordances, and social engineering tactics are manipulated by extremists to maximize reach and retention. Third, such analysis enables anticipation of adaptive strategies, as terrorist groups rapidly migrate to new platforms or modify their digital presence in response to regulatory and security interventions.

The implications for policy are profound. By identifying the complementary functions of open and closed platforms, governments and international organizations can develop differentiated and targeted interventions. Open platforms require interventions focused on content moderation, algorithmic transparency, and counter-narratives aimed at disrupting recruitment at the earliest stages. Closed ecosystems, by contrast, necessitate intelligence-led approaches, including lawful access mechanisms, digital infiltration, and international collaboration to penetrate highly secured environments. Crucially, effective policy must also address the cross-platform continuum, ensuring that strategies do not inadvertently displace terrorist activity from one sphere to another without disrupting the broader ecosystem.

In conclusion, analysing and recognizing the ways in which terrorists exploit digital ecosystems is a policy imperative. It enables the development of holistic, adaptive, and rights-conscious frameworks that can both prevent radicalisation at its source and disrupt its consolidation in protected environments. Without such recognition, counterterrorism strategies risk remaining fragmented and reactive, leaving critical blind spots that extremists are well positioned to exploit.

BIBLIOGRAPHY

Barykin, S. Y., Kapustina, I. V., Kirillova, T. V., Yadykin, V. K., & Konnikov, Y. A. (2020). Economics of Digital Ecosystems. *Journal of Open Innovation: Technology, Market, and Complexity*, *6*(4), 124. https://doi.org/10.3390/joitmc6040124

Bloom, M., Tiflati H. & Horgan, J. (2017). Navigating ISIS's Preferred Platform: Telegram1. *Terrorism and Political Violence*, DOI: 10.1080/09546553.2017.1339695

Borum, R. (2011). Rethinking Radicalisation. *Journal of Strategic Security* 4 (4), 1-6. https://digitalcommons.usf.edu/jss/vol4/iss4/1/

Bruns, A. (2019). Filter Bubble. *Internet Policy Review* 8(4). https://doi.org/10.14763/2019.4.1426

Clifford, B. and Powell, H. (2019). *Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram*. Program on Extremism: The George Washington University.

Conway, M. (2017). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism*, 40(1), 77–98.

Gill, P., Corner, E., Conway, M., Thornton, A., Bloom, M., & Horgan, J. (2017). Terrorist use of the internet by the numbers: Quantifying behaviours, patterns, and processes. *Criminology & Public Policy, 16*(1), 99–117. https://doi.org/10.1111/1745-9133.12249.

Hamid, N. and C. Ariza. (2022). Offline Versus Online Radicalisation: Which is the Bigger Threat? *Report G-NET*. https://gnet-research.org/2022/02/21/offline-versus-online-radicalisation-which-is-the-bigger-threat/

Horgan, J. (2004). *The Psychology of Terrorism*. London: Routledge.

Horgan, J. (2008). From Profiles to Pathways and Roots to Routes: Perspectives from Psychology on Radicalisation into Terrorism. *The Annals of the American Academy of Political and Social Science, 618,* 80-94.

Kruglanski, A. W., Molinario, E., Jasko, K., Webber, D., Leander, N. P., & Pierro, A. (2022). Significance-Quest Theory. *Perspectives on Psychological Science, 17*(4), 1050-1071. https://doi.org/10.1177/17456916211034825

Meleagrou-Hitchens, A., Alexander, A. and Kaderbhai, N. (2017). The Impact of Digital Communications Technology on Radicalisation and Recruitment. International Affairs 93 (5), 1233-1249.

McCauley, C. & Moskalenko, S. (2008). Mechanisms of Political Radicalisation: Pathways Toward Terrorism, *Terrorism and Political Violence*, 20 (3), 415-433, DOI: 10.1080/09546550802073367.

Moghaddam, F. M. (2005). The Staircase to Terrorism: A Psychological Exploration. *American Psychologist, 60(2),* 161-169.

Neumann, P. (2013). The Trouble with Radicalisation. *International Affairs (London)*, *89*(4), 873-893. https://doi.org/10.1111/1468-2346.12049

Pariser, E. (2011). *The Filter Bubble: What the Internet Is Hiding from You.* New York: Penguin Press.

Ribeiro, M. H., Ottoni, R., West, R., Almeida, V.A.F., & Meira Jr., W. (2020). Auditing radicalisation pathways on YouTube. *Proceedings of the 2020 Conference on*

Fairness, Accountability, and Transparency (FAT'20),* 131–141. https://doi.org/10.1145/3351095.3372879

Sageman, M. (2004). *Understanding terror networks*. University of Pennsylvania Press.

Sageman, M. (2008). *Leaderless jihad: Terror networks in the twenty-first century*. University of Pennsylvania Press.

Shin, D. and Jitkajornwanich, K. (2024). How Algorithms Promote Self-Radicalisation: Audit of TikTok's Algorithm Using a Reverse Engineering Method. *Social Science Computer Review 42*(4), 1020-1040. DOI: 10.1177/08944393231225547

Sunstein, C. (2001). *Republic. Com*. Princeton, NJ: Princeton University Press.

Tufekci, Z. (March 10, 2018). YouTube, The Great Radicaliser. *New York Times*. https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html

UNODC (2012). *The Use of the Internet for Terrorist Purposes*. https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

UNCCT &UNICRI (2021). Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

UNCCT &UNICRI. (2024). Beneath The Surface: Terrorist and Violent Extremist use of the Dark Web and Cybercrime-as-a-Service for Cyber-Attacks. https://unicri.org/beneath-surface-terrorist-and-violent-extremist-use-dark-web-and-cybercrime-service-june-2024

Weimann, G.& Masri, N. (2020). Research Note: Spreading Hate on TikTok. *Studies in Conflict & Terrorism*, DOI: 10.1080/1057610X.2020.1780027

Wiktorowicz, Q.(2005). *Radical Islam Rising: Muslim Extremism in the West*. Lanham, Md.: Rowman & Littlefield.

Wiktorowicz, Q. (n.d.) Joining The Cause: Al-Muhajiroun and Radical Islam. https://securitypolicylaw.syr.edu/wp-content/uploads/2013/03/Wiktorowicz.Joining-the-Cause.pdf

Winter, C., Neumann, P., Meleagrou-Hitchens, A., Ranstorp, M., Vidino, L., & Fürst, J. (2020). Online Extremism: Research Trends in Internet Activism, Radicalisation, and Counter-Strategies. *International Journal of Conflict and Violence*, *14*(2), 1-20. doi:10.4119/ijcv-3809

Whittaker, J. (2021). The online behaviours of Islamic state terrorists in the United States. Criminology & Public Policy, 20(1), 177-203. https://doi.org/10.1111/1745-9133.12537.

Whittaker, J. (2022). Rethinking Online Radicalisation. *Perspectives on Terrorism, 16*(4), 71-84. ISSN 2334-3745

Whittaker, J., Looney, S., Reed, A. and Votto F. (2021). Recommender Systems and the Amplification of Extremist Content. *Internet Policy Review 10* (2), DOI: 10.14763/2021.2.1565

CHAPTER 7

THE FUTURE OF COUNTERTERRORISM FOR THE INTELLIGENCE AND SECURITY AGENCIES IN THE AGE OF EMERGING AND DISRUPTIVE TECHNOLOGY

Paul HURMUZ[i]

> *"Your national security requires urgent reassessment. …last year, I visited a military base of a NATO member in Europe. They showed me a well-organized facility with a ton of equipment, all in perfect condition. They asked what I thought of it. My answer didn't please them. Without coming closer than 10 km, four teams of Ukrainian pilots could turn that place into Pearl Harbor in 15 minutes. I'm not saying this to scare anyone. I'm saying these technologies are so accessible and cheap that* ***if they fall into the hands of terrorists, 100 terrorists could upend any country's order****." (Robert Broudi aka 'Magyar', field commander of combat drone pilots in the Armed Forces of Ukraine, speaking at the 2025 LANDEURO Symposium in Wiesbaden, Germany)*[157]

Many people will take the words of Robert Broudi (aka 'Magyar') at face value. Coming from one of the most experienced drone warriors in Ukraine, it will be quite difficult to dispute his statement. We should also look at the way in which terrorist organisations have adapted and embraced new technologies, especially during the latest ten years.

The first part of this study will try to address the way the Emerging and Disruptive Technologies (EDT) have impacted terrorism, with the focus on drones and potential use of Artificial Intelligence (AI) and Autonomous Weapons. The way Daesh has used commercial drones for Intelligence Surveillance Reconnaissance (ISR), propaganda and kinetic operations deserves a systematic analysis. Also, the networks Daesh developed mostly in the Western countries for its supplies of different drone related equipment, has demonstrated not only the limitations of our security measures but also the need for prevention involving the governments, legislative bodies and private sector.

The second part of the study refers on the impact of EDT on the Intelligence and Security Agencies (ISA), especially the rise of AI which will have a huge impact. Beyond the great advantages, ISA will also have to pay due attention to the challenges generated by the EDT, in their race with state and non-state adversaries. How can ISA manage to reprioritise Strategic Intelligence and embrace Technological Adaptation without endangering their missions and current operations? This is a critical issue, being addressed mostly by the impact of AI on ISA in general but also on specific

[157] Olexander Scherbaua on X: http2s://x.com/olex_scherba/status/1948384506030768509

domains like: Human Intelligence (HUMINT), Signal Intelligence (SIGINT), CYBER and Intelligence Strategic Warning.

The third part is trying to offer some options about the future of counter-terrorism in the EDT Age. Advanced technologies present a big challenge and it is important to understand how governments can most efficiently do their job by engaging industry, streamlining cross-government cooperation, working with international partners and so on. This might also include leveraging AI and Machine Learning (ML) tools to focus on complex tracking systems to project and manage supply chain risk. It is imperative that we deepen our understanding of how terrorists are using EDT to increase their power and influence. The focus should not only be on disruption but also on prevention, and the responsibility to act must be shared across government agencies, academic institutions and technology companies.

1. Terrorism and the EDT[158]

For quite a while, we have seen some kind of democratisation of EDT, which could be used by Violent Extremist Organisations (VEO) and exploited in unexpected and destructive ways. According to the 'Lethal Empowerment Theory'[159], new technologies will be rapidly adopted and adapted by violent non-state actors when they are accessible, cheap, simple to use, transportable, concealable, and effective. Terrorists are interested in weapons that are useful in a wide range of contexts.[160] Professor Cronin explains in her book[161] the ways in which technological advances and innovation can disrupt the power of established states and shift it to non-state actors, such as lone individuals, insurgents, and terrorists. She argues that the development and proliferation of commercial drones, cyber weapons, 3D printing, military robotics, and autonomous systems can increase the mobility and reach of VEO.[162]

The war in Ukraine is showcasing innovative tactics, technological advancements, and asymmetric strategies. Terrorist groups worldwide are closely observing these developments, drawing valuable lessons to enhance their own capabilities. From drone warfare to cyber-attacks, the Russia-Ukraine war is reshaping the landscape of modern terrorism, equipping VEO with new tools and techniques to challenge conventional security measures.[163]

The Power of Drones[164]

Drones have been identified as one of the key terrorist threats by the UN Security Council Counter-Terrorism Committee. Referred also as

[158] NOTE: for the economy of this study disinformation, radicalisation, and recruitment in cyberspace will not be addressed this time but are addressed elsewhere in the collection.

[159] 'Lethal Empowerment Theory', developed by professor Audrey Kurth Cronin, describes how the spread of accessible, off-the-shelf technology is shifting the means for mass violence away from states and into the hands of individuals and non-state actors.

[160] Emerging Technologies and Terrorism, March 17, 2022, https://www.visionofhumanity.org/emerging-technologies-and-terrorists/

[161] Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*, November 1, 2019, Oxford University Press

[162] Aldon Thomas Stiles, SWJ Book Review – *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists*, January 27, 2023, https://archive.smallwarsjournal.com/jrnl/art/swj-book-review-power-people-how-open-technological-innovation-arming-tomorrows-terrorists

[163] Dr Christina Schori Liang, 'Ten Lessons from the Russia-Ukraine War', March 31, 2025, https://www.visionofhumanity.org/10-lessons-from-the-russia-ukraine-war/

[164] Many terms are used to describe these systems, like 'drones', 'remotely-piloted air systems', 'unmanned/uncrewed aerial vehicles', each of term having its individual characteristics and implications. For ease of reading this article will use the term 'drone'.

Unmanned/Uncrewed Aerial Systems (UASs), they are remotely piloted, pre-programmed, or controlled airborne vehicles.[165] Today, state and non-state actors possess the ability to acquire drones and can assemble and operate Commercial Off-The-Shelf (COTS) drone technology. Conservative estimates maintain that 65 non-state actors are now able to deploy drones.[166]

Drones hold a particular aura on the battlespace. This stems from their symbolism of the anti-terrorism campaign in the Middle East and North Africa (MENA) region, coupled to their method of air power delivery – invisible, permanent and perceptively uncontestable for the VEOs that they target. As such, to achieve even a moderate level of technical ability within this arena is a key aim of VEOs' legitimacy.[167]

"There will be imitators – crude at first – but better and better, and while reasonable people can disagree on how long it will take for terrorists, insurgents and other rogue groups to build or acquire weaponised drones that can be guided by video straight into a target, there is really no dispute that it is a question of when and not if. The day will come when such drones are available to almost anyone who wants them badly enough."[168]

Professor Villasenor[169] made this prediction in 2011. Following the proliferation of drone technology, air power, for a long time the privilege of advanced state powers, is now accessible for VEOs. COTS drones have enabled them to obtain and develop warfighting capabilities within the third dimension of the battlespace.[170] Subsequently, nation states can no longer guarantee they own the airspace above the forces they are supporting, and this new VEO capability has already proven itself to be a deadly weapon.[171]

The conflicts in Syria and Iraq have seen a proliferation of drones throughout the battlespace. Whether used for filming propaganda, as ISR asset or for command and control, drones are being used by a multitude of groups for a wide variety of missions. At the peak of the fighting around Mosul in Northern Iraq in 2016, Daesh carried out dozens of strikes per day, with multiple drones attacking a target, essentially giving the group a tactical-level air force in their fight against the international coalition.[172]

Daesh is certainly not the first group to use drones as an offensive weapon. Also, in August 2016 there was a Hezbollah-owned drone dropping MZD-2 sub-munitions. Hezbollah has claimed to have this kind of capability since September

---

[165] Dr Christina Schori Liang, *Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies*, March 15, 2023, https://www.gcsp.ch/publications/terrorist-digitalis-preventing-terrorists-using-emerging-technologies

[166] Kerry Chávez and Ori Swed, *The Proliferation of Drones to Violent Nonstate Actors*, Defence Studies 21, no. 1 (January 2, 2021), https://www.researchgate.net/publication/346298262_The_proliferation_of_drones_to_violent_nonstate_actors

[167] Flight Lieutenant Peers Lyle, *Air Power Proliferation: How 'Commercial-off-the-shelf' Drones are being used by Violent Extremist Organisations to Influence The Future of Warfare in the Air* (Air and Space Power Review Vol 22 No 3), https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/aspr/aspr-vol22-iss3-6-pdf/

[168] Don Rassler, *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology* (West Point: US Military Academy, 2016), 63.

[169] John Villasenor is Professor of Electrical Engineering, Law, Public Policy, and Management Faculty Co-Director, UCLA Institute for Technology, Law and Policy

[170] Flight Lieutenant Peers Lyle, *Air Power Proliferation: How 'Commercial-off-the-shelf' Drones are being used by Violent Extremist Organisations to Influence The Future of Warfare in the Air* (Air and Space Power Review Vol 22 No 3), https://www.raf.mod.uk/what-we-do/centre-for-air-and-space-power-studies/aspr/aspr-vol22-iss3-6-pdf/

[171] Nick Waters, *Death From Above: The Drone Bombs of the Caliphate*, *Bellingcat*, February 10, 2017, https://www.bellingcat.com/news/mena/2017/02/10/death-drone-bombs-caliphate/

[172] Pommerlau, M. (2018) How $650 drones are creating problems in Iraq and Syria. C4ISRnet, January 5, 2018. Accessed at https://www.c4isrnet.com/unmanned/uas/2018/01/05/how-650-drones-are-creating-problems-in-iraq-and-syria/

2014.[173] Some reports maintained that in 2021, affiliates of Daesh and al Qaida demonstrated a growing UAS capability in parts of West and East Africa. Al-Shabaab, in East Africa, uses drones for ISR and could conceivably launch attacks on civil aviation.[174]

The first recorded combat death from an Daesh operated COTS drone occurred in October 2016. The first X-8 in a conflict zone was spotted in 2015 near the Mosul Dam in Iraq. As of the end of 2016, 32 models from six countries had been identified in the Syria and Iraq conflict.[175]

Daesh invested millions in building an effective drone program with weaponized commercial UAS, which was soon imitated by other armed groups and state forces. This type of drone was even used in failed attempt in 2021 to assassinate the Iraqi prime minister by dropping bombs on his house in Baghdad.[176] Similar previous attempted uses of drones against political leaders were averted, including the 2015 dropping of radioactive materials on the Japanese Prime Minister's office.[177]

Daesh's approach to accessing drones, parts and components and developing its own indigenous drone program is another unique element.[178] It put millions of dollars into acquiring drones, related technologies and equipment such as pulsejet engines, micro-turbine, mobile antennas, lithium batteries and GoPro cameras shipped to Iraq and Syria.[179] Large smuggling networks were set up in Europe, including multiple fake companies to avoid raising suspicions by law enforcement. Drone footage was also sent back to supporters in the West to make professional video propaganda. This came to light after the arrest of Daesh supporters in the Western Europe and subsequent court cases.[180] More recently, Western supporters were put at trial for providing instruction to Daesh on how to use 3D printers in assembling parts and components to build single-use explosive drones.[181]

The massive investment by Daesh in research and development on weaponizing COTS drones was a turning point for this type of warfare. First, it took advantage of the propaganda value of drone imagery and used drones' ISR capabilities as their eyes in the sky to boost the effectiveness of their military campaigns. Their ability to acquire large quantities of drones through their networks

---

[173] Nick Waters, *Death From Above: The Drone Bombs of the Caliphate*, *Bellingcat*, February 10, 2017, https://www.bellingcat.com/news/mena/2017/02/10/death-drone-bombs-caliphate/

[175] ibid.

[176] PAX, *Military Drones as the Weapons of Choice in Iraq*, October 31, 2023, https://paxforpeace.nl/news/military-drones-as-the-weapons-of-choice-in-iraq/

[177] AP (2015) *Drone 'containing radiation' lands on roof of Japanese PM's office*, Associated Press, April 22, 2015. Accessed at https://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office

[178] Rassler, D. Al-Ubaydi, M. Mironova, V. (2017) The Islamic State's Drone Documents: Management, Acquisitions, and DIY Tradecraft, Counter Terrorism Center, Westpoint. January 31, 2017. Accessed at https://ctc.westpoint.edu/ctc-perspectives-the-islamic-states-drone-documents-management-acquisitions-and-diy-tradecraft/

[179] Rassler, D. (2018) The Islamic State and Drones. Supply, Scale and Future Threats. Combating Terrorism Center (CT) Westpoint. July 2018. Accessed at https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf

[180] Albæk, M.M. et al. (2020) The Controller: How Basil Hassan Launched Islamic State Terror into the Skies. CTC Sentinel. Westpoint. May 20, Volume 13, Issue 5. Accessed at https://ctc.westpoint.edu/the-controller-how-basil-hassan-launched-islamic-state-terror-into-the-skies/

[181] Murry, J. (2023) Birmingham PhD student guilty of using 3D printer to build 'kamikaze' drone. The Guardian, September 28, 2023. Accessed at https://www.theguardian.com/uk-news/2023/sep/28/birmingham-phd-student-mohamad-al-bared-guilty-using-3d-printer-to-build-kamikaze-drone

and to weaponize them with a range of munitions or turn them into airborne Improvised Explosive Devices (IEDs) became a real problem for the US-led coalition.[182]

Weaponized drones are increasing in range and precision. They can travel up to 1,500 km, ideal for attacks on military targets deep within state territory. Also, civilian infrastructure, located far from conflict zones, is now increasingly vulnerable. Since 2020, energy infrastructure, international shipping, international airports and capital cities have all been targeted by drones.[183]

On the horizon is the growing issue of saturation drone strikes. In partnership with decoys, weaponised drones can be used to pin-point and destroy air defence systems, opening the gates for an incoming volley of rockets, missiles, and other armed drones. By combining downloadable software and online tutorials, drone users can launch rudimentary 'swarms' (between five and ten drones can be 'hooked-up' to a single device).[184]

Dr. Liang[185] underlined in her contribution 'Ten Lessons from the Russia-Ukraine War', that

> "*More recently, AI has been introduced to boost such weapons. AI can process massive data and leveraging algorithms to identify and prioritize potential targets. Drones are equipped with various sensors, including high-resolution cameras, infrared sensors, radar, and LiDAR (Light Detection and Ranging). AI systems are being trained to recognize objects (vehicles, buildings, or people) with deep learning models to get a comprehensive view of the environment in real-time to deliver munitions with high precision*."[186]

As already mentioned, drones are not a new phenomenon for terrorists; a variety of VEOs, including the Taliban, Boko Haram, Houthi rebels, and Daesh have utilized drones in combat. Drone innovations by the Houthis have shown that drone attacks can be highly precise and effective at long distances. What is new in this war is that drones are being deployed with AI capabilities; innovation has transformed even cheap drones into effective guided missiles, both human-operated and AI-guided.[187] Terrorist groups may seek to exploit AI for automated targeting, according to Dr. Liang.

AI and Autonomous Weapons – the New Revolution

The declaration of Marc Andreessen that "software is eating the world"[188] has never been more relevant, especially in the context of modern warfare. Software is increasingly central to shaping military strategies and determining the outcomes of conflicts. As defence systems are challenged and data is becoming the new currency, the power of intelligence and information, traditionally controlled by global

[182] PAX, *Between Terror Strikes and Targeted Killings-The evolving role of drone warfare in Iraq*, October 31, 2023, p.19, https://paxforpeace.nl/publications/between-terror-strikes-and-targeted-killings/
[183] Dr Christina Schori Liang, *Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies*, March 15, 2023, https://www.gcsp.ch/publications/terrorist-digitalis-preventing-terrorists-using-emerging-technologies
[184] ibid.
[185] Dr. Christina Schori Liang is Head of Counter-terrorism and PVE at Geneva Centre for Security Policy (GCSP) and Faculty Member, PSIA, Sciences Po.
[186] Dr. Christina Schori Liang, *Ten Lessons from the Russia-Ukraine War*, in the Global Terrorism Index 2025 Report, p. 82, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf
[187] ibid.
[188] Marc Andreessen, *Why Software Is Eating the World*, August 20, 2011, https://a16z.com/why-software-is-eating-the-world/

superpowers and large corporations, may eventually be available to weaker, less-resourced groups like insurgents and terrorists.[189]

Technology is transforming the nature of warfare. The shift toward increasingly autonomous weapons systems has been developing over decades. 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 defence companies, resulting in large contracts for developing a range of weaponry. These companies will have a difficult time to keep the technologies for themselves. As DeepSeek has recently revealed, AI companies are openly sharing their expertise to the global community allowing access to everyone for developing their technologies. AI has further democratized access to dual-use technological innovations.[190] This way, terrorists and other rogue actors could get access to technologies that will multiply their destructive capabilities.

Terrorists can exploit software in various ways, including reverse-engineering open-source military programs to study tactics and defences. Additionally, leaked battlefield applications, drone control software, and AI targeting systems can be repurposed. 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 some 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 the concern lies in the potential for these less expensive systems to be designed and developed by terrorists globally with little effort.[191]

According to Thomas L. Friedman, Washington and Beijing will soon discover that putting A.I. in the hands of every person and robot on the planet will super-empower bad people to levels no law enforcement agency has ever faced:

> *"Remember: Bad guys are always early adopters! And without the United States and China agreeing on a trust architecture to ensure that every A.I. device can be used only for humans' well-being, the AI revolution is certain to produce super-empowered thieves, scam artists, hackers, drug dealers, terrorists and misinformation warriors. They will destabilize both America and China, long before these two superpower nations get around to fighting a war with each other."*[192]

2. The impact of EDT on the Intelligence and Security Agencies (ISA)

Nations around the world now find themselves confronted by a new multipolar order in which AI and robotics are not merely tools for economic influence but instruments for military predominance. AI is predicted to transform Command and Control (C2) systems, intelligence gathering and analysis, target recognition, and

[189] Dr. Christina Schori Liang, *Ten Lessons from the Russia-Ukraine War*, in the Global Terrorism Index 2025 Report, p. 85, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf
[190] ibid.
[191] ibid. p.84
[192] Thomas L. Friedman, *The One Danger That Should Unite the U.S. and China*, September 2, 2025, New York Times, https://www.nytimes.com/2025/09/02/opinion/ai-us-china.html

information warfare. This transformation challenges conventional notions of military primacy, accountability, national autonomy and strategic escalation.[193]

The rise of AI-enabled warfare and autonomous weapons systems has been described by some experts as an 'Oppenheimer Moment', similar to the creation of the atomic bomb. This represents a pivotal point that could either mark the beginning of a new era of great power dominance or serve as a warning of potential catastrophic consequences. 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.[194]

In this respect, deterrence models are explored, like the so-called 'Mutual Assured AI Malfunction' (MAIM). This posits that a race for AI-enabled dominance would endanger the whole world. In case of a hurried bid for superiority, one state could inadvertently lose control of its AI, putting security of all states at risk. Also, if one state succeeds in producing and controlling a highly capable AI, it likewise poses a direct threat to the survival of the other competitors. In either event, states feeling threatened may try to sabotage those destabilizing AI projects for deterrence purpose. Their interventions could range from covert operations to physical damage against infrastructure, like data centres[195]. In such a scenario, we will rapidly approach a dynamic very similar to the Nuclear Mutual Assured Destruction (MAD), in which no country would attempt to achieve the strategic monopoly, because of the risk of its own catastrophic destruction.[196]

Around the end of the Cold War an acronym became popular: VUCA (Volatility, Uncertainty, Complexity and Ambiguity).[197] The current security environment is quite VUCA consistent. Similar to the Cold War, the evolutions in EDT and their impact on National Security will be a critical requirement for the ISA. Understanding your adversary's intentions, capabilities and plans in the era of EDT will be vital. The same will be true in the case of VEOs.

After the Russian invasion of Crimea in February 2014, followed by the operations in Donbas, 'Hybrid Warfare'[198] became the buzzword for the Western Defence and Security community. The first official reference was in the NATO Heads of State Wales Summit Declaration (September 2014):

> *"We will ensure that NATO is able to effectively address the specific challenges posed by hybrid warfare threats, where a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design. It is essential that the Alliance possesses the*

[193] Daniel Araya, *National Defence and Security in the Age of AI and Robotics*, in ON TRACK, Volume 35 | January 2025, https://cdainstitute.ca/wp-content/uploads/2025/01/On-Track-Issue-35.pdf
[194] Dr. Christina Schori Liang, *Ten Lessons from the Russia-Ukraine War*, in the Global Terrorism Index 2025 Report, p. 85, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf
[195] Alex Rough, *Data Centers on the 21st Century Battlefield*, War on the Rocks, September 5, 2025, https://warontherocks.com/2025/09/data-centers-on-the-21st-century-battlefield/
[196] Dan Hendrycks, Eric Schmidt, Alexandr Wang, *Superintelligence Strategy*, April 14, 2025, https://www.nationalsecurity.ai/
[197] Herbert F. Barber, *Developing Strategic Leadership: The US Army War College Experience*, in Journal of Management Development, Volume 11 (6): 9 – Jun 1, 1992, https://www.deepdyve.com/lp/emerald-publishing/developing-strategic-leadership-the-us-army-war-college-experience-sB0uUtwql8
[198] One of the first references to 'Hybrid Warfare' was made in November 2005 by Lt. Gen. James N. Mattis and Lt. Col. (Retired) Frank Hoffman in their article *Future Warfare: The Rise of Hybrid Wars*, Proceedings Vol. 131/11/1,233, https://www.usni.org/magazines/proceedings/2005/november/future-warfare-rise-hybrid-wars

necessary tools and procedures required to deter and respond effectively to hybrid warfare threats, and the capabilities to reinforce national forces."[199]

The extensive efforts to counter terrorist threats, especially against groups such as Daesh, al Qaida or the Taliban, determined many experts to address this from a 'Hybrid Warfare' perspective. As underlined by Mr. C.M. Baker[200]*:*

"It is often characterised by the use of fictitious propaganda, deniable forces, espionage, the mobilisation of ethnic, linguistic or confessional minorities and terrorism. Most of these techniques are not new; what is new is the way they are integrated, and the presence of the internet. The internet is a force-multiplier for many old techniques, and a key enabler for many new ones, not just in cyber-attacks, but also for targeted propaganda, disinformation and for 'grooming' potential recruits."[201]

Reprioritising Strategic Intelligence

First, we need to consider the impact of 9/11 on the Intelligence Transformation. It is clear that many ISA have been evolving to keep pace with the changing character of terrorism over the past 25 years. One can argue that the Counter-terrorism (CT) focus has encouraged a tactical mindset centred on 'the enemy behind the door'. This tactical approach has caused the ISA to miss events of strategic importance.[202]

Former vice-chairman of the US National Intelligence Council, Gregory Treverton, has insisted on the need to transition from a 'puzzles'-based approach, to a 'mysteries'-focused approach to understand international adversaries' decision-making. According to him:

"Puzzles can be solved; they have answers. But a mystery offers no such comfort. It poses a question that has no definitive answer because the answer is contingent; it depends on a future interaction of many factors, known and unknown. A mystery cannot be answered, being more an attempt to define ambiguities."[203]

Strategic intelligence scholar Michael Maccoby has identified some organisational abilities required for effective strategic intelligence:

- *Foresight*: the ability to anticipate currents of change that can threaten an organization or provide opportunities;[204]

[199] NATO, Wales Summit Declaration issued by the Heads of State and Government, September 5, 2014, para 13, https://www.nato.int/cps/cn/natohq/official_texts_112964.htm

[200] Mr. Clovis Meath Baker was Director of Intelligence Production at GCHQ, 2010-2013.

[201] Clovis Meath Baker CMG OBE, *Hybrid Warfare in the Middle East: We Must Do Better*, March 7, 2017, RUSI Commentary, https://www.rusi.org/explore-our-research/publications/commentary/hybrid-warfare-middle-east-we-must-do-better

[202] Patrick Bury, Michael Chertoff, *New Intelligence Strategies for a New Decade*, The RUSI Journal, September 23, 2020, https://rusi.tandfonline.com/doi/full/10.1080/03071847.2020.1802945#d1e217

[203] Gregory F. Treverton, Risks and Riddles, Smithsonian Magazine, June 2007, https://www.smithsonianmag.com/history/risks-and-riddles-154744750/

[204] Michael J Keegan, *Perspective on Strategic Intelligence: Conceptual Tools for Leading Change with Dr. Michael Maccoby*, Perspectives: Strategic Intelligence, IBM Center for the Business of Government, 2016, p. 76, https://www.businessofgovernment.org/sites/default/files/Perspectives%20on%20Strategic%20Intelligence.pdf

- *Systems thinking*: the ability to synthesize or integrate elements rather than breaking them into parts for the purpose of analysis;[205]
- *Partnering*: the ability to make strategic alliances.[206]

Indeed, beyond the resource issue is one of capability – the correct training of analysts to deal with increasing complexity. Psychologist Robert Sternberg identified three types of intelligence: *analytic* (analysis, logic, memory and puzzle-solving), *practical* (understanding people, tact, timing and effective communication) and *creative* (imagination, pattern recognition and interactive effects).[207] All of them are needed for strategic intelligence, but creative intelligence (dealing with imagination, pattern recognition and interactive effects) is especially important in understanding intelligence 'mysteries' associated with the greater complexity of the current era.[208]

Traditionally, Strategic Intelligence has been supported by a combination of assets from HUMINT, SIGINT, Imagery Intelligence (IMINT) and Measurement and Signature Intelligence (MASINT). In particular, assets will need to be better integrated, and others reoptimized to meet new intelligence demands.[209] At the same time, the tempo of the Technological Revolution and its impact on the whole society is practically forcing the ISA to adapt, so that the traditional methods of intelligence embrace the new reality.

The Need for Technological Adaptation

It is quite evident that in order to operate in such a VUCA Environment, the ISA need to adapt their strategies, tools and methods, as part of the Whole-of-Government and even Whole-of-Society approach. The classical separation lines between external and internal, civilian and military, government and private are more and more blurred. Intelligence and Information Sharing becomes more a necessity and not an exception, both inside the states and internationally. They also need to be capable of understanding how state and non-state adversaries are able to innovate and combine different tools in order to exploit specific vulnerabilities of our societies and bypass existing structures and mechanisms designed against current and future threats. This underscores the utility of *reverse targeting* because understanding what needs to be protected and anticipating how an adversary might likely target these assets are often more effective than merely tracking the actors themselves.[210]

It seems that wars are no longer solely determined by the number of jets, ships, or tanks a country can deploy. Instead, the focus will shift to those who are equipped to defend against the new and less expensive surge of new dual-use weapons ranging from smartphones to drones. Even if terrorists will not gain the air superiority of a state, they can still access Man-Portable Air-Defence Systems (MANPADS) and drones, as already seen. The war in Ukraine has demonstrated the significant advantages drones offer for ISR. Especially cheap drones have shifted the dynamics for terrorists. The conflict has highlighted the importance of open-source technology, unmanned

[205] Michael Maccoby, *Successful Leaders Employ Strategic Intelligence*, Research Technology Management (Vol. 44, No. 3, May/June 2001), p. 58.
[206] ibid., p.59
[207] Robert J Sternberg, Beyond IQ: A Triarchic Theory of Human Intelligence (Cambridge: Cambridge University Press, 1985).
[208] Patrick Bury, Michael Chertoff, *New Intelligence Strategies for a New Decade*, The RUSI Journal, September 23, 2020, https://rusi.tandfonline.com/doi/full/10.1080/03071847.2020.1802945#d1e217
[209] ibid.
[210] Mikael Weissmann, *Future threat landscapes: The impact on intelligence and security services*, in Security and Defence Quarterly 1/2025, vol.49, https://securityanddefence.pl/Future-threat-landscapes-The-impact-on-intelligence-and-security-services,197248,0,2.html

systems, and AI. The spread of these technologies among non-state actors introduces a new asymmetry in warfare. Success will now depend on *"innovation power"*, the capacity to invent, adapt, and deploy new technologies more swiftly than adversaries.[211]

So, integrating emerging technologies into the current mission template of the ISA is necessary in the short term but wholly insufficient over the long term. Rather, the dawning era of intelligence innovation must compel these services to reimagine their tradecraft and missions to harness technology's potential and reinvent their processes, partnerships, workforce, incentives, and the culture to embrace technological transformation.[212] Technology is not just about the future. It can unleash significant improvements to intelligence missions right now. Opportunities include automating the tasking of technical collection platforms, enabling case officers to penetrate denied areas, augmenting analysts' ability to make sense of exponentially growing data, and delivering data-rich, visually engaging products to customers.[213]

Emerging technologies are already reshaping how the ISA gather, process, and evaluate information but will likely transform all core aspects of the intelligence process in the coming decades. Experts[214] believe that this change is the convergence of four technological trends:

- Massive growth in computing and processing power to process data and power AI systems, particularly through cloud computing and graphics processing units (GPUs)[215];
- Improvements in AI and ML algorithms and applications particularly suited to intelligence, such as computer vision and natural language processing (NLP)[216];
- Advances in networked multimodal sensors – systems able to collect data in different forms simultaneously—and the volume and quality of sensor-derived intelligence data;
- Exponential growth in big data in the open-source domain – enabled through cell phone and internet penetration and social media – and advances in sophisticated data analytics.

This convergence of technologies – high-performance computing, cloud, advanced sensors, AI, and data analytics – holds tremendous potential to transform a host of critical intelligence missions and processes in the near term.[217]

Other technological advances, particularly in space-based collection, additive manufacturing, quantum systems, 5/6G networks, robotics, miniaturisation and nanotechnologies, as well as synthetic biology, will also transform the ISA.[218]

---

[211] Dr. Christina Schori Liang, *Ten Lessons from the Russia-Ukraine War*, in the Global Terrorism Index 2025 Report, p. 84, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf

[212] CSIS Report by Brian Katz, *Maintaining the Intelligence Edge-Reimagining and Reinventing Intelligence through Innovation*, January 13, 2021, p. X, https://www.csis.org/analysis/maintaining-intelligence-edge-reimagining-and-reinventing-intelligence-through-innovation

[213] ibid.

[214] ibid. p.3

[215] Office of the Director or National Intelligence (ODNI), *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, DC: January 2019), https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf

[216] ibid.

[217] CSIS Report by Brian Katz, *Maintaining the Intelligence Edge-Reimagining and Reinventing Intelligence through Innovation*, January 13, 2021, p. 3, https://www.csis.org/analysis/maintaining-intelligence-edge-reimagining-and-reinventing-intelligence-through-innovation

[218] ibid.

AI Impact on ISAs

ISA must follow the broad development of AI by focusing on both open and secret advancements. AI systems have successfully developed, imposing new demands on these services. Handling lightning-fast self-learning systems with broad cognitive human capabilities will be an unpredictable problem for which one can never be fully prepared.[219] At the same time, we have to recognise the fact that ISAs have had for a long time a major interest in the technology innovation. Many agencies (especially those responsible for SIGINT and later for CYBER), have been using earlier forms of AI since the start of the Cold War.[220]

Machine translation of foreign language documents laid the foundation for modern-day natural language processing (NLP) techniques. NLP helps machines understand human language, enabling them to carry out simple tasks, such as spell checks. Towards the end of the Cold War, AI-driven systems were made to reproduce the decision-making of human experts for image analysis to help identify possible targets for terrorists, by analysing information over time and using this to make predictions.[221]

RUSI[222] was commissioned by GCHQ (the UK's National Intelligence and Security Agency for SIGINT and Cybersecurity) to conduct an independent research study into the use of AI for national security purposes. The research has found that AI offers numerous opportunities for the UK national security community to improve efficiency and effectiveness, can rapidly derive insights from large, disparate datasets and identify connections that would otherwise go unnoticed by human operators. However, in the context of national security and the powers given to ISA, use of AI could give rise to additional privacy and human rights considerations which would need to be further assessed. For this reason, enhanced policy and guidance would be needed to ensure the privacy and human rights implications of National Security uses of AI should be reviewed on an ongoing basis.[223]

The research highlights three ways in which ISA could seek to deploy AI:

- The automation of administrative organisational processes;
- For Cybersecurity, AI could proactively identify abnormal network traffic or malicious software and respond to anomalous behaviour in real time;
- For Intelligence Analysis, the so-called 'Augmented Intelligence' (AuI) systems that could be used to support a range of human analysis processes, including:
  - ❖ Natural language processing and audiovisual analysis, such as machine translation, speaker identification, object recognition and video summarisation;
  - ❖ Filtering and triage of material gathered through bulk collection;
  - ❖ Behavioural analytics to derive insights at the individual subject level.

[219] Mikael Weissmann, *Future threat landscapes: The impact on intelligence and security services*, in Security and Defence Quarterly 1/2025, vol.49, https://securityanddefence.pl/Future-threat-landscapes-The-impact-on-intelligence-and-security-services,197248,0,2.html

[220] Dafydd Townley, *Intelligence agencies have used AI since the cold war – but now face new security challenges*, The Conversation, May 4, 2023, https://theconversation.com/intelligence-agencies-have-used-ai-since-the-cold-war-but-now-face-new-security-challenges-204320

[221] ibid

[222] RUSI-Royal United Services Institute

[223] Alexander Babuta, Marion Oswald and Ardi Janjeva, *Artificial Intelligence and UK National Security-Policy Considerations*, RUSI Occasional Paper, April 27, 2020, https://static.rusi.org/ai-national-security-final-web-version.pdf

None of the AI use cases identified in the research could replace human judgement.[224]

The requirement for AI is all the more pressing when considering the need to counter AI-enabled threats to National Security. Malicious actors will undoubtedly seek to use AI to attack and the most capable hostile state actors are developing or have developed offensive AI-enabled capabilities. In time, other actors, including criminal and terrorist groups, will also be able to take advantage of the same AI innovations, manifested as:

- Threats to digital security, including the use of Polymorphic Malware[225] or the automation of social engineering attacks to target individual victims;
- Threats to political security include the use of 'Deepfake' technology to generate synthetic media and disinformation, with the objective of manipulating public opinion or interfering with electoral processes;
- Threats to physical security; increased adoption of Internet of Things (IoT) technology, autonomous vehicles, 'smart cities' and interconnected critical national infrastructure will create numerous vulnerabilities which could be exploited by our adversaries.[226]

AI Role in Intelligence Strategic Warning

Information is traveling at greater speeds, decision-making is at greater speeds, and we need intelligence insights much faster. During the Cuban missile crisis of 1962, President Kennedy had 13 days to deliberate in secret about what he would do after U-2 spy planes discovered Soviet Nuclear Missiles in Cuba. On 9/11, President George W. Bush had just 13 hours to weigh intelligence about who was responsible for that horrific attack and how the U.S. would respond. Today, decision time could be 13 minutes or less.[227]

Right now, deep in sensitive compartmented information facilities, ISA analysts are closely monitoring geopolitical developments around the world to identify potential threats and offer strategic warnings to policymakers. Strategic warnings from the intelligence community can work in two ways. First, they can be critical forecasts of events that are harmful to states' strategic interests. For example, an alert about Chinese Navy vessels moving to encircle Taiwan could indicate that Beijing is preparing to invade. Alternatively, a warning could pertain to an event that is beneficial or harmful to strategic interests, such as an abrupt movement of Russian military forces away from Ukraine and towards Moscow, predicting a potential regime crisis. In both cases, the purpose of these alerts is to give political leaders a decision advantage.[228]

Many experts are analyzing the potential of AI systems to make assessments about geopolitical events, and the path ahead for applying such tools to strategic intelligence warning. One recent report[229], has found that, while there is currently no

---

[224] ibid.

[225] Polymorphic Malware is able to frequently change its identifiable characteristics in order to evade detection.

[226] Alexander Babuta, Marion Oswald and Ardi Janjeva, *Artificial Intelligence and UK National Security-Policy Considerations*, RUSI Occasional Paper, April 27, 2020, https://static.rusi.org/ai-national-security-final-web-version.pdf

[227] Amy Zegart, *Re-Imagining Espionage in the Era of Artificial Intelligence*, August 17, 2021, https://hai.stanford.edu/news/re-imagining-espionage-era-artificial-intelligence

[228] Anna Knack, Nandita Balakrishnan, *The State of AI for Strategic Warning*, November 19, 2024, https://cetas.turing.ac.uk/publications/state-ai-strategic-warning

[229] Anna Knack, Nandita Balakrishnan, Timothy Clancy, *Applying AI to Strategic Warning*, March 27, 2025, https://cetas.turing.ac.uk/publications/applying-ai-strategic-warning

AI system that can reliably predict geopolitical flashpoints or forecast their implications with high accuracy and precision, the state of the technology is changing rapidly and the advent of Artificial General Intelligence (AGI)[230], which some experts predict could arrive within in a few years, could change the playing field. The next generation of AGI systems could provide a considerable uplift to strategic warning in several ways in the medium term, giving decision-makers more time to respond to crises. The two most promising use cases identified in this research are using AI to:

- Track conflict risk indicators more accurately, by leveraging increased quantities and types of data;
- Identify possible outcomes and scenarios immediately after a shock or trigger happens; This could be particularly valuable for regions or topics that usually receive scant attention from ISA.[231]

HUMINT in the Information Age

AI-enabled intelligence tools will enable our adversaries to deny our intelligence operations. A world of 'ubiquitous surveillance' due to advances in smarter sensors, biometrics, and surveillance will create more denied areas for HUMINT operations, a persistent risk of exposure, and the need to change or discard decades of well-honed tradecraft.[232] This will force the intelligence officers and their assets to operate undetected and if possible invisibly. In this respect they should be aware of the presence of technologies of control and surveillance, which are increasingly present around the world. All of this requires insights from data, the tools to manipulate data and, most important, the talent to turn complex data into human insight.[233] As Richard Moore, Chief of the British Secret Intelligence Service (MI6) stressed in his presentation on 'Human Intelligence in the Digital Age':

> *"There is no longer such a thing as an analogue intelligence operation in this digital world. Our intelligence targets have online lives."*[234]

Advances in quantum engineering and engineered biology will change entire industries. The huge volumes of data now available across the globe, combined with ever increasing computer power and advances in data science, will mean the integration of AI into almost every aspect of our daily lives.

At the same time, the 'digital attack surface' that criminals, terrorists and hostile states seek to exploit against our societies is growing exponentially. According to Mr. Richard Moore, we may experience more technological progress in the next ten years than in the last century, with a disruptive impact equal to the industrial revolution. In order to be able to operate in such an environment, it's necessary to understand what motivates our adversaries, what are their intentions, their plans and their methods.

---

[230] According to Meredith Ringel Morris and her co-authors, AGI is a system that is at least as capable as a human at most tasks. Meredith Ringel Morris et al., *Position: Levels of AGI for Operationalizing Progress on the Path to AGI*, Proceedings of the 41st International Conference on Machine Learning, 2024, https://openreview.net/pdf?id=0ofzEysK2D

[231] Anna Knack, Nandita Balakrishnan, Timothy Clancy, *Applying AI to Strategic Warning*, March 27, 2025, https://cetas.turing.ac.uk/publications/applying-ai-strategic-warning

[232] Jenna McLaughlin and Zach Dorfman, *'Shattered': Inside the secret battle to save America's undercover spies in the digital age*, Yahoo News, December 30, 2019, https://www.yahoo.com/news/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html

[233] IISS, Human Intelligence in the Digital Age - Speech by Richard Moore, Chief of the UK's Secret Intelligence Service, November 30, 2021, https://www.iiss.org/events/2021/11/human-intelligence-digital-age/

[234] ibid.

Also, it is important to be able to reduce the space within which they believe they can act against us without consequences-on or offline.[235]

On counter-terrorism, the focus should be on developing new agent relationships and technological capabilities needed to degrade existing terrorist groups, prevent their spread, and identify unknown threats. This is only possible by having strong cooperation with the Security and SIGINT agencies internally but also with international partners.[236]

Any intelligence service needs to be at the vanguard of what is technologically possible. These can be achieved by pursuing partnerships with the tech community to help develop world-class technologies to solve HUMINT biggest mission problems (human and operational risks, deception and misinformation, and the time-consuming and unreliable nature of building trust with sources).

Training and retaining skilled operatives, maintaining ethical standards, and adapting to rapidly changing global threats will be key priorities for HUMINT agencies. As the world becomes more interconnected and complex, HUMINT will continue to play a critical role in safeguarding national security and informing strategic decision-making, by relying on human sources for nuanced, context-rich intelligence that will remain indispensable.[237]

The Role of SIGINT and Cyber in Intelligence and Security

Paul Killworth, GCHQ Deputy Director for Strategic Policy described how AI and ML have the potential to improve the effectiveness and efficiency of various intelligence functions. However, these capabilities bring with them complex legal and ethical considerations, and there is a strong public expectation that the ISA will act in a way that protects citizens' rights and freedoms. It is clear why AI is an attractive prospect for a SIGINT agency. The volume, velocity and complexity of digital data that they are now required to process is far beyond the capacity of human analysts alone.[238]

This 'obligation to innovate' is driven by two main factors. First, SIGINT agencies face a problem of 'information overload': while intelligence gathering capabilities have progressed considerably in recent years, technology to effectively process and analyse collected data has arguably failed to keep pace. The second consideration is the rapidly evolving nature of the threat landscape. Our societies continue to face serious national security threats from a range of actors, and the ISAs' use of new technology will be crucial to ensure they are able to keep pace with innovation against their adversaries' capabilities.[239]

Killworth explained that within an organisation like GCHQ, there is a potential to use ML and AI to improve their operational outcomes. They can tackle these large problems and potentially deliver intelligence and security solutions to help keep the

[235] ibid.
[236] ibid.
[237] Perseus Intelligence, *The Evolution of HUMINT since World War Two*, June 24, 2024, https://www.perseusintelligence.co.uk/the-evolution-of-humint-since-world-war-two#:~:text=While%20these%20technological%20advancements%20provide,the%20effectiveness%20of%20their%20operations.&text=Looking%20ahead%2C%20the%20future%20of,and%20informing%20strategic%20decision%2Dmaking.
[238] Alexander Babuta, A New Generation of Intelligence: National Security and Surveillance in the Age of AI, February 19, 2019, https://www.rusi.org/explore-our-research/publications/commentary/new-generation-intelligence-national-security-and-surveillance-age-ai
[239] ibid

society safe, in ways which were not possible before. Drawing on the example of the UK's Active Cyber Defence System[240], he explained how:

> "*Defending UK Cyber Security Systems can be done in new ways using AI and ML, and in the future we will almost certainly have to do this, to keep up with the challenges we face. I can't believe that we will be doing the Active Cyber Defence work we do today in the future, without greater use of AI."*[241]

AI-enabled advances in cybersecurity and cryptography and, in the future, quantum computing could enable adversaries to harden and encrypt their systems to deny remote penetration of their networks.[242] Also, AI tools will be exploited to penetrate, manipulate, and degrade our intelligence, influence the political processes, or covertly shape our society in detrimental ways. AI-accelerated cyberattacks will target collection and communication platforms and employ intelligent malware to access, exploit, or destroy critical data and intelligence.[243] Once inside, foreign intelligence could exploit adversarial AI to insert 'poisoned' or false data into training sets to degrade ISA algorithms and cause AI systems to fail.[244]

Malicious attacks across social media platforms and the intrusion of poisoned data sets being used to train ML algorithms highlights the need to develop security measures and policies regarding the source of data being used to develop AI/ML digital networks. The issue of trust in data and the resilience of the digital networks are critical for ensuring that we are sharing information that is valid, reliable, and trustworthy as that is the foundation for mission planning and decision making.[245]

This is especially critical for the development of trustworthy AI/ML algorithms and trustworthy AI networks. According to the recent NATO Report on Cognitive Warfare[246], trustworthy AI networks, must have the following set of characteristics:

- *Validity*[247], guarantee that an AI-based system will do only but also all of what it is intended to do;
- *Security*[248], ensure robustness and resilience within adversarial conditions;

---

[240] The National Cyber Security Centre, *Introduction to Active Cyber Defence*, https://www.ncsc.gov.uk/section/active-cyber-defence/introduction

[241] Alexander Babuta, A New Generation of Intelligence: National Security and Surveillance in the Age of AI, February 19, 2019, https://www.rusi.org/explore-our-research/publications/commentary/new-generation-intelligence-national-security-and-surveillance-age-ai

[242] CSIS Report by Brian Katz, *Maintaining the Intelligence Edge-Reimagining and Reinventing Intelligence through Innovation*, January 13, 2021, p. 5, https://www.csis.org/analysis/maintaining-intelligence-edge-reimagining-and-reinventing-intelligence-through-innovation

[243] National Security Commission on Artificial Intelligence, Interim Report, November 2019, https://digital.library.unt.edu/ark:/67531/metadc1851191/

[244] Office of the Director or National Intelligence (ODNI), *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, DC: January 2019), https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf

[245] Yvonne R. Masakowski, Eskil Grendahl Sivertsen, *Defence Against 21st Century Cognitive Warfare: Considerations and Implications of Emerging Advanced Technologies*, in NATO STO Technical Report 'Mitigating and Responding to Cognitive Warfare', March 2023, p 7-5, https://publications.sto.nato.int/publications/STO%20Technical%20Reports/STO-TR-HFM-ET-356/$$TR-HFM-ET-356-ALL.pdf

[246] ibid.

[247] The validity of an AI system means that it consistently performs only what it is intended to do, is guaranteed through rigorous validation and verification processes, ensuring it is robust, reliable, and accurate. This is a continuous effort that requires ensuring the system's role is properly formulated, its data is representative, and its output is accurate.

[248] Securing AI systems involves building robustness through techniques like adversarial training to handle unexpected inputs and building resilience through features like fault tolerance and recovery mechanisms to withstand and bounce back from attacks or disruptions.

- *Explainability*[249], provide understandable and context relevant justifications and explanations;
- *Responsibility*[250], compliant with ethical, legal, and regulatory frameworks.

3. The Future of Counter-terrorism in the EDT Age

This relationship between the technology of terrorism and the technology of those fighting it can be viewed as one of the more important modern arms races, not between superpowers in missile construction but between small groups and states competing for the ability to either perpetrate or prevent low intensity conflict.[251]

Advanced technologies present a challenge for government to continually monitor and adapt. One area of research, therefore, is how government can most efficiently do this given its limited resources – this could mean engaging industry, streamlining cross-government cooperation, working with international partners and so on. Another area is how can anticipatory intelligence processes themselves incorporate advanced technologies to facilitate monitoring. This could include leveraging AI or ML tools to prioritise what human analysts focus on and using complex tracking systems to project and manage supply chain risk.[252]

Drones and AI will continue to evolve. Therefore, it is imperative that we deepen our understanding of how terrorists are harnessing technologies to increase their power in both the physical and psychological domains. The focus should not only be on disruption but also prevention, and the responsibility to act must be shared across government agencies, academic institutions and technology companies. We are finding ourselves in the trenches of an increasingly widening digital war and we have not yet mastered how to escape it while digital terrorists are marching ahead.[253]

Drone swarms are the perfect weapon for asymmetrical wars and Generative AI[254] will have an enormous impact on global security in generating new weapons and modus operandi for malicious actors worldwide. The heightened focus on Lethal Autonomous Weapons Systems (LAWS) 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.[255]

The lessons drawn from the Russia-Ukraine war underscore the evolving nature of terrorism and the challenges faced by security agencies. To mitigate these

---

[249] Explainability is the ability to understand the reasoning behind an AI's decisions, which is crucial for building trust in AI systems. For trustworthy AI, explainability ensures transparency, accountability and fairness by illuminating the 'why' behind an AI's output, rather than just the 'what'.

[250] The responsibility of trustworthy AI networks involves ensuring their systems are fair, reliable, and secure while respecting human values and legal requirements. Key responsibilities include establishing accountability and transparency, ensuring data privacy, and building in human oversight, especially for critical decisions.

[251] Brian Jackson, *Technology Acquisition by Terrorist Groups: Threat Assessment Informed by Lessons from Private Sector Technology Adoption*, *Studies in Conflict & Terrorism* 24:3 (August 2010), p. 4.

[252] Joseph Jarnecki, *Advanced Technology and Economic Resilience*, RUSI Conference Report, February 2023, https://www.rusi.org/explore-our-research/publications/conference-reports/advanced-technology-and-economic-resilience

[253] Dr Christina Schori Liang, *Terrorist Digitalis: Preventing Terrorists from Using Emerging Technologies*, March 15, 2023, https://www.gcsp.ch/publications/terrorist-digitalis-preventing-terrorists-using-emerging-technologies

[254] Generative Artificial Intelligence uses sophisticated algorithms to organize large, complex data sets into meaningful clusters of information in order to create new content, including text, images and audio, in response to a query or prompt. George Lawton, *What is GenAI? Generative AI explained*, March 13, 2025, https://share.google/W3DrRdmqbXZnHVQtZ

[255] Dr. Christina Schori Liang, *Ten Lessons from the Russia-Ukraine War*, in the Global Terrorism Index 2025 Report, p. 85, https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf

risks, counter-terrorism strategies must adapt to the changing landscape of warfare. Key measures include[256]:

- *Enhancing Drone Defence Systems*: Investment in anti-drone technology, including jamming systems and counter-drone units, is essential to neutralise the growing threat of weaponised UAVs;
- *Strengthening Cyber Security Infrastructure*: Governments and organisations must bolster their cyber defences to counter hacking attempts, disinformation campaigns, and cyber terrorism;
- *Regulating the Use of AI in Warfare*: The ethical implications of AI-driven warfare must be addressed through international regulations to prevent its misuse by non-state actors;
- *Disrupting Extremist Digital Networks*: Tech companies and ISA must collaborate to identify and dismantle extremist networks operating on encrypted platforms and social media;
- *Investing in Psychological Operations and Strategic Communication*: counter-terrorism efforts must prioritise the development of effective counter-narratives to combat extremist propaganda and radicalisation.

The Russia-Ukraine war is reshaping the future of conflict, providing terrorist organisations with a blueprint for modern warfare. As technology continues to advance, extremist groups will increasingly integrate cyber warfare, AI, and asymmetric tactics into their operations.[257]

UASs have now taken up a common place in the stocks of armed forces and VEO. With this development, there remain a number of challenges over both responsible use of military drones and how to deal with proliferation. The unique features of drones have opened up a new toolbox of targeting that has been actively exploited by states and armed groups to use lethal force. This brings serious escalation risks, undermines protection of civilians and could erode legal principles around the use of lethal force. The scale of surveillance, data collection and targeting requires proper policy and legal frameworks to prevent civilian casualties, improve accountability and oversight and adhere to international legal principles in both a humanitarian and human rights law framework.[258]

Export and subsequent use of military drones and drone technology[259]

States should establish clear, robust and binding International Standards on the export and subsequent use of military drones. Initial discussions – led by a core-group of States under the auspices of the UN – should explore opportunities that could lead to a political declaration and starting point for discussions on guiding standards around risk-analysis, export control mechanisms and legal principles around the use of lethal force with uncrewed systems.

States should establish and resource a Governmental Group of Experts on Uncrewed Systems in relation to Peace and Security. The groups should explore, inter alia, options to make a living document for export controls on drone and drone-related technology; review how existing arms and dual use export control regimes, including

[256] Dr Christina Schori Liang, 'Ten Lessons from the Russia-Ukraine War', March 31, 2025, https://www.visionofhumanity.org/10-lessons-from-the-russia-ukraine-war/
[257] ibid.
[258] PAX, *Between Terror Strikes and Targeted Killings-The evolving role of drone warfare in Iraq*, October 31, 2023, p.24 https://paxforpeace.nl/publications/between-terror-strikes-and-targeted-killings/
[259] ibid., p.25

the Arms Trade Treaty, the Wassenaar Arrangement[260] and the Missile Technology Control Regime, can be a tool for improving oversight on exports; and periodically review latest developments on the novel risk to peace and security associated with proliferation and use of uncrewed systems.

CONCLUSIONS

The impact of EDT on societies will be uneven but also unpredictable, generating a number of unintended consequences, including on terrorism. In this respect, ISA should understand how state and non-state adversaries are able to innovate and combine different tools in order to exploit specific vulnerabilities of our societies. We have to recognise the fact that new technologies will be rapidly adopted and adapted by VEO when accessible, cheap, simple to use, transportable, concealable and effective. The development and proliferation of commercial drones, cyber weapons, 3D printing, robotics, AI and autonomous systems can increase the mobility and reach of terrorist organisations. AI has further democratized the access to dual-use technological innovations, offering VEOs the potential reach to technologies that will multiply their destructive capabilities. Terrorists can exploit software in various ways, including: reverse-engineering of open-source military programs, leaked battlefield applications, drone control software, and AI targeting systems that can be repurposed.

In order to operate successfully in a VUCA Environment, ISA need to adapt their strategies, tools and methods. The spread of EDT among state and non-state actors introduces a new asymmetry in warfare. Success will now depend on *'innovation power'*, the capacity to invent, adapt and deploy new technologies more swiftly than our adversaries. These new technologies (high-performance computing, cloud, advanced sensors, AI and data analytics) offer tremendous potential to transform critical intelligence missions and processes in the near term. Other technological advances, especially in space-based collection, quantum, robotics, nanotechnologies and synthetic biology, will also offer new opportunities for the ISA.

However, these capabilities bring with them complex legal and ethical considerations, being a strong public expectation that ISA will act so that citizens' rights and freedoms are protected. The scale of surveillance, data collection and targeting requires proper policy and legal frameworks to prevent civilian casualties, improve accountability and oversight and adhere to international legal principles and treaties.

[260] The Wassenaar Arrangement is a multilateral regime for controlling the export of conventional arms and dual-use goods and technologies. The Wassenaar Arrangement, Introduction, at https://www.wassenaar.org/

CHAPTER 8

CYBER DIPLOMACY IN THE SPACE AGE: FOSTERING THE RESPONSIBLE USE OF SPACE FOR GLOBAL SECURITY

Özgün Erler Bayır[261]

Seray Baykal[262]

ABSTRACT

In today's world, humanity is grappling with transnational challenges such as cybersecurity and digital threats, transnational crime, and climate change etc. In this rapidly evolving landscape, technology is not merely a backdrop but a driving force reshaping how these issues are addressed. Among these challenges, cyber threats stand out as a significant risk to nations' digital systems, impacting critical infrastructure, financial networks, and public services. They have the potential to destabilize economies, compromise national security, and erode public trust. Moreover, as space technologies become more integrated into global communications, navigation, and defense systems, they are increasingly targeted by cyberattacks, posing new security risks. In particular, satellites and other space infrastructure have become essential to modern life, making their protection crucial for cybersecurity. In this sense, cyber diplomacy emerges as a vital tool to foster collaboration, build trust among nations, and establish norms for managing cybersecurity risks, particularly those linked to space technologies. Besides, cyber diplomacy offers a framework for mitigating risks, ensuring that space technologies are used responsibly and securely. This article examines the role of cyber diplomacy in addressing cybersecurity threats, particularly those targeting nations' digital systems and space-based infrastructure, and explores how emerging disruptive technologies, coupled with the responsible use of space, can be directed toward the common good. Thus, it underscores the potential of diplomatic efforts to transform disruptive forces into opportunities for global peace and security.

Keywords: cyber diplomacy, cybersecurity, cyberattacks, space, technology.

[261] Professor Dr., Istanbul University, Faculty of Political Sciences, Department of Political Sciences and International Relations, Istanbul, Türkiye, E-mail: ozguner@istanbul.edu.tr, ORCID: 0000-0002-5906-4362.

[262] PhD., Istanbul University, Faculty of Political Sciences, Department of Political Sciences and International Relations, Istanbul, Türkiye, E-mail: seray-yildirim@live.com, ORCID: 0000-0003-0465-248X.

Introduction

The rapid technological innovations and globalization processes of the 21st century have made the world and global relations increasingly complex and characterized by interdependencies, thereby necessitating a transformation in diplomatic practice. Beyond this, the multifaceted exploration of space and the potential for space technologies to be utilized for the benefit of humanity exert additional influence on these processes and interactions. The extensive development of technology—particularly in the field of space technologies—has generated numerous cybersecurity threats and challenges. Effectively managing these risks while prioritizing constructive, rather than destructive, approaches constitute a key responsibility for states and other actors. In this context, cyber diplomacy assumes a critical and indispensable role in the space age, acting as a central mechanism to address emerging cybersecurity challenges and ensure the responsible and constructive utilization of technological advancements.

Focusing on the intersection of cyber diplomacy and space technologies, in this article an attempt is made to investigate how cybersecurity threats to digital and space infrastructures can be managed, and how emerging disruptive technologies, when responsibly utilized, may advance humanity's shared global interests and global security. To this end, the article is organized into three principal parts. The first part titled "Cyber Diplomacy: A New Phenomenon in International Relations", primarily examines the evolution of diplomacy and the concept of cyber diplomacy, aiming to provide an analytical overview of the conceptual framework. One of the primary challenges in any study addressing emerging forms of diplomacy lies in the relative 'weakness at the level of conceptualization'. Concepts have struggled to keep pace with the rapid and unprecedented advancement of technology, and the generally accepted level of conceptual clarity in the literature is even more elaborate for new diplomatic forms, posing a significant challenge to analysis. Even international relations and diplomacy experts often encounter difficulties in distinguishing between or delineating the interconnections among various forms including digital diplomacy, cyber diplomacy, innovation diplomacy, virtual diplomacy, and space diplomacy. It needs to be recalled that diplomacy fundamentally prioritizes the peaceful resolution of international challenges, as well as the use of instruments aimed at maintaining peace in foreign policy. From this perspective, it is essential to highlight that the meaning and substance of any "new" form of diplomacy should be constructive and positive.

When it comes to global security threats and risks, negotiation and reconciliation, together with efforts to address these challenges through state-level alliances and cooperative mechanisms, constitute the fundamental approaches that diplomacy ought to embrace. Accordingly, when addressing the global security threats and risks in cyberspace and the challenges posed by disruptive technologies—the central focus of this article—the emphasis on diplomacy should not be overlooked. It is also important to highlight that cyber diplomacy entails the secure use of digital tools, as well as conducting digital diplomacy and technological activities within safe and controlled cyber environments.

In the second part of the article, titled “From Earth to Orbit: The Expanding Scope of Cybersecurity Threats”, the developments in technological infrastructure and frameworks on Earth and in space are examined, along with corresponding advancements in cyberspace, cybersecurity and cyberattacks. The advancement of space-based systems has accordingly transformed both the characteristics and magnitude of these cyberattacks. Considering the entirety of cyberattacks and their complex nature and expanding scale, their connection to space technologies is also highlighted as an additional dimension of cyber security threats. In this part, the issue is elaborated upon and diversified through examples.

In the third and final part, titled “Responsible Use of Space and the Barriers to Effective Cyber Diplomacy”, the focus is on analyzing the relationship between the effective conduct of cyber diplomacy and the responsible use of space technologies, and drawing relevant inferences. In this part we evaluate the barriers that hinder the efficacy of cyber diplomacy and explores potential solutions, particularly within the space domain, aimed at facilitating the collaborative resolution of global challenges. Another key emphasis is on the potential of leveraging space technologies to address cybersecurity threats. In this manner, technology is framed not merely as a challenge but as an opportunity to advance constructive and responsible outcomes.

Cyber Diplomacy: A New Phenomenon in International Relations

The growing complexity, interconnectivity, and fragmentation of the world have driven the evolution of diplomacy. In particular, technological advancements and globalization in the 21st century have been key drivers of this transformation (Cooper, Heine and Thakur, 2013: 10). Traditional diplomacy, which also involves conference diplomacy, summit diplomacy, and ad hoc diplomacy rooted in formality and state-centric dialogue (Cooper, 2013: 6), now faces the challenge of operating in a far more dynamic and unpredictable environment shaped by a growing number of transnational issues (Bayır, 2023: 2-3).

Today, humanity is grappling with several transnational challenges such as cybersecurity and digital threats, transnational crime, climate change and etc. (Christou, 2024: 6). Addressing these complex issues requires the involvement of non-state actors including scientists, experts, and international and intergovernmental organizations alongside traditional actors such as leaders and diplomats (Barrinha and Renard, 2017: 4-5). Certainly, this shift has contributed to the emergence of new forms of diplomacy, such as cyber diplomacy, digital diplomacy, health diplomacy, environmental diplomacy, refugee diplomacy, and others.

The most significant differences between traditional and new types of diplomacy lie not only in the increased number and diversity of actors involved but also in the expanded range of issues addressed and the variety of communication channels used (Cooper, Heine and Thakur, 2013: 1). Unlike traditional diplomacy, which primarily operates through formal diplomatic channels and official ministerial meetings, new types of diplomacy take place across multiple platforms including social media, digital forums, and even virtual environments like the metaverse (Bayır, 2023: 3). These new channels allow for faster communication, broader public engagement, and

more flexible interactions, fundamentally transforming how diplomacy is pursued and negotiated. In addition, when recent global challenges such as climate change, the refugee crisis, and cybersecurity became integral subjects of diplomacy, the nature, and priorities of diplomacy in the 21st century evolved accordingly (Hocking, 2020: 82-83).

In this rapidly evolving landscape, cyber diplomacy has emerged as a new form of diplomacy in response to the growing need for diplomatic engagement in the cyber domain. It is important to note that cyber diplomacy is less than two decades old (Lewis, 2025: 15). As cybersecurity issues began to pose greater risks to the security of both state and non-state actors through cyberattacks and other threats, it became a critical concern for international relations and an essential area for diplomatic efforts (Barrinha, 2024: 440). Undoubtedly, digitalization and new technologies have significantly increased the political and strategic importance of cyberspace.

This growing significance of cybersecurity is evident in how international organizations such as NATO and the European Union have adapted their policies to address emerging cyber threats. For instance, cyber defense was included in the Alliance's political agenda at the 2002 NATO Summit in Prague following a sharp increase in cyber threats that had become more destructive, coercive, and frequent in the 21st century. A further milestone came at the 2014 NATO Summit in Wales, where cyber defense was recognized as a core task of NATO's collective defense, enabling the potential invocation of Article 5 of NATO's founding treaty in the event of a cyber-attack (NATO, 2024). Most importantly, cyberspace was officially recognized as a domain of operations for NATO, alongside land, sea, and air at the 2016 NATO Summit in Warsaw (NATO, 2016).

Similarly, since the early 2000s, the increasing number of cyberattacks in European countries, with the most serious one occurring in Estonia in 2007, prompted the European Union to develop its first comprehensive policy document dedicated to cyberspace titled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace" in 2013 (Christou, 2024: 12). Since then, several other strategic documents that integrate cyber defence have been published, including "The EU Cybersecurity Strategy for the Digital Decade" in 2020 (European Commission, 2020) and "The Strategic Compass for Security and Defence" in 2022 (Council of The European Union, 2022), aiming to enhance preparedness and strengthen response capability of the union to cyberattacks.

In addition to NATO and the European Union, several countries have recognized cyberspace as a critical domain and have taken initiatives in recent years to address associated risks and threats. For instance, the United States' "Cyberspace Policy Review" and the United Kingdom's "Cyber Security Strategy", both published in 2009, along with China's "White Paper on the Internet in China" released in 2010, primarily focused on the domestic dimensions of cybersecurity (Barrinha and Renard, 2017: 8). Subsequently, under the Obama administration, the United States established the "Office of the Coordinator for Cyber Issues" in 2011. Following this move, countries such as Japan, Germany, and Australia also took steps to enhance the security and safety of their respective cyber domains (Christou, 2024: 10). While there are various examples of such initiatives, this chapter focuses only on selected

national and institutional approaches to illustrate key developments in the field, as a more comprehensive country-based review is beyond the scope of this study.

Cyber diplomacy involves the use of diplomatic tools to address and manage challenges arising in cyberspace. More broadly, it can be defined as diplomacy conducted in the cyber realm (Lewis, 2025: 15-16). **Cyber diplomacy aims to prevent and regulate conflicts in cyberspace among states, the private sector, and civil society, while also building bridges for cooperation and the development of shared norms and frameworks in cyberspace (**Tiirmaa-Klaar, 2025: 27). According to the US Department of Defense, cyberspace defined as *"a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"* (Jabbour and Ratazzi, 2012: 33).

Since cyber diplomacy is often employed to tackle issues that relate to the scope of digital diplomacy, the two terms are frequently used interchangeably in the literature. However, they are not entirely synonymous. Digital diplomacy refers to the use of digital tools and technologies in the conduct of diplomacy (Bjola, 2015: 4), whereas cyber diplomacy focuses on ensuring the resilience, safety, and security of citizens, government institutions, military operations, and critical infrastructure in the cyber realm. In other words, cyber diplomacy is concerned with conflict resolution and diplomatic engagement in cyberspace (Martonffy, 2022: 10).

From Earth to Orbit: The Expanding Scope of Cybersecurity Threats

In the digital age, new technologies are strongly linked to national power. Since these technologies have the ability to impact the main sources of a state's power such as military capabilities, economic strength, and political influence in the international arena, states are committed to advancing their technological capabilities (Lewis, 2025: 23). With the growing importance of cyberspace, ensuring the security of cyberspace has become a national and international strategic priority as well as a critical necessity for both state and non-state actors to build a trustworthy, safe, and resilient digital ecosystem (Barrinha and Renard, 2017: 7). This enables the maximization of benefits and opportunities presented by new technologies and digitalization in the 21st century, while minimizing the associated risks and threats.

Unfortunately, cyber threats come in various forms, including attacks on public institutions, corporate targets, and critical infrastructure; political and economic cyber espionage; interference in democratic processes such as elections; the use of offensive cyber capabilities during both peacetime and wartime; and threats targeting financial networks and public services. These threats, which range from state-sponsored cyberattacks to ransomware campaigns, have the potential to destabilize economies, compromise national security, erode public trust, and undermine the security of critical infrastructure, essential services, and the livelihood of ordinary citizens. They can also lead to the loss of sensitive government data and the online theft of intellectual property (Tiirmaa-Klaar, 2025: 26).

To have a better understanding of these threats, it is important to highlight concrete examples. One of the most well-known malicious cyber activities is undoubtedly the attack on Estonia in 2007, which lasted for 22 days. This event

marked Estonia as the first country to become a globally recognized victim of a large-scale cyberattack (Van Camp and Peeters, 2022). The incident was triggered when the Estonian government decided to relocate a Soviet-era monument from central Tallinn to a nearby military cemetery, sparking political tension between Estonia and Russia. Following the decision, protests erupted between pro-Kremlin groups and nationalists, eventually leading to a coordinated cyberattack targeting Estonia's government networks and information systems. Despite its small size, Estonia is a highly digitalized and networked country, especially in its public services. Therefore, the cyberattack caused significant disruptions, affecting not only government and business operations but also the daily lives of ordinary citizens throughout the 22-day period (Ottis, 2008: 1-2). This attack demonstrated that cyber threats whether small or large in scale pose a serious risk to national security, as evidenced by the case of Estonia.

Another significant example is the 2017 cyberattack on Qatar. During this incident, the Qatar News Agency website was hacked, along with associated websites and social media platforms. Unlike the Estonian case, this attack was shorter in duration, lasting only three hours. However, its impact was substantial, as it targeted the country's primary news agency. According to official statements, the attackers installed malicious software to fabricate and publish false stories about Qatar and the Emir himself. Qatari officials accused the United Arab Emirates and Saudi Arabia of being behind the attack, arguing that its sophistication suggested the involvement of state-level resources (Al-Rawi, 2019: 1311). Despite these accusations, it remains unclear whether the United Arab Emirates or Saudi Arabia directly orchestrated the attack or whether it was carried out by actors linked to the countries.

While both the Estonian and Qatari cases had serious national level consequences, another example, "the NotPetya" attack on Ukraine, demonstrated how cyberattacks can escalate to a global scale crisis. It was widely regarded as one of the most devastating cyber incidents to date. The NotPetya attack occurred in Ukraine in 2017. Despite ongoing debate over the responsible parties, the attack chiefly targeted Ukrainian government institutions, banks, and airports that rely on digital infrastructure (Peeters, 2022). The malware quickly spread to nearly sixty countries, disrupting global operations, and causing an estimated 10 billion USD in financial losses across many economic sectors around the world (Tiirmaa-Klaar, 2025: 28).

Building on the growing complexity and scale of such cyberattacks, it is important to highlight another critical dimension of cyber threats, whose significance has been steadily increasing in recent years: their connection to space technologies. Space-based systems are becoming increasingly integrated into global communications, navigation, and defense networks. In particular, satellites and other space infrastructure have become essential to modern life, making their protection crucial (European Union Agency for Cybersecurity, 2025: 29). While these systems play a key role in cybersecurity, they are also vulnerable to attacks, introducing new and complex security risks.

Previously, espionage and physical interference were the primary threats to satellites. However, the risk has expanded in the recent years with the advancements

in digital and AI-based tools which enable more complex and resource-efficient attacks than in past decades. Since satellites are controlled by advanced digital systems and heavily rely on software, they have become highly vulnerable to cyber interference. Cyberattacks on satellites often include jamming, hacking, or even taking full control of the system. In many cases, the effects of such attacks can range from temporary disruption to a complete system failure. While military satellites are the primary targets, it is significant to note that commercial, civilian, and other types of satellites are also frequently at risk (Patil, 2015: 20-21).

According to the US Space Force's doctrine publication titled "Operations: Doctrine for Space Forces", (2023), the domains of space and cyberspace are deeply interconnected, as space communications inherently encompass elements of cyberspace. The report underscores that the protection of space capabilities necessitates comprehensive and integrated cyber defense strategies, recognizing that vulnerabilities within cyberspace can have direct and significant impacts on space operations and overall mission effectiveness (US Space Force, 2023: 18-19).

In this sense, it is also important to highlight the view of General Stephen Whiting, Commander of the U.S. Space Command from 2020 to 2024, who emphasized the significant connection between cyberwarfare and space warfare. He describes cyberspace *"is the soft underbelly of our global space networks",* underscoring the critical vulnerabilities that cyber threats pose to space-based systems (Klein, 2024). Therefore, addressing and mitigating the growing number of cyber threats is critically important to ensure the resilience and security of space operations in the near future.

A striking example of this vulnerability was demonstrated in one of the most significant cyberattacks on satellite infrastructure: the attack on Viasat's KA-SAT satellite network, which occurred just hours before Russia's invasion of Ukraine in 2022. This network was primarily used by the Ukrainian military, but it also supported civilian services. While both the United States and the European Union attributed the attack to Russia, and the United States provided additional technical details supporting the involvement of Russian military cyber operators, Russia has denied all accusations. The attack occurred in two stages. In the first stage, the attackers targeted internet modems used by the Ukrainian army, government, and security services, effectively disrupting communications. In the second stage, they breached a ground-based network, gained remote access to the system, and ultimately took control of the satellite communication infrastructure, allowing them to issue malicious commands (ESPI, 2022: 5).

Although the Ukrainian army, government, and security services were the primarily affected, the impact of the attack spread across Europe. Since the KA-SAT satellite network is also linked to other services and operations across Europe, the attack had a broader spillover effect. To illustrate, approximately 9.000 subscribers of NordNet, a French telecommunications company, and around one third of the 40.000 subscribers of the British broadband provider BigBlu were affected. In addition, the German energy company, Enercon experienced disruptions, as the remote control and monitoring of its wind turbines became unavailable due to their reliance on the KA-SAT network. The attack also resulted in widespread loss of internet connection across various regions that heavily depended on the KA-SAT satellite network (ESPI,

2022:6). It is believed that the KA-SAT cyberattack occurred through the exploitation of vulnerabilities that had already been identified in previous threats to space systems.

Responsible Use of Space and the Barriers to Effective Cyber Diplomacy

Undoubtedly, rapid technological change and global interconnectivity have become key drivers of the intensification of malicious cyber activities, as illustrated with examples in the previous chapter. In this rapidly evolving landscape, technology can also be seen not merely as a backdrop but as a central force reshaping how these challenges are perceived and addressed (Barrinha, 2024: 448). This transformation for instance, presents significant institutional challenges particularly for ministries of foreign affairs, as they are tasked with responding to emerging threats while managing diplomatic relations in an environment increasingly shaped by technological developments (Tiirmaa-Klaar, 2025: 26).

In this context, cyber diplomacy emerges as a vital instrument for addressing these challenges by fostering collaboration, building trust among nations, and establishing norms for managing cybersecurity risks. This is particularly crucial in areas such as space technologies, where the risks are exceptionally high (Tiirmaa-Klaar, 2025: 27). The responsible use of space, therefore, emphasizes the need to protect space-based assets from cyberattacks and to ensure that space technologies are developed in ways that contribute to global peace and stability, rather than exacerbating security concerns while also promoting the application of existing international laws, agreements, and norms. Cyber diplomacy supports this effort by providing a framework for cooperation and norm-building to mitigate risks and enhance the resilience of space systems (Tiirmaa-Klaar, 2025: 28-29-30). In this sense, it should also be noted that the responsible use of space depends on the effective implementation of cyber diplomacy. However, implementing cyber diplomacy effectively remains a complex task due to various institutional, political, and technical challenges.

One of the most significant issues arises from the divergent national priorities of the countries regarding cybersecurity. While countries such as the United States, the United Kingdom, China, Australia, or highly digitalized states like Estonia began addressing cybersecurity in the early 2010s (Barrinha, 2024: 455), many other countries have recently begun to adopt policies and develop strategic documents aimed at ensuring the security and resilience of their cyber ecosystems (Lewis, 2025: 17). In general, although all the countries are concerned with security of cyber space, national priorities in this context vary widely from political and military concerns to issues such as data regulation, attribution, and the development of United Nations cyber norms (Barrinha, 2024: 459). Certainly, this divergence poses a significant challenge for cyber diplomacy efforts and makes it difficult to reach consensus on shared threats and coordinated responses to key issues.

Another issue is that, despite its growing importance, cyber diplomacy remains a domain that needs to be more ambitiously integrated into the international diplomatic agenda. The international positioning of cyber diplomacy can only be strengthened if more countries increase both the number of their cyber diplomats and the presence of dedicated cyber offices within their ministries of foreign affairs (Barrinha, 2024: 454). This considered as a crucial point, as efficient and solution-based discussions whether

at the United Nations or in committees dedicated to cybersecurity can only be effective when counterparts are able to engage and exchange views equally. For instance, Christopher Painter's, statements, the first Coordinator for Cyber Issues at the U.S. State Department (Barrinha and Renard, 2017: 9), are significant as it supports the argument. He underlined this issue by stating that in cyber diplomacy meetings, it was often very difficult to find counterparts, as many countries were sending representatives from interior or justice ministries, or bureaucrats from those departments (Barrinha, 2024: 455).

Thirdly, it is evident that preventing malicious cyber activities requires not only technical expertise but also robust international cooperation. Indeed, the United Nations plays an indispensable role in global discussions and efforts to establish globally accepted norms in this realm. However, multilateral organizations such as the Organization of American States (OAS), the Organization for Security and Co-operation in Europe (OSCE), the Association of Southeast Asian Nations (ASEAN), and the African Union which already include cyber diplomacy in their agenda also have a significant impact on fostering global negotiations at the United Nations level (Lewis, 2025: 17-18). Certainly, these regional organizations contribute to shaping the international agenda. Similarly, the development of national cybersecurity strategies in many countries over the past decade has also led to increased international attention, as reflected in the growing number of summits, meetings, and conferences dedicated to cybersecurity issues and risks in recent years (Barrinha and Renard, 2017:8). However, these efforts should be enriched in order to foster robust international cooperation especially at the United Nations level, as the United Nations remains a primary mechanism for regulating and setting global norms regarding global issues including cybersecurity.

Lastly, it is important to mention international law and binding agreements in the context of cybersecurity. Although there are binding norms and frameworks concerning emerging technologies like the Geneva Conventions and International Atomic Energy Agency (IAEA) Treaty, there is still no universally binding international agreement specifically addressing cybersecurity. For instance, in cases of armed conflict, the Geneva Conventions are the cornerstone of modern warfare and the issues arising from armed conflict. In some instances, their principles can be extended to cover technological warfare as well (Lewis, 2025:24). Similarly, the IAEA Treaty offers a legal framework and compliance mechanisms for the non-proliferation of nuclear weapons. On the other hand, the applicability and effectiveness of existing legal frameworks remain limited, particularly regarding the scope, consequences, and most importantly the compliance mechanisms of technological warfare, such as cyberattacks targeting satellite systems or the networks and infrastructure of governments (Lewis, 2025:18). This undoubtedly hinders effective implementation of cyber diplomacy by creating opportunities for malicious cyber activities and causing to anarchy in cyber domain (Barrinha and Renard, 2017: 11).

Conclusion

This article focuses on the nexus of space technologies, diplomacy, and the cyber domain. Within this framework, the concept of the responsible use of space encompasses not only benefiting from space technologies while preventing the

pollution of space and safeguarding its sustainability, but also ensuring that these technologies contribute to addressing humanity's shared global challenges. Thus, the responsible use of space is not merely about environmental preservation; it also emphasizes leveraging technological progress, particularly in space, for the common good and global security. Ensuring the responsible use of space requires, above all, the effective use of diplomacy within the cyber space.

Cyber diplomacy, in particular, requires a coherent set of critical regulations at both the state level and within international organizations. At present, however, cyber diplomacy is constrained by significant gaps in existing legal frameworks and international agreements, as well as by the absence of a universally accepted set of norms. These shortcomings hinder the effectiveness of cyber diplomacy. Rather than functioning as a tool for human-centered, norms- and rules-based solutions, technology is often perceived as a challenge that exacerbates existing problems. Nevertheless, this challenge can be reframed as a strategic opportunity. By leveraging space technologies, solutions to global (security) challenges can be developed more efficiently and effectively, provided that existing obstacles are adequately addressed. The establishment of international norms, coupled with mechanisms to ensure compliance through enforceable measures at the organizational level, would significantly enhance the efficacy of cyber diplomacy. In turn, this would facilitate the responsible use of space, while converting the potential adverse effects of technological advancement into constructive and positive outcomes.

The substantial developments and advancements in the fields of destructive technologies and space have undoubtedly generated negative effects and increased security-related risks. Nevertheless, these risks can be significantly mitigated if key underlined factors are effectively addressed, leading to their substantial reduction. At the heart of this process lies the essential requirement for the effective execution of cyber diplomacy. Once successfully operationalized, cyber diplomacy not only strengthens the responsible use of space but also enhances its own efficacy, thereby enabling both domains to function in a more coordinated, strategic, and constructive manner.

At this point, it is essential to emphasize and draw attention to the use of space technologies not in a destructive manner, but rather as instruments for addressing global security challenges—mitigating the negative impacts of wars, terrorist attacks, cyber threats, and other similar adversities. Achieving this requires a well-coordinated adaptation between technology and diplomacy. In addressing aforementioned threats, the focus should primarily be on peaceful approaches and diplomacy rather than on warfare and confrontational methods, ultimately serving the common interests of humanity and global peace and security. Since diplomacy represents a peaceful instrument in foreign policy, whether in the form of space diplomacy or cyber diplomacy, the underlying motivation remains consistent: 'to manage and resolve global challenges constructively'. The responsible use of technology to advance collaborative approaches to addressing global security challenges entails, on one hand, ensuring sustainability and maintaining equilibrium in space through the deployment of space technologies, and on the other hand, effectively harnessing the benefits these technologies provide in a constructive and accountable manner.

To sum up, in recent years, alongside rapid technological advancements, traditional diplomacy methods and practices—which have not historically aimed to extensively incorporate scientific, technological, and innovation policy considerations—have been compelled to undergo significant transformation. When the relationship between technology and diplomacy is examined, the resulting dynamics can be evaluated from a 'challenges and opportunities' perspective. In the context of cyber-related issues, the first considerations that often come to mind are cyberspace, cyber threats, and digital risks, highlighting the potentially negative and destructive impacts of technology. Such impacts constitute a technological challenge that demands systematic and effective addressing. However, in order to transform these risks and challenges into opportunities, it is essential that all these new tools and technological developments be effectively adapted to diplomacy, enabling a transition toward hybrid approaches. Through such adaptation, existing security threats and risks can be converted into advantages. At the global level, it is evident that significant progress can be achieved when collaboration and coordination among all actors—including international organizations, states, private sector, and the international community—are ensured, and the gaps outlined above are effectively mitigated, particularly through the establishment of norms and the robust development of conceptual frameworks.

In conclusion, it is important to emphasize that at the core of these considerations lies the imperative to establish a more concrete and rules-based nexus between diplomacy and science and technology. Ensuring secure and reliable engagement, particularly in digital domains and cyberspace, is a crucial factor that enhances the capacity and agency of both state and non-state actors. Moreover, with recent technological developments and new infrastructures—particularly those increasingly linked to space—the responsible use of space has gained even greater prominence. In traditional space activities, the focus was primarily on missiles, armament, and large-scale state-led investments. In the emerging "New Space" paradigm, however, actors have diversified: private companies and the commercial sector have become primary stakeholders alongside states, and costs have decreased considerably. Consequently, this development simultaneously raises both risks and opportunities. The increasing integration of space technologies across all aspects of life, coupled with cost-effective yet impactful initiatives such as CubeSat, represents a significant opportunity for addressing humanity's shared global challenges. This pathway can be facilitated through support from new forms of diplomacy, including particularly cyber diplomacy, science diplomacy, and space diplomacy. The primary responsibility, undoubtedly, rests collectively with both state and non-state actors, and the alignment of their goals and coordination efforts becomes increasingly critical in this context.

References

Al-Rawi, A. (2019). Cyberconflict, online political jamming, and hacking in the Gulf Cooperation Council. *International Journal of Communication, 13,* 1301–1322.

Barrinha, A. (2024). Cyber-diplomacy: The emergence of a transient field. *The Hague Journal of Diplomacy, 19,* 439–466. https://doi.org/10.1163/1871191x-bja10183

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs, 3*(4–5), 353–364.

Bayır, Ö. E. (2023). *Yeni-yeni diplomasi*. Altınbaş University Publications.

Bjola, C. (2015). Introduction: Making sense of digital diplomacy. In C. Bjola & M. Holmes (Eds.), *Digital diplomacy: Theory and practice* (pp. 1–9). Routledge.

Christou, G. (2024). Cyber diplomacy: From concept to a practice. *Tallinn Papers*, No. 14. NATO Cooperative Cyber Defence Centre of Excellence.

Cooper, A. F. (2013). The changing nature of diplomacy. In A. F. Cooper, J. Heine, & R. Thakur (Eds.), *The Oxford handbook of modern diplomacy* (pp. 1–14). Oxford University Press.

Cooper, A. F., Heine, J., & Thakur, R. (2013). Introduction: The challenges of 21st-century diplomacy. In A. F. Cooper, J. Heine, & R. Thakur (Eds.), *The Oxford handbook of modern diplomacy* (pp. 1–23). Oxford University Press.

Council of the European Union. (2022). *The strategic compass for security and defence*. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf

European Commission. (2020). *The EU cybersecurity strategy for the digital decade*. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European Space Policy Institute. (2022). *The war in Ukraine from a space cybersecurity perspective*.

European Union Agency for Cybersecurity (ENISA). (2025). *Space threat landscape* (E. Rekleitis & M. Adamczyk, Eds.).

Hocking, B. (2020). Communication and diplomacy: Change and continuity. In T. Balzacq, F. Charillon, & F. Ramel (Eds.), *Global diplomacy: An introduction to theory and practice* (pp. 79–96). Palgrave Macmillan.

Jabbour, K. T., & Ratazzi, P. E. (2012). Does the United States need a new model for cyber deterrence? In A. B. Lowther (Ed.), *Deterrence* (pp. 33–45). Palgrave Macmillan.

Klein, J. (2024). *Space and cyber warfare as one*. Center for Strategic & International Studies (CSIS). https://www.csis.org/analysis/space-and-cyber-warfare-one

Lewis, J. A. (2025). An overview of cyber diplomacy. In A. Salvi, H. Tiirmaa-Klaar, & J. A. Lewis (Eds.), *A handbook for the practice of cyber diplomacy* (pp. 15–24).

Martonffy, B. (2022). Cyber diplomacy: A review from the literature. In A. Molnar & B. Martonffy (Eds.), *Cyber diplomacy from the European perspective* (pp. 7–36). Ludovika University Press.

NATO. (2016). *Cyber defence pledge*. https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NATO. (2024). *Cyber defence*. https://www.nato.int/cps/en/natohq/topics_78170.htm

Ottis, R. (2008). Analysis of the 2007 cyber-attacks against Estonia from the information warfare perspective. *Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromIWP.pdf

Patil, P. A. (2015). Cyber-attacks on satellites: A paradigm shift in ASAT application. *Air Power Journal*, *10* (3), Monsoon.

Peeters, W. (2022). Cyberattacks on satellites: An underestimated political threat. *LSE IDEAS, Space Policy Project*. https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites

Tiirmaa-Klaar, H. (2013). Cyber diplomacy: Concepts and core competencies. In A. F. Cooper, J. Heine, & R. Thakur (Eds.), *The Oxford handbook of modern diplomacy* (pp. 26–44). Oxford University Press.

United States Space Force. (2023). *Space doctrine publication 3-0, operations: Doctrine for space forces*.

Van Camp, C., & Peeters, W. (2022). A world without satellite data as a result of a global cyber-attack. *Space Policy, 59.* https://www.sciencedirect.com/science/article/abs/pii/S0265964621000503

CHAPTER 9

INNOVATIVE TOOLS AVAILABLE TO NON-STATE ACTORS: AERIAL DRONES AND UNMANNED SYSTEMS AT SEA AND ON LAND

Sıtkı Egeli

Preamble

In recent years, unmanned vehicles – also referred to as uncrewed or uninhabited by some observers – have been transforming the face of modern warfare at unprecedented pace. Systems ranging from unmanned aerial vehicles to uncrewed boats and submersibles to ground vehicles have fast become standard, indispensable features of modern battlefields. Whereas the primary focus has been on drones possessed and employed by military forces of states, equally noteworthy and possibly more concerning has been rapid, at times instant proliferation of ever-more capable drone types among non-state actors. Consequently, drones in the hands of nefarious lone wolves, terrorist groups, crime syndicates and/or accomplices in hybrid warfare tactics have come to redefine and preoccupy the threat perceptions and security agendas of states around the world. Complementing this picture has been the rush to develop and deploy devices and measures aimed at countering the pressing threat posed by the seemingly unrestrained availability and employment of unmanned vehicles.

It is against this background that this chapter will seek to scrutinise first the use of drones by non-state actors, and second, the ways in which states sought to counter this growing threat. Given their two-decade headstart over sea and ground equivalents, the primary focus will be on Unmanned Aerial Vehicles (UAVs) whose historical evolution within the context of their use by and against non-state actors will be analysed in three consecutive time periods. A brief overview of the available options and technologies for defending against UAVs will also be provided. The last section of the chapter will be addressing unmanned vehicles and technologies in maritime, underwater, and land domains whose relevance has been growing in recent years.

First Phase: 1990s to 2014

Contrary to conventional wisdom, the first remotely controlled vehicle was not a plane, but a boat. In 1898, technology pioneer Nikola Tesla manoeuvred a small boat remotely utilizing radio signals emitted from a control box. Though commercial and military applications took decades to mature, this groundbreaking invention laid the foundations and set the key principles for remote-controlled vehicles which have remained unaltered to this day (Beschloss, 2013). Soon afterwards, there were early attempts at using remotely controlled aircraft as targets for gunnery practice in the

early twentieth century. During the interwar period and into the Second World War, the drone was imagined as a flying bomb and used as such by the Nazi Germany. During the subsequent Cold War period, the drone was seen as a viable surveillance platform to capture intelligence in denied areas. This has resulted in the first significant use of drones in military history. Between 1964 and 1975, more than a thousand jet-powered American drones flew over 34,000 photographic and electronic reconnaissance missions over Vietnam and all across Southeast Asia (Shaw, 2015).

Despite their early lead in drone warfare, during 1970s the Americans let the torch pass to the Israelis. Having realised the reconnaissance potential of its U.S. supplied jet-powered drones, from 1974 onwards Israel began developing less complex and inexpensive UAVs of its own. The first locally produced UAVs – Mastiff and Scout – entered operational service in 1979. Signifying the first known employment of UAVs to watch non-state actors, those UAVs were used to monitor Palestinian activity inside Lebanon. Some of those were also flown during the 1982 war over the skies of Bekaa Valley. Yet Israel's growing fleet of UAVs were flown during this period in support of ground forces just as they would be operated in a conflict against conventional armies. The turning point arrived in the early-1990s, when more capable UAVs – e.g. Searcher – emerged and began patrolling the Israeli-imposed security zone in southern Lebanon to detect infiltrations by Hezbollah militants. In 1992, a *Searcher* UAV directed helicopter gunships for the targeted killing of a Hezbollah official travelling by car inside Lebanon (Tovy, 2024, p.200-2). Those were the first publicly known instances of UAVs being deployed and employed specifically to fight an armed non-state actor (ANSA).

Besides Israel, Türkiye can be singled out during this timeframe as the second country to -deploy UAVs to combat ANSAs, in this case PKK – Kurdistan Workers Party – a designated terrorist organisation, which was engaged in a brutal and indiscriminate campaign against civilian and military targets in Türkiye's southeast. In 1992, Türkiye purchased GNAT-750 UAVs from a startup manufacturer in the U.S. Those were large and high-performance unmanned planes that could stay airborne for up to forty hours and demonstrated firsthand the biggest benefit of UAVs in combatting terrorism: 24/7 persistent and uninterrupted surveillance of potential targets and points of interest over large swaths of land. Combined with other benefits of UAVs– i.e. performing missions without putting pilots' lives at risk and reduced first acquisition and operating costs in comparison with manned aircraft – their persistence became unmanned aircraft's benchmark in a security forces' fight with non-state actors. Supplemented in 1998 by the more advanced I-GNAT derivative, GNAT series of UAVs were used exclusively in the counter-terrorism role by Türkiye (Sünnetçi, 2015, p.135). Experience gained early-on by Türkiye and the consequent realization of UAV's benefits in combatting ANSAs was instrumental in prompting Ankara's sizable industrial and budgetary investment into this domain. Its hindsight into UAV operations provided Türkiye with an important headstart and transformed the country into the world's leading UAV exporter some three decades later.

Ironically, the U.S., as the country to have originally supplied UAVs to both Israel and Türkiye, had fallen behind. Yet, this did not last long. Following on the footsteps of Türkiye, in 1994 the U.S. Central Intelligence Agency (CIA) ordered an unknown quantity of *GNAT-750* UAVs. Those were used in a more conventional miliary role and provided overhead surveillance for NATO convoys in the former Yugoslavia (Shaw, 2015). Yet they were also deployed in fifteen non-specified sites worldwide and took part in five combat operations (Aviation Week, 1998). All the while, the U.S. Air Force

too was taking notice of the benefits of long-endurance UAVs in Intelligence Surveillance & Reconnaissance (ISR) missions. In 1995, an offspring of *GNAT-750* UAV incorporating satellite dish to overcome the range limitation of line-of-sight command link was ordered and joined the U.S. military inventory as Predator. The addition of satellite dish meant American drone operators didn't have to be in the same region or continent as the UAV they were flying (Shaw, 2015).

While the initial employment of UAVs by the U.S. military was confined to supporting conventional military operations inside the former Yugoslavia, the dramatic turning point came about with the 9-11 terror attacks against American homeland. In 2001, USAF was already running tests to shorten the 'kill chain' by fitting its Predator UAVs with air-to-surface precision-guided missiles, thereby turning them into hunter-killers. After 9-11, missile-armed Predators were activated to locate and eliminate Al-Qaida linked targets and individuals first inside Afghanistan, then elsewhere around the world. Predator and its larger derivative, the Reaper's ability to hover above a target for hours, relaying high-resolution live surveillance stream day and night, and then striking that target without having to wait for manned aircraft to arrive proved invaluable. Instantly, the drones became central to the Global War on Terror and the U.S. national security strategy has since switched primarily to fighting terrorism from the skies. The consequence was dramatic expansion in the size and sophistication of drones from hand thrown models all the way to ones as same size as airliners. The quantities rushed into service exploded too. Between 2002 and 2010, U.S. inventory of drones increased forty-fold to eleven thousand, hundreds of which carried weapons. From 2001 to 2015, the U.S. used its hunter-killer drones over 500 times to kill close to 4,000 persons (Shaw, 2015).

Other U.S. allies, among them the United Kingdom, France, Italy and Germany, followed Washington's suit by purchasing Reaper, Predator and/or Israeli Heron UAVs to lend support to overseas counter-terrorism missions. Meanwhile, throughout the 2000s, Israel was busy adding ever more capable, air-to-surface missile firing models to its fleet of UAVs. But because Israel never admitted their use for attacking targets in Gaza, southern Lebanon and regions as far away as Sudan, the credit for the first use of weaponized UAVs went to the U.S. (Tovy, 2024) Otherwise, 1997 operation towards south Lebanon and the Second Lebanon War of 2006 saw dramatic expansion of Israel's employment of unmanned aircraft to survey and target Hezbollah. Likewise, during 2020 and 2023 campaigns against Hamas, UAVs were central to Israeli missions ranging from ISR and electronic interference to targeted killings (The Economist, 2023).

In retrospect, the first two decades of UAV employment against terrorist groups and other ANSAs presented clear benefits to state actors and their military and security forces. Weaponized drones fusing persistent surveillance with precision strike became the favoured weapon for states fighting ANSAs. On the other hand, this situation was about to change, and the balance was on the verge of tilting in favour non-state actors.

Second Phase: 2014 to 2022

At the outset of the UAV age, states held a strict monopoly over the ownership and employment of UAVs, especially the more sophisticated, larger variants that relied on airstrips, complex logistic and training infrastructure, and advanced defence industries. Yet, with the democratization of unmanned vehicle technologies, and the existence of states such as Iran which were keen to transfer their hardware and

knowhow to sub-state proxies, it was only a matter of time before the table was turned, and drones found their way to non-state actors.

The first documented case of a terrorist group to have considered using drones goes back to 1995. In parallel with its infamous chemical weapon attack in Tokyo's subway, Japan's apocalyptic Aum Shinrikyo cult had set its sights on using remote-controlled helicopters to disperse sarin gas (Rassler, 2016, p.IV). The next development was an uncommon incident in 1997, when Hezbollah militants in Lebanon managed to intercept surveillance footage from an Israeli UAV flying overhead and ambushed eleven Israeli naval commandos. This is the first known case of a non-state actor taking advantage of drone technology to inflict casualties on its state adversary. The incident was also a blunt reminder that militaries and security forces should never underestimate tactical and technological prowess of their non-state opponents (Katz, 2010). By mid-2000s, Hezbollah managed to acquire from Iran its own fleet of UAVs. Starting in 2004, several Iran-origin UAVs were sent into Israel's airspace for ISR as well as intimidation missions. In 2012, one of those flew all the way to the Dimano nuclear reactor before being shot down by Israeli F-16s (Gettinger and Micheal, 2014). The UAV in question was unarmed, but it nonetheless alarmed Israeli security officials to the possibility that others could fly in laden with explosives, or, worse, chemical or biological agents (Dreazen, 2014). Elsewhere, insurgents in Libya were also resorting to hobby drones to watch government forces (Ackerman, 2011).

But the real breakthrough in non-state actors' access to and employment of unmanned aircraft against their state and non-state adversaries arrived during internal conflicts in Syria, Yemen, and Iraq. In 2014, reports emerged of the Daesh militants using hand-thrown hobbyist-type drones to spy on their enemies. News then began arriving by the end of 2015 about Daesh drones rigged with explosives executing suicide dives (Schehl, 2016). Those unsophisticated, small drones resembling model aircraft were commonly referred to as First-Person View (FPV) drones. FPV drones come in various sizes and shapes. Their common characteristic is that they are readily available from commercial suppliers and could even be purchased via internet shopping. Consequently, they remain way below the catch-all proviso of existing export control regimes and arrangements, hence are accessible by all. As demonstrated very early-on by the Daesh, such drones could also be built from scratch in crude workshops using Styrofoam, plywood, duct tape and freely traded model aircraft components such as batteries, motors, RC units, and commercial cameras (Conflict Armament Research, 2016). When packed with explosives, they can easily be converted into One-Way Attack (OWA) suicide drones or loitering munitions, or else they could be employed multiple times to drop bomblets and grenades.

The Daesh did not have the monopoly over the use of FPV drones. Soon, several other ANSAs inside Syria, Iraq and Yemen ranging from Al-Qaeda affiliated groups to the PKK and the Houthis adopted the same (Gettinger, 2016). Surveillance and strike missions carried out by such FPV drones in civil war-torn countries and those adjacent to them in the Middle East and Africa have since become routine. Yet, some of the strikes executed by FPVs or comparatively lightweight OWA-UAVs stood out as the harbinger of future challenges. One case in 2017 involved the PKK hitting the Turkish military base at Şemdinli inside Türkiye's borders. This was followed in 2018 by another drone strike involving no fewer than eight PKK drones raiding the Turkish provincial centre of Şırnak. Those two strikes, plus a third one in 2021 against the Diyarbakır airport (Dri, 2021; Hambling, 2020) gave early warnings of the ease

with which FPV drones could be smuggled into and then flown from inside the territory of a targeted state, and the difficulty of dealing with such 'insider threats'.

In another incident in 2018, ten explosive-laden lightweight UAVs made of plywood and Styrofoam simultaneously flew into the Russian airbase at Humaymim, Syria, while another three hit simultaneously the Russian naval base in Tartus. Those drones flew all by themselves to the Global Positioning System (GPS) locations of targets uploaded to their crude navigation systems. They covered 50 to 100 kilometres before reaching their targets and inflicting damage on parked Russian combat aircraft (Binnie, 2018). To this day, there has been no definitive attribution citing a specific group as the perpetrator. The case in point demonstrated firsthand the challenge of attribution associated with drone strikes, and how serious a threat OWA-UAVs had become for military and civilian infrastructure.

In fact, OWA-UAVs potential in threatening states' critical infrastructure was already apparent in the way the Houthis in Yemen were already using them from 2018 onwards to strike Yemeni, Saudi and Emirati airports, oil installations, seaports and a whole variety of other civilian targets (Carlino, 2019). Yet the real wakeup call came in 2019, when eighteen delta-winged OWA-UAVs built to an Iranian design flew simultaneously into the Saudi airspace to hit at seventeen impact points and decapacitate world's largest oil refinery at Abqaiq. The event sent shockwaves through the world economy and pushed oil prices up. The suspects were the Houthis with whom the Saudis were already engaged in a fierce battle. Still, the exact launch sites were not established, and the Saudi and U.S. officials announced subsequently that the drones did not arrive from the south but from the north, implying pro-Iran proxy groups inside Iraq, Saudi territory or perhaps southwestern tip of Iran itself as possible launch points (Shaif, 2019).

What was equally if not more striking about the Abqaiq drone attack was the abysmal failure of the Saudi air defences in detecting and neutralizing the threat. Abqaiq was very well-protected by several batteries of guns and missile air defence systems, including a cutting-edge *Patriot* air and missile defence system. Besides, when the raid occurred, Saudi Arabia was a country on war-footing. The exact same OWA-UAVs had pounded the Kingdom's east-west pipeline only a few months ago, hence advance warning was present (Binnie, 2019). Increasing the severity of this raid, the attack which circumvented Saudi defences, would have been difficult to detect and neutralize for best-equipped and experienced military powers, too (Taylor, 2019). Therefore, it is not astonishing that the outcome was a loss of confidence in modern air defence systems and technologies' ability to deal with low and slow-flying, thus hard-to-detect simple and inexpensive drones. This was a truly paradigmatic shift to the disadvantage of state actors, revealing as such the weakness of the world's most advanced militaries in the face of small insurgent groups and terrorist cells, and perhaps even malign individuals accessing to cheap and unsophisticated drones. Additionally, the dilemma that was faced by state actors had a very serious cost-exchange ratio dimension. The cost asymmetry between a cheap OWA-UAV or quadcopter drone on the one hand and an expensive air defence interceptor on the other made the latter a very poor fit to counter the former. The advantage was put squarely on drone's side, and thereby in the attacker's favour (Atherton, 2019; Goudarzi, 2025).

Tilting the balance further to the disadvantage of states during this period was the ever-accelerating pace at which FPV drones continued to find their way to new

and more varied non-state actors. In 2017 and soon after bomblet-dropping FPV drones emerged in the battlefields of Middle East, they were adopted by the drug cartels in Mexico (Newdick, 2022). The drones have since become commonplace among organized crime groups in central and south America. A year later, the U.S. law enforcement authorities reported drones being used by criminal groups for criminal purposes, ranging from spotting security gaps and smuggling drugs and weapons to surveying and distracting the police during raids (Tucker, 2018). During 2018, FPV drones appeared for the first time in the hands of religiously motivated extremists in Africa (Anna, 2018). Before the year was over, flights bound for Gatwick and Newark airports in U.K. and U.S. respectively were disrupted after pilots reported FPV-type small drones hovering near and over the runways (Chutel, Pryser and Tekeli, 2025). In the case of Gatwick, environmental activists were suspected of being behind this deliberate disruption (The Economist, 2018). In retrospect, all those developments proved beyond doubt FPV drones were not a passing innovation, and they were re-shaping the way non-state actors engaged their state rivals. And the main beneficiaries of this technological shift were non-state actors.

Yet, all was not to the disadvantage of states. Perhaps one benefit accrued by certain state actors during the same period was their easier access to tactical weaponised UAVs to detect and neutralize insurgents and other armed groups spread over large swaths of their territory. Notably, states in Africa, but also in Central Asia, with comparatively week air powers have taken advantage of weaponized UAVs as affordable and effective substitutes to manned combat and ISR aircraft in their fight against ANSAs. Because the U.S. has abstained from exporting weaponized UAVs during this period, and since Israel was coordinating its UAV exports with Washington, the void in the international UAV markets was filled by the Chinese manufacturers. From the early-2020s, Turkish suppliers managed to overwhelm their Chinese competitors by offering more cost-effective, reliable and better supported UAVs such as Bayraktar TB2 (Mevlütoğlu, 2022). In the process, Türkiye has the world's leading UAV supplier. Turkish-built armed UAVs are currently found in the inventories of close to 35 states, the majority of which are located in Africa (Campbell, 2024; Sertok, 2024, p.44).

Third Phase: 2022-Onwards

The groundbreaking development of 2022 was Russia's invasion of Ukraine. This was a state-on-state confrontation whose battlefields instantly became a huge laboratory to experiment with new technologies, hardware and tactics pertaining to all sorts of weapons including unmanned systems. The lessons drawn from the fighting between the two conventional militaries were dramatic, and the impact of the resulting experiences on the conduct of warfare between state actors truly profound. Conversely though, the effects of the Russo-Ukrainian War on the unmanned systems dimension of the struggle between states and non-state actors have been more modest. In this sense, what was trumpeted as the revolutionary impact of unmanned vehicles on modern warfare have already been observed multiple times during the preceding conflicts involving non-state actors and their state adversaries. Take, for instance, the fanfare created around the Ukrainian military's Turkish-supplied *Bayraktar TB2* UAVs and the way they were decimating Russian vehicle convoys with pinpoint accuracy. Such weaponised UAVs have been used by the U.S., Israel, Türkiye and others during the preceding two decades to neutralize non-state adversaries. It is possible to argue that the impact of the Russo-Ukrainian War on the larger, more sophisticated class of UAV was to increase the interest and convince more states,

especially those in Africa and Central Asia, to order more UAVs. Given their hefty infrastructure and logistic trails, larger UAVs falling in this category remained beyond reach of ANSAs, hence continuing benefit to state actors.

OWA-UAVs, *aka*. suicide, kamikaze drones or loitering munitions, was the second category of drones whose employment first by Russia then Ukraine against military and civilian critical infrastructure targets was met with surprise and amazement. Yet, OWA-UAVs that Moscow purchased from Iran were originally supplied to Iran's proxies some thirty years ago. Some of those drones were even used in anger against military and critical infrastructure targets inside Israel, Saudi Arabia, and the United Arab Emirates (UAE). The success of OWA-UAVs in 2019 Abqaiq oil refinery raid and the failure of modern air defence systems in coping with them had already surprised international observers. With so much advance warning, advanced military powers should have been less astonished with what they saw in Russia-Ukraine war.

Still, the conflict contained some UAV novelties too. For instance, the production and employment of OWA-UAVs was raised to an industrial scale. In 2023, Russia had received a mere 600 disassembled Shaheed OWA-UAVs from Iran in total. Two years later, Russian industry was turning over 5,000 copies per month, and up to 1,000 of them were sent toward Ukraine in each raid (Sonne and Barker, 2025). Similarly, combat experience allowed both the Russians and the Ukrainians to develop elaborate tactics and better drones to circumvent air defences. For instance, waves of cheap decoy drones exhausted air defences before the ones with warheads arrived. OWA-UAVs flew higher to avoid highly effective anti-aircraft artillery. And OWA-UAVs were built to withstand electronic jamming (Gosselin-Malo, 2025). Little doubt the necessary lessons were being drawn and adjustments made accordingly not only by state, but also by non-state actors with future contingencies in mind.

A third class of UAVs with comparable if not greater influence on the conduct and direction of the Russo-Ukrainian War has been in FPV drones. When Russia launched its invasion, Ukrainian military swiftly fielded hand-thrown drones for reconnaissance, fire direction and dropping explosives on Russian troops. As the number of fielded drones increased from hundreds to thousands and then to hundreds of thousands, close to 500 private startups emerged in Ukraine to build homemade drones and their systems and components (Stern, 2025). In 2024, Ukraine manufactured 2.2 million drones and announced its target to build four million during 2025 (Caryl, 2025). Russia quickly caught up and began mass producing FPV drones in even larger quantities. The outcome was tens of thousands of Ukrainian and Russian drones hovering over the frontline at any time and in any place. In this newly transparent battlefield, troop movements by either side were tracked and reacted to in real-time. Those who dared to move, day or night. under the 'prying eye' of enemy drones were dead immediately. In retrospect, introduction of FPV drones in state-on-state conventional war between near peers has given rise to a state of stalemate reminiscent of the First World War on the western front, in which neither side was capable of a strategic breakthrough (Gady, 2023; O'Grady, 2024).

The shift in the conduct and grasp of state-on-state conflicts was truly deep. Enabled by advances in microelectronics and battery technologies, smaller and cheaper drones started to be mass-produced for commercial markets, then also exploited for military end-uses. On the other hand, within the context of non-state actors and their struggle with each other and state actors, there was little novelty about

all this. The simplicity of their acquisition and use had already transformed FPV drones into delivery vehicles favoured by non-state actors (de Troullious de Lanversen, 2025), initially in the Middle East, then in Africa and Latin America as well. This notwithstanding, an aspect of drone warfare in Ukraine to have contributed to ANSAs was a number of innovations to have rendered drones more survivable and lethal. The first among those were fibreoptic tethered drones which were rendered unjammable and undetectable to existing electronic warfare systems. In less than a year, this innovation has found its way to insurgents in Mali and Myanmar as well (Kirichenko, 2025). Similarly, the battle-proven success of Ukrainian FPV drones in engaging Russian helicopters was noted and quickly adapted to shoot down helicopters operated by government forces in Myanmar and possibly in Colombia, too (Ziemer, 2025; Altman, 2025a). This development has created a dangerous operational situation for military helicopters (Bondar, 2025) which are among security forces' most valuable counterterrorism and counterinsurgency assets. It is only a matter of time before other innovations to have been fielded in the Ukrainian battlefields end up in the hands of non-state actors. Among them are:

- Artificial intelligence (AI)-assisted advanced navigation software
- AI-enabled autonomous target selection via visual object recognition
- AI-powered swarming software allowing a pack of drones to cooperate and decide when and which one will attack the target (MacDonald, 2025).

Alone or in combination, those technological breakthroughs will be to render UAVs of all categories more survivable, nondetectable, accurate, and therefore dangerous.

Further aggravating tangible and non-tangible proliferation risks emanating from the Russo-Ukrainian conflict is the possibility of drone-related know-how and piloting skills migrating toward non-state actors. There have already been allegations about individuals linked to Mexican drug cartels enlisted in the Ukrainian International Legion to gain experience in weaponised drone operations. Similar reports emerged about Russia providing comparable expertise to non-state groups in Colombia (Ziemer, 2025). In Sudan's internal conflict, which erupted in 2023, the Rapid Support Force paramilitary deployed OWA-UAVs that bear the hallmarks of those produced up to Iranian blueprints by Houthis in Yemen, pointing to exchanges of information between warring parties of two separate civil wars (Houreld, 2025).

Last but not the least, the single event of the Russo-Ukrainian war with the deepest impact so far on the struggle between state and non-state actors has been the Operation Spiderweb. This mid-2025 Ukrainian drone operation must be included among the most fantastic raiding successes in modern warfare involved simultaneous attacks on five Russian strategic bomber bases thousands of kilometres away from Ukraine by FPV drones taking off deep inside the Russian homeland. The outcome was the confirmed 'kill' of at least a dozen aircraft – roughly ten percent of Russia's strategic bomber force. In this masterwork of clandestine operation that took eighteen months to prepare and stage, the Ukrainians have first smuggled or more likely assembled in workshops inside Russia some 150 quadcopter FPV drones costing less than a thousand dollars each. Those drones were then concealed inside modular cabins and loaded onto civilian trucks whose unsuspecting Russian drivers were instructed to park in the vicinity of Russian strategic airbases. Next, the cabin roofs were opened and 117 explosive-packed FPV drones were flown remotely by their

pilots who remained outside Russian territory and took advantage of Russian mobile phone networks to command the drones. To overcome electronic jamming that would normally be present near such high-value military facilities, Ukrainian drones were uploaded with opensource software that rendered them near or fully autonomous. More precisely, retail software was used for autopilot navigation and AI-assisted visual object recognition for the final dive onto the targeted aircraft (Lin-Greenberg, 2025; Bondar, 2025).

Above all, Ukraine's Operation Spiderweb was a colossal intelligence and internal security failure for the Russians, but at the same time it has signified the spectacular exploitation of technological novelty, organisational ingenuity and logistical mastery on the part of Ukraine (Lin-Greenberg, 2025). The raid, which marked the largest attack on a nuclear-armed state's nuclear assets to date (de Troullious de Lanversen, 2025), also exposed the irrelevance of advanced military powers' layered air defences when pitted against drone threats taking off from inside their territory. Modern air defences have been developed to keep aerial threats out, hence there not being much they can do when the threat originates inside the protected territory. Consequently, any assumption that military assets and critical infrastructure deep inside a country were protected by strategic depth was shattered (Gady, 2025). The raid served as a cautionary tale for all expensive and strategically important assets which are often stored in the open with little protection at military bases around the world. Equally deep was the psychological effects of this public humiliation, demonstrating that the depths of homeland could no longer be viewed as an impregnable sanctuary. In sum, it was revealed beyond doubt that cheap, off-the-shelf drones combined with retail software applications could inflict disproportionate strategic damage on any state (Lin-Greenberg, 2025). A further alarming dimension of this paradigmatic shift in the security perceptions of states was the knowledge that such simple drones were within easy reach of violent non-state actors and even nefarious individuals. From this angle, the range of options opened first by the Operation Spiderweb and shortly afterwards by Israel's Operation Rising Lion, which also incorporated small drones taking off from inside Iranian territory (Treloar, 2025), tilted the balance away from the state actors.

But the effects of cheap drones did not stop there. The ease with which such drones could be used as hybrid warfare tools to disrupt, intimidate and keep under constant pressure military facilities, critical infrastructure and, in fact, the entire population and economy of rival states was all too evident, and likely to be exploited to the full extent. Such activity may be executed directly by the agents and intelligence services of a hostile state, or else carried out by remote or unwitting groups and individuals coopted by states. In Europe and North America, the ever-increasing frequency of unidentified low-cost drones flying near and above sensitive military bases, energy, transportation and other critical infrastructure hubs must thus be seen as the manifestation of a new kind of hybrid warfare campaign. The U.S. military reported 350 drone sightings across 100 military installations during 2024 (Jakes, 2025). 257 such sightings took place over German military sites within the first quarter of 2025 alone (Allison, 2025). Within a span of days at the end September 2025, several international airports in Europe were closed temporarily and massive drone flight bans had to be imposed over the entire Denmark and the city of Chicago (Altman, 2025). All this revealed a coordinated pattern in a new type of 'grey zone' warfare, called 'hybrid air denial' by Bremer and Grieco, along with which adversaries' use of low-cost drones to access and deny commercial activity in the air littoral is producing

outsized effects. What makes drones especially effective in this role is their combination of easy access, low-cost and minimal perceived risk due to plausible deniability (Bremer and Grieco, 2025), especially when non-state collaborators are in the picture.

Living through such accelerating disruption and intimidation, the reaction of the public in Western countries was to demand their governments and security forces to take immediate measures to neutralize the drone nuisance. In response, the European Union (EU) has jumpstarted one of the most ambitious multi-nation defence projects in history: a Europe-wide 'drone wall' comprising a mesh of sensors, AI software, jammers and cheap interceptors to thwart small drones and OWA-UAVs (Tucker, 2025). Likewise, the North Atlantic Treaty Organization (NATO) announced a new initiative to help alliance members detect and thwart incoming drones (Benoit and Michaels, 2025). And the U.S. has rushed in several fast-track procurement projects to deploy multiple forms of counter-drone gadgetry (Trevithick, 2025). The U.S. military also moved to form mobile drone hunting teams that can respond within 24 hours to reported drone incursions over its bases (Altman, 2025c).

However, neutralizing UAVs, especially those taking off from inside own's country is easier said than done. The first technological challenge relates to timely detection and early warning. To this day, detecting and jamming command signals between the drone and its operator has been the most common technique to neutralize UAV threats. However, fibreoptic cable-tethered and autonomous drones will soon render this technique irrelevant. Further bad news is that the large, ground-based, fixed radars at the centre of current air defence architectures are not very good at detecting small, slow and low-flying objects such as drones. What is needed instead is a network of lighter, proliferated and mobile radars coupled to an even larger number of comparatively cheap passive – e.g. acoustic and optical – sensors. Development of such multi-mode, distributed architecture will not be easy, fast or cheap (Hitchens, 2025).

Once they are detected, the next step is to shoot those drones down. But here too technological and budgetary challenges are present. Air defence missiles are exponentially more expensive than the drones they try to intercept, and they will always be in short supply. Anti-aircraft guns are more cost-effective, but their range is very limited, and their bursting projectiles create significant risk of collateral damage when used above densely populated areas and fragile critical infrastructure targets such as airports and energy facilities. High-power lasers have been promoted as a no collateral damage and much cheaper option. But they have one massive drawback: they can't be used in rainy, foggy or low cloud-cover days – none of which is a rarity in central and northern Europe. As another form of directed energy weapon, high-power microwaves 'frying' the micro-circuity of drones in selected swath of airspace are also promising, especially against drone swarms. But they pose risks to nearby air traffic and the very urban and critical infrastructure targets they are designed to protect. The lessons of the conflict in Ukraine have pushed drones intercepting incoming drones to the forefront, but they too are restricted by hard-to-meet prerequisites. The time window for successful drone-on-drone interception is less than thirty seconds, pointing to the imperative for early detection and early warning of threats by offsite sensors (Matviienko and Semenovych, 2025). Finally, physical protection such as nets, cages, and the hardening of the most likely targets single out as another defensive option implemented by both Ukraine and Russia.

Given the variety of speeds and altitudes that drones of all shapes and sizes may be operating at, there can be no 'silver bullet' approach or solution countering them all. The solution lies in a composite and layered architecture comprising tightly meshed and constantly communicating sensors and shooters of several types. In Russia-Ukraine conflict, the pace of tactical and technological innovation for drones is in the order of weeks, if not days (Ziemer, 2025). This means any effective and sustainable counter-UAV endeavour would have to be modular, highly flexible and open to constant change and upgrades: no easy feat for advanced military powers' cumbersome and slow-motion defence procurement bureaucracies. An equal if not more daunting challenge for western societies will be to keep a large number of distributed sensors and shooters in the air, working and manned on a 7/24 basis. This will soon become an unbearable operational and budgetary disposition unless a country is on a full-scale war footing.

Drones overlooked: unmanned vehicles at sea and ground

The last few years have been a period of important developments and technological innovation, with emerging drone threats in unmanned vehicles' maritime, underwater and ground applications, including their employment by non-state actors. Therefore, a brief overview of major developments is well warranted. We begin with the unmanned sea vehicles (USVs). Since Nikola Tesla's successful experiment in 1898 (Beschloss, 2013), remote controlled boats have been deployed by several navies in roles such as gunnery training, minelaying and mine clearance. The idea of packing uncrewed boats with explosives and sending them towards enemy ships or ports has always been present too. But putting the theory into practice took more than a century. In 2017, not a conventional navy but a non-state actor became the first entity to strike a ship using such kamikaze boat. The Houthi fighters used three remotely controlled, explosive-laden speedboats to strike a Saudi Navy frigate off the coast of Yemen. The ship was badly stricken and two sailors killed (Conflict Armament Research, 2017). The Houthis had received remote-control kits from Iran, but the boats themselves were converted inside Yemen from readily available commercial speedboats. Few observers took notice of this important development, one which posed a serious to threat to all capital naval ships as well as coastal and offshore critical infrastructure such as seaports, shipyards, bridges and oil and gas rigs. In the past, navies were only defeated by similar sea, air or undersea forces possessed exclusively by state adversaries. Suddenly, with the help of cheap, readily accessible commercial technologies and hardware, it had become possible to attack ships and coastal facilities with OWA-USVs at little or no cost to the attacker (Ullman, 2023). 2017 through 2022, several Saudi and Emirati naval vessels were targeted and suffered damage while at sea or pier-side in Yemen. In 2020, a commercial tanker was attacked for the first time by three crewed and one uncrewed boats while sailing in the Gulf of Aden (Binnie, 2020). From the end 2021, the Houthis extended their reach to the Saudi coastline and territory. Several vessels and commercial ships in the port of Jeddah – 1.000 kilometres away from Yemen – were damaged in at least two raids launched by OWA-USVs (Binnie, 2022).

Since late-2023, the Houthis started to strike merchant ships transiting the Red Sea and the Gulf of Aden, uncrewed suicide boats have finally caught the attention of international community. Between November 2023 through January 2025 more than 100 merchant ships were attacked. Several of them were damaged and two sunk by a combination of Houthi ballistic and cruise missiles, UAVs and USVs. But the Houthis soon discovered modern merchant ships were remarkably difficult to sink with a single

hit. Therefore, they have improved their tactics to first immobilize the ships by raiding them with USVs, then firing missiles with heavier punch which were normally not as good in hitting moving targets (Sutton, 2024a). OWA-UAVs were also used, but with much less impact due to the relatively light explosive payload they can be packed with. In mid-2025, after a six-month lull, the Houthis have begun once more to target merchant ships off the coast of Yemen, this time pushing their mass-manufactured OWA-USVs to the forefront (Gambrelli, 2025).

The second event to have brought USVs to the forefront of international agenda was Ukraine's ingenious and highly effective campaign to cripple Russia's mighty Black Sea Fleet. In October 2022, Ukraine – a country with no proper naval force – carried out its first raid using USVs as suicide drones against Russian naval vessels anchored at Sevastopol. Those were purpose-built small craft carrying satellite communication antennas enabling two-way communication with their operators – a feature that did not exist in the more crude Houthi equivalents. Satellite communication meant navigation and command guidance irrespective of range and equalled to a breakout point in the evolution of USVs. During the following sixteen months, OWA-USVs in combination with anti-shipping and cruise missile strikes took out close to a third of the Black Sea fleet – 25 surface vessels and 1 submarine destroyed, 15 other damaged – and forced the remaining Russian vessels to operate in the eastern fringes of the Black Sea (The Economist, 2024a). Not only ships, but coastal infrastructure – e.g. Kerch Bridge connecting Crimean Peninsula to Russia – was also hit and crippled by OWA-USVs. The evolution of Ukrainian USVs has continued unabated to this day. Towards the end of 2024, a Ukrainian USV modified to carry guided missiles managed to shoot down a Russian helicopter (Newdick, 2024). In mid-2025, two of Russia's cutting-edge Su-30 fighter jets met the same fate at the hands of 3 USVs attacking them with heat-seeking missiles (Altman, 2025d). From the beginning of 2025, a new iteration in drone warfare was introduced when Ukraine's USVs sailing off the cost of Crimea launched their on-deck FPV aerial drones to raid Russia's inland air defence sites (Newdick, 2025). The conflict in the Black Sea may be state-on-state, but there can be little doubt that non-state actors have been closely watching with a view to adapting and employing the same tactics. If the pace with which UAV lessons and innovations disseminated from the Ukrainian battlefields to non-state actors is taken as a reference, then the same in the maritime domain may be around the corner.

Another even more interesting domain of unmanned vehicles concerns those vehicles operating below water. The so-called unmanned underwater vehicles (UUVs) are neither new nor revolutionary. Scientific communities, offshore oil and gas industries, and companies involved in undersea communication and power cable operations have long utilized them. Similarly, several navies have been using them since 1960s for deep sea recovery, seafloor survey and mapping. More recently though, advances in microelectronics, enhanced processing and machine learning gave rise to more autonomous – i.e. self-navigating and operating underwater vehicles. Likewise, rapid technological progress in electric propulsion, power storage and advanced materials have given rise to a new generation of higher performance, more reliable UUVs for commercial applications. In effect, this has been a domain shaped more by the demand from commercial companies than navies, hence comparatively easier accessibility to cutting-edge UUV technologies and hardware (Egeli, 2025).

It was against this background that Iran has possibly become the first country to pack UUVs with explosives and transform them into low-end torpedoes. The end

result was a slow moving, but long endurance and comparatively easy-to-build weapon systems have appeared that could be used for sneak attacks on stationary ships, plus offshore and coastal critical infrastructure such as oil rigs. Some observers likened them to the underwater equivalents of Iran's Shaheed OWA-UAVs, except that in the underwater domain it is more about surprise and stealth than numbers (Sutton, 2024b). In 2019 and 2021, there were several mysterious attacks on merchant ships anchored off the coast of the UAE and it was claimed that the devices used could be low-technology Iranian OWA-UUVs (Sutton, 2022). In a more worrying development, Iran is known to have supplied its OWA-UUV products and knowhow to regional proxies. In 2024, the U.S. Navy reported its destruction of two UUVs while still ashore in Yemen (Lehrfeld et.al., 2024). The Houthis have subsequently acknowledged their possession of weaponized UUVs (Adel, 2024). Iran's other proxies in the region, specifically Hezbollah, are also known to deploy OWA-UUVs (Sutton, 2023). In 2021, Israeli Navy intercepted a crude UUV launched from Gaza. The device was possibly heading towards the Tamar offshore gas rig (Gross, 2021). Two years later, October 7th raids on Israel included a makeshift semi-submersible, which was detected and destroyed by the Israeli Navy (Sutton, 2023). The field evidence illustrates the ease with which non-state actors could access or be supplied with OVA-UUVs components to assemble sneak underwater weapons to threaten state actors and their shipping, offshore and coastal infrastructure (Egeli, 2025). So far, there have been no known successful examples of such a raid, but the threat is tangible and credible.

The fourth category of unmanned vehicles concerns those used on land. Referred to as unmanned ground vehicles (UGVs), those are devices that look like remote-controlled model cars or small tanks. Historical origins go back to 1939, when the Soviet Red Army deployed remotely controlled flamethrower *Teletanks* while invading Finland. Since 1970s, UGVs have also been used widely for bomb disposal. But their use in battlefields have so far been limited mostly to logistic and engineering support roles, primarily because ground automated driving is still hard in comparison with air and sea domains (The Economist, 2024b). Another important challenge to their mass deployment is the fragility of communication link between the UGV and its operator. Datalinks are prone to fail in rugged terrain, built-up areas and beneath trees. But here too, technological progress is rapidly turning into 'a new ballgame' along with which swarms of UGVs costing less than a thousand dollars each could soon be fielded in large numbers, much like drones buzzing overhead (The Economist, 2025). They could then communicate with each other to bypass the command link obstacle and also take advantage of AI-assisted fully autonomous driving and target recognition to engage enemy troops and positions. The required software and hardware already abound thanks to the strides made in commercial driverless vehicles. There are already thousands of UGV models marketed unrestricted worldwide by hundreds of manufacturers. It may be only a matter of time before a nefarious group or individual acquires and packs commercial off-the-shelf (COTS) UGVs with explosives to send them towards high-value critical infrastructure or worse soft population targets. Explosive-laden trucks and cars have already been used with tragic results. There is no reason why non-state actors would not attempt to use smaller, cheaper, and harder to neutralize UGVs for the same purposes.

Conclusion

The first conclusion that could be drawn from the evidence presented in this chapter is that technological innovation in most categories of unmanned vehicles were adopted and used by non-state actors before the more cumbersome state actors could

adopt and take advantage of them. More precisely, the use by non-state actors of OWA-UAVs, FPV drones and OWA-USVs preceded their combat deployment by states and their militaries.

What has also been revealed is the fact that the availability of new types of unmanned vehicles and technologies has been more to the benefit non-state actors than the states. One important exception in this respect is the use of larger UAVs, whose widespread deployment in counterinsurgency and counterterrorism campaigns brought major advantages to state actors, initially in the form of ISR then eventually through surgical destruction and targeted killing of their sub-sate adversaries. Larger and sophisticated UAVs like Reapers and TB2s continued to this day be owned and operated exclusively by state actors. Yet the 2010s and 2020s witnessed the democratization of drone technologies and this was a breakthrough development allowing non-state actors to access less advanced, smaller and cheaper, yet equally if not more threatening unmanned vehicle capabilities. More precisely, widespread and unhindered availability of OWA and FPV aerial drones has tilted the balance decisively in non-state actors' favour and forced states and their security forces onto the defensive. In this respect cheap, easy-to-acquire-and-operate unmanned systems inflicted disproportionate damage when combined with creativity and intelligent targeting (Bondar, 2025). States need considerable time and resources to restructure their existing air defence architecture in order to counter drone threats. Until this point in time is reached, the states will find themselves further strained in the face of drone-quipped non-state adversaries.

Unmanned vehicles are not a passing innovation. They will continue reshaping how states and their substate opponents engage in conflict. Until another round of technological innovation neutralizes the advantages accruing to non-state actors, the states and their security apparatuses will likely see the drone threat persist and grow. Drone-related hardware and know-how become cheaper and more accessible by day. Combined with technological leaps enabling AI-enabled drone swarms, autonomous navigation and target recognition, this pattern points out to a growing, not shrinking unmanned vehicle threat to state actors. This is the new paradigm policymakers and security apparatuses must better acquaint themselves with, and prepare accordingly.

BIBLIOGRAPHY:

Ackerman, Spencer. (2011). "Libyan Rebels Are Flying Their Own Minidrone." wired.com. August 23. http://www.wired.com/2011/08/libyan-rebels-are-flying-their-own-mini-drone/

Adel, Mina. (2024). "Dealing with the Houthis." *English Ahram.* November 5. https://english.ahram.org.eg/News/534781.aspx

Allison, George. (2025). "Are Russian cargo ships operating drones in Europe?" ukdefencejournal.org.uk. August 25. https://ukdefencejournal.org.uk/are-russian-cargo-ships-operating-drones-in-europe/

Altman, Howard. (2025a). "Mi-17 Appears To Have Been Downed By FPV Drone In Myanmar." twz.com. May 22. https://www.twz.com/air/mi-17-appears-to-have-been-downed-by-fpv-drone-in-myanmar

Altman, Howard. (2025b). "Credible Threat of Drone Attacks Prompted Massive Chicago Airspace Restrictions, CNP Claims." twz.com. October 3. https://www.twz.com/air/cbp-claims-credible-threat-of-drone-attacks-prompted-massive-chicago-airspace-restrictions

Altman, Howard. (2025c) “New Quick Reaction Force Will Counter Military Base Drone Incursions.” twz.com. September 18. https://www.twz.com/air/new-quick-reaction-force-will-counter-military-base-drone-incursions

Altman, Howard. (2025d) “Two Russian Su-30 Flankers Downed by AIM-9s Fired From Drone Boats.” twz.com. https://www.twz.com/news-features/two-russian-su-30-flankers-downed-by-aim-9s-fired-from-drone-boats-ukrainian-intel-boss

Anna, Cara. (2018). “Islamic extremists are now using drones in Nigeria, leader says.” militarytimes.com. November 30. https://www.militarytimes.com/news/your-military/2018/11/30/islamic-extremists-are-now-using-drones-in-nigeria-leader-says/

Atherton, Kelsey D. (2019). “Attacks in Saudi Arabia expose a battle for asymmetry.” c4isrnet.com. September 17. https://www.c4isrnet.com/unmanned/2019/09/17/saudi-arabia-cannot-spend-its-way-out-of-asymmetry/

Aviation Week. (1998). “I-GNAT finds new use with CIA, Turkey.” January 6. https://aviationweek.com/i-gnat-finds-use-cia-turkey

Benoit, Bertrand and Daniel Michaels. (2025). “Drone Threats Ignite Burst of Counterdrone Wizardry.” *The Wall Street Journal*. October 18. https://www.wsj.com/world/drone-threats-ignite-burst-of-counterdrone-wizardry-45facf6c

Bescholess, Steven. (2013). “Object of Interest: Remote Control.” *The New Yorker*. November 22. https://www.newyorker.com/tech/annals-of-technology/object-of-interest-remote-control

Binnie, Jeremy. (2022). “Bomb boat hit Saudi naval vessel, Un experts report.” janes.com. January 31. https://www.janes.com/osint-insights/defence-news/sea/bomb-boat-hit-saudi-naval-vessel-un-experts-report

Binnie, Jeremy. (2020). “Sauid military reveals unmanned boat attacked a tanker in Gulf of Aden.” *Jane’s Defence Weekly*. May 3: p:17.

Binnie, Jeremy. (2019). “Saudis presents evidence of Iranian involvement in oil facility attacks.” *Jane’s Defence Weekly*. September 19: 4.

Binnie, Jeremy. (2018). “Russians reveal details of UAV swarm attacks on Syrian bases.” *Jane’s Defence Weekly*. January 12.

Bondar, Kateryna. (2025). *How Ukraine’s Operation Spider’s Web Redefines Asymmetric Warfare*. CSIS. June 2. https://www.csis.org/analysis/how-ukraines-spider-web-operation-redefines-asymmetric-warfare

Bremer, Maximilian K. and Kelly A. Grieco. (2025). “Hybrid air denial: The new gray zone battleground raging above Europe.” *Defense News*. October 2. https://www.defensenews.com/opinion/2025/10/02/hybrid-air-denial-the-new-gray-zone-battleground-raging-above-europe/

Campbell, Molly. (2024). *Drone Proliferation Dataset*. Center For A New American Security. September. https://www.cnas.org/publications/reports/drone-proliferation-dataset

Carlino, Ludovico. (2019). “Changing gear.” *Jane’s Intelligence Review*. May: 26-33.

Caryl, Christian. (2025). “The Ukrainians’ New Way of War.” *Foreign Policy*. June 6. https://foreignpolicy.com/2025/06/06/ukraine-russia-war-drone-attack-airbase-bombers/

Chivers, C.J. and David Guttenfelder. (2025). “How Suicide Drones Transformed the Front Lines in Ukraine.” *The New York Times*. January 1. https://www.nytimes.com/2024/12/31/magazine/drones-weapons-ukraine-war.html

Chutel, Lynse and Henrik Pryser and Maya Tekeli. (2025) “Denmark briefly closes Airports After Unexplained Drone Sightings.” *The New York Times*. September 25.

Conflict Armament Research. (2017). “Anatomy of a Drone Boat.” December. https://www.conflictarm.com/perspectives/anatomy-of-a-drone-boat/

Conflict Armament Research. (2016). *Islamic State’s Weaponised Drones*. October. https://www.conflictarm.com/perspectives/islamic-states-weaponised-drones/

De Troullious de Lanversen, Julien. (2025). “Ukrainian attack on Russian bombers shows how cheap drones could upset global security.” thebulletin.org. June 5. https://thebulletin.org/2025/06/ukrainian-attack-on-russian-bombers-shows-how-cheap-drones-could-upset-global-security/

Dreazen, Yochi. (2014). “The Next Arab-Israeli War Will Be Fought with Drones.” *The New Republic.* March 26. http://www.newrepublic.com/article/117087/next-arab-israeli-war-will-befought-drones

Dri, Karwan Faidhi. (2021) “Drones: A new tactic in PKK’s armed struggle against Turkey?” ikhrw.com. June 16. https://www.ikhrw.com/en/article/drones-a-new-tactic-in-pkks-armed-struggle-against-turkey/

Egeli, Sıtkı. (2025). *Threat From the Depths: Uncrewed Underwater Vehicles*. Rabdan Security & Defence Institute. March 21. https://rsdi.ae/en/publications/threat-from-the-depths-uncrewed-underwater-vehicles

Gady, Franz-Stefan. (2025). “What Is the Impact of Ukraine’s Raid on Russia’s Air Force?” *Foreign Policy*. June 4. https://foreignpolicy.com/2025/06/04/ukraine-russia-war-drone-attack-airbases-bombers-operation-spiderweb/

Gady, Franz-Stefan. (2023). “How an Army of Drones Changed the Battlefield in Ukraine.” *Foreign Policy*. December 6. https://foreignpolicy.com/2023/12/06/ukraine-russia-war-drones-stalemate-frontline-counteroffensive-strategy/

Gambrell, Jon. (2025). “Yemen’s Houthi rebels attack another ship in the Red Sea, killing 3.” apnews.com. July 8. https://apnews.com/article/mideast-wars-yemen-houthis-israel-6dc55ee05a9d1e78621788aa0bc52168

Gettinger, Dan. (2016). *Drones Operating in Syria and Iraq*. Center for the Study of the Drone at Bard College. December. https://dronecenter.bard.edu/drones-operating-in-syria-and-iraq/

Gettinger, Dan and Arthur Holland Michael. (2014). *A Brief History of Hamas and Hezbollah’s Drones*. Center for the Study of Drone at Bard College. July 14. https://dronecenter.bard.edu/hezbollah-hamas-drones/

Gosselin-Malo, Elisabeth. (2025). “Russia seen as boosting combat-drone output, switching attack angles.” *Defense News*. July 21.

https://www.defensenews.com/global/europe/2025/07/21/russia-seen-as-boosting-combat-drone-output-switching-attack-angles/

Gross, Judah Ari. (2021). “IDF says it thwarted underwater drone attack by Hamas from northern Gaza.” *Times of Israel.* May 18. https://www.timesofisrael.com/idf-says-it-thwarted-underwater-drone-attack-by-hamas-from-northern-gaza/

Hambling, David. (2020). “Kurdish PKK Militants Step Up Improvised Drone Bomb Attacks In Turkey.” forbes.com. August 27. https://www.forbes.com/sites/davidhambling/2020/08/27/pkk-terror-group-steps-up-improvised-drone-bomb-attacks/

Hitchens, Theresa. (2025). “Passive ground-based sensor networks could bolster air, missile defense resilience.” breakingdefense.com. July 21. https://breakingdefense.com/2025/07/passive-ground-based-sensor-networks-could-bolster-air-missile-defense-resilience-csis/

Houreld, Katharine. (2025). “Surface-to-air missiles and deadly drones spread on Sudan’s battlefield.” *The Washington Post*. September 29. https://www.washingtonpost.com/world/2025/09/29/sudan-war-weapons-rsf-darfur/

Jakes, Lare. (2025). “As Drones Transform Warfare, NATO May Be Vulnerable.” *The New York Times*. June 4. https://www.nytimes.com/2025/06/04/world/europe/ukraine-russia-drones-nato.html

Katz, Yaakov. (2010). “IDF encrypting drones after Hizbullah accessed footage.” *Jerusalem Post*. October 27. https://www.jpost.com/israel/idf-encrypting-drones-after-hizbullah-accessed-footage

Kirichenko, David. (2025). “Fiber-optic drones reshape Ukraine’s technological war.” lowyinstitute.com. August 6. https://www.lowyinstitute.org/the-interpreter/fibre-optic-drones-reshape-ukraine-s-technological-war

Lehrfeld, Jonathan et.al. (2024). “All the Houthi-US Navy incidents in the Middle East (that we know of).” Military Times. February 12 (updated October 24). https://www.militarytimes.com/news/your-military/2024/02/12/all-the-houthi-us-navy-incidents-in-the-middle-east-that-we-know-of/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru

Lin-Greenberg, Erik. (2025). “Ukraine’s smart munitions deliver a punch – and a warning about the future of warfare.” thebulletin.org. June 13. https://thebulletin.org/2025/06/ukraines-smart-munitions-deliver-a-punch-and-a-warning-about-the-future-of-warfare/

MacDonald, Alistair. (2025). “AI-Powered Drone Swarms Have Now Entered the Battlefield.” *The Wall Street Journal*. September 2. https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05

Matviienko, Oleksandr and Zoriana Semenovych. (2025). “Interceptor drones: Ukraine’s best bet against Russian Shaheds.” counteroffensive.pro. July 15. https://counteroffensive.pro/p/interceptor-drones-ukraine-s-best-bet-against-russian-shaheds-0b7b

Mevlütoğlu, Arda. (2022). “Türkiye’s drone exports: More than just a transaction.” menaaffairs.com. https://menaaffairs.com/turkiyes-drone-exports-more-than-just-a-transaction/

Newdick, Thomas. (2025). “Ukraine claims Its Drone Boats Are Now Launching Kamikaze FPV Drones At Russian Shore Targets.” January 7. https://www.twz.com/news-features/ukraine-claims-its-drone-boats-are-now-launching-kamikaze-fpv-drones-at-russian-shore-targets?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru

Newdick, Thomas. (2024). “Ukraine claims Its Drone Boat Shot Down Mi-8 Helicopter With A Surface-to-Air Missile.” twz.com. December 31. https://www.twz.com/sea/ukraine-claims-its-drone-boat-shot-down-a-russian-mi-8-helicopter-with-a-surface-to-air-missile

Newdick, Thomas. (2022). “Bomblet Dropping Drones Are Now Being Used By Cartels In Mexico’s Drug War.” twz.com. January 12. https://www.twz.com/43847/bomblet-dropping-drones-are-now-being-used-by-cartels-in-mexicos-drug-war

O’Grady, Siobhan and Kostiantyn Khudov. (2024). “Drones are crowding Ukraine’s skies, largely paralyzing battlefield.” *The Washington Post*. April 14. https://www.washingtonpost.com/world/2024/04/14/ukraine-drones-russia-war-skies/

Rassler, Don. (2016). *Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology*. Combating Terrorism Center at West Point. October. https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/

Santora, Marc et.al. (2025). “A Thousand Snipers in the Sky: The New War in Ukraine.” The New York Times. March 3. https://www.nytimes.com/interactive/2025/03/03/world/europe/ukraine-russia-war-drones-deaths.html

Schehl, Matthew L. (2016). “ISIS is expanding the reach and sophistication of its drone fleet.” *Marine Corps Times*. April 17. https://www.marinecorpstimes.com/news/your-marine-corps/2016/04/17/isis-is-expanding-the-reach-and-sophistication-of-its-drone-fleet/

Sertok, Kaan. (2024). Türkiye’s defense diplomacy and UAAV exports towards African states. Unpublished Master’s Thesis. Izmir University of Economics. https://tez.yok.gov.tr/UlusalTezMerkezi/TezGoster?key=1pwTzRXnomYf6jwqVORfUWBRZOHT_JuRrCUHU-V2n4dRxOwJ_mkQF7TrtbWCV4WH

Shaif, Rawan. (2019). “Flammable Relations.” *Jane’s Intelligence Review*. November: 29-35.

Shaw, Ian G.R. (2015). “History of U.S. Drones.” understandingempire.wordpress.com. https://understandingempire.wordpress.com/2-0-a-brief-history-of-u-s-drones/

Sonne, Paul and Kim Barker. (2025). “Russia Made Drone Production a Supreme Priority. Now It Swarms the Skies.” *The New York Times*. September 14. https://www.nytimes.com/2025/09/14/world/europe/russia-ukraine-drone-attacks-production.html

Stern, David L. (2025). “The world wants Ukraine’s cutting-edge drone, but they aren’t yet for sale.” *The Washington Post*. September 6. https://www.washingtonpost.com/world/2025/09/06/ukraine-drone-industry-export/

Sutton, H.I. (2024a). “Houthi’s Blowfish: Guide to Explosive USV Threat In Red Sea.” hisutton.com. June 30. http://www.hisutton.com/Yemen-Houthi-USV-Guide.html

Sutton, H.I. (2024b) “World Survey of Underwater Attack Drones (OWA-AUVs).” hisutton.com. January 3. http://www.hisutton.com/Guide-To-Underwater-Attack-Drones.html

Sutton, H.I. (2023). “First Details of Hamas’ New Submarine Drone Weapons.” *Naval News*. November 1. https://www.navalnews.com/naval-news/2023/11/first-details-of-hamas-new-submarine-drone-weapon/

Sutton, H.I. (2022). “New Iranian Weaponized Underwater Drone.” hisutton.com. March 16. http://www.hisutton.com/Iran-IRGC-Weaponized-UUV.html

Sünnetçi, İbrahim. (2015). “Türkiye’de Hizmetteki İHA Sistemlerine Bir Bakış-I” (A Look at Türkiye’s In-service UAV Systems). *Savunma ve Havacılık*. 169: 132-137.

The Economist. (2025) “Ukraine is inching towards robot-on-robot fighting.” June 26. https://www.economist.com/europe/2025/06/26/ukraine-is-inching-towards-robot-on-robot-fighting

The Economist. (2024b). “The growing role of fighting robots on the ground in Ukraine.” April 19. https://www.economist.com/the-economist-explains/2024/04/19/the-growing-role-of-fighting-robots-on-the-ground-in-ukraine

The Economist. (2024a). “How Ukraine sank the Caesar Kunikov–and is beating Russia at sea.” February 14. https://www.economist.com/the-economist-explains/2024/02/14/how-ukraine-sank-the-caesar-kunikov-and-is-beating-russia-at-sea

The Economist. (2018). “Several drone sightings close Britain’s second-biggest airport.” December 21. https://www.economist.com/gulliver/2018/12/21/several-drone-sightings-close-britains-second-biggest-airport

Taylor, Adam. (2019). “Billions spent on U.S. weapons didn’t protect Saudi Arabia’s most critical oil sites from a crippling attack.” *The Washington Post*. September 17. https://www.washingtonpost.com/world/2019/09/17/billions-spent-us-weapons-didnt-protect-saudi-arabias-most-critical-oil-sites-crippling-attack/

Tovy, Tal. (2024). “Defending the Sky: An Historical Analysis of Israeli Drone Use, 1971-2014.” *British Journal for Military History*. 10.1: 192-207. https://journals.gold.ac.uk/index.php/bjmh/article/view/1783/1891

Treloar, Natalie. (2025). “Special operations by Israel and Ukraine were immediate tactical success. Their strategic impact will take more time to assess.” thebulletin.org. June 30. https://thebulletin.org/2025/06/special-operations-by-israel-and-ukraine-were-immediate-tactical-successes-their-strategic-impact-will-take-more-time-to-assess/?utm_source=SocialShare&utm_medium=CopyLink&utm_campaign=CopyLink&utm_term

Trevithick, Joseph. (2025). “AeroVironment’s Freedom Eagle-1 Picked As New Counter-Drone Interceptor for U.S. Army.” Twz.com. October 22.

https://www.twz.com/land/aerovironments-freedom-eagle-1-picked-as-new-counter-drone-interceptor-for-u-s-army

Tucker, Patrick. (2025). “Inside Europe’s crash effort to create a drone wall.” defenseone.com. October 2. https://www.defenseone.com/technology/2025/10/inside-emergency-effort-create-european-drone-wall/408582/

Tucker, Patrick. (2018). “A Criminal Gang Used a Drone Swarm to Obstruct an FBI Hostage Raid.” defenseone.com. May 3. https://www.defenseone.com/technology/2018/05/criminal-gang-used-drone-swarm-obstruct-fbi-raid/147956/

Ullman, Harlan. (2023). “Cheap and terrifying surprise attacks are the new face of warfare.” thehill.com. October 16. https://thehill.com/opinion/national-security/4257190-cheap-and-terrifying-surprise-attacks-are-the-new-face-of-warfare/?utm_campaign=dfn-ebb&utm_medium=email&utm_source=sailthru&STOverlay=2002c2d9-c344-4bbb-8610-e5794efcfa7d

Ziemer, Henry. (2025). “The Future of Criminal Drone Use in Latin America.” warontherocks.com. September 9. https://warontherocks.com/2025/09/the-future-of-criminal-drone-use-in-latin-america/

CHAPTER 10

THE POTENTIAL USE OF EMERGING DISRUPTIVE TECHNOLOGIES BY NON-STATE ACTORS IN THE ENERGY DOMAIN

Mitat Çelikpala

I. Introduction

Emerging Disruptive Technologies (EDTs) are innovative advancements that have been recently created, are currently in development, or are expected soon, holding the potential to drive significant changes across various sectors, from energy to communications, and drastically change how organizations and industry's function. These include fields such as: artificial intelligence; autonomous systems; quantum computing; biotechnology; human enhancement technologies; space; energy and propulsion; novel materials and manufacturing; and next-generation communications networks, all of which are significantly transforming how organizations and industries operate. As dual-use technologies, EDTs present a range of both risks and opportunities for diverse stakeholders, including corporations, governments, and international organizations. Their growing influence affects all areas of society and is reshaping security strategies, presenting new threats from both state and non-state actors in military and civilian domains.

NATO is significantly affected by EDTs, which influence operational strategies and strategic planning among NATO member states and their allies.[263] NATO's security context changed dramatically between 2021 and 2022, including the last coalition troops leaving Afghanistan and Russia's invasion of Ukraine.[264] The new strategic concept adopted by NATO at the June 2022 Madrid Summit directly addressed these new security realities.[265] In the current global environment, Russia is recognized as significant threat to NATO, while China is viewed as a systematic challenge, prompting great-power competition to emerge as a key priority for the alliance. This rivalry encompasses efforts to exert control over critical technological and industrial sectors, as well as critical infrastructure, strategic materials and supply chains. The strategic framework also highlights the adversarial strategies employed by Russia and China, particularly their utilization of EDTs. There is a strong

[263] See NATO, "Emerging and disruptive technologies, https://www.nato.int/cps/en/natohq/topics_184303.htm.

[264] Stephen Herzog and Dominika Kunertova, "NATO and Emerging Technologies—The Alliance's Shifting Approach to Military Innovation," *Naval War College Review*, Vol. 77, No. 2, 2024, https://digital-commons.usnwc.edu/nwc-review/vol77/iss2/5

[265] NATO, NATO 2022 Strategic Concept (Madrid: 2022), www.nato.int/.

acknowledgment that NATO must foster innovation and increase investments in these technologies to maintain military interoperability and superiority. Thus, NATO defines EDTs as advanced technological innovations that have the potential to transform warfare and fundamentally reshape international security. These technologies also have the potential to disrupt conventional military operations, alter the geopolitical balance of power, and present new strategic challenges for the allies. Consequently, NATO emphasizes the necessity for a comprehensive understanding and proactive adaptation to these technological advancements to sustain thematic and strategic superiority, as well as upholding collective defense obligations.[266] To achieve this goal, NATO collaborates with entities from the public and private sectors, academic institutions and civil society organizations to promote technological innovation, establish international standards for the responsible use of emerging technologies, and maintain its competitive edge through ongoing research and development.[267]

The energy sector, characterized by its extensive interconnections with other critical industries and its inherently technology-driven and innovation-oriented nature, frequently encounters EDTs. Private companies, both national and international, play a substantial role in this sector, serving as both owners and operators, and presenting significant opportunities and risks associated with technological advancements. Consequently, EDTs are tools to revolutionize fundamental energy infrastructure, thereby transforming methodologies related to energy generation, distribution, and consumption. Considering global challenges such as climate change and the finite nature of fossil fuel reserves, these technological innovations offer a strategic pathway toward establishing a more sustainable and resilient energy future. From this perspective, EDTs play a significant role in the ongoing transition from a state of fossil fuel dependency to a renewable and clean energy base. Thus, the dynamic interaction between EDTs and critical energy infrastructures is essential for the development of a secure and sustainable energy paradigm. Embracing innovation while effectively managing associated challenges enables stakeholders to foster an energy landscape that is more resilient, efficient, and accessible. The integration of such technologies not only improves existing system performance but also lays the groundwork for a transformative energy ecosystem capable of meeting the demands of a growing global population while simultaneously safeguarding environmental integrity.[268]

Furthermore, the intersection of terrorism and EDTs presents a significant threat to global security, particularly concerning critical energy infrastructure. As the energy sector rapidly adopts innovative technologies, it inadvertently creates new vulnerabilities that malicious actors may exploit. An understanding of this nexus is crucial for developing robust defense and protection mechanisms to prevent potential attacks that could disrupt energy production, distribution, and consumption. This paper aims to elucidate the role and significance of EDTs within the energy sector, particularly in the context of their potential use by non-state actors.

EDTs and Terrorism

EDTs operate as double-edged swords, presenting both beneficial and harmful effects. On one hand, these technologies drive significant advancements that enhance daily life, offering increased comfort and improved quality through innovative

[266] NATO, "Emerging and disruptive technologies, https://www.nato.int/cps/en/natohq/topics_184303.htm.
[267] Carol V. Evans (Ed.), *Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency*, NATO COE-DAT Handbook 1, COE-DAT and USAWC SSI, November 2022.
[268] World Bank Group, *PPP Contracts in an Age of Disruption*, September 2022, https://ppp.worldbank.org/library/ppp-contracts-age-disruption-download-pdf-version

applications. Conversely, they can also introduce security vulnerabilities that may be exploited. Such weaknesses often attract non-state actors, especially terrorist organizations, who perceive them as strategic opportunities to bolster their capabilities.[269] Notable examples of these EDTs include Artificial Intelligence (AI), Augmented Reality (AR), Deepfakes, Facial Recognition (FR), the Internet of Things (IoT), Machine Learning (ML), the Metaverse, and Virtual Reality (VR). These technologies provide new pathways for non-state actors to exploit vulnerabilities. Terrorist organizations are increasingly harnessing EDTs to facilitate their activities broadly in three main ways: radicalization and recruitment; enhancing operational planning and training; and implementing strategic initiatives, including remote attacks.[270]

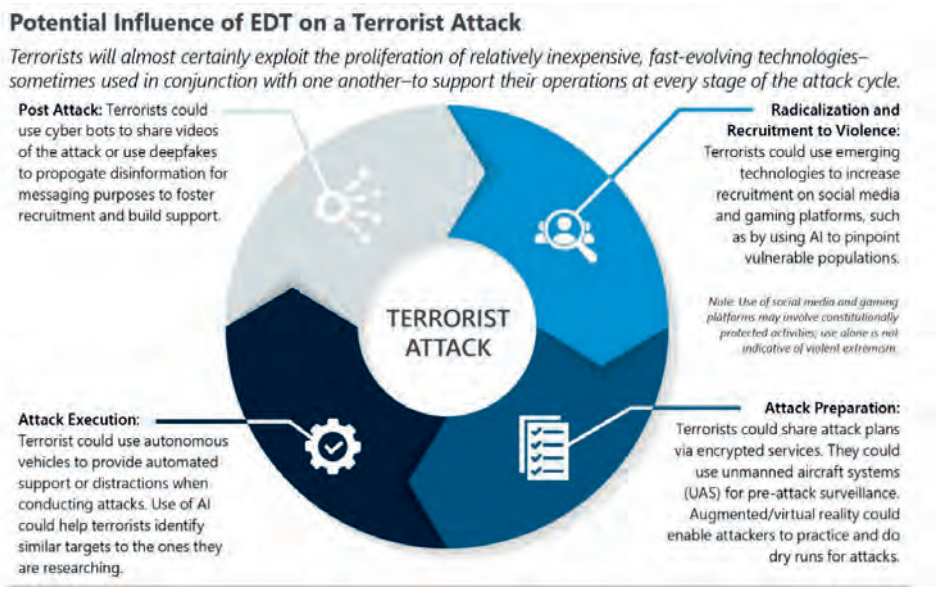
As indicated by the U.S. Office of the Director of National Intelligence's National Counterterrorism Center, EDTs significantly augment the capabilities of terrorist groups by improving their online recruitment efforts.[271] EDTs provide a new framework for expanding radicalization initiatives, considerably enhancing the ability of extremist groups to engage with a diverse range of audiences across multiple countries and regions. These groups not only capitalize on cultural and social dynamics to reach potential recruits but also enhance their ability to establish, develop, and sustain social connections. This interconnectedness amplifies their influence and creates pathways for the recruitment of new adherents to their ideology.[272]

[269] For a comprehensive perspective and analysis, see Sarah J. Lohmann (Eds.), *Countering Terrorism on Tomorrow's Battlefield: Critical Infrastructure Security and Reliability*, Handbook 2, COE-DAT and USAWC SSI, December 2022, https://www.tmmm.tsk.tr/publication/researches/15-Countering_TerrorismonTomorrowsBattlefield.pdf.

[270] For a comprehensive perspective and analysis, see Susan Sim, Eric Hartunian, and Paul J. Milas (Eds.), *Emerging Technologies and Terrorism: An American Perspective*, COE-DAT and USAWC SSI, April 2024.

[271] The U.S. Office of the Director of National Intelligence's National Counterterrorism Center, "Emerging Technologies May Heighten Terrorist Threats," https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/134s_-_First_Responders_Toolbox_-_Emerging_Technologies_May_Heighten_Terrorist_Threats.pdf.

[272] Sarah Lohman, "Chat GPT, Artificial Intelligence, and the Terrorist Toolbox," in Sim *et.al.*, *Emerging Technologies and Terrorism,* pp.23-34.



Source: The U.S. Office of the Director of National Intelligence's National Counterterrorism Center, "Emerging Technologies May Heighten Terrorist Threats," p.2, https://www.odni.gov/files/NCTC/documents/jcat/firstresponderstoolbox/134s_-_First_Responders_Toolbox_-_Emerging_Technologies_May_Heighten_Terrorist_Threats.pdf.

To achieve their goals, terrorists increasingly utilize sophisticated tools such as video manipulation and AI-assisted deepfake technologies. These advanced technologies enhance the ability of non-state actors to craft and disseminate persuasive extremist narratives that resonate with diverse audiences. By presenting manipulated images or fabricated audio and video content, they can create misleading representations of reality that appeal to emotions and beliefs, thereby influencing perceptions and actions.

Consequently, these non-state actors can effectively exploit such technologies to spread misinformation, incite violence, and cultivate virtual ideological and social communities. This not only allows them to promote their extremist views but also fosters an environment where like-minded individuals can connect, share ideas, and reinforce their beliefs, further solidifying their online presence and influence. Through these methods, radicalizers can manipulate public perceptions and recruit individuals who may otherwise have been resistant to their ideologies.

EDTs also offer new ways to plot and train for acts of terrorism. Terrorist groups are likely to be more prepared due to their time planning, preparing, and training in blending augmented and virtual reality.[273] Through comprehensive reconnaissance and careful information gathering, terrorists can create highly detailed virtual environments that accurately depict potential targets and critical infrastructure. This

[273] Kristan J. Wheaton, "Special Anchors and Dangerous Liaisons: Terrorist Collaboration in an Augmented Age," in Sim *et.al., Emerging Technologies and Terrorism,* pp.53-62.

level of advanced preparation enables them to guide their members along specific routes leading to strategic objectives during an attack. Additionally, they can develop and coordinate alternative escape routes, establish robust contingency plans, and practice their attack strategies in controlled virtual settings that minimize risk. Advancements in anonymity tools, such as encrypted communications and Virtual Private Networks (VPNs), further enhance terrorists' ability to conceal their identities and obscure their activities within these virtual domains. Moreover, augmented reality environments could significantly improve the functionality and effectiveness of virtual training camps. These camps would facilitate connections between experienced planners, whether located in remote sanctuaries or conflict zones, and potential operatives worldwide, enabling the real-time exchange of tactics and strategies.

Furthermore, the increasing realism and accessibility of first-person shooter games—particularly those that permit users to create custom environments and scenarios—may contribute to desensitizing individuals to violence. This exposure could lead to a concerning normalization of aggressive behavior, potentially resulting in real-life attacks or violent acts. As these technologies continue to evolve, the implications for security and counter-terrorism efforts become increasingly complex. In response, first responders can combat these threats by understanding how technological innovations can empower terrorist tactics and by implementing effective countermeasures.

Terrorists and non-state actors may also leverage EDTs to develop innovative attack methodologies.[274] These technologies present new opportunities for executing remote attacks, which could potentially result in high-profile incidents. Furthermore, AI, especially when integrated with machine learning, can aid terrorists in identifying new targets. This capability enables quicker decision-making and the efficient adaptation of operational strategies.

AI also has the potential to enhance both the efficiency and lethality of drone-based attacks significantly. For instance, a lone terrorist could use AI to operate multiple drones simultaneously, targeting various locations. Machine learning algorithms might empower drone swarms to circumvent defensive systems. Additionally, AI could assist drones in recognizing specific individuals or groups, facilitating targeted strikes. Fully autonomous, AI-driven systems may enable drones to identify and target security personnel, thereby creating further opportunities for potential attacks.[275]

Moreover, terrorists may exploit machine learning algorithms to identify vulnerable populations by analyzing extensive datasets, allowing them to predict the behaviors of potential targets. They can also utilize machine learning to analyze surveillance footage, aiding in the identification of open and closed routes, patrol patterns, and optimal pathways for their operations.

The emergence of autonomous vehicles introduces significant challenges in threat mitigation.[276] Self-driving cars could empower attackers to maneuver freely and deploy weapon systems without the need to concentrate on vehicle operation. Moreover, terrorists might exploit driverless vehicles for ramming attacks, thereby

[274] Susan Sim, "Emerging Terrorist Threats: Everything, Everywhere, All at Once?" in Sim *et.al., Emerging Technologies and Terrorism,* pp.1-22.
[275] See Lohmann (Eds.), *Countering Terrorism on Tomorrow's Battlefield,* pp.23-44.
[276] Sarah Lohman, "Chat GPT, Artificial Intelligence, and the Terrorist Toolbox," in Sim *et.al., Emerging Technologies and Terrorism,* pp.23-34.

initially obscuring the perpetrator's identity. In the context of physical attacks, operatives could utilize internet-connected devices, such as smart glasses, which provide augmented reality features to assist them with virtual markers and facilitate target identification. The increasing interconnectedness of the physical and virtual realms, particularly through the Internet of Things (IoT), may create vulnerabilities that can be exploited. AI and machine learning algorithms could significantly enhance the offensive cyber capabilities of terrorist actors. These technologies may help identify potential vulnerabilities for exploitation and develop machine-learning-driven attack strategies that are more difficult for defenders to detect and counter.

Terrorists have the potential to harness AI-enabled cyber capabilities, posing threats to both essential physical and digital infrastructures. For example, in April 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued an advisory highlighting the alarming availability of malware that could compromise critical systems, including power grids, factories, water utilities, and oil refineries.[277] These cyber actors could exploit Supervisory Control and Data Acquisition (SCADA) systems, manipulating the processes of critical infrastructure facilities.

Energy Landscape, EDTs, and Potential Terrorist Threats

In recent years, the energy sector has experienced profound transformations driven by geopolitical, economic and technological developments. A central aspect of this transformation is the transition from reliance on fossil fuels to the adoption of renewable and sustainable energy sources.[278] This shift is primarily motivated by concerns related to climate change and global warming, and it has been further expedited by rapid technological innovations that yield immediate, tangible benefits. Consequently, policymakers and stakeholders worldwide are strategically implementing measures to facilitate this energy transition, exemplified by the European Union's target to achieve net-zero carbon emissions by 2045. Notably, advancements in renewable energy technologies, particularly in solar and wind power, have led to increased efficiency and cost reductions, thereby enhancing their accessibility. Additionally, emerging renewable sources such as tidal and geothermal energy are gaining prominence, contributing to the diversification of the energy portfolio and reducing dependence on conventional fuels.

Simultaneously, significant progress has been made in energy storage solutions, addressing one of the critical challenges faced by renewable energy-intermittency. Innovations in battery technologies, alongside alternative storage methods, have improved the reliability and stability of renewable energy supplies by enabling energy retention during periods of low production. Furthermore, the development of innovative grid technologies, facilitated by the Internet of Things (IoT), represents a substantial advancement in energy management.[279] These grids enable real-time adjustments to supply and demand, thereby enhancing resilience, operational efficiency, and the integration of decentralized energy resources. The application of artificial intelligence and machine learning techniques further augments these capabilities through predictive analytics, which optimize energy generation and identify system inefficiencies. This data-driven approach enables utilities to make informed decisions, thereby enhancing overall system management and efficiency. All

[277] CISA, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia.
[278] See IEA, *World Energy Outlook 2024*, https://www.iea.org/reports/world-energy-outlook-2024.
[279] See Khumbulani Derrick Sithole et al., "Employing Internet of Things (IoT) devices for Monitoring and Controlling Energy Management Systems-A Review," *Journal of Electrical Systems*, 20 (11), November 2024, pp.753-760.

in all, the energy sector has evolved into a more complex system, integrating novel components alongside traditional elements that are still dependent on fossil fuels.

It is also imperative to recognize that critical energy infrastructure has become increasingly reliant on advanced technologies, rendering it more sensitive to disruptions. The interconnections of this infrastructure, both within the energy sector and across other sectors, have emerged as vital elements requiring rigorous protection. This paradigm shift in the energy sector has prioritized innovation and, consequently, the development and implementation of EDTs within the energy sector.

Ultimately, the interplay between technological innovation and energy infrastructure development is fundamental to achieving a sustainable energy future. By promoting technological adoption and addressing existing barriers, stakeholders – whether public or private – can foster a more resilient, efficient, and accessible energy system. These technological advancements not only enhance current operational capabilities but also lay the groundwork for a transformative energy ecosystem that can meet the increasing demands of the global population while ensuring environmental sustainability.

Despite these technological advancements and their progressive nature, the integration of innovative solutions encounters several formidable obstacles, including regulatory hurdles, infrastructural limitations, substantial financial costs, and both natural and human-induced vulnerabilities and threats. Furthermore, as the energy infrastructure undergoes increasing digitalization, cybersecurity issues have emerged as critical concerns, necessitating the implementation of robust protective measures to safeguard vital systems and infrastructure. Consequently, it is reasonable to assert that the transition in the energy sector – particularly through the extensive deployment of EDTs and dual-use technologies – introduces new vulnerabilities to critical energy infrastructure and security, thereby exacerbating pre-existing challenges. In other words, EDTs represent technological factors that are profoundly changing our modern daily life, which also potentially generate vulnerabilities and uncertainties in the near future.[280]

Önnered *et al.* delineate three principal perspectives or paradigms concerning energy security: sovereignty, robustness, and resilience.[281] The sovereignty perspective emphasizes geopolitical considerations, prioritizing the identification and counteraction of adversarial threats. The robustness perspective aims to optimize system capacity to withstand both immediate shocks and prolonged external pressures, thereby minimizing vulnerabilities. Conversely, the resilience perspective focuses on understanding the underlying social, economic and technological factors that contribute to the emergence of risk. In the study, they prefer a resilience perspective as a focal point and define resilience as a process encompassing "preparation, mitigation/absorption, recovery, and adaptation, and represent the ability of the energy system to cope with and respond to disturbances."[282] In this context, the threats identified by the authors are defined under five main domains: politics and policy, economic, socio-cultural, technological, and environmental. These threats can

[280] Corri Zoli *et al*., "Terrorist Critical Infrastructures, Organizational Capacity and Security Risk," *Safety Science,* https://doi.org/10.1016/j.ssci.2018.05.021.
[281] See Simon Önnered, Peter E. Johansson, Ioana Stefan and Anders Fundin, "Emerging Threats to Energy Security- A Delphi Study," *Energy Policy*, 2025.
[282] Önnered *et.al*., "Emerging Threats to Energy Security," p.2.

also be further divided into local and international levels, as well as both the short-term and the long-term.

This perspective embodies a comprehensive, holistic approach consistent with NATO's whole-of-state or whole-of-society strategy, and it offers a potentially valuable framework for the analysis presented in this article.[283] Within this context, threats to the energy sector or critical energy infrastructure, particularly those supported by EDTs, serve to amplify existing vulnerabilities. At the same time, emerging technologies introduce novel threats that demand increased attention. From this perspective, Takashi *et al.* presented technology as a vicious cycle that continuously solves problems only to create new ones, thereby deepening technological lock-in.[284] Similarly, Körner *et al.* describe the consequences of increasing complexity and interconnectedness as raising the possibility for cascading effects.[285] As Önnered *et al*. emphasized, while a fossil fuel-based energy system is facing significant threats, a more renewable, integrated, and electrified energy system introduces new challenges that need to be addressed.[286] So, addressing these technological threats necessitates the development of innovative approaches that extend beyond traditional methodologies. Although this creates a complex and cyclical challenge, it is imperative to acknowledge that the intricacies of modern life render such adaptations unavoidable.

The vulnerability of the energy sector and its critical infrastructure can manifest in various forms, impacting both the security and reliability of energy systems. Vulnerability is defined as a weakness that threats can exploit, while risk refers to the chance of loss if these threats occur. The energy system, viewed as a connected entity, and its ability to respond to emerging threats – where security is seen as an evolving vulnerability, and resilience is the capacity to reduce and adapt to these threats – are essential. This raises a key question: what are the nature and origins of these threats? In recent years, energy infrastructure has faced increasing threats from EDTs. These threats can be categorized into three groups: natural, technological, and socio-political. Examples include technological failures during production or transmission, malicious cyber or physical attacks, extreme weather events, corruption, poor governance, monopolistic practices, and political instability. As another level, private and foreign state ownership of technologies and infrastructure also poses threats because it can cause supply disruptions and sabotage, as well influencing politics, the economy, and supply chains for its own benefit. Understanding these diverse threats is crucial for creating effective strategies to improve the security and resilience of energy systems.

Inflicting maximum damage and social disruption is a primary objective for terrorist organizations. The consequences of an attack on the critical energy infrastructure could vary widely. That makes the critical energy infrastructure the primary target for terrorists. Through attacking those targets, terrorists can cause striking material and psychological losses on the nation's critical assets and deprive

[283] For NATO's whole-of-society approach see *Resolution 466-Developing A Whole-Of-Society, Integrated and Coordinated Approach to Resilience for Allied Democracies*, https://www.nato-pa.int/document/resolution-466-developing-whole-society-integrated-and-coordinated-approach-resilience.
[284] Reiko Takahashi, Ryoji Nakamura, and Yuichi Washida, "Socio-technological Scenarios of Japan's Future Energy Issues in 2050 based on Scanning-based Foresight Method", *Foresight*, Vol.21. Issue 4, September 2019, pp.467-481, https://www.emerald.com/fs/article/21/4/467/86160/Socio-technological-scenarios-of-Japan-s-future.
[285] M.F. Körner *et.al*., "Systemic Risks in Electricity Systems: A perspective on the Potential Digital Technologies," *Energy Policy*, Vol. 164, May 2022, https://www.sciencedirect.com/science/article/pii/S0301421522001264
[286] Önnered et.al., "Emerging Threats to Energy Security," p.11.

people of their basic needs. An attack has a direct impact on daily life due to its ongoing consequences for other critical systems, resulting in a spillover effect in different sectors. As far as energy is concerned, continuity is sensitive and complex to replace in the event of any interruption. The consequences of any successful attack on critical energy infrastructure are myriad and have effects on producers, consumers and transit countries. Through any attack, terrorists could deprive the supplier of the market, the transporter of income, of the consumer of energy. Critical infrastructure facilities and systems are also an outstanding target for terrorists. Any terrorist attack could be organized during the design, construction, or operational stage. That serves the basic aim of any terrorist organization at any time in the best way. What theoretical frameworks and analytical strategies can be utilized to clarify non-state actors' use of EDTs, and their engagement within the energy sector or regarding critical energy infrastructure? It is essential to examine the multifaceted interactions between the aims of terrorist groups and energy resources, considering the potential implications for national and global security. Furthermore, a comprehensive understanding of their motivations, operational methods, and strategic objectives is crucial for developing effective countermeasures to protect energy infrastructure from the threats posed by these entities. This inquiry contributes not only to the discourse on energy security but also informs policy-making and strategic planning to mitigate risks associated with non-state actors in this critical domain. When executing an attack in the physical world, terrorists could equip attackers with internet-equipped hardware, such as smart glasses, that display augmented reality objects using virtual arrows to guide them and mark targets. Furthermore, growing dependence and the intersection of the physical world and the virtual world, primarily through the IoT, will present vulnerabilities that can be exploited.

While non-state actors traditionally rely on low-tech methods for their operations, the increasing accessibility of relatively affordable technology is likely to empower many terrorists to adopt more sophisticated and effective strategies. These advancements can enhance various facets of their activities, including propaganda, recruitment, financing, communication, and the execution of attacks. In recent years, there has been a significant transformation in the way terrorists leverage EDTs, particularly within the energy sector. They are utilizing these technologies not only for spreading propaganda but also for attracting and recruiting new members and coordinating tactical operations. For example, social media platforms and encrypted messaging applications have become essential tools for recruitment and communication, enabling terrorist organizations to reach a wider audience while still maintaining the security of their channels. Moreover, the rise of cyberterrorism poses a considerable threat in this respect. Cyberattacks can disrupt critical infrastructure, such as energy systems, resulting in widespread chaos and panic. Additionally, the advent of uncrewed vehicles—like drones—has opened up new avenues for executing attacks, allowing terrorists to carry out operations remotely and with a reduced risk of detection. In conclusion, as terrorists increasingly harness these advanced technologies, it is essential to recognize the evolving landscape of threats, which now integrates cyber capabilities and automated systems as fundamental components of their strategies.

Propaganda, Recruitment, and Tactical Coordination

Terrorist organizations increasingly use social media and communication technologies to target critical energy infrastructure in various ways.[287] Extremist groups are increasingly capitalizing on social media platforms to disseminate their propaganda and further their agendas. They strategically share content that not only promotes their beliefs but also incites hostility towards critical energy infrastructure, such as oil refineries and pipelines. By circulating graphic videos and inflammatory posts, these organizations aim to provoke violent reactions and recruit new followers who may be vulnerable to their rhetoric.

Additionally, these groups utilize encrypted messaging applications to plan and coordinate their attacks on energy facilities meticulously. Such platforms facilitate secure communication, enabling them to strategize and discuss tactical operations against specific targets, such as oil fields and processing plants. This level of organization significantly enhances their operational efficiency.

Social media also plays a vital role in intelligence-gathering related to essential energy assets. Terrorists can publicly share images and videos of governmental facilities, inadvertently revealing the security measures and potential vulnerabilities. By analyzing this information, they can identify weaknesses, allowing them to formulate more effective and targeted plans for possible attacks. The dual use of social media – as both a means of recruitment and tactical planning – poses a considerable challenge for security agencies responsible for protecting critical energy infrastructure.

Terrorist organizations have increasingly leveraged social media as a powerful tool for gathering intelligence on energy infrastructure as well. This includes pinpointing the locations of critical facilities and identifying perceived vulnerabilities that could facilitate their planning and preparation for attack. By utilizing these platforms, they can effectively crowdsource valuable information from a diverse range of users, thereby enhancing their situational awareness and operational capabilities.

Numerous incidents have illustrated how terrorists exploit social media to disseminate real-time updates during active assaults, crafting sensational narratives that capture public attention and amplify the psychological impact of their actions. A notable example is the coordinated attacks in Paris in November 2015, where social media functioned as a crucial communication channel.[288] Terrorist groups utilized these platforms to relay information about the unfolding events, share images and videos, and highlight the devastation wrought by the attacks, which collectively contributed to a heightened sense of fear and urgency among both the public and authorities. This incident exemplified how social media can not only assist in operational efforts but also significantly influence public perception and media coverage.

Cyberterrorism, Cyberattacks, and Vulnerabilities in Energy Infrastructure

Energy infrastructures, particularly those characterized by smart grids and digitized systems, are increasingly susceptible to a range of cyber threats and

[287] See Megan A. Ward, "Terrorism, Disinformation, and Information Critical Infrastructure," in Lohmann (Eds.), *Countering Terrorism on Tomorrow's Battlefield,* pp.71-96.

[288] See Quinn Williams, "The Attacks on Paris: Lessons Learned," White Paper, Homeland Security Advisor Board, June 2016, https://publicpolicy.pepperdine.edu/hsac/content/hsac-paris-lessons-learned_whitepaper.pdf

attacks.[289] Such interventions have the potential to compromise the operational technology of power plants, resulting in catastrophic failures that can jeopardize human life and lead to widespread environmental degradation. The discourse on critical energy infrastructure as cyber-physical systems has led to the formulation of essential cyber resilience requirements. Cyberspace has become a prominent vector for attacks against critical infrastructure, executed by both state and non-state actors with varied objectives, including the attainment of strategic advantages in geopolitical conflicts. In an alarming trend, terrorist organizations are increasingly targeting civilian populations in proximity to defense installations to further their agendas. Consequently, cyberterrorism has emerged as a novel frontier, exploiting technological vulnerabilities to achieve ideological objectives.

Terrorist groups are increasingly adopting cyber warfare tactics, with a pronounced focus on energy infrastructure to engender disorder and assert their influence. Attacks targeting SCADA systems, which are responsible for managing energy production and distribution, can precipitate severe disruptions and safety hazards. Since the early 2010s, numerous terrorist organizations have orchestrated cyberattacks on critical energy infrastructure, thereby exposing profound vulnerabilities in energy security and underscoring the significant risks posed by these cyber threats.[290] Targeted assaults on power grids, oil refineries, and other critical energy facilities demonstrate the effectiveness of cyber operations in achieving strategic objectives and underscore their broader implications for national security and economic stability.

The Stuxnet incident of 2010 represents the first known and most notable case of a cyberattack on critical energy infrastructure.[291] This advanced computer worm specifically targeted Iran's nuclear enrichment facilities – namely, the uranium-enrichment plant at Natanz and the nuclear reactor at Bushehr, or potentially both. Evidence indicated that by the end of 2010, over 60 percent of the approximately 100,000 computers infected by Stuxnet were in Iran. The worm had been in circulation since at least mid-2009. During the latter half of that year, an unusual number of centrifuges – machines used to concentrate uranium by spinning at high speeds – were taken offline and replaced at the Natanz facility. Speculation regarding the worm's origins emerged, but the Iranian government asserted that a foreign virus had infected computers at various nuclear facilities, claiming it caused only minor disruptions. Nonetheless, experts largely agreed that Iran's challenges were far from negligible, with some suggesting that the country's nuclear program may have experienced a significant setback. While it was impossible to attribute these difficulties to the Stuxnet worm definitively, it became clear to cybersecurity specialists that Iran had encountered a cyber-attack involving what might be the most sophisticated malware ever created. By disrupting industrial processes in a critical sector of a sovereign nation, Stuxnet represented a potent offensive cyber weapon, marking a significant escalation in the capabilities and willingness of states and state-sponsored

[289] Venkatachary Sampath Kumar, Jagdish Prasad and Ravi Samikannu, "A critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector," *International Journal of Critical Infrastructure*, Vol.14, No.2, 2018, pp 101-119, ; Daniela Oliveira, "Cyber-Terrorism & Critical Energy Infrastructure Vulnerability to Cyber-Attacks," *Environmental & Energy Law & Policy Journal,* 5, Fall 2010, pp.519-526.

[290] Sampath Kumar Venkatachary et.al, "Cybersecurity and cyber-terrorism challenges to energy-related infrastructures – Cybersecurity frameworks and economics – Comprehensive review," *International Journal of Critical Infrastructure Protection*, Vol. 45, July 2024.

[291] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired Security, 3 November 2014, https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

groups to engage in cyber warfare. In essence, the attack highlighted how cyber threats could inflict severe damage to critical energy infrastructure by sabotaging operational capabilities and causing physical harm to equipment.

Other early instances of cyberattacks include the Shamoon malware attack on Saudi Aramco in August 2012, which resulted in the erasure of data from thousands of computers integral to the company's operations, thereby disrupting its activities and highlighting the significance of cyber threats to national energy security.[292] A self-replicating virus targeted the computer network of Saudi Aramco in an attack that infected approximately 30,000 Windows-based machines. Despite the company's extensive resources as Saudi Arabia's national oil and gas firm, reports indicate that it took almost two weeks for Aramco to recover from the damage. While viruses are a common occurrence on the networks of multinational corporations, the scale of this attack against a company so vital to global energy markets is particularly concerning. The virus, later referred to as Shamoon, caused significant disruption for the world's largest oil producer. Its primary function seemed to be the indiscriminate deletion of data from computer hard drives. Although this did not result in an oil spill, explosion, or any major operational failures, the attack affected the company's business processes. It likely resulted in the loss of some drilling and production data. Additionally, Shamoon spread to the networks of other oil and gas companies, underscoring the ongoing warnings about the risks of cyberattacks on critical infrastructure.

The WannaCry ransomware attack of 2017 further exemplifies how swiftly essential services can be endangered by cybercriminal activities, with potentially dire implications for energy infrastructure should terrorist entities employ analogous methods.[293] The 2021 Colonial Pipeline ransomware attack, executed by the cybercriminal group known as DarkSide, serves as another pivotal case study in the realm of cybersecurity.[294] This attack specifically targeted the Colonial Pipeline in the United States, resulting in significant disruptions to the fuel supply along the East Coast. On 7 May 2021, the incident captured global attention, with images depicting long lines of cars at gas stations throughout the region. Many Americans panicked, resorting to filling bags with fuel out of concern over their ability to commute to work or transport their children to school. This event highlighted the vulnerabilities inherent in our interconnected society, the weakness of the security apparatus, and underscored the critical importance of cybersecurity for ordinary people.

The ongoing conflict in Ukraine provides a crucial context for understanding the evolving landscape of cyberattacks and their implications for critical sectors, particularly through hybrid warfare tactics aimed at disrupting critical energy infrastructure.[295] Along with direct physical attacks, a notable example is the 2015 cyberattack on Ukraine's power grid, attributed to Russian cyber operatives who infiltrated utility companies to manipulate operational processes and shut down substations. This sophisticated cyber intervention resulted in widespread blackouts and had profound repercussions for the country's energy security. Recent

[292] Christopher Bronk and Eneken Tikk-Ringas, "The Cyber Attack on Saudi Aramco," *Survival*, Vol.55, No.2, 2013 pp.81-96, https://doi.org/10.1080/00396338.2013.784468.
[293] Jennifer Gregory, "WannaCry: How the Widespread Ransomware Changed Cybersecurity," IBM, https://www.ibm.com/think/x-force/wannacry-worm-ransomware-changed-cybersecurity.
[294] Suraj Srinivasan and Li-Kuan Ni, "Ransomware Attack at Colonial Pipeline Company," Harvard Business School Case 123-069, March 2023.
[295] Dr. Karen Guttieri, "Energy Sector Cyber Resilience Reconsidered," 2025, https://www.sto.nato.int/document/energy-sector-cyber-resilience-reconsidered/

developments underscore that attacks on Ukraine's energy infrastructure – particularly by Russian state-sponsored actors – constitute significant threats not only to Ukraine but also to several neighboring nations. Given the capacity of terrorist organizations to adapt and learn from such incidents, it is anticipated in the foreseeable future that new threats and cyberattacks will emerge.

The 2019 Norsk Hydro ransomware attack further exemplifies the far-reaching ramifications of cyber incidents.[296] Targeting the Norwegian aluminum producer, this attack disrupted operations on a global scale, significantly impacting energy supply chains. This incident illustrates how cyberattacks can extend their influence beyond immediate targets, thereby affecting energy supply and production processes. Moreover, similar threats may affect related sectors that impact the energy industry, as illustrated by the 2020 SolarWinds Supply Chain Attack.[297] This incident exemplified a classic supply chain assault, where attackers did not target their victims' networks directly. Instead, they infiltrated the systems of a third-party supplier with access to the networks of their intended targets, which in this case was SolarWinds. Many of SolarWinds' customers employed a system known as Orion, a performance monitoring solution that tracks the operational status of its users. Orion possesses privileged access to gather performance data and information from the logs generated by the customers' IT assets, making SolarWinds an appealing target for hackers. The attackers successfully gained access to the networks of thousands of companies by exploiting vulnerabilities in software updates, thereby posing a considerable threat to both energy operations and sensitive data.

The examples above collectively underscore the significant vulnerabilities inherent within critical energy infrastructure, thereby accentuating the pressing necessity for enhanced cybersecurity measures to mitigate the escalating threat of cyberterrorism. Furthermore, Artificial Intelligence (AI) and machine learning algorithms possess the potential to augment the offensive cyber operations conducted by terrorist entities. These technologies may help identify exploitable vulnerabilities and facilitate the development of sophisticated, machine-learning-driven attack methodologies that are more challenging for defenders to detect and counter. Moreover, terrorist groups could harness AI-enabled cyber capabilities to pose threats to the energy sector and other vital physical and digital infrastructures.

Use of Uncrewed Vehicles (UVs)

EDTs are creating new avenues for terrorists to utilize innovative remote attack methods and carry out high-profile strikes. In this context, uncrewed vehicles (UVs), commonly referred to as drones, represent a significant category of EDT relevant to terrorism.[298] Drones—whether deployed on land, in the air, or at sea—are becoming increasingly affordable and accessible. This trend empowers individuals and small groups to conduct reconnaissance or even execute kinetic attacks on critical infrastructure. Terrorist organizations have already demonstrated the willingness to employ drones for such attacks, as observed in various global conflicts.

---

[296] Bill Brigs, "Hackers hit Norsk Hydro with Ransomeware: The Company Responded with Transparency," https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

[297] Fortinet, "SolarWinds Cyber Attack," 2025 Threat Landscape Report, https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack

[298] See Sıtkı Egeli, "Innovative Tools Available to Non-State Actors: Aerial Drones and Unmanned Systems at Sea and on Land," in this volume.

In the energy sector, a drone strike aimed at critical infrastructure such as a refinery, power plant or transmission lines can result in extensive damage and catastrophic consequences.[299] The immediate impact would involve physical destruction of vital components, which could halt production and disrupt energy generation. However, the repercussions extend far beyond mere physical damage. Such an attack could trigger widespread panic among the public, leading to a loss of confidence in the stability of energy supplies.

The disruption of energy supplies can have a domino effect on daily life, affecting everything from home heating and cooling systems to the operation of businesses that rely on consistent energy availability. This could result in significant economic losses, including job disruptions and financial instability for businesses, particularly those heavily dependent on electricity.

In light of these potential threats, security agencies face the urgent task of developing effective counter-drone technologies and comprehensive strategies to mitigate these risks. This includes enhancing surveillance capabilities, implementing robust response protocols, and collaborating with other agencies to ensure the safety and security of critical energy infrastructure.

Terrorist organizations have increasingly resorted to using drones to attack vital energy infrastructure, showcasing advancements in both technology and tactics. A significant case occurred in September 2019, when Houthi rebels launched coordinated drone strikes against Saudi Aramco, the state-owned oil company of Saudi Arabia.[300] These targeted attacks hit two key facilities: the Abqaiq oil processing plant, which is crucial for the processing and stabilization of crude oil, and the Khurais oil field, one of the largest oil fields in the country.

The assaults resulted in extensive damage, leading to a dramatic reduction in oil production and a temporary disruption of approximately 5% of the global crude oil supply. This incident not only underscored the vulnerability of critical infrastructure to drone warfare but also highlighted the geopolitical implications of such attacks, as they can significantly impact global oil markets and energy security.

Between 2016 and 2017, various reports revealed that Daesh implemented the use of drones modified with explosives to conduct targeted attacks on oil facilities in Iraq.[301] This marked a significant evolution in their approach to asymmetric warfare, as they adopted advanced technologies to enhance their operational capabilities. These drones were not only employed for surveillance and reconnaissance missions, allowing for real-time monitoring of strategic locations, but they also served as delivery systems for bombs, enabling precise strikes against critical infrastructure. These vehicles were designed to carry out assassination attempts, demonstrating the group's willingness to adapt its tactics to exploit technological advancements for its strategic aims. This combination of drone warfare and uncrewed ground vehicles highlighted a concerning trend in modern combat, where non-state actors are leveraging sophisticated technology to challenge conventional military forces.

---

[299] Akhilesh Kootala, Ahmed Mousa, and Philip W. T. Pong, "Drones are Endangering Energy Critical Infrastructure, and How We Can Deal with This," *Energies*, Vol.*16*, No.14, 2023, 5521; https://doi.org/10.3390/en16145521

[300] IntelBrief, "Houthis Drone Attack Targets Major Saudi Oil Facilities," The Soufan Center, 16 September 2019, https://thesoufancenter.org/intelbrief-houthis-drone-attack-targets-major-saudi-oil-facilities/

[301] Serkan Balkan, *DAESH's Drone Strategy: Technology and the Rise of Innovative Terrorism*, SETA Report, 2017, https://media.setav.org/en/file/2017/08/daeshs-drone-strategy-technology-and-the-rise-of-innovative-terrorism.pdf

These examples highlight the evolving threats posed by UAVs and underscore the need for comprehensive security measures to protect critical energy infrastructure from such innovative tactics. AI, particularly when enhanced by machine learning, may ease terrorist organizations ' ability to identify new targets, make quicker decisions, and implement operational adjustments. AI has the potential to make drone attacks more efficient and lethal, such as by enabling a lone terrorist to pilot drones directed at multiple targets. In contrast, machine learning could enable drone swarms to overwhelm mitigation systems. AI may also assist drones with targeted killings by identifying specific people or members of a targeted ethnic group. Fully autonomous, AI-powered systems could enable drones to locate and target security forces, thereby clearing a path to their intended targets.

Terrorists could use machine-learning algorithms to identify vulnerable populations by processing large quantities of data to analyze and predict the behavior of potential targets. Terrorists could also use machine learning to analyze surveillance footage to identify open and closed routes, patrol patterns, and efficient routes. Autonomous vehicles present unique challenges to mitigating active threats. Self-driving cars could allow an attacker the freedom to maneuver and use weapon systems without needing to focus on vehicle operation. Terrorists could also use driverless vehicles in vehicle-ramming attacks, initially obscuring the identity of the responsible party.

Conclusions

What specific measures can stakeholders implement to enhance cybersecurity in energy infrastructure? How can organizations effectively balance innovation in energy technologies with the need for security? What role do international collaborations play in addressing the security implications of emerging energy technologies?

To answer these questions, it is important to recognize that EDTs represent not only a wave of innovation but also present complex challenges in the ongoing battle against terrorism. Technologies such as artificial intelligence, blockchain, and advanced surveillance systems offer significant benefits; however, they also introduce new vulnerabilities that malicious actors may exploit. This dynamic landscape requires a thorough reevaluation of our strategies and methods to effectively counter these threats.

The transformation of the energy sector through EDTs introduces numerous vulnerabilities that terrorist organizations could exploit. The increasing reliance on digital systems, smart grids, and Internet of Things (IoT) devices in energy production and distribution has made critical energy infrastructure increasingly susceptible to both physical threats and cyberattacks. To mitigate these evolving risks, it is essential for stakeholders – including government agencies, private sector entities, and international organizations – to engage in vigilant monitoring, innovative problem-solving, and robust inter-sectoral collaboration.

By prioritizing security measures and fostering resilience within the energy sector, stakeholders can build more effective defenses against potential terrorist actions. This involves investing in advanced cybersecurity protocols, conducting thorough and regular risk assessments, and ensuring that energy infrastructure is fortified against both physical and cyber threats. Such proactive measures not only

protect essential services, such as electricity and fuel supply, but also promote broader societal stability by maintaining public trust in critical systems.

The intersection of terrorism and EDTs poses significant challenges to global security, particularly regarding the integrity of critical energy infrastructure. As the energy sector increasingly incorporates innovations such as renewable energy sources, Artificial Intelligence and automation, it inadvertently creates new vulnerabilities that malicious actors may exploit. A nuanced understanding of this relationship is crucial for developing effective strategies to prevent potential attacks that could disrupt energy production, distribution and consumption.

Moreover, stakeholders must stay informed about the latest technological advancements and their security implications. This includes comprehending how techniques such as drone technology, sophisticated hacking methods and social engineering tactics can be employed to compromise energy systems. By adopting a proactive and comprehensive approach to security – one that includes continuous education and awareness programs – the energy sector can better prepare for and mitigate the risks associated with terrorism in an increasingly interconnected global environment.

The multifaceted nature of the challenges we face, particularly in critical sectors such as energy, underscores the need for a detailed, technology-focused approach. The interconnectedness of our modern world means that a breach in one area can have cascading effects across others, amplifying potential risks. Therefore, it is imperative to adopt comprehensive strategies that harness the advantages of EDTs while addressing their associated risks.

To effectively address potential threats and capitalize on emerging technological advancements, we must undertake several key actions. Firstly, raising awareness about these threats and improving our understanding of new technologies is essential. Enhancing technological literacy across all levels of the organization, ranging from leadership to staff, is critical. Both public and private institutions should invest in comprehensive technology training and collaborate with stakeholders to explore innovative technologies and identify best practices.

Secondly, ongoing assessments of resource needs are vital. States or related bodies must proactively evaluate their resource allocation and investment requirements to ensure that their capabilities keep pace with technological advancements. This involves identifying and anticipating implications for operational readiness, broadening the variety of information collected, and enhancing the tools used for data sorting and organization. Such tools may include advanced biometric identification, data mining techniques, full-motion video analysis and metadata analysis. Additionally, resources for data analytics should encompass emerging technologies related to these areas.

Findings, Conclusions, Lessons Learned, and Recommendations for NATO

In conclusion, this volume, 'Emerging Disruptive Technologies and Terrorism', elucidates the profound implications of the intersection between Emerging Disruptive Technologies (EDTs) and terrorism in contemporary society. The essays compiled herein critically examine the myriad ways in which these technologies are transforming the capabilities of terrorist organizations, thus complicating the endeavors of investigators and first responders tasked with mitigating these multifaceted threats.

The study highlights that terrorist entities are becoming increasingly adept at leveraging EDTs for a range of objectives. These include enhancing their radicalization and recruitment strategies, refining operational planning and execution, as well as adopting innovative methodologies for executing remote attacks. Such advancements necessitate a comprehensive understanding among policymakers and first responders regarding the potential for terrorist tactics to be empowered through technological innovation, thereby informing the development and implementation of effective countermeasures.

Foremost among the disruptive impacts of EDTs is their role in expanding radicalization efforts. These technologies have substantially augmented the capability of extremist groups to disseminate their ideologies to diverse audiences across global contexts. This is achieved not only through the exploitation of cultural and social dynamics to attract recruits, but also by fostering enhanced social connectivity that amplifies their influence. As a result, these non-state actors can adeptly utilize such platforms to propagate misinformation, incite violence, and create virtual communities that reinforce extremist narratives. This environment cultivates a robust ecosystem for ideological propagation, facilitating the recruitment of individuals to their radical ideologies.

Furthermore, the integration of EDTs into terrorist training methodologies and planning processes signifies a paradigm shift in the preparedness of these groups. The investment in augmented and virtual reality tools for training purposes denotes a strategic pivot that may enhance their operational readiness. Simultaneously, the accessibility and realism of first-person shooter games, which permit users to customize scenarios, may inadvertently contribute to the desensitization to violence. Such exposure risks normalizing aggressive behaviors, potentially laying the groundwork for real-world attacks.

As these technological advancements continue to progress, the implications for security and counter-terrorism become increasingly complex. Therefore, first responders and policymakers must remain vigilant and proactive in understanding how these EDTs can be employed by terrorist organizations, ensuring that they can devise well-informed strategies to counter these evolving threats.

NATO allies and partner nations are similarly affected by the dynamics of EDTs. These technologies have exerted a considerable influence on the operational strategies and strategic planning processes of NATO member states and their allies, thereby lessening the risks associated with EDTs. NATO has undertaken collaborative initiatives with member states to formulate responsible, innovative, and flexible policies concerning these technologies. As a testament to this commitment, NATO leaders established an Emerging and Disruptive Technology Implementation Roadmap in 2019, which outlines seven critical areas: data, artificial intelligence (AI), autonomy,

quantum technologies, biotechnology and human enhancement technologies, hypersonic technologies, and space. Since that time, NATO has developed various organizations to address the challenges posed by EDTs, including the NATO Data and AI Review Board, the NATO Innovation Board, the Transatlantic Quantum Community, the Digital Policy Committee, the Conference of National Armaments Directors, the Science and Technology Organization, and the NATO Communications and Information Agency, among others. These initiatives and formal bodies underscore NATO's strong commitment to EDTs, which is intrinsically linked to collaboration with stakeholders across the public and private sectors, academia, and civil society. Given that many defense-related applications of EDTs arise through partnerships with the private sector, engagement with industry – especially start-ups – remains crucial. The North Atlantic Council has organized several technology-focused sessions that facilitate exchanges between Permanent Representatives and industry executives leading technological innovations.

Moreover, NATO is actively promoting the rapid adoption and integration of new technological advances among its member countries. By cultivating partnerships with relevant stakeholders in academia and the private sector, NATO aims to maintain its technological superiority and military preeminence, thereby enhancing its ability to deter aggression and protect Allied nations. The endorsement by NATO Defence Ministers of the first comprehensive strategy, 'Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies', in February 2021, serves as NATO's overarching framework for guiding its engagement with EDTs. This strategy bifurcated its objectives into two key domains: fostering a cohesive approach to the development and adoption of dual-use technologies that address both commercial markets and defense applications to strengthen the Alliance's technological edge; and establishing a forum for Allies to bolster their defenses against the exploitative uses of EDTs by adversarial entities, while also safeguarding their own technological innovations and ecosystems from interference and manipulation. These strategic objectives are fundamental to maintaining NATO's strategic effectiveness and dominance.

At the 2021 Brussels Summit, Allied Leaders reached a consensus to establish the Defence Innovation Accelerator for the North Atlantic (DIANA). This initiative aims to bolster transatlantic collaboration on critical technologies, enhance interoperability, and leverage civilian innovation through engagement with both academia and the private sector. Launched in 2022, DIANA collaborates with leading researchers and entrepreneurs, spanning early-stage startups to more established enterprises, to address pressing defense and security challenges through dual-use technologies. DIANA's operations involve issuing competitive industry challenges focused on significant defense or security issues, inviting innovators to create advanced dual-use technologies as solutions. Selected participants in DIANA's programs receive non-dilutive grants—investment capital that enables them to maintain equity and ownership of their enterprises.

During the 2021 Brussels Summit, NATO leaders also formalized the creation of the NATO Innovation Fund to facilitate direct investments in startups located within member states. This €1 billion venture capital initiative is designed to make strategic investments in startups that are developing dual-use EDTs critical for the security of Allied nations. Many deep-tech startups struggle to obtain sufficient funding due to extended time-to-market timelines and the considerable capital intensity required for their research efforts.

Moreover, the strategic concept adopted by NATO during the June 2022 Madrid Summit articulates the principal challenges confronting the Alliance and delineates the approach NATO will employ to address them. It recognizes that EDTs pose both substantial opportunities and inherent risks, fundamentally changing the nature of conflict and gaining increased strategic significance in the global competition arena. Consequently, the Allies reached a collective agreement within the Strategic Concept to foster innovation and escalate investments in EDTs, thereby preserving NATO's interoperability and military advantage. Member states will cooperate to adopt and integrate new technologies, engage with the private sector, safeguard their innovation ecosystems, establish standards, and adhere to principles of responsible usage in alignment with the democratic values and human rights upheld by the Alliance.

To realize its objectives, NATO collaborates with a diverse array of stakeholders, encompassing public and private sectors, academic institutions, and civil society organizations. This collaboration seeks to promote technological innovation, establish international standards for the responsible application of emerging technologies, and maintain a competitive edge through ongoing research and development. Recognizing the strategic imperative to keep pace with technological developments beyond the Alliance, Allied Leaders endorsed NATO's Rapid Adoption Action Plan at the 2025 NATO Summit in The Hague. This initiative aims to markedly accelerate the adoption and integration of new technological products into Allied armed forces, targeting a timeframe of 24 months or less. The plan outlines shared objectives and best practices that enhance adoption procedures, allocate resources, and embrace calculated risks, all with the support of NATO. This initiative will empower Allies to expedite their national processes for the rapid procurement and integration of new technologies into their armed forces.

In conclusion, NATO is undertaking a comprehensive review of its strategies and organizational structures to effectively address both traditional and emerging threats posed by state and non-state actors. This evaluation is critical for ensuring that member states are adequately equipped to navigate the complexities of an increasingly dynamic global environment. Within this framework, countering terrorism has emerged as a primary focus of NATO and is integral to its operational agenda. The Alliance acknowledges that the nature of terrorism is evolving, with extremist organizations increasingly exploiting new technologies and social dynamics to further their agendas. By reframing these extremist threats as opportunities for innovation, NATO highlights the need for a proactive and multifaceted approach to counterterrorism. Such an approach involves enhancing collaboration among member nations, facilitating the sharing of intelligence, and developing strategies that integrate both military and non-military resources to achieve common objectives. Moreover, NATO is committed to fostering an environment of collaboration wherein shared experiences and best practices can be leveraged to strengthen collective security. This innovative perspective in the fight against terrorism is essential, not only for neutralizing existing threats but also for preempting the emergence of new ones in the future.


CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
2004
TÜRKİYE

NATO COE-DAT