Centre of Excellence Defense Against Terrorism
COE-DAT

TERRORISM EXPERTS CONFERENCE & DAT EXECUTIVE LEVEL SEMINAR REPORT

15-16 OCTOBER 2025

ANKARA, TÜRKİYE

CENTRE OF EXCELLENCE

DEFENCE AGAINST TERRORISM

Combined

Terrorism Expert Conference &

Defence Against Terrorism – Executive Level Seminar 2025

United Against Terrorism: Securing the Future

CONFERENCE REPORT

by the

Centre of Excellence Defence Against Terrorism

15-16 October 2025

Ankara, Türkiye

DISCLAIMER

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

CONTENT

Terrorism Experts Conference 2025

TEAM

Activity Director

Col. Ahmet EROL (TÜR A)

Deputy Activity Directors

Col. Pınar ALPER (TÜR AF)
Ms. Demet UZUNOĞLU (TÜR CIV)

Academic Advisor

Dr. Zeynep SÜTALAN, Ankara, Türkiye.

Speakers & Moderators & Organizations

Mr. Thomas GOFFUS, NATO Assistant Secretary General for Operations and NATO Secretary General's Special Coordinator for CT, NATO HQ, Belgium.
Dr. Zeynep SÜTALAN, Free-Lance Researcher, Türkiye.
Prof. Mitat ÇELIKPALA, Kadir Has University, Türkiye.
Dr. Christina SCHORI LIANG, Geneva Centre for Security Policy, Switzerland.
Prof. János BESENYŐ, Óbuda University, Hungary.
Mr. Stephen HARLEY, PhD Candidate, University of Strathclyde, UK.
Mr. Alexander PALMER, Center for International Strategic Studies (CSIS), USA.
BG (ret) Russell D. HOWARD, Howard Consulting Services, USA.
Dr. Andrea GILLI, University of St Andrews, UK.
Mr. Jan HEINEMANN, International Kriegsspiel Society, Germany.
Ms. Jessa MELLEA, Global Internet Forum to Counter Terrorism (GIFCT), USA.
Dr. Thomas SPAHR, US Army War College, USA.
Mr. Sabri Anıl KAYA, Secretariat of Defence Industries Presidency of the Republic of Türkiye.
Col. Ecevit Özgür TAŞÇI, NATO Stability Policing COE, Italy.
Mr. Yaşar Başar AKSOKU, INTERPOL, France.
LTC Pedro CAVALEIRO, NATO Strategic Direction - South Hub, Italy.
Prof. Uğur GÜNGÖR, Başkent University, Türkiye.
Mr. Mario Alberto ORTIZ BARRAGAN, Ministry of Defence of Colombia.
Maj. Adel SAOUD, Ministry of Defence of Tunisia.

Rapporteurs

Ms. Elif Merve DUMANKAYA, Bilkent University, Türkiye.
Ms. Yağmur AŞIK, Bilkent University, Türkiye.

Biographies

Mr. Thomas GOFFUS

NATO Assistant Secretary General for Operations and NATO Secretary General’s Special Coordinator for Counter-Terrorism.

Tom Goffus was appointed Assistant Secretary General for Operations in January 2022. He advises the Secretary General on strengthening defence capabilities of NATO partners, preparing NATO for the defence of Alliance territory, and responding to crises. In October 2023, Tom Goffus was also appointed as NATO Secretary General's Special Coordinator for Counter-Terrorism.

Prior to joining the NATO International Staff, he served as Policy Director on the U.S. Senate Armed Services Committee, Deputy Assistant Secretary of Defense for European and NATO Policy, National Security Staff Director for Strategic and Eastern European Affairs, and Senior Military Advisor for European and Eurasian Affairs at the State Department. He graduated from the United States Air Force Academy, was commissioned in the Air Force, and flew the F-15, T-6, and T-37 aircraft.

Dr. Zeynep SÜTALAN —Academic Advisor

Academic Advisor, Free-Lance Researcher, Türkiye.

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 a 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. Mitat ÇELİKPALA

Professor, Kadir Has University, Türkiye.

Prof. 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 İstanbul. 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 Center of Excellence for Defence Against Terrorism in Ankara from 2009 to 2012, concentrating on regional security dynamics and critical infrastructure protection. Additionally, he was a Strategic Research and Study Center (SAREM) board member under the Turkish General Staff from 2005 to 2011. He was Academic Advisor to the Center for Strategic Research (SAM) at the Turkish Foreign Ministry between 2002 and 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 contemporary international relations and security studies challenges.

Ms. Christina SCHORI LIANG

Geneva Centre for Security Policy, Switzerland.

Dr. Christina Schori Liang is Head of Counterterrorism and Preventing Violent Extremism at the Geneva Centre for Security Policy in Geneva, Switzerland. At GCSP, she delivers courses on Preventing Violent Extremism and Transnational Organised Crime. Dr. Liang leads GCSP's monthly Geneva Security Debates which feature the world's leading thinkers on important security challenges.

Dr. Liang is a prolific writer and has given over a hundred academic and policy-related presentations in 35 countries. Dr Liang has recently contributed chapters to three books – A book published by NATO on The Effects of the Russia-Ukraine War on Counterterrorism and a chapter on "New and Emerging Technologies for Terrorists" in the Routledge Companion on Terrorism Studies as well as a chapter on "Decoding the New Geopolitics of Cyberspace, Hybrid Operations and Emerging Technologies and Their Impact on States and Society" in a Manchester University Press book entitled Negotiating Identity Conflicts in a Fragmenting World Order. She is also currently the editor of a NATO book that will be published at the end of the year entitled Terrorism in 2040: How to Counter Asymmetric Warfare in a Hyperconnected World.

She has been teaching courses at the Paris School of International Affairs, Sciences Po, Paris since 2017. She holds a doctorate in International Relations from the Graduate Institute of International and Development Studies, Geneva, Switzerland.

Prof. János BESENYŐ

Óbuda University, Hungary.

Professor János Besenyő (1972), between 1987 and 2018, he served as a professional soldier in the Hungarian Defence Forces. He has been involved in several peace operations in Africa (Western-Sahara and Darfur) and Afghanistan. During his service, he received 27 different Hungarian and foreign medals. He received his PhD in Military Science from Miklós Zrínyi National Defense University in 2011, and in 2017, he received a habilitated doctorate at Eötvös Lórant University. As Colonel, he established the Scientific Research Center of the Hungarian Defence Forces General Staff in 2014, and was the first leader of it from 2014-2018.

From 2018 he is a full professor at the Óbuda University, Doctoral School for Safety and Security Sciences and head of the Africa Research Institute (Hungary, Budapest). His research interests include contemporary and recent history of Africa, migration and the Middle East, and peacekeeping, military logistics, Hungarian peacekeeping operations in Africa, with particular reference to Western Sahara, and in addition, comparing political cultures, political communication and intercultural communication, DDR programs in Africa, terrorism, and Christian-Muslim relationship on the continent. He is not teaching only at Óbuda University, Doctoral School for Safety and Security Sciences but ELTE Doctoral School of History, EKE Doctoral School of History, and National Public Service University, Doctoral School of Military Sciences. He is a visiting professor of Stellenbosch University, The Centre for Military Studies (South Africa). He wrote several books and articles. His most recent publication is “Darfur Peacekeepers – The African Union Peacekeeping Mission in Darfur (AMIS) from the perspective of a Hungarian military advisor” (L’Harmattan, Paris 2021).

Mr. Stephen HARLEY

PhD Candidate, University of Strathclyde, UK.

Mr. Stephen Harley is a former British Army officer who has latterly worked in Iraq & the pan-Arab region for the US government, in Afghanistan for NATO and in Somalia for the UN and the UK Foreign & Commonwealth Office in the fields of counter-terrorism, Preventing & Countering Violent Extremism (P/CVE) and Strategic Communication. He currently works for the UK Foreign, Commonwealth & Development Office as a consultant with a broad remit for countering the al-Qa'ida linked terror group, al- Shabaab.

He has published extensively on Somalia, contributing two articles to the UN's seminal study, 'War and Peace in Somalia: National Grievances, Local Conflicts & Al-Shabaab. He also contributed two chapters to COE DAT's 'Good Practices in Counter-terrorism' on 'Hard, Soft & Smart Power' and 'Negotiated Settlement in Counter-terrorism', and edited and illustrated COE DAT's recent 'Counter-Terrorism and Counter-Insurgency: A NATO COE DAT Research Project'. He also covers East African issues for The Economist Group and is a PhD candidate at the University of Strathclyde in Glasgow, writing under the topic, 'Creative Writing as a Treatment for PTSD'.

Mr. Alexander PALMER

Center for International Strategic Studies (CSIS), USA.

Alexander Palmer is a fellow in the Warfare, Irregular Threats, and Terrorism Program at the Center for Strategic and International Studies (CSIS). Before joining CSIS, he worked in Afghanistan, providing security analysis to humanitarian and UN personnel before and after the withdrawal of international military forces in August 2021. He holds a Master in Public Policy from the Harvard Kennedy School of Government. Palmer has authored the Global Terrorism Threat Assessment 2025, contributing to CSIS's analysis of global terrorist threats.

BG (Ret) Russell D. HOWARD

Howard Consulting Services, USA.

Brigadier General (retired) Russell Howard is a farmer in Minnesota and the President of Howard's Consulting Services. He is also a Distinguished Senior Fellow at the Joint Special Operations University. He currently consults for Audia Corporation in Washington, Pennsylvania and has served as an advisor to several organizations including Laser Shot, in Houston, Texas; Development Alternatives Incorporated in Bethesda, Maryland; and the Home Team Academy in Singapore. Previously BG Howard was the Director of the Jebsen Center for Counterterrorism studies at the Fletcher School in Medford, Massachusetts. BG Howard retired from the Army as Head of the Department of Social Sciences and the Founding Director of the Combating Terrorism Center at West Point. His previous positions include Deputy Department Head of the Department of Social Sciences, Army Chief of Staff Fellow at the Center for International Affairs at Harvard University, and Commander of the 1st Special Forces Group (Airborne) at Fort Lewis, Washington. Other past assignments include Assistant to the Special Representative to the Secretary General during UNOSOM II in Somalia, Deputy Chief of Staff for I Corps, and Chief of Staff and Deputy Commander for the Combined Joint Task Force Haiti / Haitian Advisory Group. Previously, General Howard was Commander of 3rd Battalion, 1st Special Warfare Training Group (Airborne) at Fort Bragg, North Carolina. He also served as the Administrative Assistant to Admiral Stansfield Turner and as a Special Assistant to General Max Thurman, the Commander of SOUTHCOM.

As a newly commissioned officer, General Howard served as an "A" Detachment Commander in the 7th Special Forces Group from 1970 to 1972. He left the active component and then served in the U. S. Army Reserve from 1972 to 1980. During this period, he served as an Overseas Manager, American International Underwriters, Melbourne, Australia, and China Tour Manager for Canadian Pacific Airlines. He was recalled to active duty in 1980, and served initially in Korea as an Infantry Company Commander. Subsequent assignments included Classified Project Officer, U.S. Army 1st Special Operations Command, at Fort Bragg, and Operations Officer and Company Commander, 1st Battalion, 1st Special Forces Group in Okinawa, Japan.

General Howard is the co-author/editor or seven counter-terrorism books. General Howard holds a Bachelor of Science degree in Industrial Management from San Jose State University, a Bachelor of Arts in Asian Studies from the University of Maryland, a Master of Arts degree in International Management from the Monterey Institute of International Studies, and a Masters of Public Administration degree from Harvard University. General Howard was a Senior Service College Fellow at the Fletcher School of Law and Diplomacy, Tufts University and a Senior Fellow at the Weatherhead Center for International Affairs at Harvard.

Dr. Andrea GILLI

University of St Andrews, UK.

Andrea Gilli is Lecturer in Strategic Studies at the University fo St Andrews, Associate Fellow of the Institute of European Policy-Making of Bocconi University, and Expert Mentor of NATO DIANA. Previously, Dr. Gilli worked in various capacities at the NATO Defense College, Harvard University, Stanford University, Columbia University, Johns Hopkins University, the European Union Institute for Security Studies, the Hague Center for Strategic Studies, the International Institute for Strategic Studies, the Italian Air Force, the Office of Net Assessment of the U.S. Department of Defense, and Leonardo, among others. Dr. Gilli holds a PhD from the European University Institute, and for his dissertation he won the 2015 Best thesis award from the European Defence Agency, an MSc from the London School of Economics and a BA from the University of Turin.

Mr. Jan HEINEMANN

International Kriegsspiel Society, Germany.

Jan Heinemann is a historian and wargaming practitioner with a wide ranging network in the professional wargaming communities. He's working with international partners, administrations, armed forces, civic organizations, and focusses on resilience, hybrid warfare, training critical skills and historic-political education. He is a guest lecturer at the German Command and Staff College and Board Director for Fight Club International, Coordinator for Fight Club Deutschland, member of the Connections

Online wargaming conference organizing staff, Admin Wargaming and Europe for the International Kriegsspiel Society.

Jessa MELLEA

Global Internet Forum to Counter Terrorism (GIFCT), USA.

Jessa Mellea is the Incident Response Associate at the Global Internet Forum to Counter Terrorism. She operates incident response protocols, conducts investigations, and produces intelligence reports for GIFCT member companies. Previously, she has worked as researcher on terrorism and violent extremism at Harvard University, George Washington University Program on Extremism, and the Center for Monitoring, Analysis, and Strategy.

Dr. Thomas W. SPAHR

US Army War College, USA.

Dr. Thomas W. Spahr is an Associate Professor at the U.S. Army War College. He served for 27 years in the U.S. Army before retiring in October, 2024. Dr. Spahr served his last four years as faculty at the U.S. Army War College and the final two as Chair of the Department of Military Strategy, Planning and Operations (DSMPO). Dr. Spahr holds an M.S. and a Ph.D. in History from The Ohio State University and an M.S.S. from the Army War College. His scholarship is focused on Intelligence and technology.

Mr. Sabri Anıl KAYA

Secretariat of Defence Industries- Presidency of the Republic of Türkiye.

Mr. Sabri Anıl Kaya is a Defence Industry Expert and Director of Operations Coordination at the Presidency of Defence Industries (SSB), where he has worked for over 11 years. In his current director role, he is responsible for Urgent Capability Acquisition and Rapid Adoption, leading lean-agile procurement for software-intensive platform development projects. He also oversees the development of advanced technologies like drones, autonomous robots and reconnaissance software systems. Previously, he served as a Technical Project Manager for aerospace projects such as F-35, A400M and Turkish Fighter Jet KAAN and began his career as a Diplomat with the Ministry of Foreign Affairs, coordinating secure IT system development.

Mr. Kaya holds a Master of Science in Programme and Project Management from the University of Warwick , a Master of Public Administration from Gazi University, and a Bachelor of Science in Computer Engineering from Başkent University. His expertise lies in complex Project Management and Agile Project Management.

Col. Özgür Ecevit TAŞCI

NATO Stability Policing COE, Italy.

Özgür Ecevit Taşcı is a Colonel of the Turkish Gendarmerie. He was born in 1974. He graduated from Maltepe Military High School in 1992 in İzmir and from the Turkish Military Academy in 1996 in Ankara. At the rank of lieutenant, he completed specialized training in infantry tactics, heavy weapons & ammunition, counterterrorism/commando operations and law enforcement at the Land Forces Infantry School (1996-1997) in İstanbul, Gendarmerie Commando School (1997) in İzmir and Gendarmerie Officers School (1997-1998) in Ankara respectively. He completed his master's degree in Social Anthropology program at İstanbul Yeditepe University in 2003 and attended the NATO Defense College Seniors Course in Rome, Italy in a sixth-month program in 2019. Colonel Taşcı served in different Gendarmerie units in Türkiye and NATO missions abroad between 1998-2024 as Gendarmerie Border Platoon Commander on the Turkish-Iraqi border line (1998-2000), Company Commander of Gendarmerie Special Public Order Training Company (2000-2001), Strategist at the Ministry of Interior Strategy Center (2003-2005), Çat-Erzurum District Gendarmerie Commander (2005-2007), Eyüp-İstanbul District Gendarmerie Commander (2007-2010), Head of Special Security Branch (2010-2012), Head of Operations and Training Branch in Mardin and Kastamonu Provinces (2012-2015), Gendarmerie Commando/Counter-Terrorism Regiment Commander (2016-2018) in Bingöl Province and Head of Gendarmerie Road Traffic Department at Gendarmerie HQ (2018-2024). He served as the Intelligence Plan Officer at the Turkish Battalion Task Force Command of NATO SFOR Operation for six months in Bosnia-Herzegovina (2003-2004) and as the Liaison and

Monitoring Team (LMT) Commander of NATO KFOR Operation for fifteen months in Kosovo (2015-2016). Colonel Taşcı is currently serving as the Deputy Director at the NATO Stability Policing Centre of Excellence (NSPCOE), in Vicenza, Italy.

Mr. Yaşar Başar AKSOKU

INTERPOL, France.

3rd Degree Police Superintendent Yasar Basar Aksoku is a Criminal Intelligence Officer at INTERPOL's Counter-Terrorism Department, with over 19 years of experience in international police cooperation and intelligence led counter-terrorism operations.

He has served in senior operational posts within the Turkish Police Intelligence Department, including overseas deployments with the OSCE Special Monitoring Mission to Ukraine. He completed long-term assignments in China, studying the Chinese policing system.

His work at INTERPOL focuses on advancing global counter-terrorism efforts through strategic intelligence sharing, biometric data integration, and operational support, helping to disrupt foreign terrorist fighters and transnational threats.

LtC. Pedro CAVALEIRO

NATO Strategic Direction - South Hub, Italy.

Lieutenant Colonel Pedro Cavaleiro is an officer in the Portuguese Army Infantry Branch and currently serves as Head of the Comprehensive Research and Analysis Section at the NATO Strategic Direction-South Hub, Allied Joint Force Command Naples, Italy. He holds a degree in Military Sciences from the Military Academy and a Master's degree in International Relations from the Faculty of Economics at the University of Coimbra. He is also a graduate of the Army Staff Course and the Joint Staff Course at the Military University Institute in Lisbon. With 30 years of active service, Lieutenant Colonel Cavaleiro has held a variety of command, staff, and teaching positions. Until 2023, he was an instructor for the Peace Operations and Humanitarian

Action Course and regularly collaborates with the University of Coimbra's Human Rights Centre on the Postgraduate Course in Armed Conflicts and Human Rights. Prior to his current position, he served as Commander of the 1st Mechanized Infantry Battalion, which was one of the combat units assigned to the Very High Readiness Joint Task Force 2022 Land Brigade. His operational experience includes deployments to Kosovo (2005) and Afghanistan (2010–2011), as well as advisory missions in Angola and Mozambique. He is married and has two daughters.

Prof. Uğur GÜNGÖR

Başkent University, Türkiye.

Prof. Uğur Güngör graduated from Kuleli Military High School in 1987 and the Turkish Military Academy in 1991. He completed his master's degree at the Department of Political Science and International Relations of Boğaziçi University in İstanbul and his Ph.D. degree from the Department of International Relations at Bilkent University in Ankara. As a Visiting Fellow, he pursued his post-doctoral studies on International Security and Terrorism at Princeton University in 2011-2012. Prof. Güngör, who had received the degree of Associate Professor in International Relations in 2014, was appointed as full Professor at Başkent University in 2019.

Prof. Güngör, who had served at various positions of the Turkish Armed Forces since 1991, worked as a lecturer of International Relations at the Turkish Military Academy between 1997-2005 and at the Azerbaijan Military Academy in 2000. He received training (Commanding and Headquarters Officer) at the Army War College in 2005-2006. Prof. Güngör, who had served as the International Relations Advisor to the Chief of General Staff between 2008-2011, the Chief of Staff of the NATO Centre of Excellence, Defense Against Terrorism in 2012-2014, and as the Military Advisor to the Commander of the Turkish Army in 2014-2015, also served as the Deputy Chief of Staff of Kabul Regional Command, as Chief of Liaison Officers and a Military Advisor at NATO ISAF Mission in Afghanistan between 2010-2011. He retired from the Turkish Armed Forces in 2015 at the rank of Senior Colonel.

He has been working as Prof. of International Relations, the Director of the School of Foreign Languages at Başkent University since 2015 and founder Director of Ankara Cervantes

Institute (Spanish Language School). He teaches at Başkent University, National Defense University, NATO School (Oberammergau), NATO Centre of Excellence Defense Against Terrorism (COE-DAT), Partnership for Peace Training Center and Anadolu Agency News Academy. He has also been lecturing on Conflict Management and Negotiation Techniques in Mediation Training for Lawyers since 2018.

He is the author of the book titled "Why States Contribute to Peace Operations" published in 2012, and numerous other national and international articles and book chapters in the field of International Security. Prof. Güngör, who is on the advisory and referee boards of many journals, was the chief editor of the Defense Against Terrorism Review (DATR) during the years of 2018-2024.

Mr. Mario Alberto ORTIZ BARRAGAN

Ministry of Defence of Colombia.

Mario Ortiz is an economist with a Master’s degree in Economics from Universidad de los Andes, Colombia. His academic background combines theoretical depth and quantitative rigor, with a strong focus on institutional analysis, public policy, and security. Throughout his career, he has led the design, evaluation, and monitoring of public policies across the sectors of national defense, citizen security, criminal justice, human rights, and mass transportation. His approach integrates statistical tools, econometric modelling, geospatial analysis, and microsimulation to support institutional design and strategic decision-making.

As Director of National Security at the Ministry of National Defense, he has overseen the formulation of sectoral policies aimed at safeguarding sovereignty, countering terrorism, and protecting critical infrastructure. His leadership has been instrumental in strengthening national resilience and coordinating institutional capabilities to address complex threats.

In the Human Rights Observatory of the National Police, he has contributed to strategic inputs for the Office of the Human Rights Commissioner, focusing on risk prevention for vulnerable communities. He has also participated in the design of institutional bulletins and research products that enhance analytical capacity in human rights. At the National Planning

Department, he coordinated technical teams in the development of drug policy, studies on deterrence through sentencing, and the characterization of individuals deprived of liberty in transitional detention centres. He led the creation of the Effective Access to Justice Index and designed systemic models to optimize the penitentiary system in collaboration with academic institutions. In the urban security sector, he developed the Comprehensive Security Strategy for Mass Transit Systems (EISSTP) for TRANSMILENIO S.A., structuring inter-agency coordination mechanisms, designing teams for civic engagement, and implementing monitoring indicators to prevent crime in high-density public spaces.

As Security Coordinator at Bogotá's District Secretariat for Security and Justice, he led econometric evaluations of policing services, spatial-temporal prioritization of patrol deployment, and geospatial analysis of urban conflict. He developed automated bulletins, statistical models, and impact evaluation documents, including studies on football-related crime and park safety in Bogotá.

His technical experience includes demographic microsimulation modelling, policy evaluation in public health and social security, client valuation in the financial sector, and comparative regulatory analysis of mobile payment systems in Latin America. He is proficient in R, SQL, PostGreSQL, and GIS, applying these tools in institutional, academic, and operational contexts. Mario Ortiz stands out for his ability to integrate technical analysis, institutional sensitivity, and strategic vision in high-complexity environments. His work has contributed to strengthening the articulation between public policy, empirical evidence, and international standards, with a focus on rights protection, institutional efficiency, and citizen security.

Maj. Adel SAOUD

Ministry of Defence of Tunisia.

He began a distinguished military career in the Tunisian National Army in September 2007. He graduated with honors from the military Academy in 2012 and holds a master's degree in Legal Sciences and Management, which enhances his expertise with a strong foundation in judicial principles and organizational management.

He served on the staff of the Land Army for five years and joined the Defense Intelligence and Security Agency in 2017. Major Saoud specialized in counter-extremism and terrorism. Following his successful completion of the staff course, he attained the rank of Major in 2024.

He has coordinated intelligence missions alongside multidisciplinary teams. His excellence in these areas has been recognized through multiple medals awarded for outstanding performance in leadership.

Major Saoud's strategic insight and analytical acumen have consistently contributed to the effective planning and execution of various intelligence missions, furthering the agency's objectives with distinction.

Additionally, he has extensive experience in strategic planning in the field of countering violent extremism and terrorism, as well as in evaluating the sectoral action plans of the Ministry of National Defense.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
Centre of Excellence Defence Against Terrorism
Terrorism Experts Conference & Defence Against Terrorism Seminar (Executive Level)
UNITED AGAINST TERRORISM: SECURING THE FUTURE
15 - 16 October 2025
Ankara, Türkiye
Col. Pinar ALPER
Col. Ahmet EROL

TERRORISM EXPERTS CONFERENCE 2025

ACKNOWLEDGEMENTS

Col. Ahmet EROL[*]

Centre of Excellence Defence Against Terrorism (COE-DAT) successfully hosted the "**Terrorism Experts Conference and Defence Against Terrorism Executive Level Seminar"**, which is the center's flagship event and part of its 2025 Programme of Work, on October 15-16, 2025, in Ankara, Türkiye. The event brought together 18 speakers from 10 countries and 117 participants from 35 countries. Additionally, the Secretariat of Defence Industries organized an exhibition during the conference to present the products and capabilities of Türkiye's defence industry companies. First and foremost, the accurate identification of the main theme of the activity to be conducted, with the careful selection of relevant sub-themes and topics addressing the future trends in Counter Terrorism (CT), has increased interest in the activity. This diamond event has successfully clarified the challenges that will arise in the future, established a common understanding on the measures to be taken in the fight against terrorism and informed participants through both expert presentations and substantive contributions from attendees. The process was managed correctly and effectively, with comprehensive and detailed promotional activities for the conference commencing sufficiently in advance. The support provided by the Directorate and Senior National Representatives (SNRs), demonstrating their belief in the activity, is commendable.

This conference clearly demonstrated the importance of COE-DAT's role in the fight against Terrorism, the support it provides in achieving NATO's objectives in CT related topics and the commitment of COE-DAT and all its personnel to its mission. COE-DAT will continue to adhere to NATO's values and principles in CT related issues, as it has done in the past, and will continue to carry out its counterterrorism tasks with efficiency and determination. I am honored to be a member of such a dedicated and exceptional team that contributed to the successful implementation of this activity from the planning and preparation stage onwards. The positive feedback we received from the speakers and participants further reinforced our satisfaction and pride. I would like to extend my special thanks to certain individuals, particularly my team, for their contributions to the preparation and organization of the event.

I would like to begin by expressing my deepest gratitude to Colonel Halil Sıddık AYHAN, Director of COE-DAT, for his exemplary leadership, unwavering support and the trust he has placed in me and my team. He has made a significant contribution to the success of the activity by sharing valuable information and insights with us at every stage. We had the opportunity to consult with him on every issue right up to the very end of the activity and he supported us in making the right decisions.

I would also like to express my gratitude to COE-DAT Deputy Director Colonel John CHRISTIANSON and all our SNRs for their continued commitment, contributions to the activity, and kind understanding. They provided consistent support throughout the project, offering valuable insights and contributing to its success.

And especially, to my colleagues who have been by my side since the very beginning of the activity, who ensured that the right decisions were made and successfully implemented, and who spared no effort in supporting the successful execution of the conference; first and foremost, my team members Col. Pınar ALPER, Ms. Demet UZUNOĞLU, 2nd Lt. Utku Cem

[*] TÜR A, Chief of Staff at the Centre of Excellence Defence Against Terrorism (COE-DAT)

TATAR, 3rd Lt. Kaan KARAKURUM and who provided their generous support for the conference to be held in the most successful manner possible; our valuable Academic Advisor, Dr. Zeynep SÜTALAN, who, with her knowledge and experience in the field of counter-terrorism, provided support in many areas, including the preparation of the programme, the selection of speakers and the moderation of the activity; and the CIS Branch personnel, MSGT. Fikret ÖZDEMİR and Mrs. Selvi KAHRAMAN, who ensured the technical aspects ran smoothly; Col. Yaşar LAFÇI and his valuable team members, who demonstrate full competence in logistics matters, including transportation, accommodation, and catering; our rapporteurs Ms. Elif Merve DUMANKAYA and Ms. Yağmur AŞIK, who deserve recognition for their support and meticulous work in compiling up the discussions; and the COE-DAT personnel, whose names I cannot mention individually, but who contributed to the success of the conference and kept smiling throughout the event.

To Mr. Thomas GOFFUS, NATO Assistant Secretary General for Operations and NATO Secretary General's Special Coordinator for Counter-Terrorism, I extend my sincere thanks and gratitude for presenting the main theme of the conference and NATO's approach and efforts in combating terrorism and for setting the stage for discussions with his opening speech, thereby adding value to our conference. I would also like to thank Mr. Leonardo SCANAVINO and all the staff who contributed to the successful execution of the process, from inviting him to participating.

Finally, I would like to extend my special thanks to the distinguished speakers and participants of the conference, each of whom are distinguished and effective academics and experts in their respective fields, for their valuable opinions, the important information they shared, and their contributions to the productive discussions.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
"United Against Terrorism: Securing the Future"

INTRODUCTION

Dr. Zeynep SÜTALAN[*]

COE-DAT conducted Terrorism Experts Conference together with the Defence Against Terrorism Executive Level Seminar as a combined event on 15-16 October 2025 in Ankara/Türkiye with the participation of 18 speakers from 10 countries and 117 attendees from 35 countries. Terrorism remains a persistent and adaptive challenge to Allied security, shaped by rapid technological innovation, geopolitical competition, and the emergence of multi-domain vulnerabilities. As the discussions throughout the conference made clear, terrorist actors are learning from ongoing conflicts, exploiting commercial and dual-use technologies, and seeking to undermine social cohesion and political stability across the Euro-Atlantic area. These developments reinforce the continued relevance of counterterrorism within NATO's overarching 360-degree approach to deterrence and defence.

Across two days of dialogue, six panels brought together practitioners, military leaders, law enforcement professionals, researchers, and international partners to assess how the terrorist threat is evolving and what this means for NATO's future posture. The conference opened with a horizon-scanning perspective, charting the shifts in terrorist means and methods, from increased decentralization and low-tech high-impact attacks to cyber-enabled capabilities and adaptations inspired by the Russia–Ukraine war. Discussions on the Sahel as the epicentre of contemporary terrorism illustrated how terrorism in fragile regions can generate spillover effects that directly affect the Euro-Atlantic security environment, highlighting the need for sustained cooperation with regional actors.

Subsequent panels examined the conceptual and operational frameworks shaping Allied counterterrorism efforts. Speakers underlined that modern terrorism increasingly blurs the boundaries between counter-terrorism, counterinsurgency, and hybrid threats, demanding integrated approaches that combine military effects, political engagement, and influence activities. The experiences discussed highlighted that winning and maintaining the support of local populations, countering hostile information activities, and aligning security measures with political objectives are critical to achieving long-term stability. The exploration of Multi-Domain Operations (MDO) further demonstrated that counterterrorism in the coming years will require synchronizing efforts across land, air, maritime, space, cyber, and information domains. Therefore, MDO has the potential to enhance NATO's counter-terrorism efforts through strengthening early warning, improving decision-making, and enabling more integrated and precise efforts. Wargaming, as emphasized by several contributors, will play a critical role in enhancing preparedness, testing assumptions, and building resilience across the Alliance.

The second day highlighted the technological and cooperative dimensions of counterterrorism, from AI-enabled detection systems and digital interventions to the integration of biometrics and battlefield evidence across agencies and borders. Discussions underscored that while technology offers significant opportunities, its operational value depends on shared standards, responsible governance, and the ability of institutions to collaborate effectively. As Allies incorporate new and emerging technologies into their security architectures, issues of legality, ethics, governance and interoperability will remain central. Effective cooperation between military, law enforcement, intelligence communities, industry, and international organizations is essential to translate data into actionable intelligence, and ultimately, into accountability. The experiences shared by NATO members and partners reinforced a key lesson: terrorism manifests differently across regions, but the core requirements for effective

[*] Independent Researcher

counterterrorism are universal including the unity of effort, interoperability, the importance of cutting financial and logistical networks of terrorists and the imperative of ensuring that military action is integrated with political engagement, institution building and societal resilience.

Taken together, the insights from the conference signal a decisive shift in the nature of the terrorist threat and in the tools required to counter it. The theme of this year's conference, *United Against Terrorism: Securing the Future,* is not only aspirational, but also reflects a strategic necessity. In an era where threats cross borders, domains, and digital ecosystems at unprecedented speed, unity of effort, shared understanding and adaptive thinking are the only reliable foundations for security. Therefore, the insights from the conference point toward a future where counter-terrorism must be increasingly multi-domain, technologically enabled, and grounded in close cooperation among Allies, partners, and relevant civilian actors.

Against this background, this report is composed of the contributions of the distinguished speakers as well as the key findings and recommendations emerging from the discussions throughout the panels, identifying the most pressing trends, operational challenges, and strategic implications. By this way, the report intends to support the Alliance's ongoing efforts to mitigate terrorist threats, and secure a safer future for Allied and Partner populations.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
"United Against Terrorism: Securing the Future"

Opening Remarks

Generals,

Distinguished lecturers and participants,

As the Director of COE-DAT, it is a distinct honor to welcome you all to this year’s Combined “Terrorism Expert Conference & Defence Against Terrorism – Executive Level Seminar 2025”, conducted under the central theme: “*UNITED AGAINST TERRORISM: SECURING THE FUTURE*”.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO
OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE &
EXECUTIVE LEVEL
DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: Securing the Future"
Col. Halil Sıddık Ayhan

This theme reflects a crucial reality: unfortunately, terrorism continues to evolve, crossing borders and exploiting vulnerabilities in our interconnected world. No single nation or institution can address this challenge in isolation. Only through unity — of purpose, of vision and of action — can we build a future free from terrorism.

For those who are just getting to know our Centre of Excellence, allow me first to provide you a brief introduction of the center. The Center of Excellence Defence Against Terrorism (COE-DAT), established in Ankara in 2005, serves as NATO’s hub of expertise on Counter-Terrorism. Its mission is to support the Alliance and partner nations by providing education, training and academic research on the evolving nature of terrorism and methods to confront it. By organizing workshops, courses and seminars, COE-DAT helps military and civilian leaders strengthen their ability to anticipate, prevent and respond to terrorist threats in all domains.

In addition, COE-DAT plays a vital role in fostering international cooperation. It brings together experts from NATO member states, partner nations, academia and international organizations, creating a platform where diverse perspectives converge into common strategies. Through this collaborative approach, COE-DAT contributes directly to NATO’s core tasks of “deterrence and defense, crisis prevention and management and cooperative security” — ensuring that the fight against terrorism remains both united and forward-looking.

In this context, this conference is a practical manifestation of that effort. Over the next few days, our collective focus will be on sharing knowledge, exchanging perspectives, and identifying practical solutions. Terrorism today stands as one of the greatest threats to humanity, a phenomenon that disregards ethical norms, human rights, and international law. If left unchallenged and not confronted together, it risks the safety and well-being of our citizens, the security and stability of our nations and an erosion of the international order, opening the door to anarchy and destruction. This gathering, therefore, is more than a platform for dialogue; it is a living testament to our collective determination to protect our citizens, safeguard our values, and uphold international security.

In this spirit, the Center of Excellence Defence Against Terrorism remains committed to supporting NATO and its partners by fostering collaboration, driving innovation and enhancing resilience against evolving terrorist threats. Our task is clear: to transform shared expertise into actionable strategies that will strengthen deterrence, prevention and response.

As we embark on these discussions, let us remember that the strength of this community lies in its diversity and its solidarity. together, we can transform our shared vision into meaningful progress.

Allow me to express my sincere gratitude to our distinguished speakers, participants and partners for their commitment to this cause. Your presence here demonstrates a powerful truth — that when united, we can indeed secure the future against terrorism.

Let us move forward with confidence and determination. Thank you very much.

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

DAY I

Keynote Speech

Mr. Thomas GOFFUS

NATO Assistant Secretary General for Operations and NATO Secretary General’s Special Coordinator for Counter-Terrorism.

Excellencies, Ladies and Gentlemen, I am Tom Goffus, the NATO Secretary General’s Special Coordinator for Counter-Terrorism and Assistant Secretary General for Operations at NATO Headquarters in Brussels.

It is therefore a great honour for me to be able to join you, albeit virtually, to share some ideas and views.

Let me start by expressing my gratitude for your participation in this important event.

I know there are a lot / a lot / of Counter-Terrorism conferences, and you need to pick ones that add value to your efforts.

So I value your time and your dedication to making our people safer from the threat of terrorism.

Up front / my mandate / and the mandate of the NATO CT staff / in its entirety / is to try to facilitate a more coherent and more effective Alliance response to terrorism.

First the state of play of NATO Counter-Terrorism at NATO.

In 2024, for the first time since they were adopted in 2012, NATO’s Policy Guidelines on Counter-Terrorism were revised and adapted to the evolving threat landscape.

We tried to reflect the most recent technological trends.

Terrorists have money and are continually evolving their Tactics, Techniques, and Procedures.

Building on NATO’s new policy, we updated the Counter-Terrorism Action Plan in 2024.

We intended to clarify a clear set of actions to be taken to further NATO’s role in counter-terrorism.

Both documents stress the importance for NATO to adapt to the threat.

Terrorists and terrorism are a thinking beast.

Both Russian and Terrorist ambitions, drive the role of new technologies to the forefront of NATO's ability to fight.

NATO will integrate emerging and disruptive technologies into the counter-terrorism effort.

For example, on the battlefield in Ukraine, counter drone has superseded counter IED in prominence.

Roughly 80% of battlefield casualties are now from drones. And terrorism is fully online.

It's how they get money, it's how they get followers, it is how they influence.

I asked a senior military leader from North Africa whether Terrorists are using Organized Crime to forward their objectives, or Organized criminals are using terrorism. He said yes.

And disturbingly, he said that kids in North Africa now aspire to be terrorists.

Because they want money, power and prestige.

And in North Africa, that means becoming a terrorist.

A sad, harsh reality we must face, and if possible, alter.

When I grew up, I wanted to be an astronaut and, on the side, I would play professional baseball for the Pittsburgh Pirates.

Neither of those worked out, but think on that problem set, kids wanting to grow up to be terrorists.

The threat is real, it is persistent, and it affects all of us.

At NATO, our key counterterrorism effort / other than shared situational awareness and developing Allied CT capabilities / is cooperation with our partners especially on capacity building.

While there has been a shift from prioritizing countering violent extremism and countering terrorism to the preparation for inter-state conflict, working with partners to enhance capabilities remains a NATO priority.

We strive to build relationships with partner countries and other entities such as the academia and other international organisations to/ as I said / facilitate a more coherent and more effective Alliance response to terrorism counter-terrorism.

The center of gravity of terrorism is shifting south and west to the African continent.

All that means we remain focused on NATO's Southern Neighbourhood.

Every border that is secured in the Southern Neighbourhood, makes our partners more secure, and the Euro-Atlantic more secure.

NATO also seeks engagement with other international organizations and international actors including the United Nations and the European Union.

Multilateral international cooperation and coordination avoids duplication and enhances our collective effort.

NATO strives to further increase exchange of knowledge and best practices with Allies and partners on counter-terrorism, both formal and informal.

This conference is a fantastic opportunity to do just that.

We foster cooperation between NATO and partners through tailored capacity-building activities, the invitation of our partners to activities such as this one, and bilateral engagements.

We will continue to encourage cooperation through training, activities at our Centres of Excellence, and diverse programmes in support of partners led by our military colleagues.

Partners can provide unique insights into the international fight against terrorism as my discussion of young North Africans want to grow up to be terrorists, rather than football players, engineers, or architects.

NATO will remain seized of this cultural trend as well as the proclivity of terrorists towards tech exploitation such as drone and internet warfare.

As a senior representative of NATO, I thank our partners for trusting us and allowing us to build a relationship that can help develop critical capabilities to support the global fight against terrorism.

Let me thank the Defence Against Terrorism Centre of Excellence.

Their work on counter-terrorism helps consolidate and share knowledge, awareness and analysis of terrorism and counter-terrorism capabilities.

We will use this platform to exchange views, knowledge, best practices, and learn from one another.

Finally, once again, I would also once again like to express my gratitude to this conference's participants for their engagement in such an important and beneficial event.

Thank you and I wish you all an excellent Conference.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: Securing the Future"
DAY 1 Wrap-Up

Panel 1: Horizon Scanning the Terrorist Threat: Understanding Trends in Terrorist Means, Methods and Capabilities

Evolving Tactics, Persistent Threat: Analyzing Latest Trends in Terrorist Modus Operandi for Future Projection

Prof. Mitat ÇELIKPALA,

Vice Rector, Kadir Has University.

The modus operandi (MO) of terrorist operations is predominantly characterized by the application of physical violence, which has become emblematic of their activities. This emphasis on violence has prompted extensive analyses by researchers, policymakers, and security experts regarding the diverse attack methodologies utilized by terrorist organizations. These methodologies encompass a wide range of tactics, including but not limited to kidnappings, shootings, hijackings, hostage crises, lone-wolf attacks, suicide bombings, and the deployment of both conventional explosives, such as dynamite, and unconventional explosives, notably improvised explosive devices (IEDs), which are frequently homemade and readily concealable.

In recent years, the evolution of the terrorism landscape has been significantly influenced by the emergence of new concepts and strategies. A notable development is the exploitation of dual-use technologies that serve civilian and military purposes, which has increasingly characterized terrorist tactics. Furthermore, the utilization of vehicles in the execution of attacks, commonly referred to as vehicular terrorism, represents a disturbing trend in operational strategies. Incidents involving cars and trucks are becoming more frequently reported across diverse geographic locations.

The rise of disinformation campaigns also serves as a crucial instrument for terrorists, who effectively leverage social media and other digital platforms to disseminate propaganda and facilitate recruitment efforts.

In addition, the domain of hybrid warfare and the misuse of Emerging and Disruptive Technologies (EDTs) have garnered significant scholarly and operational focus in the context of terrorism. The rapid advancement of technology presents an evolving challenge for states and societies, as such technologies can be readily accessed and misappropriated by terrorist entities. EDTs, including artificial intelligence (AI), quantum computing, biotechnology, nanotechnology, cyber technology, robotics, unmanned systems (inclusive of drones), blockchain, cloud computing, and the Internet of Things (IoT), create unprecedented avenues for terrorists to augment the scale and impact of their malevolent activities. For instance, AI may be employed to engineer more sophisticated cyberattacks, while drones can be used for reconnaissance or the delivery of explosives, thereby broadening the spectrum of potential threats.

Consequently, terrorist tactics are evolving, responding dynamically to shifts in politics, technological advancements, and operational constraints. Recent empirical reports indicate a concerning trend toward increased lethality per attack, with numerous incidents resulting in higher casualty figures. Moreover, there is a marked rise in the utilization of uncrewed systems and cyber-enabled capabilities by terrorist actors. This trend toward decentralization is further reflected in the increase of lone-actor and low-tech attacks, as well as shifts in terrorist financing and logistical networks that challenge conventional counter-terrorism measures.

Global metrics indicate that, although the overall number of terrorist incidents has diminished in specific locales, the average lethality of these attacks has escalated. Casualties tend to be concentrated in high-conflict zones and during conspicuous events, as evidenced by findings from the Global Terrorism Index (GTI) 2024. This significant report, alongside related analyses, underscores the growing lethality of terrorist attacks and their concentration in regions presently experiencing active conflict.

Regional law enforcement reporting in Europe reveals a limited number of high-impact incidents but also underscores the persistent threats posed by a diverse array of ideologies, including religious extremism, right-wing extremism, and activities perpetrated by lone individuals. Europol’s Terrorism Situation and Trend Report (TE-SAT) documents the operational variety employed by terrorists, highlighting the adaptive utilization of rudimentary weapons and vehicles, as well as efforts to gain access to more sophisticated capabilities.

Furthermore, analyses conducted by the United Nations and US intelligence agencies emphasize the increasing salience of the digital domain in the operational framework of terrorism. This domain encompasses recruiting new members, command and control over operations, virtual training platforms, fundraising endeavors, and sharing tactical methodologies across disparate conflict zones. In an era of digital connectivity, the capacity to exploit the internet for these purposes has fundamentally transformed the traditional landscape of terrorism.

Finally, investigations into counter-terrorism finance reveal the shifting paradigms of terrorist funding. There is a notable upsurge in the use of informal value transfer systems, such as *hawala*, and digital assets, which enable terrorists to obfuscate their financial transactions and resource procurement. This evolving complexity in financing mechanisms presents novel challenges for governments and organizations striving to mitigate the threat of terrorism.

Key Evolving Tactics in Modern Operations

Under current circumstances, it has become more challenging than ever to protect, prevent, mitigate, and defend against the use of these technologies by terrorist entities. The rapid convergence of civilian and military technological innovations introduces new dynamics into modern conflicts. Technologies once exclusive to states, such as unmanned systems, AI-driven targeting, or quantum encryption, are now more commercialized and accessible to non-state actors, enabling them to conduct asymmetric warfare that transcends conventional battlefields.

The growing role of the private sector in producing these novel technologies and their dual use adds further complexity to counterterrorism efforts. This situation is compounded by geopolitical competition among major powers, increasing the risk of EDTs being misused by terrorists and necessitating stricter counterterrorism policies, practices, procedures, and measures.

In the defense realm, there has been a clear shift towards a non-linear approach that integrates five operational domains: land, air, sea, cyber, and space. Based on this reality, organizations such as NATO, the EU, the UN, and the OSCE have adopted a multi-domain approach to tackle the asymmetric threat posed by terrorism.

As different EDT components are integrated, an EDT- enabled terror attack could trigger a domino effect in other areas, leading to substantial damage in both physical and virtual domains. For instance, a serious cyber-attack on critical infrastructure could impose extremely high costs on the security and prosperity of states and societies.

All competent authorities and institutions should continue to develop adaptable and integrated structures and procedures for preventing, mitigating, deterring, defending against, and combating EDT-enabled terrorism.

Proliferation of Small Uncrewed Aerial Systems (UAS) and Remote Effects

In recent years, terrorist and insurgent organizations have increasingly integrated small, commercially available drones, known as uncrewed aerial systems (UAS), into their operational frameworks. These UAS perform multiple roles, including intelligence, surveillance, and reconnaissance missions, as well as the capacity to deliver small-scale strikes employing explosive or incendiary devices. Incorporating UAS into their tactical repertoire is a significant force multiplier, empowering these groups to execute coordinated attacks with enhanced efficiency and effectiveness. The lowered operational threshold for conducting standoff attacks poses substantial challenges to the perimeter defense strategies of larger organizations. Drones can engage numerous targets from considerable distances, complicating the threat landscape for conventional defense mechanisms. Recent intelligence assessments indicate that UAS are not solely utilized in high-intensity conflict zones, such as those in the Middle East, but are also deployed in localized attacks, highlighting their versatile application across a broad spectrum of combat scenarios characterized by varying intensity levels.

Integration of Cyber and Information Operations

The contemporary operational environment has witnessed a sophisticated convergence of cyber capabilities and information warfare tactics, enabling various non-state actors to significantly bolster their operational effectiveness. These groups leverage cyber intrusions for comprehensive reconnaissance, identifying potential soft targets for attacks while utilizing multiple online platforms to facilitate fundraising initiatives. By employing encrypted communications, they can effectively manage logistics and coordinate resources and personnel without detection. The amalgamation of information operations amplifies the psychological impact of their campaigns, thereby supporting recruitment efforts and the dissemination of ideological narratives while fostering a digital environment saturated with disinformation. Evaluations from the United Nations and national intelligence agencies underscore the alarming trend of online ecosystems acting as accelerators for the proliferation of extremist ideologies, thereby enabling decentralized coordination among operatives. This decentralization complicates traditional methods of tracking and countering such movements, thereby prolonging the challenges law enforcement and intelligence agencies face.

Decentralized, Low-Sophistication but High-Lethality Attacks

A notable trend in contemporary conflicts has emerged towards “low-tech, high-impact” attacks characterized by decentralized execution and straightforward implementation. These attacks frequently employ standard methods such as vehicle ramming, stabbings, arson, and small-arms shootings, often executed by lone actors or small cells that may lack formal affiliations with larger organizations. Although individual attacks may not exhibit the complexity associated with larger, orchestrated strikes, the cumulative impact of multiple incidents can result in mass casualties and significant loss of life. Recent reports indicate that these actors utilize diverse uncomplicated tactics that exploit vulnerabilities in target-rich environments, making them difficult for law enforcement and intelligence agencies to anticipate. Furthermore, their ability to exploit spontaneous opportunities adds additional complexity, complicating pre-emptive measures to mitigate the risk of such attacks.

Adaptive Logistics and Financing

The financial landscape that supports terrorist and insurgent groups has undergone significant evolution in recent years. Once predominantly characterized by large-scale state sponsorship, traditional funding models have increasingly diverged to include hybrid financial strategies. These strategies encompass tapping into local criminal economies, receiving financial remittances from diaspora communities, and utilizing informal financial systems that circumvent conventional banking channels. A noteworthy trend is the growing adoption of digital assets and cryptocurrencies; however, the prevalence of this practice varies among different groups. Financial intelligence agencies have expressed concern regarding the increasingly opaque and diversified nature of terrorist financing, which complicates efforts to track and mitigate these funding sources. This evolution in financing mechanisms complicates counter-terrorism initiatives and underscores the adaptive strategies employed by these organizations to secure resources.

Persistence of Insider and Hybrid Threat Vectors

The risk posed by insiders, individuals who facilitate attacks through coercion, infiltration, or the exploitation of grievances within organizational structures, remains a significant concern, especially in contexts involving critical infrastructure and vulnerable targets, such as public venues. Emerging tactics increasingly combine cyber intrusions with physical attacks, leveraging compromised access credentials to heighten the risk of significant security breaches. Intelligence assessments have underscored the severity of this persistent threat, emphasizing the necessity for enhanced vigilance and proactive measures to address potential insider threats effectively. Continued attention to these evolving tactics is essential for safeguarding national and public security.

Near-Term Projections

Normalization of Affordable Remote Strike Options: Over the next few years, we can expect a substantial increase in the deployment of UAS for strike operations across various conflict zones. This trend will likely coincide with an intensifying arms race focused on developing countermeasures and advanced anti-drone technologies. Non-state actors, including insurgent groups and terrorist organizations, are anticipated to increasingly exploit commercially available drones and UAV technology to enhance their operational capabilities. These developments raise critical questions regarding regulation and governance, particularly as traditional military frameworks struggle to adapt to the realities of decentralized warfare.

Hybridization of Cyber-Physical Attacks**:** The convergence of cyber capabilities with conventional military operations is projected to undergo significant advancements, facilitating the execution of physical attacks and bolstering the strategic planning that underpins these operations. Cyber tools will play a pivotal role in enabling precise target identification, data aggregation, and network infiltration, thereby equipping attackers to circumvent traditional defenses. Additionally, information warfare will be intricately linked to these physical assaults, utilizing tactics that amalgamate disinformation, psychological operations, and social media campaigns to maximize disruption and instil fear within both populations and target states. This hybrid methodology complicates defensive strategies, necessitating a comprehensive reconsideration of countermeasures.

Continued Decentralization and Tactical Copy-Catting: The rapid proliferation of effective tactics across diverse regions will sustain its significance as a critical trend, with guerrilla warfare strategies—including the repurposing of vehicles as weapons and the construction of simple, cost-effective IEDs—becoming increasingly prevalent. Technologies such as small drones, previously exclusive to state militaries, will become increasingly accessible to non-state actors. These tactics will likely disseminate rapidly through online forums, social media, and encrypted communications, creating a decentralized knowledge network of operational methodologies that various groups can readily adapt and replicate. This phenomenon will contribute to a more chaotic battlefield environment, characterized by the rapid proliferation and evolution of asymmetric threats.

Growing Financing Opacity: The financial ecosystem supporting non-state actors is anticipated to evolve in a manner that renders it increasingly opaque, as informal value chains and privacy-preserving cryptocurrencies gain prominence. These financial mechanisms facilitate greater anonymity and can obfuscate the flow of funds, thereby complicating counter-terrorism financing efforts. Although regulatory bodies and anti-money laundering initiatives may achieve some success in mitigating specific channels of financial support, trends indicate a significant increase in opacity that will present considerable challenges to law enforcement and intelligence agencies tasked with tracing illicit financing. This evolving landscape underscores an urgent need for innovative financial tracking methodologies and enhanced international cooperation to address these challenges effectively.

Policy and Operational Recommendations

Layered Counter-UAS and Perimeter Strategies: It is imperative to formulate comprehensive strategies integrating advanced technological measures for detecting, attributing, and mitigating threats associated with UAS. This multifaceted approach should prioritize the rapid and flexible deployment of scalable sensor networks tailored to diverse environmental contexts, encompassing both urban and rural settings. Additionally, establishing clear legal frameworks defining the rules of engagement for interception and mitigation is critical to ensure compliance with national and international legal standards while safeguarding civilian populations and critical infrastructures, including power generation facilities, transportation systems, and large public gatherings.

Integrated Cyber-Physical Threat Fusion Centres*:* Establishing dedicated centers that unite cyber and intelligence experts with tactical law enforcement units is essential for facilitating real-time identification of pre-emptive indicators of threats. These centers should primarily focus on correlating online behavioral patterns, such as planning and coordination on social media platforms, with physical reconnaissance activities. Investments in developing robust analytic pipelines that leverage an extensive range of intelligence sources—including open-source intelligence, signals intelligence, and financial transaction records—are pivotal in enhancing situational awareness and response capabilities.

Community Resilience and Soft-Target Hardening: In light of the enduring threat posed by low-technology attacks, it is crucial to prioritize the implementation of effective and economically viable strategies that enhance security for soft targets, which include public spaces, educational institutions, and commercial districts. Such a strategy may encompass architectural modifications to restrict access points, traffic management protocols to improve crowd control, and ongoing public awareness campaigns to educate communities on recognizing and reporting suspicious activities. Moreover, empowering local stakeholders through the establishment of direct reporting channels to law enforcement, along with fostering community engagement in resilience-building initiatives, is essential.

Financial Transparency: There is an urgent need to enhance the oversight of informal financial networks and services, which, while protecting user privacy, also harbor the potential for misuse. This enhancement entails refining monitoring mechanisms to avert illicit financial flows, including money laundering and terrorist financing. Cooperation with international partners is vital to constructing comprehensive frameworks designed to close off safe havens for illegal financial activities, thereby promoting transparency in financial transactions and reinforcing the overall integrity of the economic system.

Responsible Information-Space Interventions: Formulating targeted strategies that encompass counter-messaging initiatives, establishing effective content takedown protocols for harmful online materials, and developing digital literacy programs to inform citizens about the perils of misinformation and online radicalization are essential. Such interventions are designed to mitigate the swift dissemination of extremist ideologies and recruitment tactics through digital platforms, fostering a more informed and resilient digital populace capable of critically assessing online content.

Conclusions

The modus operandi of terrorism is increasingly recognized as heterogeneous, demonstrating a shift away from a uniformly high-tech paradigm. This diversity indicates a pragmatic amalgamation of low-cost, low-skill methodologies alongside a selective incorporation of advanced technologies, including drones, cyber capabilities, and encrypted communication networks. These technological instruments serve not merely as enhancements but as potent catalysts that significantly amplify the overall impact of terrorist activities. Therefore, effective counter-terrorism strategies require robust cross-domain integration, encompassing cyber, financial, and kinetic domains. This multidimensional approach enables the rapid deployment of scalable technical defenses pertinent to emerging threats, such as drone strikes and hybrid cyber-physical attacks.

Furthermore, it underscores the necessity for strong international collaboration aimed at disrupting funding avenues and impeding the diffusion of innovative tactics among terrorist networks. Continuous monitoring and appraisal of these evolving trends are imperative, leveraging the latest intelligence and insights from public reporting sources, such as the Global Terrorism Index (GTI), the United Nations Office of Counter-Terrorism (UNOCT), Europol, and various national assessments. This vigilance is crucial for maintaining a proactive posture toward potential threats.

To effectively dissect the latest trends in terrorist tactics, it is essential to transcend a mere focus on technical attributes and delve into the underlying strategies, which can be categorized into coercive, manipulative, and persuasive dimensions. The coercive aspect is characterized by actions based on “the power to hurt,” evident in overtly violent tactics like bombings, shootings, and other forms of physical aggression that instil fear and serve political purposes. Conversely, manipulative tactics exploit “the power to deceive,” employing psychological strategies designed to shape beliefs, alter perceptions, and construct narratives that advance the terrorist agenda. Finally, the persuasive dimension relies on "the power to convince," utilizing ostensibly positive or appealing strategies—such as community engagement or humanitarian assistance—to garner support and legitimacy.

We need a holistic approach to terrorism analysis, proposing the integration of the three modes of influence—coercion, manipulation, and persuasion—within four analytical categories: physical/material, symbolic, institutional, and strategic. This comprehensive framework fosters an enriched understanding of the dynamic and evolving nature of terrorism. It emphasizes the significance of considering a coordinated system of actors and their interactions, rather than confining the analysis to the activities of a single non-state entity.

The evolving nature of warfare elucidates that workforce and traditional military hardware are no longer the exclusive instruments available to non-state actors or terrorist organizations seeking to exert influence. These groups increasingly adopt tactics beyond mere violence, engaging in disinformation campaigns, manipulating educational content, fostering relationships with diaspora communities, and making strategic investments—all within a framework that permits them to operate beneath legal thresholds. Such methodologies obfuscate the attribution of their actions and conceal their true intentions. This nuanced perspective on hybrid threats suggests that both state and non-state actors can exploit systemic vulnerabilities within societies, employing a diverse range of conventional and unconventional tactics to achieve their strategic objectives.

To effectively assess and counteract the nascent tactics of terrorist organizations, it is essential to dismantle the barriers that artificially separate nonviolent activities from those that are violent. A holistic analysis of these organizations must account for their ideological underpinnings, strategic aims, and overarching modus operandi, rather than limiting the evaluation to their use of coercive or illegal tactics. This comprehensive understanding is critical for formulating effective countermeasures and anticipating future threats.

The Impact of The Technologies Used in Russia-Ukraine War on Terrorist Capabilities

Dr. Christina SCHORI LIANG, Head of Counterterrorism and Preventing Violent Extremism at the Geneva Centre for Security Policy in Geneva.

Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: ...ing the Future"
CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO
OTAN
COE-DAT

Introduction

Throughout modern history, certain acts of terrorism have dramatically reshaped the way we understand this phenomenon. 9/11 was such an event. The 26/11 attacks in Mumbai were another. The Russia–Ukraine war is similarly reshaping global security thinking. Increasingly, terrorism is no longer a local issue; it is global. 9/11 is a clear example of how globalized terrorism has become. The terrorist operation was designed in Malaysia, supervised from Afghanistan, planned in Germany, rehearsed in Spain, and ultimately executed in the United States in three different locations.

Terrorists are not passive observers. They are increasingly learning, studying and monitoring everything that we do in the CT space. When we look at 26/11 in 2008, Mumbai was another watershed moment for terrorism. It was the first time that we saw a new model of terror, where you had 10 people literally hijacking a city of 19 million people for 60 hours. This is the first time where terrorists were using GPS, they were using lives, and handlers, and they were literally paralyzing a city.

The Russia–Ukraine War: A New Kind of Conflict

The war that we see in Russia and Ukraine is a completely different war. If you look at it from many different aspects, you will see that it is the first commercial space war, the first full-scale drone war, the first 3D-printing war, the first AI war, and perhaps the first LAWS war.

The Russia-Ukraine War is also important, because it is an innovation hub for terrorists. We now see the acceleration and advancements in the scale, speed, and range of drone operations. These developments are not only transforming the modern battlefield, but also they are creating new opportunities for terrorists to enhance their operational impact, engage and surprise.

The Role of Corporations in Modern Warfare

Another critical factor to be mentioned is the involvement of the corporates. In fact, without corporates, this war would have ended very soon. Three of the biggest companies in the world, SpaceX, Palantir Technologies, and Microsoft have literally transformed the war. They have enabled Ukraine access to some of the most advanced AI technologies in the world, and they have helped ensure Ukraine's access to high-speed internet. It is, according to Federov, Ukraine's Minister of Digital Transformation, the "blood of our entire communications infrastructure." Palantir Technologies have provided Ukraine with advanced data and analytics that have helped Ukrainians to understand the battlefield, intelligence, and also helped in their military decision-making. Microsoft basically kept the government alive. Without Microsoft, the government would have shut down, and it literally helped it to keep on track. It allowed Zelensky to continue to talk to his people. The Growing Power of Technology

The growing power of technology is not always benign; it also raises concerns about its exorbitant influence. If we consider the case of a single individual—Elon Musk—he exemplifies how one person, or one company, can reach a position where, at any given moment, they may influence the course of a war, simply by the ability to deactivate satellite systems. This reflects an extraordinary and highly significant expansion in the power of technology.

Ten Lessons from the War in Ukraine

Lesson 1: Software Is Transforming Warfare

Mark Anderson famously declared that "Software is eating the world." This has never been more relevant than in the context of modern warfare. Software is increasingly central to shaping military strategies and determining the outcome of conflicts. As defense systems are challenged and data becomes the new oil, the power of intelligence and information, traditionally controlled by global superpowers and large corporations, may eventually be harnessed by weaker, less resourced groups, such as insurgents and terrorists. Software allows combatants to hack into enemy networks, disable critical infrastructure, disrupt communication, and gather intelligence. Therefore, while it is a very good thing, it can also be used in a negative way.

Lesson 2: Drones Are Reinventing Military Operandi

Drones have significantly impacted how wars will be fought in the future. We are already witnessing the emergence of advanced deep-strike drones, such as the Iranian Shah drones used by Russia, and long-range drones developed by Ukrainian startups. In large numbers, these drones can surpass even sophisticated air defenses. Drone innovations by the Houthis have shown that drone attacks can be highly precise and effective. A Houthi drone was able to fly for some 16 hours from Yemen over a distance of more than 2,600 kilometers to strike Tel Aviv in July 2024.

We have seen the evolution of drone usage by the terrorist groups. DAESH, for instance, was one of the first terrorist groups that really embraced the use of drones, first for surveillance, but later by weaponising drones to attack enemies. Increasingly, we are witnessing a diversification of tactical evolution and continued innovation. Use of drones by violent non-state actors has expanded far beyond DAESH, and now multiple groups have begun adopting them.

Lesson 3: Do-It-Yourself Weapons and 3D Printing

The war has introduced literally the concept of ‘do-it-yourself’. The widespread availability of easily designed software, off-the-shelf devices, and 3D printing has accelerated the ability of innovative minds to build their own weapons. 3D printing means non-state actors can print whatever they need, wherever they need it. User-friendly software and specialized AI microchips have become powerful tools. These systems may not match military-grade sophistication, but the concern lies in their accessibility to terrorists globally.

Makeshift factories and labs have emerged across Ukraine, producing remote-controlled machines of various sizes, ranging from long-range aircraft and attack boats to inexpensive kamikaze drones, known as F.P.V.s, or first-person view drones, guided by pilots wearing VR-like goggles that provide the drone's perspective. Ukrainian entrepreneurs, engineers and military units are using code found online and components from hobbyist computers like Raspberry Pi that can be purchased from hardware stores or Best Buy. There is also a global volunteer network, including the ‘Wild Bees Poland’, producing 3D-printed items like casings for Starlink satellite receivers, magazine clips, drone recovery claws to retrieve drones downed by electronic warfare, and lifesaving gadgets like trench periscopes. While this is great for Ukraine, we must consider: what if there are terrorist ‘bees’ building 3D weapons?

Lesson 4: PSYOPs and Cognitive Warfare are a Powerful Weapon

The Russia-Ukraine war has demonstrated that we are entering a new form of cognitive war in which cyberattacks, information campaigns, and psychological operations (PsyOps) play a central role. Disinformation, misinformation, post-truth dynamics, and broader processes of ‘truth decay’ have emerged as powerful tools capable of shaping public opinion and destabilizing societies, not only among the war combatants but across the globe. Social media has significantly amplified these effects, while deepfakes and propaganda increasingly influence public perception and sow discord. PsyOps have also proven effective in misleading adversaries regarding the timing and location of offensives, contributing to notable operational successes. Looking ahead, both states and terrorist organizations are likely to further embrace the disinformation domain, with terrorists in particular potentially deploying PsyOps as a critical element of asymmetric strategy, a trend that deepfakes are expected to intensify. As Mark Twain said: “A lie can travel halfway around the world while the truth is still putting on its shoes.”

Lesson 5: Non-State Actors Worldwide are Sharing Expertise

Terrorists are not passive observers in modern warfare, they actively monitor, study and incorporate new modus operandi. The Center for Information Resilience documented that fighters in Myanmar uploaded approximately 1,400 online drone-flight videos between 2021 and 2023. These videos have enabled terrorist actors worldwide to innovate. Platforms such as Discord and Telegram provide access to information on 3D-printing blueprints for fixed-wing drones, as well as tactics and guidance on pilot training and methods for bypassing default software on commercial drones to conceal their locations.

Lesson 6: David and Goliath-New Asymmetry in Wars

Warfare is no longer determined solely by the number of jets, ships, or tanks a country can deploy; it is increasingly shaped by the speed at which both states and non-state actors can innovate. New dual-use technologies, ranging from smartphones to drones, are increasingly weaponized, providing terrorists with capabilities they did not previously possess. While not equivalent to state-level air superiority, these developments have nonetheless enabled terrorist groups to contest airspace and, increasingly, maritime domains. Terrorists can also access MANPADS and drones, and we continue to observe the significant operational advantages conferred by drones and other intelligence, surveillance, and reconnaissance capabilities.

Readers are encouraged to consult Power to the People by Audrey Kurth Cronin, which examines the diffusion of power from states to individuals and non-state actors. Never before have individuals possessed such lethal potential, nor have terrorist actors had comparable access to both emerging and existing technologies. This unprecedented convergence of accessibility, knowledge, and capability defines what can be described as an age of lethal empowerment. Therefore, we live in an age of lethal empowerment.

Lesson 7: Companies are Expanding AI

Technology is fundamentally transforming the nature of warfare, a shift that has been unfolding over decades with the increasing move toward autonomous weapons systems. The growing combat demand for tools that integrate human and machine intelligence has driven substantial investments by both governments and private companies seeking to enhance the efficiency, cost-effectiveness, and speed of military operations. This demand has proven highly beneficial for technology and defense firms, resulting in major contracts to develop a wide range of capabilities, including lethal autonomous drones, unmanned fighter aircraft, and underwater vehicles. Companies are actively expanding their AI applications, drawing lessons from ongoing conflicts, as is the case with the war in Ukraine, by testing, refining, and observing their technologies in operational environments.

While companies themselves are not the problem, unlike militaries they are not trained to keep such technologies under strict control. As a result, advanced capabilities increasingly diffuse beyond intended users. Recent developments, such as the success of DeepSeek, illustrate how AI companies openly share expertise with the global community, enabling rapid further development. This openness, while beneficial for innovation, has further democratized access to dual-use technologies, raising concerns that violent non-state actors and terrorist groups can exploit these innovations to enhance their own capabilities.

Lesson 8: The Oppenheimer Moment: The AI Military Race

The rise of AI-enabled warfare and autonomous weapons systems is increasingly described as an ‘Oppenheimer moment’, drawing direct parallels to the creation of the atomic bomb. This analogy represents a pivotal point that could either mark the beginning of a new era of great power or dominance or serve as a warning of potential catastrophic consequences. As AI technologies continue to advance rapidly, they are poised to fundamentally reshape society’s relationship with war and technology, leading to growing reliance on machines for critical decision-making. This trajectory raises concerns about a dystopian future reminiscent of apocalyptic fiction. At the same time, AI may also represent a saving grace for humanity, with the potential to enhance resilience and collective intelligence. Importantly, as Pierre Bourdieu argued in his work on social and cultural production, this is not a simple dichotomy of AI versus human society; rather, AI exists within an ongoing cycle of social and cultural production, in which humans shape AI through language and practice, and AI, in turn, shapes human behavior and cognition.

Lesson 9: The Importance of Regulation of Lethal Autonomous Weapons (LAWS)

Drone swarms represent a particularly effective weapon in asymmetrical warfare, underlining the importance of keeping meaningful human control over the use of force rather than relinquishing critical decisions to machines. Generative AI is expected to have a profound impact on global security by enabling new weapons and operational methods, potentially empowering malicious actors worldwide. While the past year’s focus on lethal autonomous weapons systems (LAWS) and artificial intelligence has given regulation advocates cautious optimism that political pressure for international agreements may increase, governance visions continue to diverge globally. Nonetheless, both the United States and China share a common concern about preventing terrorist organizations from acquiring autonomous weapons, offering a potential foundation for international cooperation on how to address the challenges posed by LAWS.

Lesson 10: A More Transparent World

The world is becoming increasingly transparent, a development with significant implications for security and accountability. This growing transparency is making it progressively more difficult for terrorists and insurgents to hide, both in physical spaces and in the digital domain. Satellite imagery now enables the documentation of mass atrocities worldwide, while nanosatellites can track vessels globally through identification systems. In addition, amateur sleuths increasingly support security actors in examining criminal behaviour. Advances in social media forensics assist law enforcement in collecting evidence from online platforms, and digital forensics enables investigators to analyse digital evidence on a global scale. Together, these developments underscore how technological transparency is constraining the operational space available to violent non-state actors.

Conclusion

A.J.P. Taylor argued that war has always been a driver of innovation, as seen in World War I with the introduction of the tank and in World War II with the development of the atomic bomb. The Russia–Ukraine war once again illustrates this dynamic, but in a fundamentally different form, characterized by rapid advances in drone innovation, intelligent weaponized systems, lethal autonomous weapons, and generative AI. This evolution signals the emergence of a new type of warfare, one that terrorist actors are closely observing, learning from, and adapting to.

The Sahel: NATO’s Possible Future Battlefield

EXECUTIVE LEVEL
DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKIYE
15-16 October 2025
"United Against Terrorism: Secur ne Future"
Prof. János
BESENYŐ

Prof. János BESENYŐ, Professor at the Óbuda University, Doctoral School for Safety and Security Sciences and head of the Africa Research Institute in Budapest.

Since its inception, NATO has been constantly confronted with changing security circumstances and has sought to adapt to them. This has been the case with the end of the Cold War, the end of the bipolar world system, the outbreak of the Balkan conflict and now the conflict between Russia and Ukraine. Although the organisation was not originally intended to play a major international role, it quickly ’outgrew’ its original framework and began to play an increasingly active role on the world political stage. It became involved not only in Europe, but also in its immediate surroundings (Middle East, North Africa) and even further afield (Asia). Today, the defence organisation has interests and cooperation on almost every continent. The research book project that we did for COE-DAT looks at the relationship between NATO and the Sahel, but this relationship can only be fully understood within the broader context of NATO's engagement with the African Union (AU), so I will briefly address this area as well.

NATO has had a permanent presence on the African continent since 2005, where it has developed a strategic partnership, notably with the AU. The first joint cooperation started in 2005, when NATO, at the request of the AU, provided assistance to the AU peacekeeping operation (African Union Mission in Sudan/AMIS) to stop the genocide in Darfur, providing financial, logistical and air support for the deployment and withdrawal of African troops to the area of operations. It also provided advisers and experts to the peace operation (Besenyő, 2021, pp. 119-123; Segell, 2008, pp. 10-18). It provided ongoing operational support, training support and structural support to AU member states at the request of the AU. It also provided substantial support (material, logistical, strategic airlift and sealift support, planning, etc.) for the launch and operation of the AU mission in Somalia (later African Union Transition Mission to Somalia/ATMIS) after Operation Darfur (Giegerich, 2013, p. 313; Marsili, 2020, p. 199). The cooperation was not limited to individual missions, but became permanent and institutionalised. Thus, officers from African countries received training at NATO institutions (NATO School in Oberammergau, Germany, and the NATO Defense College in Rome, Italy), participated in joint exercises, and, if necessary, NATO even provided tailor-made training in African countries through NATO's Mobile Education and Training Teams (NATO 2023). NATO also played a role in the design, deployment and operation of the African Stand-by Force (Pasquali, 2018, p. 90). Cooperation has been steadily strengthening over the years, to the extent that NATO has established its own liaison office at the AU headquarters in Addis Ababa, where its staff are in daily contact with African partners and the international organisations and countries that work with them. Following the Warsaw Summit in 2016, NATO has further strengthened its cooperation with the AU. This was also the time when NATO's Framework for the South was established, which aims to facilitate NATO's regional engagement and activities in Africa, including through the deployment of military units (NATO Response Force deployment) (Brandsma, 2019). In 2017, the Strategic Direction-South HUB (NSD-S HUB) was established and is located in the NATO Joint Force Command (Naples), which monitors events on the African continent. In November 2019, NATO and the AU signed an agreement to strengthen cooperation, followed by new agreements in March 2020. In 2021, NATO expanded the military cooperation offered to the AU and in 2022, AU Commissioner for Political Affairs, Peace and Security Ambassador Bankole Adeoye visited NATO headquarters (NATO 2023).

NATO and the Sahel

Since the early 2000s, NATO and its member states (especially the southern European countries) have been facing increasing security challenges from the North African (especially Libya) and Sahel countries (especially the G5 Sahel countries such as Burkina Faso, Chad, Mali, Mauritania and Niger), which have been affected by various economic, economic, governmental, security and counter-terrorism cooperation (Pan-Sahel initiative, G5S Joint Force's project, etc), and then through peace operations such as MINUSMA, EUCAP Sahel Niger, EUCAP Sahel Mali, EUTM Mali, EUMPM Niger, Operation Serval and Operation Barkhane (D'Amato & Baldaro, 2024). In these processes, NATO and some of its member countries have also sought to play a role, mainly in the defence of the southern borders of the European continent (Herráez, 2025, pp. 4-5). Also important for NATO is the economic and other cooperation with the region, and the fact that the region's population is growing at a very rapid pace and, with a significant proportion unable to manage in their homelands, migration to Europe is being boosted. The organisation has therefore been working for years to develop mutually beneficial cooperation with the Sahel countries. The organisation is primarily interested in security cooperation and crisis management to stabilise the countries of the region. To this end, it has launched Defence and Security Capacity Building (DCB) programmes, through which it has cooperated with some of the Sahel countries (Niger, Mali) and provided limited training for the heads and officers of the armed forces and law enforcement agencies. And through NATO's Mediterranean Dialogue Partnership programme, support was provided to equip, train and deploy the armies of the countries of the region against terrorist groups, mainly in the fight against terrorism. The organisation has developed a very good relationship with Mauritania, which joined NATO's Mediterranean Dialogue partnership programme in 1995, but actual cooperation only started in 2013 through NATO's Defence Education Enhancement Programme. NATO has not only been involved in the training of the Mauritanian army, for example, NATO Allied Special Operations Forces Command (SOFCOM) has played a significant role in equipping and training Mauritania's special forces, but has also been actively involved in the establishment of four crisis management centres in the country. In January 2021, the President of Mauritania visited NATO headquarters, where he met the Secretary General of NATO, Jens Stoltenberg. In June 2022, Mauritania was invited to the Madrid Summit as a „non-NATO partner" and was awarded the Defence Security Capacity Building Package, which will allow the Mauritanian army to be further strengthened and modernised (Ramani, 2023).

However, the Sahel countries have not only cooperated with NATO itself as a defence/military organisation, but also with several NATO member states through bilateral relations. A good example of this is Italy, which, in cooperation with Niger, launched a separate operation (Operation MISIN) against terrorist groups operating in the region, and also aimed to reduce the level of migration to Italy (Spagnolo, 2019, pp. 209-230).

In 2022, the Sahel countries of Niger, Burkina Faso and Mali were the victims of successful military coups, which led to the expulsion of their former allies (EU, France, USA) from the region, with serious security consequences (Csicsmann & Romaniuk, 2024, pp. 1-6). The governance of these countries has also faced many problems in previous years, but the situation has deteriorated further under military governments, which are less receptive to democratic norms. In the vacuum that has been created, terrorist groups have gained ground, military governments are unable to guarantee the security of their citizens, and even use the fight against terrorists as an excuse to act against certain social groups, minorities and those who challenge their rule in any way (NGOs and civil society elements, journalists, rights defenders, etc.) (see Romaniuk & Njoku, 2021; Romaniuk, 2021). The arrival of new allies (mainly the Wagner group) to replace the former Western allies has contradicted the expectations of the population, as they are incapable of taking effective action against terrorist organisations (Herráez, 2025, pp. 5-6). Indeed, they are often used by military governments as a tool against groups critical of them. Public security is steadily deteriorating, security risks are increasing, corruption is on the rise, economic performance is declining, poverty is rising and migration towards Europe is increasing. Unfortunately, terrorist groups have already established a foothold in neighbouring countries (Ghana, Guinea, Togo, Benin, Ivory Coast), putting the stability of the region at risk.

Although many have suggested that NATO could play a role in stabilising the region, this carries considerable risk, especially in light of the significant influence that Russia and China have gained in recent years in the Sahel countries, with which the organisation would not engage in open conflict. A number of new players have emerged in the region, including Iran, which would like to obtain uranium from Niger in exchange for drones and weapons for the junta. Iran is also seeking to develop better cooperation not only with Niger, but also with Mali and Burkina Faso (Vial & Bouvier 2025). This could also complicate NATO's possible involvement and activities in the region. Or, as an external intervener, it could provoke local resentment, which could also have negative consequences. The possible intervention could also pose other risks. If NATO were to act inappropriately, as it did in Libya (Besenyő, 2013), it could potentially increase the rate of migration from the region to Europe, which, in addition to posing a security risk, could weaken cohesion within the organisation. Especially if the organisation does not provide adequate support/guarantees to its member countries affected by migration. Therefore, NATO would be able to gain/strengthen its influence in the Sahel countries mainly through humanitarian, social and economic support. It is also important to continue to cooperate with regional organisations (ECOWAS, Accra Initiative) and other countries in the region that are open to it in the fields of security, military and counter-terrorism. This will prevent further destabilisation in the region (D'Amato & Baldaro, 2024). However, it is essential that the organisation clarifies its intentions and strategy for the region, defines priorities and the framework through which member states can engage in the region and communicates them appropriately. It is also important to implement possible structural (setting up a research institute for the region, etc.) and other changes so that any NATO involvement can be implemented quickly and smoothly.

COE-DAT book project on Sahel, which has been compiled to provide the appropriate background and information on the Sahel countries, can help with the possible NATO involvement. Book is divided into three main parts. The first part (regional overview) contains a chapter on the geography and characteristics of the Sahel, in which the author makes it clear that "The Sahel region, which forms a diverse environmental unit, presents significant challenges both for the states of the region and for external power actors seeking to assert their geopolitical interests in the area" (Péter Miletics, Geography of the Sahel). This could be the motto of the whole book, which illustrates the challenges NATO may face. In the second chapter, András Türke, head of the Europa Varietas Institute, Switzerland, who has considerable knowledge of French activities in the region and in Africa, traces the past, lesser known and current events in the states of the region (András Türke, History of the Sahel). In the third chapter, the reader will learn about the economic life of the countries of the region, their characteristics and their impact on various processes (political, security, etc.). A special section deals with the impact of climate change, political instability, the role of external actors, and the author even offers a kind of forecast of the economy and formulates strategies and proposals for stabilising it (Animesh Roul, Economy of the Sahel: Challenges, Opportunities, and Geopolitical Tensions).

The second part (Global and national relationships with the region) contains eight chapters. In the first chapter, the authors examine a specific segment of the EU's relations with the Sahel countries, namely the fight against terrorism. This is also a very important issue for NATO, as a strategic partner of the EU, which cannot be ignored in its relations with the Sahel countries (Mariann Táncos; Katalin Horváth, The European Union's counter terrorism activity in the Sahel).), Tamás Csiki Varga, Senior Researcher and Lecturer at the John Lukacs Institute for Politics and Strategy of the Ludovika University of Public Service (Budapest, Hungary), examines NATO's engagement and cooperation with the Sahel states (especially Mauritania) so far, and the possible direction of further cooperation. However, this will not be easy, as a recent evaluation from NATO's Southern Hub even concluded that "the gap between Western nations and Sahel countries in terms of cooperation has widened due to rapidly changing security dynamics, divergent priorities, and inconsistent". (NSD-S Hub & UFV, 2024, 14) The third chapter presents the role and activities of the African Union in the Sahel. It describes and reviews its strategy for the region and highlights how it has cooperated with regional organisations to address key security challenges. It describes the achievements and shortcomings of the AU's efforts in the Sahel and makes recommendations aimed at improving the organisation's capacity to address the region's deteriorating security situation (Ntaka Buyisile Sinqobile: The African Union and the Sahel Region). The fourth chapter (Tibor Pintér: United States and the Sahel) focuses on the military presence of the United States in the Sahel region and its results and effectiveness. The author also discusses US aid and economic policies, in line with geostrategic interests and the US ambition to increase its diplomatic, economic and military influence in Africa. In the fifth chapter, the authors examine the very pragmatic relationship between China and the Sahel countries, based mainly on economic and diplomatic cooperation, especially in the light of the efforts of China to replace France and other Western countries leaving the region, alongside Russia, India and Türkiye (Zoltán Vörös; Jean-Pierre Cabestan: China and the Sahel). In the sixth chapter (János Besenyő; Zsolt Szabó: Russia and the Sahel), the two authors show how Russia has gained increasing space and influence in the Sahel over the last 10 years, mainly through diplomatic, military and security instruments, and to a lesser extent through economic ones. This can be seen in particular in the increasing visibility of the activities of the Russian PMCs (Wagner Group, Africa Corps), especially in Burkina Faso, Niger and Mali, countries where the army has seized power by coup (Romaniuk & Besenyő, 2023). In the next chapter (Elem Eyrice-Tepeciklioğlu; Ali Onur Tepeciklioğlu: Türkiye's Growing Footprint in the Sahel), we will trace Türkiye's rise in the region. We can see how the Turkish leadership has begun to increase its diplomatic, economic, humanitarian and military/security engagement in the region, which is a clear indication that not only Africa, but also the Sahel region within it, has become a significant focus of Turkish foreign policy. The authors in this chapter analyse the factors that underline Türkiye's engagement in the region through three general categories: business ties, soft power tools and defence and security engagements. In the eighth and final chapter (Nail Elhan: Iran in the Sahel: Strategic calculations and geopolitical maneuvers in the shadows), the author describes Iran and its activities as a less known 'player' in the region. The Shi'ite middle power has emerged in the region in the past year, seeking to build better diplomatic, political, economic and military ties to counter the influence of Western powers, Saudi Arabia and the Sunni Gulf states. Iran seeks to establish bilateral and multilateral relations with the Sahel countries and expand its influence in the region. It has done so spectacularly in Nigeria, Burkina Faso and Eritrea. However, this has raised concerns in several countries with influence or aspiring to influence in the region, not least because the emergence of Iran and its rivalry with these powers has turned the region into a battlefield for influence, complicating local security dynamics and contributing to instability in the region.

The third part of the book (Regional security challenges) contains a further ten thematic studies/chapters. In the first chapter (Dávid Vogel: Sahel and security: situational overview and challenges ahead), the author analyses the security situation in the region, not only as a researcher but also as a person who has served as a soldier, peacekeeper in the Central African Republic and later as an aid worker in Chad. In his chapter he uses Barry Buzan's sectoral concept of security, reviewing the situation through the political, economic, societal, environmental and military aspects. Accordingly, he analyses and evaluates various databases on the countries of the region and draws his conclusions. In the second chapter, the authors examine the military coups and their consequences in some Sahel countries (Mali, Niger, Sudan, and Burkina Faso) and the relationship and interaction between state fragility and coups (Scott N. Romaniuk; László Csicsmann: Military coups and state fragility in the Sahel). The authors use data from the Fund for Peace's Fragile States Index and the Armed Conflict Location and Event Data (ACLED) Conflict Index. Chapter three introduces the reader to water security and its impacts in the Sahel and the opportunities for improving water security (Viktor Glied; Attila Pánovics: Sahel and Water Security). Chapter four is written by two experts who have been involved in several food security-related programmes in the region and have been conducting research on food security for many years. The chapter on food security in the region has managed to find the right balance between theoretical and practical issues. At the end of the chapter, they propose the initial steps needed to define a strategy for food security in the Sahel (Szilvia Veress Juhászné; Péter Gergő Juhász: Food security in the Sahel). The following chapter, written by Pieter Van Ostaeyen, traces the events that have led to the strengthening of terrorist groups in Mali, Niger and Burkina Faso to the point where they are now able to negatively influence the functioning of governments. The author describes the activities of the terrorist groups JNIM (Jama'a li-Nusra al-Islam wa'l-Muslimin), ISSP (the Islamic State in Sahel Province) and ISWAP (the Islamic State in Western Africa Province), in particular but not exclusively (Pieter Van Ostaeyen: Terrorist and counter-terrorist activities in the Sahel). In the sixth chapter, Lieutenant Colonel Norbert Daruka, one of the most experienced bomb disposal officers of the Hungarian Defence Forces, and his co-author Professor László Lukács show how decades of armed conflict in the region have contributed to the proliferation of weapons and explosives and the security risks they pose, not only to the participants in the conflicts but also to the civilian population (Norbert Daruka; László Lukács: Improvised explosive devices and the threat they pose in the Sahel and beyond). In chapter seven, Adeyemi Saheed Badewa, a researcher at the Center for African Studies, University of Pittsburgh, United States examines the multifaceted nature of forced displacement in the Sahel, analysing both its root causes and humanitarian implications. His study provides insights into efforts to address the humanitarian crisis in the region, albeit with little success. The author, who is himself an experienced expert in this field, makes several suggestions for their improvement (Adeyemi Saheed Badewa: The Sahel: Migration, Displacement and Refugee Crisis). In the next chapter, readers can learn about the coexistence and relations of Christian-Muslim communities in the countries of the region from different perspectives (László Csicsmann; Scott N. Romaniuk: Christian-Muslim relations and the future of coexistence in the Sahel region). The ninth chapter focuses on the humanitarian situation in the region and the challenges related to human trafficking (János Besenyő; Krisztina Kállai: Management of Humanitarian Operations and Situation in Sahel by applying resilience-based methods in relation to human trafficking). The last chapter also focuses on the humanitarian situation, with Dr. Béla Szilágyi, who as the head of the Hungarian Baptist Aid, shares his experiences in various humanitarian projects in Chad. The Hungarian NGO is not only involved in projects related to the care of refugees and refugee camps, but also in projects that are important for the host community and can only be tackled in a complex way. Most importantly, they do not only address the immediate needs of IDPs and refugees, but also run long-term, sustainable programmes (Béla Szilágyi: Chad humanitarian and forced migration situation, a Hungarian experience).

Bibliography

Bastian Giegerich (2013). NATO and Interorganizational Cooperation. In: E. Hallams, L. Ratti, B. Zyla (eds) *NATO Beyond 9/11: The Transformation of the Atlantic Alliance*. Cham, Springer, pp. 297-317.

Besenyő, J. (2013). War at the Background of Europe: The Crisis of Mali. AARMS – *Academic and Applied Research in Military and Public Management Science,* 12(2), 247–271. https://doi.org/10.32565/aarms.2013.2.7

Besenyő, J. (2021). Darfur Peacekeepers - The African Union peacekeeping mission in darfur (AMIS) from the perspective of a Hungarian military advisor, Paris, Éditions L'Harmattan

Brandsma, C. (2019). NATO and the Mediterranean, IEMed. *Mediterranean Yearbook 2019*, pp. 232-235., https://www.iemed.org/wp-content/uploads/2021/01/NATO-and-the-Mediterranean.pdf

Csicsmann, L. & Romaniuk, S. N. (2024). Introduction to the issue: Coups and Terror in the Sahel: Terrorist Groups' Exploitation of State Fragility and Ungoverned Spaces. *Journal of Central and Eastern European African Studies*, *4*(2), pp. 1-6.

D'Amato, S. & Baldaro, E. (2024). Does the Sahel need NATO? *The International Centre for Counter-Terrorism (ICCT)*, 26 Aug 2024, https://icct.nl/publication/does-sahel-need-nato-0

Glen Segell (2008) The first NATO mission to Africa: Darfur. *Scientia Militaria: South African Journal of Military Studies 36* (2), pp. 1-18, https://journals.co.za/doi/abs/10.10520/AJA10228136_75

Herráez, P. S. (2025). The Sahel: another epicenter of global reconfiguration? IEEE 20/2025 Analysis Paper. 25p, https://www.defensa.gob.es/documents/2073105/2392118/el_sahel_tambien_epicentro_de_la_reconfiguracion_global_2025_dieeea20_eng.pdf

Marco Marsili (2020) Towards a strategic EU-NATO security partnership in Africa. *Proelium* VIII (4), 195 – 208, https://zenodo.org/records/3634718

NATO (2023) *Cooperation with the African Union*, NATO homepage, https://www.nato.int/cps/cn/natohq/topics_8191.htm

NSD-S Hub & UFV (2024). *Sahelian local perspectives on Western models of security collaboration*. NATO Strategic Direction-South Hub – Universidad Francisco de Vitoria. https://thesouthernhub.org/systems/file_download.ashx?pg=9952&ver=9

Pasquali, L. (2018). NATO and Peace Maintenance in Africa. In Giovanni Cellamare, Ivan Ingravallo (eds.) *Peace Maintenance in Africa: Open Legal Issues*. Cham, Springer, pp. 77-110.

Ramani, S. (2023). Why Everyone Is Courting Mauritania. *Foreign Policy*, September 21, 2023, 8:42 AM, https://foreignpolicy.com/2023/09/21/mauritania-green-energy-china-nato-russia-gulf/

Romaniuk, S. N. (2021). *Under Siege: Counterterrorism and Civil Society in Hungary*. Rowman & Littlefield.

Romaniuk, S. N. & Besenyő, J. (2023). Wagner Mercenaries: A Potential Lifeline for the Niger Junta. *Geopolitical Monitor*. http://geopoliticalmonitor.com/wagner-mercenaries-a-potential-lifeline-for-the-niger-junta/

Romaniuk, S. N. & Njoku, E. T. (2021). *Counter-Terrorism and Civil Society: Post-9/11 Progress and Shallenges*. Manchester Univesrity Press.

Spagnolo, A. (2019). The Conclusion of Bilateral Agreements and Technical Arrangements for the Management of Migration Flows: An Overview of the Italian Practice. *The Italian Yearbook of International Law Online 28*(1), 209-230. https://doi.org/10.1163/22116133_02801013

Vial, A-S. & Bouvier, E. (2025). Iran on the offensive in Africa. *Moyen-Orient*, 17/01/2025, https://www.lesclesdumoyenorient.com/Iran-on-the-offensive-in-Africa.html

TERRORISM EXPERTS CON
EXECUTIVE LEVEL
DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: Securing the Future"
Horizon Scanning the Terrorist Threat: Unders
Persistent Threat Analyzing Latest Trends in Terrorist Modus Operandi for Future Projec
Kadir Has University
"The Impact of the Technologies Used in Russia-Ukraine War on Terrorist Capabilities"
Geneva Centre for Security Policy
"The Sahel: NATO's Possible Future Battlefield"
Óbuda University
Q&A SESSION

Panel 2: Blurred Lines or Clear Boundaries? Exploring the Nexus between CT and COIN

Counter-Terrorism (CT) And Counter-Insurgency (COIN): Overlapping Threats and Diverging Responses?

Stephen HARLEY, PhD Candidate at University of Strathclyde in Glasgow and Consultant for the UK Foreign, Commonwealth & Development Office.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO
OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE &
EXECUTIVE LEVEL
DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: ...ing the Future"

NATO COE DAT's recent research project, 'Counter-Terrorism & Counter-Insurgency' (2024) offered a discussion of a number of aspects of CT & COIN. At the heart of the discussion was the acknowledgement that a considerable number of those aspects are changing: the understanding of CT & COIN with the broader realm of conflict; the role and recognition of civilians in conflict, including women; the changing nature of technology, including drones, Artificial Intelligence and communications including social media; and the increasing role of other actors, including rogue states, organised criminal networks and less obviously ideological cohesive terrorists and insurgents, including Mixed, Unclear & Unstable ideologies (MUUs) such as Incels. Another critical element is the role the experience of recent campaigns such as Afghanistan, the lessons of which are still only now being identified.

As a result, this paper addresses the following questions:

- How can we best address a wide-spread, diverse, global and technically adaptive terrorism/insurgency?

- How are globalized, pervasive, 'always on' communications shaping the processes of socio-political violence?

- How do we come to terms with the seeming randomness of 'stochastic terrorism', where the linkages between the terrorist/ insurgent, the victim and the counter-actor are seemingly random, unpredictable and disconnected?

- Can states and institutions such as NATO go 'glocal', combining our understanding of global context and local conditions within existing doctrinal frameworks and analytical vocabularies?

Section One: 25 years on: Lessons Identified in the Global War on Terror

Colonel Daniel W. Stone USAF served in Afghanistan in a number of roles and was also COE DAT Deputy Director. His observations provide a useful starting point for this discussion.

As Colonel Stone notes, 'never say never': there is every likelihood that a counter-terrorism/counter-insurgency mission will most likely will occur again. But even now, he asserts, the lessons have not been clearly identified (he suggests five based on his own experience and analysis), the lessons have yet to be integrated into the military and other parts of government and, in some cases, the wrong lessons have been 'learned' (IE 'we will never fight a counter- insurgency campaign again as they are un-winnable').

In order to properly address this deficiency, he suggests that any actor embarking on a CT/COIN campaign must first clearly identify the problem, and then propose a solution that must address and solve that problem. While this might seem blatantly obvious, the conduct of the campaign in Afghanistan from 2001-2021 was characterised by constant shifting of focus - counter- narcotics, for example, or anti-corruption within a government capacity building effort - which inevitably limited the ultimate effectiveness of the mission. The deliberate division of the counter-terrorism campaign (US-led) and the counter-insurgency campaign (ISAF-led) equally constrained the Afghanistan mission.

Colonel Stone also notes a fundamental misunderstanding of counter-terrorism/counter-insurgency: that military power alone cannot win a mission. Instead, greater integration of the elements of power - not just military, but also diplomatic, economic the informational and many others - is required and that simply did not happen in Afghanistan.

Both Colonel Stone and Dr. Harmonie Toros also highlight the role of the population, 'the sea in which the insurgency swims', something that was patchy at best in Afghanistan and often hindered by cultural divides and social mores. But Colonel Stone notes that partnerships with local forces can work - if done right. Building a security force is difficult, he acknowledges, especially a foreign one, but it can be done as part of a fully integrated, coherent campaign. Colonel Stone, while he accepts that the Afghanistan mission was ultimately a failure, notes that it did not have to be and that a future campaign, if conducted differently, has the potential to succeed.

Section Two: The Changing Nature of Terrorism & Insurgency

While understanding what happened in Afghanistan, Iraq and elsewhere, Dr Richard Warnes also suggests the requirement for insight into how the nature of terrorism and insurgency is changing, almost day-to-day.

As he notes, terrorists and insurgents instinctively exploit advances in technology and it is inevitable that they will seek to exploit drone technology in the air, on the land and both on and under the sea. Equally, these groups have proved adept at a adapting to communications technology, taking advantage of social media and the deep and dark web to move beyond publicity to radicalisation, requirement, procurement and both storing and dispersing funds. Artificial Intelligence too provides the terrorist/insurgent with the ability to enhance its planning, targeting and delivery, while cyber-attacks on critical infrastructure are also potentially a source of significant disruption.

Equally, identifying terrorists and insurgents has become considerably more difficult with the emergence of Mixed, Unclear and Unstable (MUU) ideologies: no longer easily trackable by a fixed system of beliefs and a network of identifiable connections, threats can now be as small as a single individual actor with a loose, inscrutable ideology that possibly even they do not themselves understand. Also, with the breakdown of the international rules-based system, and the parallel rise of state sponsored disruptions such as sabotage and widespread disinformation, we are already seeing the increasing use of terrorists and insurgents as deniable proxies by nefarious actors. This allows those actors to remain in the 'grey area' of deniability until the last moment prior to initiating open hostilities.

The changes in the nature of terrorism and insurgency are rapid and the onus is on institutions to try to keep up. How effective that effort might be may be as a much a matter of luck as deliberate action.

Section Three: How Can NATO Adapt?

The challenge for NATO, as well as other institutions and individual nation states is, as it was in the 1990s, to adapt to the threat and the environment. NATO and NATO member states have existing doctrines around counter-terrorism and counter-insurgency: these will require constant review to meet the changing nature of the threat. NATO is already focusing on current developments in the field, with, for example, recent COE DAT publications focusing on technological shifts ('The Weaponization of Artificial Intelligence: The Next Stage of Terrorism and Warfare', 2025) and lessons identified from ongoing campaigns or in particular regions ('The Effects of the Russia-Ukraine War on Counter-Terrorism', 2025, and a planned one on the Sahel region, to be published in 2026): this effort will continue to be essential. This presentation does not, however, provide solutions: but it does offer suggestions as to what else can NATO do to remain relevant.

Recommendation 1: Constantly review and update the strategies and doctrines for CT/COIN

Firstly, while NATO has definitions and, in some areas, strategies, for CT/COIN, these require constant review and updating. Even then, every terrorist or insurgency group is unique in its own way: consider al-Qa'ida in Iraq and DAESH, for example. Every environment where a terrorist group operates is different as well: DAESH in Iraq/Syria is very different from DAESH in Afghanistan or Libya or the Sahel or Somalia. Broad, blanket definitions are fine but of limited use in terms of implementation, where the group and the environment must be understood and strategies and tactics adapted accordingly. As an aside, the author himself, with nearly two decades of constant CT/COIN experience in Iraq, Afghanistan and Somalia, prefers a more practical definition: 'An illegitimate response to a legitimate grievance.'

Recommendation 2: Focusing on the root problems within the relevant society that spawns the terrorist/insurgent group

This leads to the second recommendation: placing emphasis on understanding the origins of the terrorist or insurgent group and, while dealing with the day-to-day tactical response to these groups, placing equal if not greater emphasis on addressing the grievances within those groups and the wider society. To achieve this, greater understanding of the politics, history, economics, infrastructure, geography, culture and so on, and associated 'soft power' capacity to respond will be required. NATO should consider how it might use its existing capabilities or restructures itself to meet this critical component of any CT/COIN campaign.

Recommendation 3: Placing CT/COIN within a wider context of P/CVE, Conflict Transformation & Peace-building

Thirdly, NATO may wish to consider framing definitions beyond CT/COIN within a broader structure that encompasses P/CVE, Conflict Transformation/Peace-building, Gender Equality & Social Inclusion within the realm of Human Security, and then define clearly how it views the way in which these different elements interact with each other to produce a comprehensive campaign strategy that can be implemented effectively.

Recommendation 4: Re-balancing between enemy-centric and population centric approaches

Fourthly, understanding society means understanding all of society, not just the political elite, the security forces and 'friendly' local advisors and employees: this includes women, but not just as women, along with minorities, the marginalized and, critically, the moderate middle, who are often assumed to be happy to remain quietly in place, neither pro-terrorist/ insurgent nor pro-government institutions. NATO should consider how it can achieve this level of understanding, building on well-intentioned but poorly delivered concepts such as Human Terrain Teams, Female Engagement Teams and so on.

Recommendation 5: Yet more focus on Emerging Threats

Fifthly, NATO already has a highly effective Emerging Threats branch and this should be supported in its continuing efforts to track developments in areas such as CT/COIN but also climate change, technology, space and so on.

There are other areas for focus as well: negotiated settlement, strategic communication, improving integration with other actors, including humanitarians, Non-Government Organisations, Civil Society Groups and so on. The initiative will always initially lie with the terrorist or insurgent: the degree to which an institution like NATO can respond and adapt is therefore critical. These recommendations will be essential in building that ability.

Talking As Fighting: Taliban Influence Operations and The Fall of The Islamic Republic of Afghanistan

Mr. Alexander PALMER, Fellow in the Warfare, Irregular Threats, and Terrorism Program at the Center for Strategic and International Studies (CSIS).

Politics played a major role in the fall of the Islamic Republic of Afghanistan in 2021, but military factors played a central role. The Taliban attacked psychological and military vulnerabilities of the Afghan National Security Forces (ANSF) through a coordinated campaign of kinetic and information operations. Military factors were critical in the defeat, civilians’ exhaustion with the violence undermined the ANSF, more effective use of money allowed the Taliban to induce surrenders, and signals of support were vital for conducting a proxy war.

The Debate

The Islamic Republic of Afghanistan government fell to the Taliban in August 2021, triggering a wave of debate over whether the Taliban had achieved a military victory or whether the ANSF collapsed for political reasons. For example, one unnamed former ANSF spokesman said: “I do not consider this a military defeat. I consider it a political defeat… Nowhere in Afghanistan did the Taliban take over territory with military power and tactics; it was all political maneuvers [ellipsis in original]” (SIGAR, 2023, 105).

Misunderstanding Afghanistan as a purely political defeat risks missing important lessons for future NATO or Allied efforts to support partner militaries against terrorists and insurgents. One U.S. political scientist wrote after the collapse “No amount of technical assistance or better-targeted logistical support would have sustained this fighting force, because these soldiers believed they had nothing left to fight for” (Murtazashvili, 2022). If that is true, then it would be difficult to learn any lessons about technical assistance and logistical support for partner militaries from the case of Afghanistan.

In reality, 2020 and 2021 saw some of the war's fiercest fighting (Clark, 2020, 2021; UNAMA, 2021; Gibbons-Neff & Rahim, 2021). That many ANSF personnel chose to 'fight to the death' against the advancing Taliban without any hope of reinforcement or resupply, in the words of one longtime analyst, "belies the claim that the ANDSF simply did not fight" (Schroden, 2021, 55). Interviews conducted by the Afghanistan Analysts Network (AAN) during and immediately after the 2021 offensive also undermine the narrative of a non-military victory. They repeatedly involve statements like this one made by a man from Pul-e Khumri, Baghlan province: "In the area where I live, there was fighting for 40 days. . . So many buildings were destroyed during the fighting – petrol stations, shops, homes" (AAN Team, 2022).

Close examination of the Taliban's information operations during the last year of the war reveals how military and political factors were intertwined. The success of the Taliban's political strategy was built on its military strength and control over territory. Had the Taliban been weaker or the ANSF more capable, the events of 2021 could have gone differently.

The Doha Agreement

The chain of events that led to the collapse of the ANSF began in 2020 when the United States and the Taliban signed the Doha Agreement in 2020 (US Dep.of State, 2020; Coll Entous, 2021; Miller, 2025; Malkasian, 2021). The agreement had three key provisions. The first was the commitment to withdraw U.S. forces (Cronk, 2021). The second was a set of restrictions on U.S. support for offensive operations against the Taliban and U.S. airstrikes (Sanger, et.al., 2020). The third was the release of 5,000 Taliban prisoners, many if not most of whom quickly returned to the battlefield, in exchange for 1,000 Taliban-held government personnel (O'Donnell, 2025).

The Doha Agreement had material and psychological effects. The end of U.S. support for offensive operations prompted ANSF to move to a strategy of 'active defense' while allowing the Taliban to move openly without fear of airstrikes (SIGAR, 2020). Taliban took advantage by massing fighters (some of whom had been recently released from Republic prisons) and exerting increased control over Afghanistan's roads, which put cities and ANSF defensive positions under siege (SIGAR, 2023; Ruttig & Sadat, 2021; Gibbons-Neff et al., 2021). The agreement, particularly the secrecy surrounding the classified annexes, also created an atmosphere in which rumors that the United States or Kabul government had agreed to hand over the country to the Taliban flourished (SIGAR, 2023; Nikzad, 2021; Amiry, 2021; Van Bijlert & AAN Team, 2021). It also changed the risk calculus of individual Republic and ANSF personnel, making surrender more appealing (Mukhopadhyay, 2023).

The agreement helped create the conditions that the ANSF found itself in at the beginning of 2021; hunkered down in increasingly isolated positions across the country and under increasingly frequent attack from the Taliban, who could now mass and move freely without fear of U.S. airstrikes. It was also critical for the success of Taliban information operations.

Taliban Information Operations

A huge number of ANSF positions (and even provincial capitals) fell after negotiations rather than close combat. The frequency of these deals in the closing days of the war and reports that the messaging was controlled by Taliban institutions suggests that they were the product of a concerted Taliban political-military strategy. The Taliban's Patkya strategy, for example, was designed by a 'six-member commission' that kept lower-level commanders' messages on-theme (Ruttig & Sadat, 2021).

The Taliban information campaign was characterized by four main messages, all of which played on vulnerabilities created or exacerbated by the Doha Agreement. The bedrock was coercion. Taliban social media and local elders carried a consistent message to ANSF personnel: “Surrender or die” (Zucchino & Rahim, 2021). This message was supported by a very real campaign of violence (Schroeden, 2021).

The Taliban also cultivated a sense of isolation among ANSF personnel. Afghans reported that local elders carried a message of abandonment to the ANSF: “reinforcements aren’t coming” (Zucchino & Rahim, 2021). The elders were right. Many district centers had been under siege for weeks or months, with some reporting being reduced to drinking rainwater or running out of ammunition (Sabawoon, 2021; Van Bijlert & AAN Team, 2021). According to one former local government official, “We had weapons and ammunition to last us a whole year, but we couldn’t send them to the districts because Taliban blocked all the roads” (Van Bijlert & AAN Team, 2021). These conditions were partly created in Doha (SIGAR 2023).

The third theme of the Taliban propaganda campaign was the notion that Afghans “were all brothers” (Van Bijlert & AAN Team, 2021). This was part of the Taliban’s package of inducements offered to ANSF personnel who surrendered. The Taliban allegedly paid “500 to 1,000 afghanis” to ANSF personnel who surrendered (Van Bijlert & AAN Team, 2021). Other sources reported different numbers, but the theme was consistent (Zucchino & Rahim, 2021; George, 2021). The message of brotherhood also built on nationalist and religious arguments the Taliban had made for decades. While the role of the narrative remains hotly contested, it seems likely that it pushed at least some wavering ANSF personnel to surrender (Malkasian, 2021; Miller, 2021).

Finally, the Taliban cultivated a narrative of inevitability. The Taliban clearly wanted to “portray government forces as unwilling or unable to resist them” (Foschini, 2021). This allowed Taliban success in one area to build momentum in others, contributing to the domino effect that eventually toppled the government.

Avenues of Influence

The Taliban influenced ANSF personnel through three major avenues. The most frequently discussed has been Afghanistan’s local elders (Van Bijlert & AAN Team, 2021; Clark, 2021). Some elders were already predisposed toward the Taliban for tribal or ideological reasons. (Van Bijlert & AAN Team). The Taliban allegedly paid others for their cooperation (Van Bijlert & AAN Team, 2021). Finally, some elders represented their communities’ desire to avoid further violence.

The second avenue was ANSF members’ families. Sometimes the Taliban contacted ANSF members’ families directly, threatening to kill their sons if they did not surrender (Ruttig & Sadat, 2021). Other times, they worked indirectly through tribal leaders, who delivered a similar message. (Ruttig & Sadat, 2021). The Taliban backed up many of these threats with a well-documented campaign of targeted killings and several alleged executions of ANSF personnel who surrendered after fighting until they were overrun (George and Tassal, 2020; Adkins, 2024).

Finally, the Taliban propagated their narratives through social media, most frequently Facebook and WhatsApp. The group had spent the previous decade building a robust digital infrastructure of highly active official and unofficial accounts (Booking, 2021). According to Taliban sources, the effort was well-organized and resourced, including a division of labor between different platforms, which targeted different audiences (Atiq, 2021). The Taliban media infrastructure was frequently far more active than that of the government (Bahar, 2020).

Lessons

The fact that so many ANSF positions fell after negotiations rather than being overrun seems to suggest that the defeat was primarily political. But examining the Taliban's information operations suggest that there are important military and security cooperation lessons to be learned from the ANSF's defeat.

The first is that military pressure mattered. Decision makers should not overestimate the promise of information operations. Many ANSF positions had to be overrun. In Faryab, for example, Qaisar was taken after a massive car bomb allowed the Taliban to close with ANSF, and Dawlatabad was taken after close combat with ANSF commandos who had recaptured the district center from the Taliban (Clark; 2021b). In addition, in Ukraine, where similar information operations were not paired with the physical isolation of well-supplied units, the defenders refused to surrender and the attackers' rapid advance was stymied (Watling et al., 2023).

The second is that the civilian population was a center of gravity. Civilians (especially local elders and ANSF members' families) played an important role in persuading them to defect. Communities were harmed by the fighting and recognized that ANSF positions were a magnet for fighting (Quilty, 2020). Economic concerns also played a role in communities' push for ANSF surrenders. Business owners were 'worried about losing everything' and supported efforts to mediate ANSF withdrawals or surrenders (Van Bijlert & AAN Team, 2021). Farmers were worried about missing the harvest season, which was ongoing during the Taliban offensive (Sabawoon, 2021; Clark, 2021; Quilty, 2020). Communities frequently did not see the ANSF as a positive presence and were happy to see them gone. According to one man in Bamyan, "Neither the government nor the army intended to fight, nor did the people want them to" (Van Bijlert & AAN Team, 2021).

The third is that effective use of financial resources was critical, and the Taliban effectively won the financial War. One longtime Afghanistan observer pointed out in February 2021 that "It is common knowledge in Afghanistan that many fighters only fight as long as they are paid and as long as they believe they can win" (Ruttig, 2021; Milward, 1980). By August 2021, many ANSF personnel had not been paid in a long time and were no longer sure they could win. With the Taliban offering both cash and amnesty, the incentives to defect were overwhelming.

The fourth is that signals of support were vital. Without continued U.S. support, the Taliban message of "surrender or die" gained credibility. The secrecy of the Doha Agreement also created an atmosphere of paranoia that the government did little to dispel. Afghan witnesses have said that districts were abandoned before any withdrawal was negotiated (Sabawoon, 2021). ANSF personnel told international analysts that they received orders not to fight (Van Bijlert & AAN Team, 2021). The common rumor that the United States was planning to hand the country over to the Taliban would hardly seem incredible to an Afghan watching those developments and unfamiliar with domestic U.S. politics.

References

AAN Team. (2022, August 12). Transition to a New Political Order: AAN dossier takes stock of Afghanistan's momentous year. *Afghanistan Analysts Network*. https://www.afghanistan-analysts.org/en/reports/political-landscape/transition-to-a-new-political-order-aan-dossier-takes-stock-of-afghanistans-momentous-year/

Adkins, R. [@RonnieAdkins_] (2024, August 30). One of the things that sticks with me from the fall of Kabul, of course beyond the 13 killed at HKIA, is a video of Afghan SOF surrendering to the Taliban. Rumor is that they had run out of ammo. I worked alongside Ktah Khas during my second deployment. When this video dropped a https://t.co/yDtMTSsKUB. *Twitter*. https://x.com/RonnieAdkins_/status/1829580766075863221

Amiry, S. (2021, June 17). Past 24 Hours Sees Fighting in 200 Areas in Afghanistan. *TOLOnews*. https://tolonews.com/afghanistan-172909

Atiq, S. (2021, September 6). The Taliban Embrace Social Media: "We Too Want to Change Perceptions". *BBC News*. https://www.bbc.com/news/world-asia-58466939

Bahar, H. M. (2020). Social Media and Disinformation in War Propaganda: How Afghan Government and the Taliban Use Twitter. *Media Asia 47*(1–2), 34–46. https://doi.org/10.1080/01296612.2020.1822634.

Booking, E. T. (2021, August 26) *Before the Taliban Took Afghanistan, It Took the Internet*. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/before-the-taliban-took-afghanistan-it-took-the-internet/

Clark, K. (2020, October 27). Behind the Statistics: Drop in civilian casualties' masks increased Taliban violence. *Afghanistan Analysts Network*. https://www.afghanistan-analysts.org/en/reports/war-and-peace/behind-the-statistics-drop-in-civilian-casualties-masks-increased-taleban-violence/

Clark, K. (2021, July 1). A Quarter of Afghanistan's Districts Fall to the Taleban amid Calls for a 'Second Resistance.' *Afghanistan Analysts Network.* https://www.afghanistan-analysts.org/en/reports/war-and-peace/a-quarter-of-afghanistans-districts-fall-to-the-taleban-amid-calls-for-a-second-resistance/

Clark, K. (2021a, July 26). New UNAMA Civilian Casualties report: The human cost of the Taleban push to take territory. *Afghanistan Analysts Network*. https://www.afghanistan-analysts.org/en/reports/war-and-peace/new-unama-civilian-casualties-report-the-human-cost-of-the-taleban-push-to-take-territory/

Clark, K. (2021b, December 30). Afghanistan's Conflict in 2021 (2): Republic collapse and Taleban victory in the long-view of history. *Afghanistan Analysts Network*. https://www.afghanistan-analysts.org/en/reports/war-and-peace/afghanistans-conflict-in-2021-2-republic-collapse-and-taleban-victory-in-the-long-view-of-history/

Coll, S. & Entous, A. (2021, December 10). The Secret History of the U.S. Diplomatic Failure in Afghanistan. Annals of War. *The New Yorker*, https://www.newyorker.com/magazine/2021/12/20/the-secret-history-of-the-us-diplomatic-failure-in-afghanistan

Cronk, T. M. (2021, April 14). Biden Announces Full U.S. Troop Withdrawal From Afghanistan by Sept. 11. U.S. Department of Defense. https://www.war.gov/News/News-Stories/Article/Article/2573268/biden-announces-full-us-troop-withdrawal-from-afghanistan-by-sept-11/

Foschini, F. (2021, August 9). The Fall of Nimruz: A symbolic or economic game-changer? *Afghanistan Analysts Network*. https://www.afghanistan-analysts.org/en/reports/war-and-peace/the-fall-of-nimruz-a-symbolic-or-economic-game-changer/

George, S. & Tassal, A. (2020, October 10). With U.S. Troops Gone, Taliban Expands Influence in One Afghan Province. *Washington Post* (Gardez, Afghanistan). https://www.washingtonpost.com/world/2020/10/10/afghanistan-us-troop-withdrawal/

George, S. (2021, August 15). Afghanistan's Military Collapse: Illicit Deals and Mass Desertions. *The Washington Post*. https://www.washingtonpost.com/world/2021/08/15/afghanistan-military-collapse-taliban/

Gibbons-Neff, T. & Rahim, N. E. (2021, June 17). Afghan Forces Suffer Horrific Casualties as Taliban Advance. *The New York Times*. https://www.nytimes.com/2021/06/17/world/asia/afghanistan-military-casualties.html.

Gibbons-Neff, T. et al. (2021, February 15). The Taliban Close in on Afghan Cities, Pushing the Country to the Brink. *The New York Times*, https://www.nytimes.com/2021/02/15/world/asia/taliban-afghanistan.html

Malkasian, C. (2021). *The American War in Afghanistan: A History*. Oxford University Press.

Miller, P. D. (2025). *Choosing Defeat: The Twenty-Year Saga of How America Lost Afghanistan*. Cambridge University Press. https://doi.org/10.1017/9781009614382

Miller, P. D. (2021). Review. *H-Diplo Roundtable XXIII-44*.

Milward, A. S. (1980). *War, Economy and Society, 1939-1945*. 1st ed, History of the World Economy in the Twentieth Century Series, v. 5. University of California Press.

Murtazashvili, J. B. (2022). The Collapse of Afghanistan. *Journal of Democracy 33* (1), 40–54.

Mukhopadhyay, D. (2023, January 18). The Afghan Stag Hunt. *Lawfare.* https://www.lawfaremedia.org/article/afghan-stag-hunt

Nikzad, K. (2021, June 15). 20 People Killed, 3 District Centers Fall in Past 24 Hours. *TOLOnews*. https://tolonews.com/afghanistan-172864.

O'Donnell, Lynne. (2025, October 2). Defying Peace Deal, Freed Taliban Return to Battlefield. *Foreign Policy*. https://foreignpolicy.com/2020/09/03/defying-peace-deal-freed-taliban-prisoners-return-battlefield-afghanistan/

Quilty, A. (2020, October 12). Taleban Opportunism and ANSF Frustration: How the Afghan conflict has changed since the Doha agreement. *Afghanistan Analysts Network*, https://www.afghanistan-analysts.org/en/reports/war-and-peace/taleban-opportunism-and-ansf-frustration-how-the-afghan-conflict-has-changed-since-the-doha-agreement/

Ruttig, T. and Sadat S. A. (2021, August 14). The Domino Effect in Paktia and the Fall of Zurmat: A case study of the Taleban surrounding Afghan cities. *Afghanistan Analysts Network*. https://www.afghanistan-analysts.org/en/reports/war-and-peace/the-domino-effect-in-paktia-and-the-fall-of-zurmat-a-case-study-of-the-taleban-surrounding-afghan-cities/

Sabawoon, A. M. (2021, August 4). Taleban Victory or Government Failure? A security update on Laghman province. *Afghanistan Analysts Network.* https://www.afghanistan-analysts.org/en/reports/war-and-peace/taleban-victory-or-government-failure-a-security-update-on-laghman-province/

Sanger, D. E. et al. (2020, March 8). A Secret Accord with the Taliban: When and How the U.S. Would Leave Afghanistan. *The New York Times*. https://www.nytimes.com/2020/03/08/world/asia/taliban-afghanistan-annexes-peace-agreement.html

Schroden, J. (2021). Lessons from the Collapse of Afghanistan's Security Forces. *Combatting Terrorism Center at West Point 14* (8), 45-46.

Special Inspector General for Afghanistan Reconstruction (SIGAR). (2023). *Why the Afghan Forces Collapsed*. SIGAR Evaluation Report. https://www.sigar.mil/Reports/Article-Display/Article/3997656/why-the-afghan-security-forces-collapsed/

SIGAR. (2020, July 30). *Quarterly Report to Congress*. https://www.sigar.mil/Reports/Article-Display/Article/4022083/july-30-2020-quarterly-report-to-congress/

UNAMA. (2021, July 26). Civilian Casualties Set to Hit Unprecedented Highs in 2021 Unless Urgent Action to Stem Violence. UN Report. https://unama.unmissions.org/civilian-casualties-set-hit-unprecedented-highs-2021-unless-urgent-action-stem-violence-%E2%80%93-un-report

US Department of State. (2020, February 29). *Agreement for Bringing Peace to Afghanistan between the Islamic Emirate of Afghanistan Which Is Not Recognized by the United States as a State and Is Known as the Taliban and the United States of America*. https://www.state.gov/wp-content/uploads/2020/02/Agreement-For-Bringing-Peace-to-Afghanistan-02.29.20.pdf.

Van Bijlert, M. &AAN Team. (2021, December 28). Afghanistan's Conflict in 2021 (1): The Taleban's sweeping offensive as told by people on the ground. *Afghanistan Analysts Network.* https://www.afghanistan-analysts.org/en/reports/war-and-peace/afghanistans-conflict-in-2021-1-the-talebans-sweeping-offensive-as-told-by-people-on-the-ground/

Watling, J. et al. (February 2022–February 2023). *Preliminary Lessons from Russia's Unconventional Operations During the Russo-Ukrainian War*. Special Report. Royal United Services Institute, 2023. https://www.rusi.orghttps://www.rusi.org.

Zucchino, D. & Rahim, N. (2021, May 27). A Wave of Afghan Surrenders to the Taliban Picks Up Speed. *The New York Times*, https://www.nytimes.com/2021/05/27/world/asia/afghan-surrender-taliban.html

Ruttig, T. (2021, February 25). A Deal in the Mist: How much of the US-Taleban Doha agreement has been implemented? *Afghanistan Analysts Network*. https://www.afghanistan-analysts.org/en/reports/war-and-peace/a-deal-in-the-mist-how-much-of-the-us-taleban-doha-agreement-has-been-implemented

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
"United Against Terrorism: Securing the Future"
PANEL 2

Panel 3: Integrating Multi Domain Operations (MDO) into Counter-Terrorism (CT)

Integrating MDO Principles into CT Strategy: A Doctrinal Shift

BG (ret.) Russell D. HOWARD, President of Howard's Consulting Services, and Distinguished Senior Fellow at the Joint Special Operations University.

The Civilian Component of Multi-Domain Principles and CT Strategy

Civil-Military Operations and Their Role in Counter-Terrorism

Civil-Military Operations (CMO) are an essential element of modern Counter-Terrorism (CT) strategies, serving as a bridge between security forces and civilian populations in conflict or post-conflict environments. These operations aim to foster stability, enhance legitimacy, and address the social, economic, and political conditions that often give rise to extremism. In essence, CMO represent the non-kinetic dimension of CT, complementing military force with efforts that build trust, promote governance, and reduce the appeal of violent ideologies. By engaging with communities, supporting development, and strengthening institutions, Civil-Military Operations help undermine the root causes of terrorism while ensuring sustainable peace and stability.

The Concept and Framework of Civil-Military Operations

Civil-Military Operations are defined as activities conducted by military forces to establish, maintain, or influence relationships between military organizations, civil authorities, and the civilian population. The objective is to facilitate the accomplishment of the military mission while supporting broader political and humanitarian goals. In CT contexts, CMO are designed not merely to win battles but to win hearts and minds, a strategic necessity in asymmetric warfare, where the population’s support often determines success or failure.

CMO typically involve coordination among military units, local governments, international organizations, and non-governmental organizations (NGOs). Their focus areas include humanitarian assistance, infrastructure development, governance support, public information, and security cooperation. When applied effectively, these operations enhance the legitimacy of the host nation government and reduce the influence of terrorist groups that exploit social grievances and governance vacuums.

Building Trust and Legitimacy

One of the most significant contributions of CMO to CT is the establishment of trust between the state and its citizens. Terrorist and insurgent groups thrive in environments where populations feel alienated, oppressed, or abandoned by their governments. In such settings, extremists exploit distrust and provide alternative sources of authority, protection, or welfare. CMO work to reverse this dynamic by demonstrating the state’s commitment to the well-being of its people.

Through humanitarian assistance programs, medical outreach, education initiatives, and disaster response, military forces can project an image of compassion and reliability. For example, in regions affected by terrorism, such as parts of the Sahel or Southeast Asia, CMO teams have conducted health clinics, distributed food, and repaired essential infrastructure. These actions humanize the military presence and counter extremist propaganda that depicts government forces as hostile or indifferent. As trust deepens, communities are more likely to share intelligence, resist recruitment, and cooperate with CT operations.

Enhancing Stability and Security

CMO also play a vital role in creating stable environments where CT efforts can succeed. Stability is not merely the absence of conflict but the presence of legitimate institutions capable of maintaining order and delivering essential services. CMO contribute to this stability by strengthening local governance, restoring basic services, and facilitating reconstruction in conflict-affected areas.

For instance, during post-conflict stabilization in Iraq and Afghanistan, Civil Affairs units worked alongside civilian agencies to rebuild schools, repair roads, restore electricity, and train local police. Although these efforts were not without challenges, they demonstrated how military involvement in reconstruction could help transition from combat operations to sustainable peace. By improving living conditions and reinforcing public order, CMO reduce the social and economic vulnerabilities that terrorist groups exploit.

Moreover, CMO help establish safe spaces for humanitarian organizations and local authorities to operate. By providing security for development projects, Civil-Military teams ensure that progress is not undone by continued violence or intimidation. This collaboration between security and development actors creates a positive feedback loop: as stability improves, the need for military presence declines, and governance structures become more self-sufficient.

Addressing the Root Causes of Extremism

Terrorism rarely emerges in a vacuum. It often takes root in conditions of poverty, political exclusion, ethnic tension, and weak governance. While military force can neutralize immediate threats, lasting CT success depends on addressing these underlying causes. CMO provide a framework for doing so through community engagement, conflict resolution, and support for inclusive governance.

For example, CMO teams frequently facilitate dialogues between local leaders, religious authorities, and government representatives to address grievances and prevent radicalization. By involving local voices in decision-making, these operations enhance the sense of ownership and reduce the allure of extremist ideologies. In Nigeria’s fight against Boko Haram, for instance, civil-military cooperation programs have emphasized education, youth empowerment, and community resilience as tools to prevent recruitment and rebuild trust in state institutions.

Furthermore, CMO can support economic development initiatives that provide alternatives to violence. Job creation, vocational training, and microfinance programs help reintegrate former combatants and give vulnerable populations a stake in peace. When communities see tangible benefits from stability, extremist narratives lose credibility and support.

Integration with Broader CT Strategies

CMO are most effective when integrated into comprehensive CT strategies that combine security, governance, and development. In this approach, military and civilian agencies work together under a unified framework to achieve long-term objectives. The U.S. military's concept of 'whole-of-government' operations, for example, emphasizes coordination among defense, diplomacy, and development efforts. Similarly, the United Nations promotes 'Integrated Mission Planning,' which aligns military stabilization with political and humanitarian goals.

Effective integration requires clear communication, shared objectives, and mutual respect between military and civilian actors. Civil Affairs personnel often act as mediators, ensuring that military actions support -not undermine- local governance and human rights. This coordination minimizes duplication of effort and ensures that CT operations do not alienate the very populations they aim to protect.

Moreover, intelligence derived from Civil-Military engagement can inform more precise and ethical military operations. Local partnerships often yield insights into terrorist networks, recruitment patterns, and community dynamics that traditional intelligence methods cannot capture. In this sense, CMO contribute both to the 'soft' and 'hard' dimensions of CT.

Challenges and Limitations

Despite their advantages, CMO face several challenges. Coordination between military and civilian agencies can be complex due to differing mandates, cultures, and priorities. Excessive militarization of humanitarian space may also raise concerns among NGOs and local populations, potentially undermining trust. Furthermore, if CMO are not carefully planned, they risk being perceived as tools of occupation or propaganda, especially in areas with a history of foreign intervention.

Resource constraints and political instability can also limit the effectiveness of CMO. Sustained progress requires long-term commitment, but many operations are constrained by short funding cycles or shifting political priorities. Additionally, success depends heavily on the competence and integrity of local partners; without effective governance, even the best Civil-Military initiatives may struggle to produce lasting change.

Nonetheless, these challenges can be mitigated through transparency, collaboration, and adherence to humanitarian principles. Continuous training, cultural awareness, and monitoring mechanisms can ensure that CMO remain credible and beneficial to local communities.

Conclusion

CMO represent a vital bridge between security and development in the global fight against terrorism. By building trust, enhancing stability, and addressing the root causes of extremism, CMO provide a sustainable pathway toward peace and resilience. They demonstrate that CT is not solely a military endeavor but a multidimensional effort that requires partnership, empathy, and strategic patience.

In a world where terrorism adapts rapidly and exploits human vulnerability, CMO offer a powerful tool to strengthen societies from within. Through collaboration, compassion, and commitment, they help transform conflict zones into foundations for peace, fulfilling the ultimate goal of CT: not only to defeat terrorists but to eliminate the conditions that allow terrorism to thrive.

Multi-Domain Operations and Counter-Terrorism: Challenges for NATO

Dr. Andrea GILLI, Lecturer in Strategic Studies at the University of St Andrews, Associate Fellow of the Institute of European Policy-Making of Bocconi University, and Expert Mentor of NATO DIANA.

Introduction

In the twenty-first century, NATO faces an increasingly complex security landscape where the boundaries between conventional warfare, hybrid conflict, and terrorism have become blurred. The Alliance's evolving doctrine of Multi-Domain Operations (MDO) - originally designed for state-on-state competition- must now adapt to counter the fluid, networked, and technologically empowered terrorist threats of today. This paper explores how MDO can inform and transform NATO's approach to counter-terrorism (CT). It begins by tracing the doctrinal origins of MDO, then examines how non-state actors are exploiting the diffusion of dual-use technologies to operate across multiple domains. It assesses the operational and organizational challenges this poses for NATO, draws on recent lessons from high-intensity urban warfare, and concludes with policy recommendations to ensure that the Alliance remains both effective and cohesive in confronting twenty-first-century terrorism.

Origins and Logic of Multi-Domain Operations

The concept of Multi-Domain Operations emerged from the recognition that modern warfare transcends the traditional domains of land, sea, and air. Contemporary conflicts are fought simultaneously in space, cyberspace, and increasingly within the information and cognitive spheres. Originally, MDO was developed to counter Anti-Access/Area-Denial (A2/AD) environments created by peer competitors. Its purpose was to integrate capabilities across all domains to generate synchronized effects, disrupting adversary command chains, penetrating contested spaces, and maintaining escalation control. By linking land manoeuvre with space-enabled targeting, cyber-disruption, and information operations, MDO aims to create tempo and decision superiority across a connected battlespace. Yet, the same principles that make MDO effective against major powers are also essential for confronting adaptive terrorist organizations. Today's non-state actors exploit the same technological interdependencies and vulnerabilities that MDO seeks to master. They operate across domains, blur the line between war and peace, and weaponize technologies once monopolized by states.

Terrorism in the Multi-Domain Age

Terrorism has entered a new technological phase. The lowering of technological barriers—especially in drone production, communications, and digital infrastructure—has enabled non-state actors to operate across land, air, sea, cyber, and cognitive domains simultaneously. Commercial drones have been weaponized for reconnaissance, surveillance, and attack. Across several theatres—from the Sahel to the Levant—terrorist networks have deployed low-cost unmanned systems capable of delivering explosives or conducting real-time aerial intelligence. These systems erode conventional militaries' monopoly on airpower and provide tactical agility at minimal cost. In the cyber and information domains, encrypted messaging platforms and social media ecosystems have transformed how terrorists communicate, recruit, and influence.

Sophisticated use of digital tools enables decentralized command, algorithmic targeting of potential recruits, and the amplification of extremist narratives. Cyberattacks on government databases, energy grids, and communication networks illustrate how terrorists have learned to exploit the connectivity of advanced societies. Some have even employed electronic warfare techniques—jamming or spoofing signals to mislead surveillance and navigation systems. In this environment, the distinction between physical and virtual battlefields collapses. Terrorist campaigns now span multiple domains, seeking not only to inflict casualties but also to undermine trust, disrupt governance, and manipulate perceptions. The battlefield is as much cognitive as kinetic.

Applying MDO Principles to Counter-Terrorism

Offensive Implications

Modern counter-terrorism operations must be multi-domain by design. Recent campaigns against technologically enabled militant networks demonstrated that the integration of air, space, and naval assets with cyber and information operations can create converging effects. Precision airstrikes guided by space-based sensors degraded terrorist capacity, while cyber and information operations targeted propaganda networks and recruitment pipelines. However, these operations also revealed the limits of traditional command structures. Terrorists have adapted by embedding within civilian populations and exploiting complex urban terrain, effectively neutralizing conventional advantages. In such settings, command-and-control (C2) must fuse data from multiple domains to enable rapid, precise, and discriminating targeting. Machine learning, sensor fusion, and AI-enabled decision support systems are essential to achieving the tempo and accuracy required in densely populated areas.

Defensive Implications

Defensively, NATO must anticipate that terrorist organizations will continue exploiting emerging technologies and hybrid tactics. The democratization of innovation means that capabilities once exclusive to state militaries—such as autonomous systems, cyber intrusion tools, and artificial-intelligence-based propaganda—are now accessible to small, dispersed groups. This poses risks far beyond the battlefield. Attacks on critical infrastructure, transportation networks, and communication systems could disrupt Allied societies even in peacetime. Counter-terrorism, therefore, must not only locate and neutralize terrorists abroad, but also defend against their penetration into Allied information systems and social fabric. An MDO-inspired CT posture must integrate defensive cyber operations, infrastructure protection, and societal resilience. The goal is to create a multi-layered defence architecture that extends from forward-deployed forces to domestic institutions and the civilian population.

Organizational and Political Challenges for NATO

Command-and-Control Complexity

MDO demands fluid coordination across domains, services, and nations. Traditional hierarchical C2 systems are ill-suited to the speed and simultaneity of modern operations. NATO must build distributed, data-driven C2 architectures that allow for real-time information sharing and decentralized decision-making across the Alliance. However, this faces both technical and political barriers. Cross-domain synchronization requires deep integration of national intelligence systems—raising issues of trust, classification, and sovereignty. Building a truly interoperable MDO C2 system within a 32-nation alliance will require not only technology but also diplomacy.

The Cost and Pace of Digitalization

Implementing MDO is resource-intensive. It requires resilient communications networks, high-bandwidth data links, secure cloud environments, and AI-enabled analytics. These investments compete with other priorities in national defence budgets and demand continuous upgrading as technologies evolve.

Uneven Technological Capacity Among Allies

A further risk lies in widening capability gaps. Larger allies—especially those with advanced defence industries—are likely to adopt digitalized, AI-enabled operational concepts faster than smaller members. Unless NATO establishes mechanisms for technology sharing and capability pooling, MDO could unintentionally undermine Alliance cohesion by creating "two-speed interoperability."

Blurred Civil-Military Boundaries

Finally, modern terrorism operates across domains that are not exclusively military. Cyberattacks on hospitals or propaganda campaigns on social media cannot be countered by armed forces alone. MDO in counter-terrorism therefore demands whole-of-government and whole-of-society integration—linking the military with intelligence services, law enforcement, private industry, and civil society.

Operational Lessons from Recent Urban Campaigns

Recent high-intensity urban operations offer important insights for NATO's approach to multi-domain counter-terrorism. Analyses from multiple researchers have highlighted several key lessons relevant to MDO—lessons that are generalizable beyond any specific conflict. First, urban warfare is no longer a sequential fight from above ground to underground; it is a simultaneous, multi-layered struggle across physical and electromagnetic spaces. Forces must operate above, below, and through dense infrastructure, maintaining continuous surveillance and communication despite obstruction and debris. Second, urban environments generate extreme C2 and mobility challenges. Rubble, destroyed landmarks, and electromagnetic congestion complicate navigation and identification. Without reliable, real-time data integration, even technologically superior forces can lose situational awareness. Third, the proliferation of unmanned aerial systems (UAS) on both sides of a conflict saturates the electromagnetic spectrum, creating risks of fratricide and forcing constant adaptation of airspace management. This highlights the importance of electromagnetic-spectrum dominance as a new operational domain within MDO. Fourth, the information domain can be strategically decisive. Even highly capable militaries may find that tactical success on the ground is offset by the loss of narrative control in the information environment. Adversaries who skillfully manipulate images, stories, and perceptions can erode legitimacy and strategic patience faster than kinetic attacks. Fifth, the provision of humanitarian assistance has become an operational factor in itself. The destruction of urban infrastructure complicates civilian relief, while adversaries can exploit humanitarian dynamics for political gain. Effective MDO thus requires planning for stabilization, governance, and communication as integral components of operations—not as afterthoughts. Together, these lessons underscore that in modern conflict—whether against state or non-state actors—the domains are interdependent. Success depends on synchronizing military power, information control, and societal resilience in a unified campaign plan. For NATO, the implication is clear: counter-terrorism operations must prepare for multi-domain saturation—urban, cyber, informational, and psychological—all occurring at once.

Policy and Operational Recommendations

Modernizing Command-and-Control

NATO should prioritize the modernization of its C2 architectures to enable rapid, distributed, and cross-domain operations. This entails: Developing AI-assisted data-fusion systems that integrate intelligence from space, cyber, and human sources. Building resilient, redundant communications to sustain decision-making under electronic attack. Training commanders to operate within multi-domain decision loops, emphasizing flexibility, initiative, and decentralized execution.

Collaborative Investment and Capability Pooling

To avoid widening technological gaps, NATO must establish shared development programs for key MDO enablers—such as sensor networks, autonomous platforms, and electromagnetic-spectrum management tools. Joint investment frameworks and technology-transfer mechanisms should ensure that all allies, large and small, can participate meaningfully in the MDO transition.

Whole-of-Government and Whole-of-Society Integration

Counter-terrorism in the multi-domain era cannot be a purely military function. The Alliance should expand structured cooperation between NATO commands, national intelligence agencies, law enforcement, and private-sector critical-infrastructure operators. Additionally, establishing national multi-domain coordination cells linked to NATO headquarters to synchronize military, cyber, and civil responses is fundamental. Conducting multi-domain exercises that simulate attacks on infrastructure, disinformation campaigns, and cyber incidents alongside traditional kinetic operations would also help.

Building Strategic Resilience

Resilience must become a central pillar of NATO's CT posture. This includes protecting information systems, energy grids, and communication networks from hybrid attacks; promoting digital literacy and civic education to strengthen societal immunity against manipulation and radicalization; and finally, integrating public communication, cyber defence, and infrastructure protection into a unified deterrence framework. In essence, NATO must view resilience not only as the ability to recover from attacks but as a continuous process of adaptation—technological, institutional, and psychological.

Conclusion

Multi-Domain Operations provide NATO with a powerful conceptual framework for addressing the evolving terrorist threat landscape. They compel the Alliance to think holistically—linking physical, cyber, and cognitive dimensions of conflict; integrating military and civilian instruments of power; and preparing for simultaneous operations across domains. Yet the adoption of MDO in counter-terrorism also exposes key vulnerabilities: the complexity of multinational coordination, disparities in technological capacity, and the need to sustain political unity amid digital transformation. Overcoming these challenges will require sustained investment, cultural change, and a clear vision of how NATO defines success in an age where deterrence, disruption, and defence are inseparable. As I have emphasized elsewhere, counter-terrorism in the multi-domain era is no longer just a military task. It is a collective, cross-sectoral effort to protect the stability, resilience, and legitimacy of Allied societies. The future of NATO's counter-terrorism posture lies in its ability to integrate across domains, disciplines, and communities, ensuring that technological superiority is matched by institutional agility and strategic coherence.

Wargaming Counter-Terrorism in The MDO Environment

Jan HEINEMANN, Guest lecturer at the German Command and Staff College, Board Director for Fight Club International, Coordinator for Fight Club Deutschland, member of the Connections Online wargaming conference organizing staff, Admin Wargaming and Europe for the International Kriegsspiel Society.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: ...ing the Future"
Mr. Jan HEINEMANN

Introduction

Wargaming as a critical method provides synthetic experiences in a competitive safe-to-fail-environment and a framework for teaching, analyzing and exploring Counter- Terrorism (CT) in a Multi-Domain Operations (MDO) environment beyond the classic kinetic understanding of warfare. Employing models and intertwined mechanisms highlighting the interdependency of domains and importance of information, psychological, cyber and hybrid warfare prompts towards the complexity of future CT operations and highlights the necessity of civilian, societal and cultural harm mitigation and capabilities as an integral part of NATO wargaming efforts. Applying wargaming efforts on a broad scale throughout the alliance will foster civilian, societal and cultural, as well as military resilience against future terrorist threats and develop crucial skills and capabilities to counter them.

Wargaming

After 200 years since its establishment professional wargaming is on the rise again, as it is being (re-)implemented on a broad scale across NATO and partner, as well as competing nations. While the Prussian Chief of the General Staff von Müffling claimed “this is not a game, it is a school for war” when reviewing Reisswitz’ Kriegsspiel in 1824, it is important to note that wargaming as a critical method has diversified in its military application at the end of the 19th and during the early 20th century, after which it was also applied for investigating political, economic, diplomatic and social aspects of reality and is used in plenty of formats and for many purposes today.

Although the professional wargaming community has still not managed to settle the everlasting debate of what a wargame specifically is and isn’t, nor proposed a definitive catalogue of wargaming formats and standardizations, there are a number of definitions with considerable overlap. NATO defines wargames as “representations of conflict or competition in a safe-to-fail environment, in which people make decisions and respond to the consequences of those decisions”. Usually this includes human players competing against each other under the condition of uncertainty, communication and time and/or resource constrains, creating synthetic experiences within a model of reality which translates data into a simulation based on human interaction confined by game mechanisms.

Wargames are specifically designed and applied for three different purposes: as tools for education, analysis or research and exploration. Because wargames are abstracted models of reality steered by human interaction, they can never provide definite answers, but can greatly inform decision-making, convey understanding of structural conditions, interdependencies of various factors and ideally help identifying black swans, that is finding the unknown unknowns.

Designing, facilitating and analysis wargames requires a wide range of professional skills and knowledge.

Wargaming Counter-Terrorism in MDO

The prolific wargame designer Brian Train who specialises in asymmetric warfare and the representation of civilians in wargames has identified four key elements of terrorism:

- Terrorism's power lies in its psychological effect.
- Its effect is nonlinear, but not completely unpredictable.
- Information, intelligence and communication networks are paramount.
- Resilience trumps terrorists' tactical initiative.

Wargaming CT in the multi-domain environment must thus focus on the aspect of cognitive warfare which includes psychological and influence warfare as well as the information environment beyond the classical domains of land, air, sea, space, cyber and electronic spectrum. Its goal has to be to identify critical capabilities, requirements and vulnerabilities of society, civic and military actors impacting and being impacted by terrorist operations in order to solve the core issue of the multi-domain operations doctrine: its lack of a theory of success which can be put to the test and falsified in order to be improved. Such theory should be informed by thorough analysis of past counterterrorism operations, social studies research on qualitative data concerning the human factor. This might be a challenge for purely military institutions and highlights the necessity for civil-military cooperation and expansion of institutionalized wargaming capabilities on all levels.

Keith Scott has provided a model for gaming multi-domain operations which can be adapted based on the subject of interest and used to identify aspects and interdependencies of crucial importance to be included in the model. He suggests joining the PMESII (Political, Military, Economic, Social, Infrastructure, Information) and ASCOPE (Area, Structures, Capabilities, Organizations, People, Events) frameworks to form a base-layer matrix. This matrix can be expanded into the third dimension by either domains (land, sea, air, space, cyber, electronic), DIME (Diplomacy, Information, Military, Economy), levels of operations (tactical, operational, strategic), five ways of attack (disrupt, deny, degrade, destroy, deceive) or other contexts of interest. In order to operate such complex models, the use of technologies such as virtual and augmented reality, computer simulation and AI might assist the design and facilitation process, but should not replace manual play and facilitation as a basis for training and analysis.

Mechanisms

Wargaming formats range between free Kriegsspiel and rigid Kriegsspiel formats, that is ad-hoc facilitation with no to little mechanisms and complex sets of rules and mechanisms with little leeway in facilitation. Which format suits the purpose of a game best is defined by requirements and goals. Some mechanisms lend themselves well to wargaming multi-domain operations. This list, however, is not extensive and should be understood as a source of inspiration:

• Matrix wargames are argument-based games exploiting subject matter expertise to gain (analytical insights into specific scenarios. Each player represents an actor, faction or country and may suggest an event, its effects and three arguments why they believe it would likely occur within the reality of the game world, after which everybody around the table has the opportunity to suggest one argument against. The facilitator or a committee of subject matter experts rates the arguments and a modified die-roll decides whether or not or to which degree the event occurs.

• Civilian Harm Mitigation and Response and Cultural Property Protection wargames such as Horizon Strike include mechanisms for the behavior, role and impact of operations by and on civilians, which might be governed by a game system or human players.

• Littoral-Commander and Multi-Domain Brigade Operations are classic hex-and-counter (or block) wargames expanded by domain specific sets of Joint Capability Cards providing capabilities within air, submarine, autonomous, cyber, space, electronic, influence, information areas of operation.

• Maneuver Warfare provides a multi-domain operations model completely card based and heavily inspired by Magic the Gathering and other card-trading games. This allows high flexibility in the combination and application of capabilities in various domains for different effects.

• Malign uses card combinations to represent influence and information warfare with different degrees of effects.

• Pax Pamir combines capability card and court management with adaptable domain focus to highlight the complexity and influence of combined action chains within different domains (Politics, Economic, Military, Information).

Cards and shifting domain focusses are one of many feasible ways to model multi-domain operations in manual wargames. Computer simulation and technology assisted games are capable of modelling the simultaneity of operations, highlighting the necessity of speed and adaptability of capabilities and action execution, potentially at a risk of preventing profound understanding of interdependencies and the impact of individual factors on the whole. However, this selection of mechanisms in abstract models of multi-domain environments prove that MDO wargames can be designed and played by a wide range of personnel throughout the alliance and can inform CT operations and strategy development.

Conclusion

In a global world of growing technological, social, cultural and political complexity, wargaming can provide the insights and help develop skills necessary for states, militaries, NGOs, and other actors to understand, adapt and exploit dynamics and developments threatening peace development and stability in order to mitigate harm and increase the efficiency of operations. Institutionalizing and further developing the method is thus of crucial importance.

Wargaming is a critical method for training personnel, developing foresight and organizational and societal resilience, understanding systemic conditions and dynamics, as well as one own and opponents' availability and lack of capabilities, and detecting potential blind spots well in advance. Wargaming CT in a Multi-Domain Environment demands an open-ended approach, interdepending mechanism to properly represent the human factor, electronics, cyber, hybrid and information warfare on top of kinetic operations through all domains.

Recommendations for NATO

• Modelling MDO in a playable yet meaningful way might be hard, but not as difficult as is often claimed.

• Bringing in civilian wargamers and designers helps pushing the limits, foster understanding of current trends and helps building wargaming capabilities throughout the Alliance.

• NATO should prompt its members to institutionalize wargaming on all levels.

• Playing wargames with civic decision-makers and civilians helps increasing overall societal resilience (against hybrid and terrorist attacks, climate change, radicalization etc.). Those who are not 'blinded by doctrine' and come from diverse backgrounds can provide valuable perspectives which might otherwise be missed.

• The complexity of future conflict demands concepts that provide mitigation of civilian, societal and cultural harm, which need to be considered an integral part of all wargaming activities.

• Within its concept of 'unrestricted warfare' the PLA understands wargaming as part of warfighting and begins fostering civil-military wargaming cooperation formats similar to Fight Club International, and so should NATO and its member states.

Bibliography

Bae, S. J., ed. (2022). *Forging Wargamers. A Framework for Professional Military Education*. Marine Corps University Press. https://www.usmcu.edu/Portals/218/Forging%20Wargamers_web.pdf.

Caffrey M. (2019). *On Wargaming. How Wargames Have Shaped History and How They May Shape the Future.* https://www.govinfo.gov/content/pkg/GOVPUB-D208_200-PURL-gpo120656/pdf/GOVPUB-D208_200-PURL-gpo120656.pdf.,

Curry, J., Ed.(2012). *Peter Perla's The Art of Wargaming. A Guide for Professionals and Hobbyists*. History of Wargaming Project, London.

Ellison, D. & Sweijs, T. (2024, January 22). Empty Promises? A Year Inside the World of Multi-Domain Operations. *War On The Rocks*. https://warontherocks.com/2024/01/empty-promises-a-year-inside-the-world-of-multi-domain-operations/.

Grandi, M.; Keenan, M. & van der Zeijden, W. (2022, March 22). *Future Wars. Protecting Civilians in High-Intensity Urban Warfare*. https://www.stimson.org/2022/future-wars-protecting-civilians-in-high-intensity-urban-warfare/.

Lund-Hansen, K. & Reilly, J. (2024, November 11). The Multi-Domain Operations Approach to Intermediate PME. *War Room*. https://warroom.armywarcollege.edu/articles/competencies-6/.

NATO Modelling & Simulation Centre of Excellence. (2025). Learning From Wargaming And Foresight Methodologies And Practices Applied To Education And Training For Multi-Domain Operations. *2024 Annual Review*, Vol. 7. Rome.

Paul, C., Wong, Y. H. & Bartels, E. M. (2022). *Opportunities for Including the Information Environment in U.S. Marine Corps Wargames*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2900/RR2997/RAND_RR2997.pdf.

Perla, P. P. & McGrady, ED. (2011). Why Wargaming Works. *Naval War College Review 64* (3) https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1578&context=nwc-review.

Roberts, B. (Ed.). (2021). *Getting the Multi-Domain Challenge Right*. Lawrence Livermore National Laboratory.

SAS-172 Multi-Domain Operations Wargame Research Task Group. (2023, September 06). Connections UK Conference. https://www.professionalwargaming.co.uk/23-MDWargaming.pdf.

Scott. K. (2022). 'Out Beyond Jointery': Developing a Model for Gaming Multi-Domain Warfare. In *Proceedings of the 17th International Conference on Information Warfare and Security* (pp. 599-608). Reading.

DAY 2

October 16, 2025

Panel 4: Innovating Security: The Role of Technology in Counterterrorism

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL
DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism Securing the Future"
Ms. Jessa MALLEA

Digital Interventions in Online Terrorism

Ms. Jessa MELLEA, Incident Response Associate at the Global Internet Forum to Counter Terrorism (GIFCT).

The Global Internet Forum to Counter Terrorism (GIFCT) is a unique tech-led non-profit organization dedicated to preventing terrorists and violent extremists from exploiting digital platforms. GIFCT brings together more than 35-member technology companies and works closely with governments, civil society, practitioners, and academia to advance collective counterterrorism efforts.

We have seen that adversarial actors like terrorist groups have adapted their strategies both online and offline in light of counterterrorism efforts. As they move to diversify their online presence and methods, it is vital to create opportunities for cross-sector and cross-platform collaboration and communication, allowing platforms to learn from each other and identify common solutions.

Multistakeholderism is a key tenet of our work with GIFCT, and we work closely with key stakeholders from industry, government, civil society, and academia to foster essential collaboration and information-sharing to counter terrorist and violent extremist activity online, all the while working with our own counterterrorism and technical experts.

GIFCT advances collective efforts to disrupt terrorism and violent extremism (TVE) online by supporting its members with tools and interventions to better understand and address online harms. The organization works to prevent the exploitation of digital platforms by terrorists and violent extremists (or TVE actors) through four key tools: cross-platform information sharing, the hash-sharing database (HSDB), global research and analysis, and the Incident Response Framework (IRF).

At GIFCT we recognize that preventing and countering TVE requires a whole-of-society approach, and no single sector or state can alone address the myriad of challenges or leverage all of the opportunities.

The online threat landscape today is inherently cross-platform and transnational. TVE actors create vast online networks to recruit and engage members from around the world. The relative ease with which individuals can find and participate in these networks has led to an increase in the overlap and blending of various types of violent extremist ideologies, as well as different online harm types, such as the production of child sexual abuse material (CSAM).

TVE actors are also savvy internet users, creating and iterating on new tactics to avoid moderation and disruption by platforms. The networks they create across various platforms are designed to be resilient to moderation attempts, both by exploiting specific features of different online platforms and by maintaining several points of contact with members in the event one is taken down. In the ever-changing online landscape, solution building must also be cross-platform, international, as well as multi-sector by nature, and GIFCT works to facilitate this process.

Preventing this exploitation requires a cooperative approach. GIFCT serves as a platform for fostering information-sharing and collaboration among our members; both in signal sharing and solution development.

GIFCT maintains communication channels between members and facilitates strategic engagements, allowing tech companies to share vital information about TVE content (TVEC) online, emerging trends, and strategies to disrupt TVE activity.

GIFCT facilitates not only signal sharing, but also knowledge sharing and knowledge production. We advance understanding of TVE through an academic research arm, based in Kings College London, the Global Network on Extremism and Technology (GNET), which offers our members and the wider community open access to cutting edge research and analysis on the intersections of tech, terrorism, and counterterrorism.

The organization also produces research internally, based on the needs of member companies, including bespoke reports and analysis, expert briefings, and workshops.

Beyond these resources, our multistakeholder Working Groups serve as platforms for collaboration among industry, government, and civil society, to share information on trends, solutions and good practices. 2025 Working Groups focus on the following three themes: Investigators Community of Practice; Artificial Intelligence: Threats and Opportunities; and Addressing Youth Radicalization and Mobilization.

Another key tool is the hash-sharing database. GIFCT maintains the HSDB for known terrorist content, designed to support member companies in identifying and responding to harmful content in line with their own policies. It allows the sharing of hashes, or digital fingerprints, rather than the content itself or any private user information associated with it.

Finally, the incident response framework allows GIFCT to work with members and external partners to respond to the online dimensions of offline terrorist and mass violence attacks. The IRF has been activated 10 times in 2025 as of October and was recently revised following a consultation with a wide variety of stakeholders across various industries, including an independent review of GIFCT's incident response policies and a multi-stakeholder Working Group. This revised version of the IRF creates a more streamlined process designed to respond to the current threat landscape and the needs of our member companies.

The IRF now consists of three types of activations, each designed to respond to a different scenario: The Perpetrator Content Incident (PCI), Digital Footprint Incident (DFI), and Incident Advisory.

The PCI is a protocol that is activated in response to a terrorist or violent extremist event where a piece of content was produced as part of the event and is circulating online. During this response, GIFCT coordinates intel sharing among our members and stakeholders. In the PCI protocol, TVEC is hashed and added to the HSDB to aid moderation efforts.

The DFI is a similar protocol that occurs when there is evidence of online behavior of a perpetrator of a terrorist or violent extremist attack that is related to the event, but not produced as part of the attack. In these cases, there is not hashable content, but GIFCT provides a variety of other forms of support to members, including sharing relevant open-source intelligence findings, conducting bespoke research, and providing language assistance.

Finally, the incident advisory, unlike the PCI and DFI, is a flexible framework designed to respond to events that are not obviously time bound in the short-term. For every incident advisory, GIFCT alerts members and its Independent Advisory Committee, then assesses what actions are needed, such as specific guides for our members, targeted support, bespoke research, and more.

In all its work, GIFCT remains committed to protecting human rights. A commitment to respecting human rights is key criteria for tech companies to become GIFCT members. Centering our respect for fundamental and universal human rights in our membership criteria ensures that our work to develop technical solutions and resources is grounded in the values of the organization.

AI and Machine Learning for Terrorist Threat Detection: Policy Implications and Operational Use

Dr. Thomas W. SPAHR, Associate Professor at the U.S. Army War College.

Ankara/TÜRKİYE
15-16 October 2025
"United Against Terroris... curing the Future"
CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO
OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE &

Global military powers are investing in methods to employ artificial intelligence (AI) in warfare, primarily focused on great power competition, but with equal applicability to the enduring threat of terrorism. This essay describes ways NATO military and police forces can use AI to detect and disrupt terrorist operations. It argues that NATO must integrate AI into counterterrorism to keep pace with its adversaries. The essay identifies opportunities to exploit AI throughout the stages of a terrorist attack, then describes an early application of AI to predict insurgent attacks in Afghanistan in 2020. NATO should apply AI to identify and interdict terrorist operations across the terrorism execution cycle. This requires investment in expertise and open-source intelligence, as well as partnerships with the commercial sector, and a culture that is willing to experiment with innovative technologies. NATO should simultaneously lead efforts to establish governance surrounding the use of AI in warfare. To lead efforts to govern AI, NATO must understand and be capable with this technology.

Advances in Technological Applications to Intelligence

The growing importance of the internet, cloud technology, and AI has transformed military intelligence and targeting. Soon, militaries will primarily collect, store, and correlate information using artificial intelligence. A famous example of failed intelligence correlation is the missed indicators before the September 11, 2001 attacks on the United States. Computer-assisted screening systems at airports selected 10 of 19 terrorists for additional investigation, but these alerts weren't put together and considered in the context of reports of Arab males associated with terrorist groups training to fly aircraft (National Commission on Terrorist Attacks upon the United States, 2004, p. 271, 451, Note 2). There was too much data for humans to process in 2001, and the challenge is exponentially greater today. Analysts in the future must look across the terrorist planning cycle using AI to analyze different data sets like criminal databases, airport travel logs, and security cameras, then push anomalies and indicators to All

Source analysts augmented by AI to build the entire picture (Lowrance & Pfaff, 2025, pp.101-104). Cloud technology enables analysts to coordinate and access volumes of publicly-available data, work collaboratively from anywhere, and to run algorithms against these large data pools (CSIS, 2025). AI will enhance analytical capability across the intelligence cycle.

A related development is the emergence of open-source intelligence (OSINT) and publicly available information as critical sources of intelligence. Several senior intelligence leaders have recently argued that intelligence analysis should now rely on 80% open source and 20% classified material, versus the opposite ratio practiced in the past (Hockenhull, 2025), and this estimate has also been referenced in presentations by Lieutenant General (ret.) Robert Ashley at the U.S. Army War College. The terms open source and publicly available information include social media, internet blogs, messaging apps, commercial multispectral imagery, commercial synthetic aperture radar, and photos taken by civilians on cell phones. For example, many of the images of the Russian invasion of Ukraine used by intelligence analysts came from civilians with cell phones uploading pictures to cloud-based databases (Cronin, 2023).

Ethical bounds and governance must evolve alongside these technologies, but they are slower to adapt. Analysts cannot wait; otherwise, NATO will fall behind its adversaries and risk losing the ability to control these powerful and dangerous technologies.

General Stages of Terrorist Attacks and How AI Can Intervene

Terrorist operations often adhere to a pattern in planning and execution of attacks that experts have classified into eight steps (Office of the Director of National Intelligence, 2024; Sageman, 2004). Figure 1 shows the progression from **Ideation and Motivation** through **Execution and Exploitation**. Lowrance and Pfaff identified potential places AI can aid analysts in detecting and intervening to stop terrorist attacks. I summarize below (Lowrance and Pfaff, 2025, pp. 94-96).

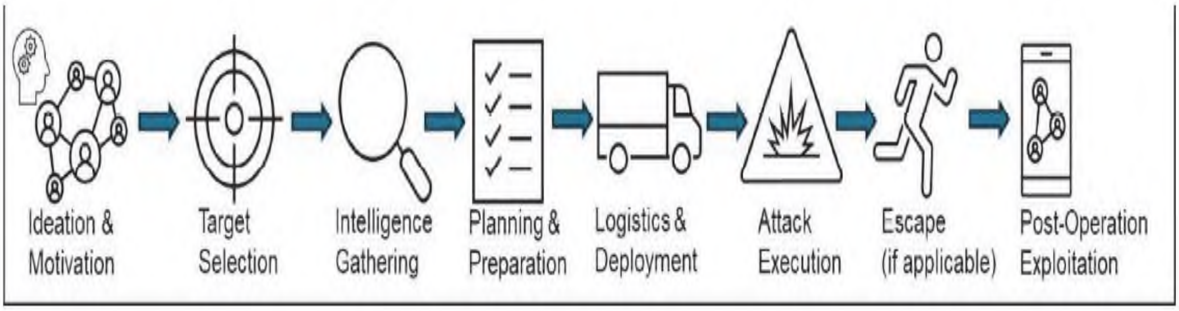

Figure 1: Stages of a Terrorist Attacks

During the **Ideation and Motivation** stage and the **Post-Operation Exploitation** phase, AI can monitor online behavior and detect early signs of radicalization. The volume of information and the variety of languages employed across the internet make it impossible to monitor everything. Still, AI can vastly increase the reach of human analysts monitoring terrorist activity. AI can work rapidly and detect key words to help focus human analysts on likely social media or internet blogs where terrorists are recruiting. It can latch onto language style and dialect and trace them across different social media platforms to help identify the perpetrators. AI models can read and translate many languages, expanding the scope of material an analyst can access (Lowrance & Pfaff, 2025).

Analysts can train AI to automatically remove extremist content from the internet to prevent the spread of violent ideologies. In time, militaries could train AI agents to develop narratives and counteract terrorist recruitment in their native language with minimal human intervention (Lowrance & Pfaff, 2025). Soon, the counterterrorism community could have AI agents arguing online with terrorists who are trying to recruit vulnerable youth, pointing out the logic flaws in the extremist view.

During the **target selection and intelligence gathering** phases, AI can examine large volumes of historical data to identify patterns and predict where and when future terrorist attacks might occur. AI can identify patterns and correlations that humans cannot detect and often do not fully understand. For example, the data company Fraym pulled large volumes of data on historic vaccination rates in Burkina Faso, then linked these to state access and state effectiveness, and found low vaccination rates correlated with areas most vulnerable to terrorist influence (Devermont, 2025). AI can analyze big data and help humans draw correlations or links that might not have otherwise been obvious.

During the **intelligence gathering** phase, AI could be incorporated into surveillance equipment around potential targets to identify anomalous behavior associated with terrorist surveillance. Law enforcement has applied algorithms to surveillance video by training it on the faces or vehicles of suspected terrorists. Security personnel can also train AIs to identify indicators like persons loitering outside of security gates or a specific vehicle continually present and possibly conducting surveillance of a target (Lowrance & Pfaff, 2025). The Ukrainians have pulled faces of Russian soldiers off social media and built databases that led to the arrest of Russians trying to infiltrate Ukrainian bases (Cronin, 2023).

AI can also assist analysts during the **planning and preparation** and **logistics and deployment** phases by managing and interpreting large datasets, including **financial transactions** from known accounts or the **movement of logistics** that could be associated with attacks. An AI can alert analysts to anomalous behavior, especially when historical patterns or known terrorist-affiliated accounts or supply companies are involved.

The key to achieving AI's full potential is applying the technology to a variety of sources across the terrorist planning cycle and then correlating the indicators or anomalies from different phases to paint a picture of the terrorist plan. Intelligence analysts can apply algorithms to many different databases and pick up subtle signs previously difficult for humans to notice, then a higher-level algorithm could gather the indicators from the subordinate models looking across space and time to alert of a possible attack. Perhaps the movement of supplies itself wouldn't trigger an alert, but when correlated with the movement of large amounts of money from historic terrorist influencers and reports of increased surveillance at a potential target, the AI could point analysts towards a developing attack (Lowrance & Pfaff, 2025).

The challenge for analysts is gaining access to the relevant databases because of privacy and legal restrictions. These hurdles will always exist, and complete access is neither necessary nor realistic. Furthermore, with strong justification and persistence, it seems possible to gain access to enough of the important databases. For example—and not specific to counterterrorism—the U.S. military is using big data from across many sources to track readiness of soldiers and units by looking at sleep data, leave data, nutrition data, exercise data, number of deployed days, etc. (Shields & Spahr, 2025; Sayers & Spahr, 2025). The same concept can be applied to indicators of terrorist attacks once organizations gain necessary access to databases.

Raven Sentry

An early case study of how AI can help predict terrorist attacks by correlating multiple indicators is the U.S. military's use of an AI model called Raven Sentry in Afghanistan in 2000. Intelligence leaders contracted with Silicon Valley engineers and built an AI model that identified anomalies in data derived from commercial imagery, synthetic aperture radar, hyperspectral imagery, as well as local newspapers, social media sites, and blogs, among other unclassified, commercially available sources. They correlated these anomalies with insurgents' planning of attacks on Provincial and District Headquarters, focusing on known areas associated with attacks, such as historic supply routes, sympathetic neighbourhoods, mosques, and madrassas where insurgents regularly gathered in preparation for attacks. Indicators included lights being left on in certain areas beyond normal hours, dark areas appearing earlier than usual, and vendors in the towns closing early (the locals often knew when insurgents were in town). The team found that if a historic attack was big enough to hit the news, there was generally commercial imagery, news reporting, and social media available from around the time to train the algorithm. Eventually, as analysts ran more attacks through the AI model and the pool of labelled data grew, the machine began to learn and predict on its own, providing analysts with regions potentially associated with insurgent preparations. These were labelled "Warning Named Areas of Interest." The system even identified indicators analysts didn't expect, like an increased percentage of carbon dioxide in the air prior to attacks.

By the time the coalition left Afghanistan, Raven Sentry's predictions of pending attacks were over 70% accurate. For example, in November 2020, Raven Sentry predicted an attack in Jalalabad coming from the areas labelled Red and Purple on Figure 2.

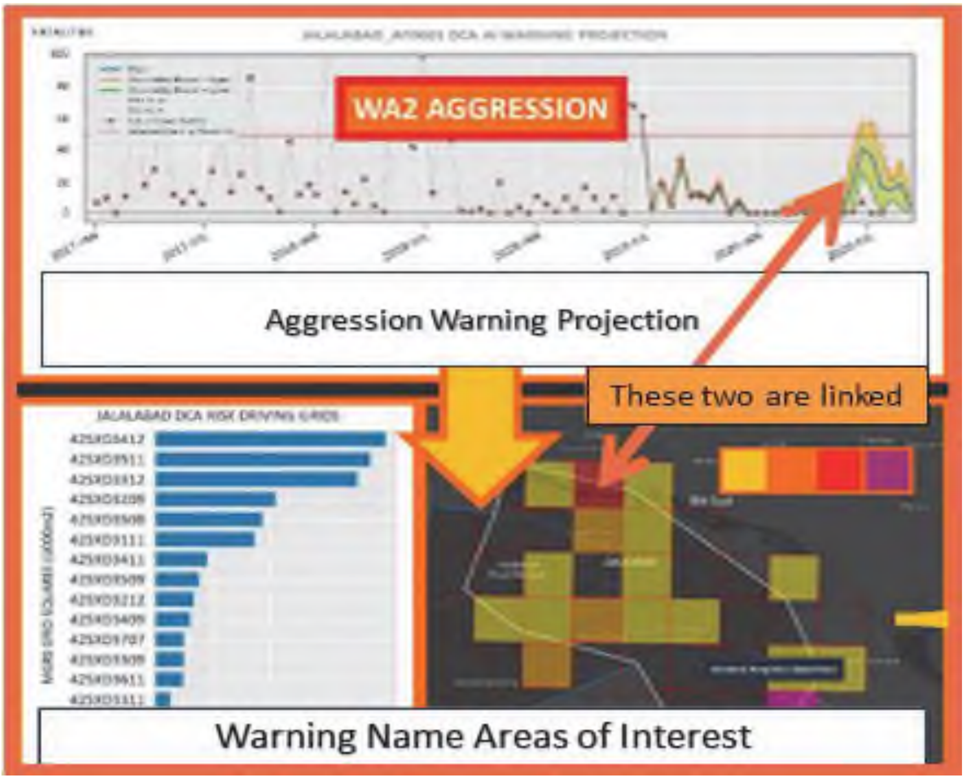

Figure 2: Raven Sentry Warning Names Areas of Interest

Raven Sentry was not perfect, and the AI was not directing anything; rather it was queuing the analysts to focus collection and analysis in certain areas. Essentially saying: "there is behavior that could indicate a coming attack in this location, and you should look here" (Spahr, 2025).

NATO can draw lessons from the Raven Sentry and similar experiments for the future use of AI in Counterterrorism:

1. **Integration with the Commercial Sector:** The military cannot keep up with the commercial sector and academia in developing AI, and should increase partnering. The Ukrainian experience transitioning commercial technology for military use further supports this point (Cronin, 2023).

2. **The increasing importance of Open Source information:** Raven Sentry utilized only unclassified data from publicly available sources. There is an ever-growing amount of data available in modern society, and AI can help correlate that data into intelligence.

3. The **Internal Culture** of an organization is important when innovating. The leadership in Afghanistan late in the war fostered experimentation and allotted resources and time to promising projects. Additionally, there was pressure to find innovative ways to maintain situational awareness in Afghanistan as the United States and NATO prepared to exit the country.

4. **Investment in Expertise is a necessity:** The intelligence team in Afghanistan in 2019-2020 had a talented group of analysts experienced with artificial intelligence. The U.S. intelligence community and military invested in these skill sets, and the leaders in Afghanistan made difficult choices to consolidate AI-trained analysts and allow them to work on this project, even when it meant sacrificing other missions.

5. **Leaders must be aware of the shortfalls of AI systems:**

a. Analysts can build up automation bias and stop questioning AI-produced answers, becoming overly reliant on these systems. AI is imperfect and relies on clean, uncorrupted data, a reliable network connection and a steady power supply, which are not always available in combat.

b. The enemy will adapt. Corrupt data, cyber infiltrations of algorithms, and an enemy that quickly adjusts their tactics and techniques can undermine AI recommendations. AI models are a long-term investment that require regular quality checks and updates.

c. There are clear ethical dilemmas surrounding the use of AI in warfare and debate about where humans will be in the loop as models become more advanced (Hill & Gerras, 2024). Governance of these systems is failing to keep up, and there is danger employing AI in combat where passion and hatred could drive irresponsible use of untested algorithms.

Today, AI models are accomplishing much more in Ukraine and Gaza than Raven Sentry was capable of in Afghanistan. NATO should invest in building systems to keep pace but must apply equivalent effort to developing international law around the application of AI in warfare. Falling behind in the development of these technologies is a dangerous proposition in the ongoing struggle against terrorism.

References

Center for Strategic and International Studies (CSIS). (2025, January 16). Does Ukraine Already Have Functional CJADC2 Technology? *CSIS*. https://www.csis.org/analysis/does-ukraine-already-have-functional-cjadc2-technology

Cronin, A. K. (2023, August 25). Open Source Technology and Public-Private Innovation Are the Key to Ukraine's Strategic Resilience. *War on the Rocks.* Retrieved Oct 19, 2025 from https://warontherocks.com/2023/08/open-source-technology-and-public-private-innovation-are-the-key-to-ukraines-strategic-resilience/

Devermont, J. (n.d.). How Fraym Explains Extremist Violence in Burkina Faso. *Fraym.* https://fraym.io/blog/violence-in-burkina-faso/.

Hill, A. & Gerras, S. (2024, September 25). *Beyond Intuition: AI's Role in Strategic Decision-Making*. Podcast. War Room. U.S. Army War College. https://warroom.armywarcollege.edu/tag/ai-vs-intuition/

Hockenhull, J. (2022, December 9). *How open-source intelligence has shaped the Russia–Ukraine war*. GOV.UK. Retrieved November 9, 2025, from https://www.gov.uk/government/speeches/how-open-source-intelligence-has-shaped-the-russia-ukraine-war.

Lowrance, C. & Pfaff, C. A. (2025). Using Artificial Intelligence to Disrupt Terrorist Operations. In C. A. Pfaff (Ed.), *The Weaponization of Artificial Intelligence, The Next Stage of Terrorism and Warfare* (pp.93-106). Centre of Excellence Defence Against Terrorism, Ankara, Türkiye.

National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. U.S. Government Printing Office, Washington, D.C.

Office of the Director of National Intelligence. (n.d.). *JCAT counterterrorism guide for public safety personnel*. Retrieved August 6, 2024, from https://www.dni.gov/nctc/jcat/index.html

Sageman, Marc (2004). *Understanding Terror Networks*. University of Pennsylvania Press

Sayers, M. & Spahr, T. W. (2025, August 19). *Seamless Systems: Operational Data in the First Army*. A Better Peace Podcast. War Room. U.S. Army War College. https://warroom.armywarcollege.edu/podcasts/seamless-systems/

Shields, S. & Spahr, T. W. (2025, June 17). *Americans Helping Americans: The Castle Brigade's Busy Year*. A Better Peace Podcast. U.S. Army War College. https://warroom.armywarcollege.edu/podcasts/castle-part-2/

Spahr, T. W. (2025). *Raven Sentry:* Employing AI for Indications and Warnings in Afghanistan. In C. A. Pfaff (Ed.), *The Weaponization of Artificial Intelligence, The Next Stage of Terrorism and Warfare* (pp.77-91). Centre of Excellence Defence Against Terrorism, Ankara, Türkiye.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: Securing the Future"
Terrorism Experts Conference & Defence Against Terrorism Seminar (Executive Level)
UNITED AGAINST TERRORISM: SECURING THE FUTURE
15 - 16 October 2025
PANEL 4
Innovating Security: The Role of Technology in Counterterrorism
Q&A SESSION

Turkish Defence Industry and Counter Terrorism Capabilities

Mr. Sabri Anıl KAYA, Defence Industry Expert and Director of Operations Coordination at the Presidency of Defence Industries (SSB) in Türkiye.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
"United Against Terroris... ecuring the Future"
Mr. Sabri Anıl KAYA

The presentation provided a comprehensive overview of the Turkish Defence Industry, its institutional evolution, technological capabilities, and operational contributions, with a particular emphasis on counter-terrorism, border security, and integrated defence solutions. Over the past four decades, Türkiye's defence ecosystem has undergone a profound transformation, evolving from a procurement-oriented structure into a globally competitive, technology-driven, and innovation-focused industry. Today, the Turkish Defence Industry not only fulfils national security requirements but also delivers interoperable, cost-effective, and operationally proven solutions to allied and partner nations.

At the heart of this transformation lies a strategic vision centred on indigenous design, rapid capability development, and operational effectiveness. The Turkish Defence Industry is distinguished by its ability to design and manufacture systems tailored precisely to end-user needs through agile development methodologies. These systems comply with international quality and production standards, optimize lifecycle costs, and continuously integrate emerging technologies in alignment with Türkiye's national strategic objectives. This approach has significantly strengthened operational readiness, deterrence, and strategic autonomy.

Overview of the Secretariat of Defence Industries (SSB)

The Secretariat of Defence Industries (SSB) functions as the central authority responsible for formulating, coordinating, and implementing defence industry policies and programs. Its core areas of responsibility cover the entire defence capability lifecycle, including project and program management, strategy and cost planning, incentive and credit mechanisms, industrial participation and offset policies, international cooperation, research and development management, logistics support, and quality, testing, and certification activities.

Since its establishment in 1985 as the Undersecretariat of Defence Industries (SSM), the institution has followed a deliberate, phased, and systematic development path. Initially focused on direct procurement from foreign suppliers, it progressively transitioned toward licensed production, co-development initiatives, and ultimately full indigenous design and manufacturing. This structured evolution enabled the emergence of nationally developed platforms such as the ALTAY Main Battle Tank, ANKA unmanned aerial vehicle, Bayraktar TB2 armed UAV, HÜRKUŞ training aircraft, and the MİLGEM national naval ship program. In 2017, the institution was affiliated directly with the Presidency, and in 2018 it was restructured and renamed as the Secretariat of Defence Industries (SSB), further strengthening strategic governance, inter-agency coordination, and decision-making efficiency.

Industrial Growth and Ecosystem Strength

Over the last 15 years, the Turkish Defence and Aerospace Industry has demonstrated sustained and remarkable growth across all key performance indicators. Industry revenues increased year by year, and achieved global export success. This progress reflected a substantial reduction in external dependency and a significant enhancement of national technological depth.

This growth has been enabled by a broad, resilient, and multi-layered defence ecosystem. Today, the Turkish defence landscape integrates more than 203 universities, 83 technoparks, 27 military factories, 4 military shipyards, 3,500 private sector companies. This ecosystem fosters close collaboration between academia, industry, and end users, enabling rapid prototyping, technology transfer, operational feedback, and continuous capability improvement. As a result, innovation cycles have shortened, and solutions can be adapted rapidly to evolving operational needs.

Defence Cooperation and Export Performance

Türkiye has emerged as a trusted defence partner and supplier, delivering a wide range of land, naval, air, and electronic systems to international customers. Over the past decade, Turkish defence companies have exported more than 5,000 land vehicles to 40 countries, naval platforms including six MİLGEM corvettes and over 140 naval vessels to multiple nations, more than 3,500 missiles to 42 countries, ATAK attack helicopters, advanced radar systems, and over one million small arms and light weapons.

In addition, Türkiye has secured international orders for key platforms such as the HÜRKUŞ training aircraft and unmanned aerial systems, with confirmed UAV orders from more than 50 countries. These exports reflect not only technological maturity but also operational credibility gained through extensive real-world deployment in demanding environments. Türkiye's defence exports increasingly emphasize long-term partnerships, training, sustainment, and co-production, strengthening interoperability and strategic alignment with partner nations.

Security Challenges and Operational Requirements

Türkiye faces complex, multi-dimensional, and evolving security challenges, particularly along its land and maritime borders. These challenges include terrorist attacks targeting border cities and military outposts, irregular migration flows, and organized crime activities such as human smuggling and trafficking networks. The diversity of terrain, climate, and threat profiles requires flexible, adaptive, and technology-driven solutions capable of operating under all conditions.

In response, Türkiye has developed a holistic Border Security Concept structured around five interlinked and continuously evolving phases: surveillance, detection, intervention, assessment, and improvement. This concept emphasizes persistent situational awareness, rapid response, coordinated command and control, and data-driven adaptation. The effective operational employment of indigenous defence industry products has significantly enhanced mission success, operational tempo, and deterrence along Türkiye's borders.

Platforms Supporting Counter-Terrorism and Border Security

A wide range of indigenous platforms contribute directly to counter-terrorism operations and border security missions. Mine-Resistant Ambush Protected (MRAP) armored vehicles provide high levels of protection against ballistic threats, mines, and improvised explosive devices, while maintaining mobility even under severe damage conditions. These platforms are equipped with modular weapon stations, automatic target tracking systems, laser rangefinders, and integrated fire suppression systems, enhancing both crew survivability and combat effectiveness.

Unmanned aerial systems form a cornerstone of Türkiye's operational success. The Bayraktar TB2 armed UAV has demonstrated highly effective reconnaissance, surveillance, intelligence, and precision strike capabilities, while the AKINCI unmanned combat aerial vehicle extends these capabilities through higher payload capacity, longer endurance, advanced sensors, and multi-munition integration. Kamikaze FPV (First Person View) Drones provide precise, low-cost strike options against time-sensitive and high-value targets, increasing tactical flexibility and reducing risk to personnel.

Cargo and surveillance UAVs support logistics, resupply, and persistent intelligence gathering, particularly in difficult terrain and remote areas. Advanced multispectral imaging drones integrate deep learning and anomaly detection algorithms, enabling enhanced target identification and offline data analysis under contested conditions.

Integrated and Layered Border Security Solutions

Türkiye's border security solutions are built upon an integrated and multi-layered architecture that combines passive and active systems through centralized command and control. Passive components such as border walls, patrol roads, and fiber-optic intrusion detection systems are complemented by active sensors including ground surveillance radars, electro-optical cameras, seismic and PIR sensors, UAVs, aerostats, and remote-controlled weapon systems.

Unmanned surveillance towers and ballistically protected towers provide continuous 24/7 monitoring under all weather conditions, integrating long-range electro-optical sensors, radars, and weapon systems. Modular bases and outposts enhance force protection, area dominance, and secure communications. Ground surveillance radars enable detection of personnel and vehicles at ranges of up to 10 kilometers, while wide-area surveillance systems provide automated detection, tracking, and classification of multiple target types in real time.

Advanced Detection, Response, and C2 Capabilities

Türkiye has developed a comprehensive portfolio of advanced detection technologies. Acoustic and shot detection systems enable rapid identification of sniper fire and hostile activity, while non-lethal acoustic systems support border enforcement and public security missions. Seismic early warning and motion detection sensors employ artificial intelligence for intelligent classification, early warning, and sabotage alerts.

Counter-drone systems incorporating radar, electronic attack, and spoofing capabilities address the growing threat posed by hostile UAVs. Change detection systems using high-resolution 3D modelling enable precise identification of terrain alterations and suspicious activities. Renewable-energy-powered portable surveillance systems ensure sustained operations in remote and austere environments.

All platforms and sensors are unified through integrated and joint command and control systems that provide real-time situational awareness, data fusion, decision support, and interoperability across land, air, and maritime domains. These systems enable coordinated national and multinational operations, significantly enhancing operational effectiveness and deterrence.

Conclusion

In conclusion, the Turkish Defence Industry represents a mature, resilient, and innovation-driven ecosystem capable of delivering end-to-end defence and security solutions.

Its emphasis on indigenous development, operational validation, and integrated system architectures enables Türkiye to safeguard its national security while contributing meaningfully to the collective security of allied and partner nations. Through advanced technologies, proven operational performance, and a strong industrial base, Türkiye continues to enhance deterrence, mission effectiveness, and strategic stability in an increasingly complex and contested security environment.

Panel 5: International and Interagency Cooperation in Biometrics and Battlefield Evidence Collection in Countering Terrorism

Enhancing Military-Law Enforcement Cooperation in Collecting and Sharing Battlefield Evidence in Counter-Terrorism

Col. Özgür Ecevit TAŞCI, Turkish Gendarmerie, Deputy Director- NATO Stability Policing Centre of Excellence (NSPCOE).

Introduction

Ankara/TÜRKİYE
15-16 October 2025
ited Against Terrorism: ...uring the Future"
CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM

During domestic or international operational missions, military units collect material or information belonging to the adversaries on the battlefield for further exploitation for military and intelligence purposes (NATO, 2020; NATO, 2025a). Evidence collection also applies to domestic security operations conducted by law enforcement agencies (LEAs) or, when authorized, by military units. Terrorist attacks or armed confrontations with terrorists within a country requires a judicial investigation and the proper collection of evidence. However, in circumstances where military units are engaged and LEAs cannot intervene, the responsibility for evidence collection must be undertaken by the military units, and the collected evidence must be transferred to LEAs for inclusion in the investigation. Similar conditions may also arise in international operations with counterterrorism (CT) and counterinsurgency (COIN) characteristics, where the likelihood of serious violations of International Humanitarian Law (IHL) and Human Rights Law (IHRL) is high. Due to circumstances of the conflict environment, the evidence collected by the military units may be used to ensure that terrorists are held accountable before the law.

The Evolution of the Battlefield Evidence Collection (BEC)

The systematic violations of IHL and IHRL during the wars in Bosnia (1992-1995) and Kosovo (1998-1999), and humanitarian catastrophe symbolized by mass civilian casualties highlighted the crucial importance of wartime collection of evidence in the prosecution of war criminals. Transnational terrorist attacks, including 9/11 against US (2001) and the subsequent incidents in Allies' territories in Istanbul, Madrid, and London (2003-2005), combined with Allied/NATO operations in Afghanistan and Iraq conducted in chaotic environments, where adversaries systematically disregarded the law of armed conflict, have reaffirmed the essential requirement for interoperable, mission-tailored BEC capabilities.

The phenomenon of Foreign Terrorist Fighters (FTFs)[1] that emerged during the Syrian Civil War (2011-2025) has, in turn, brought the concepts of battlefield evidence (BE) and battlefield evidence collection (BEC) to the forefront of the agendas of the UN, EU, NATO, and other relevant international organizations (IOs).

The main rationale behind this growing interest in the BEC is that, in operational conditions where LEAs cannot intervene, where delay would be detrimental, and which involve high security risks, items recovered on the battlefield that are properly collected, preserved and shared by military units in accordance with procedures can assist in holding the adversary, including FTFs, accountable before the law.

Throughout NATO's operational history, numerous efforts have been made to integrate expertise normally considered non-military, but which falls within the remit of LEAs, particularly in BEC, technical exploitation (TE)[2] , and biometrics[3] (JALLC, 2023). This integration remains vital today, especially in the current context where the risk of violations of IHL and IHRL are higher due to the rise of transnational terrorism, insurgencies, urban warfare, and, more broadly, irregular and hybrid forms of conflict.

NATO's understanding of terrorism has evolved from seeing it as merely 'another risk' to recognizing it as the most direct asymmetric threat to the Alliance (NATO, 2022). This evolution, coupled with NATO's out-of-area operations and exposure to hybrid and irregular threats, has made adaptation to certain new capabilities, including BEC, imperative, a strategic necessity.

Within NATO, counterterrorism remains a national responsibility, however NATO supports member and partner nations through three main areas: (1) Awareness, (2) Capability Development and Preparedness, and (3) Cooperation. BEC, together with biometrics and TE efforts, and along with several other counter measures, fall within NATO's Defence Against Terrorism Programme of Work (DAT POW) (NATO, 2025b).

The issue of FTFs made BEC essential for bringing FTFs to justice, and gained global attention with UNSCR 2396 (2017), which calls upon states to enhance battlefield and digital evidence collection and sharing to ensure returning FTFs can be prosecuted with properly preserved and admissible evidence.

Key Battlefield Evidence Principles

In military contexts, battlefield evidence (BE) refers to information or material obtained during NATO operations that may later support law enforcement purposes and judicial proceedings (NATO, 2020; NATO, 2025a). BE, if properly handled, can become legally admissible forensic evidence. It should be noted that a crucial element of the BE process is the chain of custody, ensuring every action taken with evidence is documented for legal admissibility.

[1] UNSCR 2178 (2014) defines FTFs as "individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict".

[2] A related concept to the battlefield evidence is technical exploitation, where collected materials (like digital devices or weapon fragments) are examined to extract evidentiary data.

[3] NATO defines Biometrics as the process of recognizing an individual based on measurable anatomical, physiological, or behavioral characteristics (STANAG 6515 JINT (Ed. 2) (AIntP-15)).

The concept of ‘battlefield’ is relative; it extends beyond areas of armed conflict to encompass any operational zone or domain in which military units are deployed. In this context, a road checkpoint aimed at identifying FTFs using biometrics can also be considered a form of battlefield. Similarly, a cyber operation center operated by a military entity, as well as digital environments where psychological operations and information warfare are conducted, can be recognized as fronts in modern warfare.

BEC is a national responsibility, and the authority to decide whether collected evidence will be shared with other Allies or relevant judicial authorities rests with the respective nation. NATO Allies are encouraged to share time sensitive evidence with the relevant parties in a timely manner, provided that such sharing does not conflict with the mission being conducted or with national legislation. Shared BE or contextual information should not be classified unless disclosure risks the source, method, mission, or operator (NATO, 2020; NATO, 2025a).

The primary tasks of NATO forces are to achieve the designated operational objectives. Any BEC support that may be conducted should not compromise the success of the mission. However, planning processes should also take into account that, in certain operational environments and conditions, military units may be specifically tasked with BEC. Before military units are assigned BEC tasks, both kinetic and prosecutorial priorities must be balanced, and responsibilities should be clearly defined within legal frameworks as well as rules of engagement (ROE), Status of Forces Agreement (SOFA), and Standard Operating Procedure (SOP).

According to prevailing national practices, national legislation does not contain any provisions that prevent information or material collected by military units from being used as evidence in judicial investigations. The ultimate decision on the admissibility of such evidence lies with the court. However proper contextualization and TE of battlefield findings, and most importantly the strict observance of the chain of custody significantly increase the likelihood that these materials will be accepted as evidence before a court.

Enhancing the BEC capabilities of military units requires the establishment of an explicit legal mandate within national legislation.[4] Once a legal mandate is defined, military units will be able to develop the necessary technological infrastructure for BEC. They can also establish specialized forensic units, and initiate personnel training programs. Ultimately, these measures will enable military units to conduct BEC activities in accordance with international legal norms and scientific standards.

Until the issue of legal authority is resolved, military units may prioritize steps to align with the BEC Policy and enhance cooperation with national LEAs as part of operational readiness. In this context, military may adopt core capabilities in BEC, some others may prefer more advanced practices. Training existing personnel in BEC and/or overall criminal investigation and forensics remains a viable approach. Alternatively, rather than having military units acquire BEC capabilities, this task can be carried out by LEAs with military status (namely Gendarmerie-Type Forces), military police units or by the national police units embedded in military units (The US Departments of State, Justice, and Defence, 2021; UN CTED, 2019).

BEC Scenarios and Military-LE Cooperation

Different scenarios apply to cooperation between military and LEAs in BEC in CT efforts. Under normal circumstances, the responsibility for CT and BEC within domestic territory rests with LEAs. However, when military units are tasked with supporting LEAs or are given direct responsibility for CT operations, they may also conduct BEC activities. In

[4] This requirement equally applies to the use of Biometrics and TE.

situations where border protection duties, carried out by the military, intersects with CT operations, military units may also perform BEC, at least as the first responder. Nevertheless, whenever conditions allow, it should be prioritized that BEC be conducted in cooperation with, and under the supervision of, LEAs. In international missions, military units act as first responders until civilian or law enforcement actors assume control. Evidence collection should be performed by military units only when necessary, and preferably by law enforcement authorities whenever conditions allow.

Conclusion and Recommendations

To counter hybrid threats effectively, NATO forces must possess hybrid or eclectic capabilities — able to operate across multiple domains and integrate military, law enforcement, or many other diverse functions and capabilities within a unified framework.

The issue of BEC has often been associated with FTFs, yet its significance extends to all warfare. Both conventional and unconventional warfare demand that BEC be recognized as a fundamental capability. There is a growing need for systematic studies and lessons-learned analyses on how BEC capabilities can enhance both military effectiveness and the pursuit of justice.

In future conflict environments in which NATO may become involved, military units might specifically be assigned tasks such as collecting evidence or identifying and apprehending individuals suspected of committing war crimes. To effectively carry out such missions, it is essential to develop capabilities in areas such as BEC, TE, and Biometrics, or to ensure that these capabilities are provided in cooperation with LEAs through legal authorization, structural arrangements, technical infrastructure and training programs.

For Allied and Partner Nations, several key recommendations emerge:

- Initiate legal authorization procedures for employing LE capabilities within military operations,

- Ensure personnel receive basic BEC training from national LEAs, and train some specialized forensic experts to direct BEC efforts,

- Include GTFs, MP, or police units in operational planning and mandate processes.

At the NATO level, for further capability development through establishing SPUs within rapid deployable and high-readiness forces, creating a NATO Gendarmerie Force similar to European Gendarmerie Force (EUROGENDFOR), and incorporating more GTF forensic units into NATO exercises might be groundbreaking solutions.

References & Further Readings

European Union Agency for Criminal Justice Cooperation (EUROJUST). (2020, Sep.). *EUROJUST Memorandum on Battlefield Evidence.*

Global Counterterrorism Forum (GCTF). (2018). *The Abuja Recommendations on the Collection, Use and Sharing of Evidence for Purposes of Criminal Prosecution of Terrorism Suspects, Including Battlefield Evidence*. The Hague: International Centre for Counter-Terrorism (ICCT).

NATO. (2020, July). AC/342-D(2020)0002. *NATO Battlefield Evidence Policy*.

NATO. (2022). Madrid Summit Declaration. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2022/06/29/madrid-summit-declaration.

NATO. (2025a, Feb. 25). MC 0699. *Military Committee Policy on Battlefield Evidence.*

NATO. (2025b, Aug. 6). *Countering terrorism.* (Last updated: 06 Aug. 2025 10:35). https://www.nato.int/cps/en/natohq/topics_77646.htm.

NATO Joint Analysis and Lessons Learned Centre (JALLC). (2023, Dec.). *Technical Exploitation and Battlefield Evidence Factsheet*.

The US Departments of State, Justice, and Defence. (2021, Sep.). *Non-Binding Guiding Principles on Use of Battlefield Evidence in Civilian Criminal Proceedings.*

UN Counter-Terrorism Committee Executive Directorate (CTED). (2019, Dec.). *Guidelines to facilitate the use and admissibility as evidence in national criminal courts of information collected, handled, preserved and shared by the military to prosecute terrorist offences ("Military Evidence Guidelines").*

UNSC CTC. (2015, Dec.). *Madrid Guiding Principles.* (2018 Addendum to 2015 Madrid Guiding Principles).

UNSC Resolutions 1373 (2001), 2178 (2014), 2396 (2017).

van Ginkel, B., & Paulussen, C. (2015, May 15). *The Role of the Military in Securing Suspects and Evidence in the Prosecution of Terrorism Cases before Civilian Courts: Legal and Practical Challenges* (ICCT Research Paper, Vol. 6, No. 4). International Centre for Counter-Terrorism (ICCT) – The Hague.

van Ginkel, B. (2016, May), *Prosecuting Foreign Terrorist Fighters: What Role for the Military?* ICCT Policy Brief.

INTERPOL's Perspective on Interoperability and The Collection and Sharing of Biometric Data

Mr. Yaşar Başar AKSOKU, Criminal Intelligence Officer, INTERPOL Counter-Terrorism Operations Unit.

Introduction

Terrorism and transnational crime increasingly exploit global mobility, digital technology, and gaps in information exchange between jurisdictions. Preventing these threats depends on the ability of institutions to share and act on reliable data across borders. Interoperability—the smooth connection between systems, agencies, and regions—is therefore at the heart of effective global security.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: ...ring the Future"

As the world's largest international police organization, INTERPOL connects 196 member countries through a secure network linking law enforcement, border, and intelligence agencies. Among the most effective tools in this network is the use of biometric data (fingerprints, facial images, and other identifiers) that enable the accurate and consistent identification of individuals regardless of aliases or forged documents.

INTERPOL's work in this area reflects a comprehensive approach to counter-terrorism, grounded in operational cooperation, the integration of biometrics into law enforcement practice, and the exchange of military-derived information to support investigations. These combined efforts demonstrate how data can become a shared instrument for collective security.

Operational Foundations of Interoperability

INTERPOL provides a global platform that allows national authorities to communicate securely and in real time. Through its network, police agencies can exchange alerts, verify identities, and coordinate operations with partners thousands of kilometers away. This system makes it possible for a single piece of information—such as a stolen passport number or a wanted person's name—to reach every member country within moments.

A central feature of this network is the system of international notices and diffusions, which standardizes how countries share alerts. Red Notices request the arrest of wanted individuals for extradition; Blue Notices seek information on a person's identity or location; and Green Notices warn about offenders who may reoffend across borders. Other notices have specialized purposes, such as locating missing persons (Yellow), identifying unknown deceased (Black), warning of dangerous materials (Orange), or describing criminal methods (Purple). Each follows a unified legal and operational format that ensures immediate usability worldwide.

INTERPOL's global databases extend this communication framework into frontline environments. The Stolen and Lost Travel Documents (SLTD) and Travel Documents Associated with Notices (TDAWN) databases allow border and immigration authorities to verify travel credentials instantly. When a document or biometric identifier matches a record in these systems, a 'hit' is generated, triggering alerts that can lead to arrests or further investigation.

This architecture turns local data into shared global intelligence. A passport scanned at a small border checkpoint can expose a fugitive wanted on another continent. Every successful match demonstrates the practical value of interoperability: information collected by one country strengthens the security of all.

INTERPOL's Counter-Terrorism Strategy, adopted in 2021, formalized this data-driven approach. It focuses on four priorities—disrupting threats, building the global threat picture, providing targeted operational support, and representing law enforcement interests internationally. The strategy encourages member countries to view data as an operational asset, not simply as information to be stored. Each exchange becomes an opportunity to prevent movement, track financing, or dismantle networks before they strike.

Biometrics as a Strategic Enabler

Biometric data has become one of the most powerful tools available to law enforcement. Unlike names or documents, biometric identifiers are unique and resistant to falsification. They make it possible to confirm identity with precision, even when suspects attempt to conceal it.

INTERPOL's 3B model—Biometrics, Border Security, and Battlefield Information—integrates this capability into a broader operational framework. The model connects identity data gathered in different contexts: fingerprints taken from detainees, facial images captured at border crossings, or biometric traces recovered from conflict zones. When these data points are linked, they reveal the full trajectory of individuals and networks involved in terrorism.

Member countries receive support to collect and upload biometric information using standardized methods that ensure compatibility across systems. Once entered into INTERPOL's databases, the data become accessible worldwide. A fingerprint collected in one region can generate an immediate match in another, providing critical leads for investigations.

A key initiative advancing this work is Project FIRST (Facial Imaging Recognition, Searching and Tracking). The project helps countries strengthen biometric screening, develop national procedures, and train frontline officers. It also provides analytical follow-up when positive matches occur, ensuring that information translates into operational action.

These capabilities are applied in Operation HOTSPOT, a coordinated series of deployments in the Western Balkans and Central Europe. The operation targets foreign terrorist fighters and other serious offenders attempting to exploit irregular migration routes. Using mobile biometric devices, national agencies collect fingerprints and facial images on site and cross-check them against INTERPOL's databases. The results have been concrete: numerous identifications, arrests, and confirmations of existing notices.

Such operations illustrate how the strategic use of biometrics turns border control into early warning. Instead of responding after incidents occur, authorities can detect suspects as they move, close security gaps, and disrupt networks before they reach their destination. The integration of biometrics into everyday policing represents a shift from reactive investigation to preventive intelligence.

Bridging Military and Law Enforcement Information

Terrorism often emerges from conflict zones, where military forces gather vast amounts of data on individuals, communications, and materials. This information can be invaluable for police investigations but has traditionally remained within defense structures. Closing this gap ensures that intelligence collected in combat environments contributes to long-term law enforcement outcomes.

INTERPOL's Military-to-Law Enforcement Exchange (Mi-LEx) mechanism bridges this divide. Developed through earlier projects in Iraq and Afghanistan and later expanded to North Africa, the Sahel, and Southeast Asia, Mi-LEx facilitates the secure transfer of declassified military data to law enforcement agencies. The data (fingerprints, personal records, or communication details) are verified, sanitized, and integrated into INTERPOL's global systems, where they become available to authorized investigators worldwide.

The mechanism ensures that a fingerprint lifted from a weapon or a device in a conflict area can later identify a returning fighter at a border crossing. By transforming battlefield intelligence into judicial evidence, Mi-LEx allows countries to link conflict-zone activity with criminal accountability at home.

Beyond its operational impact, Mi-LEx represents a broader evolution in security cooperation. It demonstrates that effective counter-terrorism depends on institutional as well as technical interoperability, the willingness of military and police actors to coordinate objectives, share information responsibly, and respect mutual constraints. Expanding collaboration with NATO would further strengthen this model, aligning defense and law enforcement perspectives and ensuring that intelligence gathered through military operations directly supports the rule of law.

Conclusion

The fight against terrorism depends on more than national strength; it relies on the ability to connect information, people, and institutions. INTERPOL's experience shows that interoperability—anchored in shared data, common standards, and trust—is the foundation of collective security.

Through its notices, databases, and biometric initiatives, INTERPOL enables countries to detect threats earlier and respond faster. The 3B model provides a practical framework that combines identity management, border security, and battlefield information. Initiatives such as Project FIRST and Operation HOTSPOT have turned these principles into action, demonstrating that effective data exchange leads directly to operational success.

Bridging military and police intelligence through mechanisms like Mi-LEx completes the picture. It ensures that what is learned on the battlefield contributes to justice and prevention, not only to defense. Expanding this model through cooperation with NATO would enhance interoperability across domains and strengthen both operational impact and accountability.

In an interconnected world, every border crossed by a traveler, every fingerprint collected, and every alert shared contributes to a global network of security. The collective effort of interoperable systems transforms information into protection. INTERPOL remains committed to advancing this approach—connecting police for a safer world.

Panel 6: Sharing Good Practices and Lessons Learned (LL) of NATO and NATO Member and Partner Nations in Counterterrorism

Adapting Counterinsurgency Lessons to Counter-Terrorism in The Sahel

LTC Pedro CAVALEIRO, Lieutenant Colonel (PRT-A), NATO Strategic Direction-South Hub.

Introduction

Ankara/TÜRKİYE
15-16 October 2025
t Terrorism: Securing t
re"
NAT
CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE &
EXECUTIVE LEVEL
DEFENCE AGAINST TERRORISM SEMINAR

The global epicentre of terrorism has shifted to Africa, with the Central Sahel bearing the greatest impact (IEP, 2005). Today, the Sahel stands among the world's most complex and consequential areas of conflict. Across this vast territory, Violent Extremist Organisations have evolved from insurgents into de facto governors. They collect taxes, adjudicate disputes, and impose social order where state authority has receded (Rupesinghe et.al.,2021; UNDP, 2025). The paradox is stark: after more than two decades of international counterterrorism (CT) efforts, terrorist governance structures are expanding rather than contracting (Nsaibia, 2025).

This compels us to question our strategic assumptions. Are states fighting the right kind of war—or simply applying the wrong logic more efficiently? We argue that the traditional CT paradigm—focused on rapidly disrupting networks through kinetic precision—has reached its limits, especially in Central Sahel. What is now required is a strategic shift from CT to create good governance, adapting the enduring principles of counterinsurgency (COIN) to the specific realities of the Sahel.

This article follows an overall guiding question: What lessons from COIN can be adapted to strengthen CT strategies in the Sahel? In practical terms, if NATO or one of its allies were to support countries in the Sahel, or be directly involved in Operations in the Sahel region, which elements of a comprehensive strategy should they draw from COIN lessons?

The Strategic Problem

The Sahel represents not only a security crisis but also a crisis of legitimacy.

Violent Extremist Organizations now control or contest vast areas of central Sahel. In many regions, these groups function as the de facto government—providing security, dispute resolution, and basic welfare. In Weberian terms, they have seized the state's monopoly on violence, even though illegitimately[5].

This underscores a fundamental truth of COIN: where the state abdicates governance, non-state actors fill the vacuum. Some studies that revise insurgencies throughout history, found that insurgencies rarely prevail through superior firepower, but through political endurance and population control. In a RAND study (Paul et. al, 2013) evaluating 71 modern insurgencies, the decisive variable was not troop numbers or weapon sophistication, but the host nation's legitimacy and its ability to protect and provide for its population.

Root Causes of Insurgencies

Insurgencies stem from multiple, interconnected factors, not a single root cause. They normally are interrelated, and we should always have a multi-causal approach to every insurgency. Here are some root causes considered in NATO doctrine –AJP-3.27. Allied Joint Doctrine for Counterinsurgency (NATO, 2023) with some highlights about the Sahel:

1. Identity grievances – Marginalised ethnic, religious, and communal groups are often excluded, a vulnerability exploited by extremists.

2. Corruption – It erodes institutional trust and fairness, undermining state legitimacy.

3. Repression – Excessive force and political exclusion push communities toward insurgents.

4. Foreign presence and exploitation – Economic or military interference fuels perceptions of occupation and injustice.

5. Lack of essential services – The absence of education, healthcare, and infrastructure leaves populations vulnerable, allowing insurgents to fill governance gaps.

These drivers create a self-perpetuating cycle of grievance and recruitment that cannot be broken by military means alone. Integrated, context-sensitive strategies are essential.

Proximate Causes

NATO's AJP 3.27 distinguishes between root causes (grievances, corruption, repression, and poor services) and proximate causes (security failures, abuses, and elite exploitation), which are all evident in the Sahel. Nevertheless, root causes usually need some elements that help galvanize part of the population into the insurgency movement and help it endure. These elements come up as true catalysts and are termed 'proximate causes'. Here are the main six:

1. Amalgamating grievances.

2. Failed security.

3. Abusive behaviour.

4. Elites' agendas.

5. Individual empowerment.

[5] As we submit this paper, Mali's capital Bamako is surrounded by insurgents from the terrorist coalition *Jama'at Nusrat al-Islam wal-Muslimin* (JNIM), that imposed a fuel blockade to the city. Analysts are predicting that the capital will probably fall into the hands of terrorist groups during the next days or weeks. ("Suffocated by", 2025).

6. Community compliance.

Lessons from Historical Counterinsurgencies – David Galula's "Prerequisites for A Successful Insurgency"

History is instructive. From Malaya to Iraq, the Philippines to Sri Lanka, successful counter-insurgencies share common traits. Galula, in his classic Counterinsurgency Warfare: Theory and Practice, lays down the pre-requisites for a successful insurgency that I believe we are witnessing in the Sahel:

1. A compelling cause resonating with the population.

2. Favourable terrain.

3. Weak or illegitimate governance.

4. External support sustaining insurgent capacity.

5. Effective leadership and organisation.

The inverse defines counterinsurgent success: unity of effort, legitimacy, intelligence-driven operations, adaptability, and host-nation commitment.

Lessons from Historical COIN Approaches

Historical COIN experiences provide valuable practical guidance for CT efforts in the Sahel. One of the most comprehensive studies conducted in the past decade is the RAND report Paths to Victory: Lessons from Modern Insurgencies (Paul et al., 2013), in which the research team analysed evidence from 71 cases[6] of completed counterinsurgency campaigns worldwide between 1944 and 2010. The study builds upon and expands the case selection and methodological framework of the earlier project Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency (Paul et al., 2010). It offers both an overview and an in-depth assessment of the key concepts, practices, and factors that consistently characterize successful COIN operations, drawing on the conclusions of the earlier study. The following are the ten key principles derived from those historical experiences with insurgencies and counterinsurgency approaches that can be applicable to CT in the Sahel:

1. Effective COIN practices tend to 'Run in Packs'.

2. Disrupting insurgent support.

3. Host-Nation commitment and motivation.

4. Flexibility and adaptability.

5. Unity of effort and clear lines of command.

6. Understanding local culture and society.

7. Legitimacy of the Host-Nation government.

8. Integrated Civil-Military Operations.

9. Intelligence-Driven Operations.

10. Winning hearts and minds vs repression.

Lessons from Contemporary COIN Approaches

[6] From the UK experience in Palestine (1944-1947) to the Democratic Republic of the Congo (anti-Kabila) (1998–2003).

Recent experiences in Iraq and Afghanistan yield vital modern lessons. Some of them are applicable to current CT approaches in the Sahel.

1. Legitimacy of governance: No external aid or military power can compensate for a government that lacks public trust.

2. Population-centric operations: COIN is about protecting and empowering communities, not destroying enemies.

3. Intelligence-driven targeting: Precision operations minimise civilian harm and maintain legitimacy.

a. Integrated civil–military efforts: Security, governance, and development must advance together.

b. Adaptability to local context: Context-specific strategies are crucial; what works in one area may fail in another.

c. Undermining insurgent support networks: cutting off financing, logistics, and community support.

d. Tactical and Operational restrain and Protection of civilians remains both a moral and strategic necessity; civilian harm strengthens insurgent propaganda.

e. Unity of effort and coordination among local, regional, and international actors is essential for coherence.

f. Success requires patience and sustained commitment, recognising that transformation is gradual.

g. Finally, the information domain is decisive: legitimacy is also a narrative battle. Winning hearts and minds require offering hope, justice, and inclusion where extremists offer only fear.

For the Sahel, this means a shift from military solutions to rebuilding credibility, protecting civilians, and empowering communities as partners in their own security.

The Challenges to CT in the SAHEL

The Central Sahel remains one of the most challenging theatres of CT. Despite years of engagement, instability persists due to interrelated political, social, and structural challenges:

1. Weak governance and legitimacy: Fragile institutions and political instability erode public confidence.

2. Fragmented regional responses: Overlapping initiatives and lack of coordination.

3. Governance substitution by the Terrorist Groups and Violent Extremist Organizations**:** Extremists fill the governance void, controlling territories and populations.

4. Geographic and logistical constraints: Vast distances and poor infrastructure limit state presence.

5. Ethnic and communal manipulation: Extremists exploit grievances to deepen divisions.

6. Limited capabilities of the security and armed forces (IISS, 2025)**:** Forces face workforce, mobility, and intelligence shortfalls.

7. Illicit economies**:** Trafficking and smuggling finance extremist networks.

8. Regional spillover: Violence spreads toward the Gulf of Guinea and the West African countries.

9. Porous borders and shifting alliances: These hinder sustained interventions.

Adapting COIN Principles to CT in The SAHEL (Ends)

To develop a sustainable, population-centred approach, COIN lessons must guide CT in the Sahel:

1. Support the population: The population, not territory, is the centre of gravity. Restoring state presence must begin with providing security, justice, and essential services.

2. Build resilience: Strengthen economic, educational, and social programs to reduce extremist appeal and sustain local stability.

3. Contain spillover: Support Gulf of Guinea states with early-warning systems, border security, and development aid to prevent expansion.

4. Balanced international support: Replace fragmented bilateral efforts with a coordinated, multilateral framework under UN guidance.

5. Shift from kinetic CT to comprehensive COIN: Integrate military, political, and civil dimensions, prioritising governance and population protection over offensive operations.

Adapting Coin Principles to CT in The Sahel (Ways)

1. Integrated regional response: The emerging Sahel States Alliance Confederation offers an opportunity to create genuine regional ownership of security and stabilization efforts. The recent created combined force should be supported and boosted by international support. If adequately supported, this alliance and its joint force could coordinate cross-border operations, intelligence sharing, and political engagement in ways that transcend fragmented national efforts. For this to succeed, partners must view the confederation not as a rival to international initiatives but as a regional centre of gravity capable of shaping its own destiny.

2. International Coalition for the Sahel: An African Union–led coalition, backed by key international and regional partners, could help align objectives and avoid the competing agendas that have often diluted effectiveness. Such a coalition would enable a coherent strategy—one that brings together military, developmental, and diplomatic efforts under African leadership, with sustained external support and mutual accountability.

3. Local governance (local context): Empowering local governance structures and community leaders is essential to restoring trust between citizens and the state. Stability cannot be imposed from above; it must be built from within communities. Engaging traditional and religious leaders, supporting local service delivery, and ensuring transparency in resource management are practical steps that strengthen governance from the ground up. Local empowerment is the bridge between national policy and the daily realities of people living under threat.

4. Legitimacy of the governments: Engagement with transitional authorities is another pragmatic necessity. Many Sahelian states are currently governed by military juntas, and while political transitions must ultimately lead back to civilian rule, total isolation of these authorities risks undermining security cooperation. Constructive engagement—combined with firm advocacy for a clear, time-bound democratic transition—offers a balanced path: containing immediate threats while promoting long-term political normalization.

5. Protect the population (Clear-Hold-Build): The now old ‘clear, hold, build’ approach is a useful framework: clear areas of insurgent presence, hold them securely with legitimate and

disciplined forces, and build governance structures that deliver tangible benefits to local communities. This population-centric approach recognizes that true victory lies not in the number of enemies defeated, but in the number of citizens who feel safe, represented, and hopeful.

6. Information Operations and Strategic Communication: In today's environment, the contest is not only on the battlefield but in the battle of narratives. This was already referred by several speakers.

Terrorist groups in the Sahel skilfully exploit grievances and portray themselves as defenders of justice and faith. To counter their influence, governments and partners must prioritize credible communication—grounded in truth, delivered through trusted community figures, and reinforced by visible improvements in people's lives. Winning hearts and minds is not about propaganda; it is about restoring confidence in legitimate institutions and giving communities reasons to believe in the state.

7. Capacity building of the Armed Forces: International partners can provide training, mentoring, and resources, but genuine progress comes when those forces are professional, accountable, and connected to the populations they protect. Building institutional capacity means strengthening command systems, logistics, and discipline while promoting respect for human rights and civilian authority. When armed forces are seen as protectors rather than aggressors, they become a source of stability rather than grievance.

8. Intelligence-driven operations: Territorial control alone is not enough; it must be paired with precise, intelligence-led targeting that minimizes harm to civilians. Reliable information from local communities—combined with technological and regional intelligence—allows security forces to act surgically, disrupting networks and leadership without alienating the very populations whose trust they depend on.

9. Intelligence, surveillance, and reconnaissance (ISR): ISR serve as critical enablers in this process. In the Sahel's vast terrain, these capabilities enhance situational awareness and operational precision. However, technology must be integrated with human understanding and guided by ethical and legal safeguards. When used responsibly, ISR helps prevent attacks, protect communities, and verify incidents, thereby building both security and legitimacy.

10. Disrupting external support networks to TGs: Terrorist groups in the Sahel, particularly those affiliated with DAESH, draw strength from transnational financial, logistical, and arms smuggling networks. Following the money and dismantling these supply chains is therefore crucial. This requires stronger financial intelligence, regional coordination, and international partnerships aimed at closing the channels that sustain extremist operations. This is one of the key topic that we believe should be studied in 2026.

Taken together, these principles reaffirm a central truth: success in CT, as in COIN, is achieved not through firepower alone, but through legitimacy, precision, and partnership. The Sahel's path forward depends on integrating these lessons into a coordinated, population-centered strategy—one that protects civilians, strengthens state credibility, and systematically erodes the influence and capacity of terrorist groups.

Conclusion

To conclude, it should be emphasized that those who have spent their careers studying or practicing COIN often speak in doctrinal terms—of 'lines of effort," "centres of gravity," and "stability mechanisms." Yet behind these abstractions lie human communities—villages, families, and individuals—whose trust is the true currency of stability. This was evident in Iraq and Afghanistan, and every nation involved learned from those experiences. Nevertheless, these hard-won lessons, paid for in blood on the battlefield, seem to have been forgotten.

NATO should continue advancing toward the future through the implementation of Multi-Domain Operations. At the same time, it should reintegrate some of the effective practices that were codified into doctrine during the Alliance's COIN campaigns in Iraq and Afghanistan. Furthermore, NATO should take a leading role in fostering an international coalition in the Sahel, aimed at supporting local governments in confronting terrorist groups and assisting their citizens—many of whom face a stark dilemma between two untenable choices: standing alone and likely perishing, or joining the insurgency.

References

Institute for Economics & Peace (IEP). (2025). Global Terrorism Index 2025: Measuring The Impact of Terrorism. Sydney. https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf

International Institute for Strategic Studies (IISS). (2025). The Military Balance 2025. London. https://www.iiss.org/publications/the-military-balance/2025/the-military-balance-2025/

Nsaibia, H. (2025, March 27). *New frontlines: Jihadist expansion is reshaping the Benin, Niger, and Nigeria borderlands.* Report. ACLED. https://acleddata.com/report/new-frontlines-jihadist-expansion-reshaping-benin-niger-and-nigeria-borderlands

NATO. (2023). Allied Joint Publication AJP-3.27, Edition A, Version 2, ALLIED JOINT DOCTRINE FOR COUNTER-INSURGENCY. Brussels.

Paul, C., Clarke, C. P., Grill, B. (2010). *Victory Has a Thousand Fathers: Sources of Success in Counterinsurgency*. RAND, Santa Monica CA. https://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG964.pdf

Paul, C., Clarke, C. P, Grill, B., Dunnigan, M. (2013). *Paths to Victory: Lessons from Modern Insurgencies.* RAND, Santa Monica https://www.rand.org/pubs/research_reports/RR291z1.html

Rupesinghe, N., Naghizadeh, M. H. & Cohen, C. (2021) *Reviewing Jihadist Governance in the Sahel.* Working Paper 894. Norwegian Institute of International Affairs (NUPI).

Suffocated by jihadists despite truce push, Mali on the brink. (2025, November 08). *The Arab Weekly*. https://thearabweekly.com/suffocated-jihadists-despite-truce-push-mali-brink-while-domino-effect-feared

United Nations Development Programme (UNDP). (2025, July 24). *Future of Governance in the Sahel: (Re)building Social Cohesion and Public Trust*. https://www.undp.org/africa/waca/publications/future-governance-sahel

Türkiye's Fight Against Terrorism: Successes and Lessons for The Future

Prof. Dr. Uğur GÜNGÖR, Professor of International Relations and the Director of the School of Foreign Languages at Başkent University.

Introduction

Türkiye is one of the countries most damaged by the terrorist attacks around the world. Since its foundation, the Turkish Republic came under systematic attacks by terrorist organizations with various ethnic, religious, sectarian, and ideological masks. It lost tens of thousands of its citizens to terrorism and suffered irreparable financial damage. Tragically, countless civilians and security personnel have been martyred as a result of terrorist attacks over the years.

Türkiye has been struggling bitterly with terrorist organizations in its territory such as PKK and FETÖ as well as within the neighbouring countries, Iraq and Syria. Although our state is able to protect its citizens and territory from the threat of domestic terrorism, terrorist organisations near our borders pose a grave threat to the national security of our nation. In that regard, Türkiye carried out several cross-border operations in northern Syria against PKK/YPG and actively participated in global and regional activities in order to ultimately defeat DAESH such as Global Coalition Against DAESH. Türkiye has made significant contribution to fight against DAESH on the battle field.

Therefore, learning from Türkiye's experiences in the military, political, economic, and sociological battles against terrorists would create a unique opportunity to promote peace and stability around the world.

The Global Terrorism Index (GTI) 2025

The Global Terrorism Index (GTI) is a comprehensive study analysing the impact of terrorism for 163 countries covering 99.7 per cent of the world's population. One of the key aims of the GTI is to examine these trends. It also aims to help inform a positive, practical debate about the future of terrorism and the required policy responses.

The four terrorist groups responsible for the most deaths in 2024 were DAESH, Jamaat Nusrat Al-Islam wal Muslimeen (JNIM), Tehrik-e-Taliban Pakistan (TTP), and al-Shabaab. These four groups were responsible for 4,204 terrorism deaths, or 80 per cent of deaths that were attributed to a specific group.

In 2014, these four groups were responsible for less than 40 per cent of terrorism deaths that were attributed to a group, highlighting the large global shifts in terrorism over the past decade.

In 2014, most deaths were caused by Boko Haram and the Taliban, with these groups respectively accounting for 17 and five per cent of the global total.

DAESH expands its operations to 22 countries and remains the deadliest terrorist organisation in 2025 GTI, causing 1,805 deaths, with 71% of its activity being in Syria and Democratic Republic of the Congo (DRC).

- Tehrik-e-Taliban (TTP) emerged as fastest-growing terrorist group, with 90% increase in attributed deaths.

- Deaths in sub-Saharan Africa (excluding the Sahel) are now at their lowest since 2016, dropping by 10%.

- Terrorist attacks jumped by 63% in the West, Europe was most affected where attacks doubled to 67.

- In 2024, several Western countries reported one in five terror suspects as under 18, with teenagers accounting for most DAESH-linked arrests in Europe.

- Seven Western countries are in the first 50 most impacted countries on the Global Terrorism Index. Türkiye ranks number 32 overall in the most impacted countries from terrorism.

Türkiye's Fight Against FETÖ, DAESH, PKK/YPG

Türkiye has been effectively countering terrorism in all its forms and manifestations for decades, ranging from FETÖ terrorists to the ethnic separatist PKK terrorism, and from extreme leftist DHKP-C to terrorist groups exploiting religion such as Al Qaeda and DAESH, as well as 'ASALA' terrorist organizations.

Türkiye has adopted a holistic counterterrorism strategy which comprises political, cultural, social and economic dimensions, as well as a focused attention on international cooperation. Türkiye's fight against terrorism has been based on several key pillars. First, determined security operations both at home and abroad have neutralized terrorist networks. Second, terrorist financing channels and logistics support have been cut. Third, Türkiye has worked with international partners to prevent external support to the organization. Finally, Türkiye strived to strengthened the resilience of her society against terrorist propaganda.

The Secret Armenian Army for the Liberation of Armenia (ASALA)

It can be said that the struggle against the Armenian terrorist organization ASALA-Marxist-Leninist in ideology, inspired by Mao's revolutionary people's war strategy, and particularly targeting Turkish diplomats abroad-marked the beginning of Türkiye's confrontation with modern terrorism.

ASALA was founded in 1975 in Beirut, Lebanon during the Lebanese Civil War by Hagop Hagopian and Kevork Ajemian. The principal goal of ASALA was to establish a United Armenia that would include the formerly six provinces of the Ottoman Empire. The group sought to claim the area (so-called Wilsonian Armenia) that was promised to the Armenians in the 1920 Treaty of Sèvres, based on the claim of so-called 'Armenian genocide', which Türkiye openly denies.

ASALA particularly targeted Turkish diplomats abroad. ASALA's last attack, on 19 December 1991, targeted the limousine carrying the Turkish Ambassador to Budapest. ASALA was dissolved after the assassination of Hagopian. According to some sources, another reason is that financial backing was withdrawn by the Armenian diaspora after the 1983 Orly Airport attack. The Orly Airport attack was the 15 July 1983 bombing of a Turkish Airlines check-in counter at Orly Airport in Paris, by ASALA. The explosion killed eight people and injured 55.

PKK

One of the longest-standing terrorist threats to Türkiye has been PKK. Since the 1980s, this terrorist organization has carried out numerous terrorist attacks, causing the loss of thousands of civilian and security lives. PKK terrorism has not only affected the social fabric but also the economic development and political contexts in Türkiye. It created anxiety and hatred in the minds of many people.

PKK was founded on November 27, 1978 in the village of Fis located in the province of Diyarbakir-Lice with the PKK's initial and founding Congress. The goal of PKK was to establish allegedly 'Independent United Kurdish State' comprised of the territories from Türkiye, Iraq, Iran, and Syria.

However, PKK's first armed attacks on August 15, 1984, occupy a special place in Turkish fight against terrorism. Since its foundation in 1978, more than 40.000 people lost their lives because of PKK terrorism which is founded on separatist ethno-nationalism. PKK's primary targets include police, military, economic, and social assets in Türkiye. PKK also attacks civilians and diplomatic and consular facilities. It is also involved in extortion, arms smuggling, and drug trafficking.

Since 2016, as a result of the consistent efforts, Türkiye has achieved significant success in neutralizing the PKK threat. Türkiye launched 4 cross-border operations in northern Syria to prevent the formation of a terror corridor, and enable the peaceful settlement of residents: Euphrates Shield (2016-2017), Olive Branch (2018), Peace Spring (2019), and Operation Spring Shield (2020). In this direction, we have made significant contributions to our border security and ensured peace and stability in the region by neutralising hundreds of terrorists. Cross-border operations were crucial for the future of Syria and the region, and what the proposed safe zone means for Syrian refugees. Home to more refugees than any other country, Türkiye, the world's top contributor of humanitarian assistance, continues to help some 3.7 million displaced Syrians.

PKK terrorist organization's capacity has been reduced to minimal levels. Recently, the PKK even announced its own dissolution. On February 27, 2025, PKK has been called on to lay down its arms and dissolve itself, a move that could end its 40-year terror attacks. Following this call, the PKK held its 12th congress between May 5–7, 2025 and announced its decision to disband and disarm. The PKK's decision to dissolve its organizational structure and cease armed activities constitutes a historical turning point in Türkiye's long-standing counter-terrorism policy, shaped by shifting military, political, and regional dynamics.

In addition to PKK terrorist organization, Türkiye has been fighting against FETÖ and DAESH terrorism.

FETÖ

The coup attempt of 15 July 2016, carried out by the FETÖ terrorist organization against Türkiye's democratic order, state institutions, and civilian population, was defeated through public resistance and institutional loyalty. The epic resistance against the treacherous coup attempt with state and national unity set an example for the entire world.

In the aftermath, countering FETÖ's activities beyond Türkiye's borders became a priority. The organization's efforts to expand political and economic influence, often through educational, civil society, and commercial networks, have mirrored the methods previously employed inside Türkiye. This demonstrates that FETÖ represents a transnational security risk extending beyond the Turkish context.

Accordingly, Türkiye has intensified diplomatic engagement to raise international awareness of the threat. Current initiatives focus on the closure or transfer of FETÖ-affiliated institutions, as well as preventing organization members from using foreign jurisdictions as safe havens to evade accountability and the rule of law.

DAESH

Türkiye did not avoid a direct encounter with DAESH in the early stages of the war in Syria for two simple reasons. For one, Türkiye was not militarily present inside Syria until the summer of 2016 and, naturally, had no direct encounter with the organization. As a second reason, Türkiye had not sensed an imminent DAESH threat since the organization prioritized territories in Syria and Iraq for a long time rather than stretching the front further into Türkiye. Yet, when the organization began to target Türkiye, Türkiye did not hesitate to retaliate.

At the same time, Türkiye, which has been on the forefront of the intellectual battle against DAESH terrorists, took most sincere and conclusive steps against the terrorist group. Türkiye designated DAESH as a terror organization as early as October 10, 2013, seeing it as an affiliate of the Al Qaeda organization and therefore, decided to freeze the financial assets and economic resources of the organization and its affiliates with a Cabinet decision.

When DAESH opened fire on the patrol teams of the Cobanbey Border Station, Türkiye responded with tanks and howitzers, hitting a number of DAESH targets, including a convoy of the organization, as early as January 29, 2014.

Türkiye experienced more DAESH attacks and is among the countries that suffered casualties the most. Türkiye has long suffered from DAESH terror attacks in its own metropoles and also from cross-border gunfire and rocket attacks almost on a routine basis in its border cities, such as Kilis. While the May 11, 2013, Reyhanlı bombing in Hatay province was very likely a DAESH attack, the deadliest Türkiye had ever suffered up until that time, DAESH suicide bombers killed hundreds of people, most notably on July 20, 2015 in Suruc, Şanlıurfa (34 killed, 104 injured); October 10, 2015 in Ankara (109 killed, over 500 injured); March 19, 2016 in Taksim, İstanbul (5 killed, 36 injured); January 12, 2016 in Sultanahmet, İstanbul (12 killed, 15 injured); June 28, 2016 at İstanbul’s Ataturk Airport (45 killed, 239 injured); and January 1, 2017 in Ortaköy, İstanbul (39 killed, 70 injured).

As DAESH intensified its targeting of Türkiye, Türkiye gradually dropped its cautious ‘border safety first’ policy and started taking offensive measures to safeguard its security. Türkiye conducted Operation Euphrates Shield in 2016 and cleansed the last pocket of DAESH territory near the Turkish border.

Conclusion

Terrorism has been a major problem in Turkish history and particularly in its recent past. It has not only affected the social context but also the economic and political contexts in Türkiye. It created anxiety and hatred in the minds of many people.

Türkiye’s counter-terrorism policy has proven effective at the national level, while also reinforcing regional stability and contributing to global security. We believe that a comprehensive and coordinated approach is essential to fight terrorism effectively. For this reason, Türkiye continues to call for stronger and more consistent international cooperation in the global fight against terrorism.

Today, Türkiye combats all terrorist organizations, regardless of their ideologies, and sectarian motivations, or ethnic references, without distinction. Türkiye remains vigilant and committed to ensuring that no terrorist threat can re-emerge. At the same time, Türkiye’s counter-terrorism experience contributes not only to our national security, but also to regional and global security.

"If the fight against terrorism is conducted decisively and in line with the spirit of partnership, all of humanity will find peace." Türkiye continues to meet its responsibilities and to fight terrorism in all its forms and manifestations for the sake of world peace and international security.

References

Alan, E. (2020). *Terör–PKK: 40 yıllık ihanet*. Bilgi Yayınları.

Alptekin, H. (2017, November 14). *Past, present, future of Turkey's fight against Daesh*. SETA. https://www.setav.org/en/past-present-future-of-turkeys-fight-against-daesh

Aslan, M. (2023). Türkiye'nin terörle mücadele süreci: An ve sonrası. *Kriter*, 8(84). https://kriterdergi.com/dosya-100-yil/turkiyenin-terorle-mucadele-sureci-an-ve-sonrasi

Bila, F. (2016). *İdeolojik kodlarıyla kağıt üstündeki PKK*. Doğan Kitap.

Gök, A., & Mavruk, Ç. (2023). The new terrorism and analysis of the PKK in the context of learning terrorist organizations. *Journal of Defence and War Studies*, 33(1), 65–100.

Institute for Economics & Peace. (2025). *Global terrorism index 2025: Measuring the impact of terrorism*. https://www.economicsandpeace.org/wp-content/uploads/2025/03/Global-Terrorism-Index-2025.pdf

İşeri, R. (2008). *Türkiye'de etnik terör: ASALA ve PKK örneği* (Unpublished master's thesis). Atılım University, Institute of Social Sciences.

Metin, R. (2021). July 15 coup attempt and the FETÖ terrorist organization. In Ö. Akman, F. O. Atasoy, & T. Gür (Eds.), *Education, social, health and political developments in Turkey between 2000–2020* (pp. 300–312). ISRES Publishing.

Presidency of the Republic of Türkiye, Directorate of Communications. (2020). *Turkey's counter-terrorism perspective*. https://kulakver.iletisim.gov.tr/uploads/Turkey%E2%80%99s_Counter_Terrorism_Perspective.pdf

Seren, M. (2019). Terörizmle mücadelenin değişen yönü ve Türkiye. *Kriter*, 4(39). https://kriterdergi.com/siyaset/terorizmle-mucadelenindegisen-yonu-ve-turkiye

Republic of Türkiye. (n.d.). *Resmî Gazete* (No. 28791). https://www.resmigazete.gov.tr/

Yeşiltaş, M. (2025, May 12). *The PKK's dissolution and the path to lasting peace*. SETA. https://www.setav.org/en/the-pkks-dissolution-and-the-path-to-lasting-peace

Colombian Counterterrorism Policy: Good Practices and Lessons Learned

Mr. Mario Alberto ORTIZ BARRAGAN, Director of National Security at the Ministry of National Defense.

Colombia's Public Policy Advances in National Security: An Integrated Strategy Against Terrorism, Border Threats, and Weapons of Mass Destruction

Colombia's experience in public policy formulation within the security and defense sector reflects a multidimensional and adaptive approach to emerging global threats. While the country has not historically implemented a standalone public policy on terrorism, its strategic response is embedded within the National Criminal Justice framework, particularly through the 2021–2025 Criminal Justice Plan. This plan includes targeted actions to disrupt illicit activities that sustain criminal networks, including terrorism and its financing, and promotes international cooperation mechanisms to enhance the State's operational and institutional response.

In 2024, the Ministry of National Defense developed the Sectoral Counterterrorism Strategy, designed to prevent and confront terrorist actions, mitigate their impact, and protect the Colombian population and institutions. This strategy was formalized through Permanent Directive 003, signed in early 2025, which outlines specific objectives and operational guidelines for the security and defense sector. It integrates intelligence, operational readiness, and interagency coordination, while reinforcing Colombia's commitment to international standards and collective security.

A key component of Colombia's counterterrorism architecture is its participation in NATO's Operational Capabilities Concept Evaluation and Feedback (OCC E&F) program. Since 2022, the Joint Special Operations Command (CCOES) has declared a Special Operations Task Group (SOTG) under this framework. The unit, known as "Ares," is the first Colombian military formation certified under NATO standards, with Level 1 OCC E&F and Level 2 SOFEVAL evaluators. This certification, valid through 2028 and renewable every four years, demonstrates Colombia's operational interoperability and its role as a strategic partner in global counterterrorism efforts.

Complementing these efforts, Colombia has launched the 2025–2030 Border Security Strategy, aimed at strengthening human security in terrestrial, maritime, fluvial, and aerial border zones. This strategy focuses on prevention, surveillance, deterrence, and rapid response through the modernization of equipment, deployment of advanced technologies, and development of intelligence and investigative capacities. It also promotes interagency coordination and international cooperation to address transnational organized crime and reduce the incidence of illicit activities in border regions.

In parallel, Colombia's Defense and Security Strategy Against Weapons of Mass Destruction (WMD) seeks to prevent, detect, and respond to threats involving WMDs or related materials. This strategy includes strengthening control mechanisms, enhancing the capabilities of the security forces, and modernizing detection infrastructure. It also incorporates specialized training in crime prevention, crisis management, initial response, site decontamination, and resilience operations.

International collaboration is central to this strategy. Colombia actively participates in global frameworks such as UN Security Council Resolution 1540, the International Atomic Energy Agency (IAEA) programs, the Chemical Weapons Convention, and the Biological Weapons Convention. These engagements reflect Colombia’s commitment to global and hemispheric stability and its alignment with international non-proliferation norms.

Together, these three strategic lines—counterterrorism, border security, and WMD defense—form a cohesive and forward-looking policy framework. They reinforce Colombia’s national security architecture, enhance its institutional resilience, and position the country as a reliable and capable partner in the international security community. Through these efforts, Colombia contributes not only to its own stability, but also to the shared goals of NATO and its global partners in confronting complex and evolving threats.

Tunisian Counterterrorism Policy: Good Practices and Lessons Learned

Maj. Adel SAOUD, Ministry of Defense of Tunisia.

NATO
OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE &
EXECUTIVE LEVEL
DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
"United Against Terror ecuring the Future"
Mr. Mario Alberto
ORTIZ BARRAGAN

Overview of the Development of Violent Extremism in Tunisia

The phenomenon of violent extremism development in Tunisia has gone through three main phases. Phase one is between 2011 and 2012, and it is the Revolutionary Phase. The general security situation was characterized by instability and the emergence of extremist groups like “Ansar Al-sharia”, which exploited the fragmentation of security efforts to recruit and attract youth, especially from vulnerable groups, under the guise of advocacy and charitable activities.

- The dispersion of security efforts immediately after January 14, 2011.
- General legislative amnesty.
- The emergence of some severe and banned religious factions.

During this phase, the country experienced an unprecedented political openness, which led to a security vacuum at certain times, exploited by extremist groups to expand their influence and spread their radical thought.

The second phase, between 2013 and 2015, is characterized by an escalation of violence. Religiously motivated extremist groups have been able to recruit a significant number of young people to join terrorist organizations and groups carry out several terrorist operations, especially the Operation of the Bardo Museum in 2015 and the Operation of the Imperial Hotel in Sousse in 2015. This period witnessed a peak in terrorist activity, resulting in significant human and material losses. Lastly, phase three, since 2015, has been focused on restoring cohesion, taking the initiative, and gaining control. The security situation has improved significantly, and terrorist operations have diminished thanks to military and security efforts and preemptive operations that have allowed for the elimination of the leadership of terrorist groups and uprooting them. This phase was characterized by huge support for military and security operational capabilities.

Tunisian Counter-Terrorism Policy

It is worth mentioning that the last stage of the development of violent extremism in Tunisia represented the first step towards establishing a national approach in the field of counter-terrorism. The first approach was primarily focused on military security, aiming to enhance security and military capabilities, modernize equipment, and develop electronic surveillance systems, as well as strengthen intelligence, monitoring, and tracking systems. Despite the success in reducing and neutralizing the phenomenon, this approach proved insufficient, so a broader and more effective strategy was pursued that encompasses all state components involved in combating extremism and terrorism.

The National Strategy for Combating Extremism and Terrorism

In February 2015, the President of the Republic approved the preparation of the national strategy to combat extremism and terrorism. In March 2015, preparation for the national strategy to combat extremism and terrorism commenced. In August 2016, the Basic Law No. 26 of 2015 dated August 7, 2015, concerning the fight against terrorism and the prevention of money laundering was issued. In August 2016, the Establishment of a National Committee for Combating Terrorism and a judiciary authority specialized in legal follow-up took place. In October 2016, the formulation of the first strategy to combat extremism and terrorism was approved by the National Security Council. November 2016 was when the endorsement of the strategy by the President of the Republic was translated into ministerial and sectoral action plans under the supervision of the National Committee, with the government presidency taking charge of evaluating it and ensuring regular follow-up, as well as issuing directives that could prevent extremism and terrorism. The objective of the strategy was establishing a unified and participatory vision among various ministries (National Defense, Interior, Justice, Religious Affairs, Social Affairs, Youth and Sports, etc) aimed at utilizing all their capabilities and uniting their efforts to prevent violent extremism, combat terrorism, and prevent its funding to ensure that they are not scattered in unilateral initiatives and isolated programs.

The national strategy for combating extremism and terrorism has been formulated in several phases within a defined methodological framework to ensure the development of comprehensive national plans. These phases started with the **formation of a working team** to formulate the strategy, which includes all ministries and structures directly or indirectly related to the counter-terrorism file. The following phase involved all ministries and relevant structures in formulating the strategy, ensuring a **participatory and comprehensive approach**. The other phase included **request for support** in strategic planning from international bodies to enhance the planning process with global best practices. This is followed by the **formation of specialized teams** for drafting, coordinated by the National Committee for Combating Terrorism, in collaboration with specialized institutions in the field of **'Methodology for Transforming Strategies into Action Plans'**. The formulation of the national strategy foresaw **involving experienced individuals** in strategic planning and seeking input from international experts to prepare robust strategies. The strategy also necessitated the **supervision and transformation into actionable plans** by a unified national structure (The National Committee for Combating Terrorism), ensuring that all stakeholders help translate the national strategy into effective sectoral action plans.

As we can see, the **First National Strategy (2016)**, the reference document that emerged from the national strategy for combating extremism and terrorism, included strategic objectives at a theoretical level, as well as detailed action plans (prepared at the ministerial level based on a unified methodology and work models under the supervision and support of the committee). This document included the necessary measures to achieve sectoral objectives through a series of programs and practical activities. This strategy is based on 4 pillars: **prevention, protection, tracking, and response.** Prevention involves avoiding extremism and recruitment. Protection is strengthening protection and mitigating its consequences. Tracking is a pursuit aimed at stopping terrorist attacks. Lastly, response is responding to reduce the effects of terrorist attacks. Then the need to update the national strategy arose. The updates are implemented in three phases. The first phase is composed of forming two working teams to update the national strategy. The first working team focuses on the prevention component, and the second working team focuses on the protection, tracking, and response components. The second phase included the evaluation of the National Strategy for Combating Extremism and Terrorism 2016/2021, and defining the foundations of the new National Strategy by setting the guidelines, determining the mission and vision, setting the strategic goals, sub-strategic goals, and specific objectives.

Lastly, the third phase involves the formulation of the new National Strategy, and also developing its executive plan that includes procedures, programs, activities, priorities, accountable structures, and organizing workshops to examine comparative experiences and best practices in preparing and shaping executive plans. Part of the third phase is the development of a communication plan to introduce it to the public with the aim of ensuring the involvement of all active parties in implementing the strategy and ensuring the engagement of civil society components, authorities, public institutions, and regional and local authorities, as well as introducing the national strategy to 80% of international parties. It is essential to note that the new national strategy was approved by the National Security Council in August 2023 and has been in effect since that date. It includes 2 strategic objectives, 28 specific objectives, and 62 projects. To ensure efficiency, the committee released concurrent outputs, including a National Strategy, an Executive Plan, and an awareness-raising flash, aimed at introducing the strategy and ensuring its reach to all parts of society.

Good Practices

The best practices adopted in the Tunisian policy include:

- Defining the main national strategic objectives

- Identifying threats and analyzing risks with the assistance of various analysis centers and National Security Documents

- Translating the strategy into action plans through the use of relevant studies

- Preparation of annual reports involves continuously evaluating them

- Monitoring statistics and indicators that enable the assessment of the effectiveness of dealing with the phenomena of extremism and terrorism

- Holding in-depth discussions with all stakeholders in the fight against terrorism and the prevention of violent extremism

- Organizing workshops for civil society components

- Involving youth in the process through conducting a public opinion survey on the website of the National Committee for Combating Terrorism.

Lessons Learned

The most important lessons that can be learned from the Tunisian experience are:

- Taking into consideration of infrastructure development for various state facilities in updating the National Strategies

- Monitoring and staying up-to-date with the threats associated with the emergence of new methods used by terrorist groups and changes in their areas of influence

- Anticipating the health threats that may hinder the implementation of some planned programs

- Accurate assessment of the progress rates in achieving the strategy's goals

- Keeping up with changes and supporting them with practical proposals whenever necessary. And especially, strengthening coordination at the national level and developing regional and international cooperation.

Conclusion

This presentation has outlined the development of violent extremism in Tunisia, highlighted the key pillars of the national counter-terrorism policy, and reviewed essential good practices and the most valuable lessons learned. It becomes clear that collaborative efforts and ongoing adaptation are fundamental to strengthening the effectiveness of national security strategies. Continuous evaluation and improvement remain vital for ensuring lasting safety and stability for all.

KEY FINDINGS

Terrorist Adaptation, Learning and Evolving Tactics

1. Recent terrorist trends show a clear shift toward 'low-tech, high-impact attacks' marked by decentralized execution and minimal operational complexity. These operations often rely on readily available means such as vehicle rammings, knife attacks, arson, and small-arms fire and are frequently carried out by lone actors or small, loosely connected cells with little or no formal organizational linkage.

2. Misuse of Emerging and Disruptive Technologies (EDTs) by terrorist groups has been a challenge for the states and societies. EDTs include artificial intelligence (AI), quantum computing, biotechnology, nanotechnology, cyber technology, robotics, unmanned systems (inclusive of drones), blockchain, cloud computing, and the Internet of Things (IoT).

3. An EDT- enabled terror attack could trigger a domino effect in other areas, leading to substantial damage in both physical and virtual domains.

4. Terrorist organizations have increasingly integrated small, commercially available drones, known as unscrewed/unmanned aerial systems (UAS), into their operational frameworks. These UAS perform multiple roles, including intelligence, surveillance, and reconnaissance missions, as well as the capacity to deliver small-scale strikes employing explosive or incendiary devices.

5. A noteworthy terrorist financing trend is the growing adoption of digital assets and cryptocurrencies; however, the prevalence of this practice varies among different groups.

6. Terrorist organizations boost their operational effectiveness by merging cyber capabilities and information warfare tactics. Terrorist groups increasingly use cyber intrusions for reconnaissance, selecting soft targets and raising funds across multiple online platforms. Encrypted channels allow them to coordinate logistics and personnel with reduced detection risk, while integrated information operations magnify the psychological effects of their campaigns and drive recruitment through disinformation-heavy narratives.

7. Terrorist actively study open-source reports, and adapt accordingly.

8. Gaps in prior international intervention strategies, such as leaving weapons stockpiles in Libya unaddressed, contributed to longer-term regional volatility.

9. Russia relies heavily on asymmetric tools, such as proxy forces, disinformation, irregular tactics, and cyber operations to pursue its objectives, but it faces persistent difficulties gaining genuine support or acceptance from local populations in the areas where it operates.

10. Contemporary terrorist organizations are exhibiting increasingly ambiguous and hybrid ideological profiles. Rather than articulating concrete political end-states or governance models, groups are selectively borrowing narratives, symbols, and grievances from disparate extremist traditions. This fluidity reduces the effectiveness of traditional counter-radicalization frameworks built around fixed ideological taxonomies.

11. Terrorist actors are increasingly engaging in multi-vector harm, including crimes that are not purely instrumental to financing (e.g., production and dissemination of child sexual abuse material). These activities reflect a shift toward violence and exploitation as intrinsic objectives, expanding both the moral and operational threat landscape.

Near-Term Terrorist Threat Trajectory

1. Cyber tools will increasingly support physical operations through precise target identification, data aggregation, and network infiltration. These integrated capabilities will help attackers bypass traditional defenses.

2. The widespread adoption of commercially available drones and UAVs by non-state actors including terrorist groups will expand their strike capabilities and challenge traditional military frameworks.

3. As drone use proliferates across conflict zones (which coincides with widespread terrorism), states will intensify efforts to develop advanced countermeasures, raising urgent governance and regulatory concerns.

4. Disinformation, psychological operations, and social-media manipulation will be used for amplifying disruption and fear from the physical attacks.

5. Online forums, social media, and encrypted channels will fuel a decentralized exchange of operational know-how, accelerating adaptation and replication.

6. Effective tactics like vehicle-ramming, low-cost IEDs, and improvised weapons will spread rapidly across regions.

7. Small drones and other technologies once limited to state forces will become widely accessible to non-state actors including terrorist organizations.

8. Informal value networks and privacy-focused cryptocurrencies with the anonymity they provide will complicate countering terrorism financing efforts.

9. This rising anonymity will challenge counter-terrorism financing efforts and require innovative tracking tools and stronger international coordination.

Public–Private Cooperation and Governance of Technology

1. Modern counterterrorism increasingly depends on capabilities and data controlled by the private sector, from AI and satellite surveillance to digital platforms that shape information environments. However, cooperation between governments, militaries, and technology companies remains fragmented. As corporations gain strategic power and global reach, traditional state-led security frameworks struggle to keep pace. Without stronger, flexible governance models and shared responsibility, technological advantages risk becoming vulnerabilities that terrorists and violent extremists can exploit.

2. Institutional silos hinder coordination. Security institutions, law enforcement, and private actors often work in isolation, limiting situational awareness, adaptability, and innovation.

3. Technological power is shifting toward corporations. Private companies now own and operate capabilities, such as digital networks, satellites, and advanced analytics that are critical to national and international security.

4. Dual-use risks are insufficiently governed. Tech firms sometimes prioritize innovation, profit, and public image over safety, allowing harmful exploitation of emerging technologies.

5. Governments retain legislative authority but struggle to regulate global corporations that shift jurisdictions or resist compliance.

6. Conventional organizations like NATO and governments retain narrow institutional mindsets that hinder adaptation and flexible coordination.

7. Organizations like NATO and national governments can be hampered by bureaucratic inertia and outdated operational concepts, limiting their ability to coordinate effectively with agile private actors.

Sovereignty, Data Governance and Private-Sector Power in Modern CT

1. AI systems, commercial satellites, cloud infrastructure, and digital platforms are now critical enablers of counter-terrorism (CT). As corporations gain unmatched technological

reach, deterrence and defence increasingly depend on capabilities that are not government-owned.

2. While states retain legislative authority, multinational tech firms can bypass regulation through jurisdiction shifts, lobbying influence, and global operational flexibility, challenging security governance and accountability.

3. The traditional Westphalian notion of state monopoly over security is challenged by privately owned digital infrastructures. Protecting societies now requires new models of shared responsibility across public, private, and civil actors.

4. Governments must protect citizens and critical infrastructure from terrorism. However, attempts to regulate data flow can generate public resistance and perceptions of overreach, especially in democratic societies.

5. Technological change is outpacing bureaucratic transformation. NATO, Allies, and partners need modernized frameworks that enable secure data sharing, whole-of-society participation, and risk-responsive governance in fast-moving threat environments.

Online Terrorist Threat

1. Terrorist and violent extremist actors operate across multiple digital platforms simultaneously, creating resilient networks that transcend national boundaries and exploit differences in platform features and moderation practices.

2. Extremist groups continuously adjust their tactics to evade detection, diversify their online presence, and maintain redundancy across platforms. This adaptability challenges single-platform or isolated countermeasures.

3. Effective prevention and disruption of terrorist exploitation of digital platforms requires sustained collaboration among technology companies, governments, civil society, and academia.

4. Mechanisms such as hash-sharing, signal exchange, and coordinated incident response improve the speed and consistency of content moderation and reduce the ability of terrorist content to re-emerge elsewhere.

5. Research, analysis, and structured dialogue through academic partnerships and multistakeholder working groups play a critical role in understanding evolving extremist tactics, emerging technologies, and overlapping online harms.

6. The online dimensions of offline terrorist attacks require coordinated and timely responses. Flexible incident response frameworks enable platforms to act collectively while adapting to different threat scenarios.

7. Embedding respect for human rights into membership criteria and operational practices strengthens legitimacy, trust, and long-term effectiveness in countering terrorist and violent extremist content online.

8. Young people are increasingly exposed to extremist narratives online due to a combination of misinformation, targeted propaganda, and the interactive nature of digital platforms. Social media, gaming environments, and closed online communities provide fertile ground for recruitment by fostering a sense of belonging, anonymity, and constant engagement. While algorithms are not the root cause of radicalization, they intensify exposure by amplifying sensational and polarizing content, accelerating vulnerable users' pathways toward extremist networks. This convergence of online influences makes youth a primary target for terrorist and violent extremist manipulation.

Strategic Communication, Information Operations and Public Trust

1. Terrorist organizations treat the information environment as a primary battlespace in shaping perceptions, exploiting grievances, and mobilizing support faster than governments can respond. Terrorists prioritize influence as their main line of effort, using propaganda, disinformation, and emotional storytelling to radicalize individuals and erode trust in institutions. On the other hand, governments still approach communication as an adjunct to traditional operations. This imbalance undermines legitimacy, weakens public resilience, and enables adversaries to dominate the narrative. Strategic communication must therefore be recognized as a core operational effort in modern counterterrorism.

2. Many security actors continue to conceptualize communications as 'public relations' rather than a decisive tool of prevention and disruption in CT. Therefore, there is a strong need to change institutional mind-sets.

3. NATO communication practices often remain reactive and militarized, rooted in 1990s paradigms that emphasize operational updates instead of narrative shaping, community engagement, and digital influence campaigns.

4. In the CT context, poor or delayed crisis communication damages legitimacy, allowing misinformation to fill information vacuums and fueling distrust among affected populations.

5. Soft power, while essential for shaping perceptions, legitimacy, and influence, is rarely effective when employed in isolation. States that successfully project soft power typically do so in conjunction with credible hard-power capabilities. This complementary relationship (the 'carrot' supported by a 'stick') ensures that soft-power initiatives have strategic weight and are not easily dismissed by adversaries.

6. Relying on 'counter-narratives' keeps governments on the defensive. Instead of responding to extremist propaganda, states must focus on proactive strategies that offer positive identities, civic participation opportunities, and credible visions of the future, particularly for youth who are vulnerable to recruitment.

7. Communication is a shared strategic responsibility in CT; it is no longer the exclusive domain of governments or militaries. International organizations, national institutions, NGOs, private companies, and civil society actors all actively shape the information landscape surrounding terrorism. Whether intentionally or not, every statement, campaign, policy announcement, or content moderation decision becomes part of the strategic communications environment. Therefore, all actors involved in CT must internalize the responsibility to communicate deliberately, consistently, and in support of collective objectives. Without coordinated messaging and shared narratives, terrorists and violent extremists will continue exploiting information gaps to gain influence, legitimacy, and recruitment advantages.

MDO and CT

1. Multi-Domain Operations (MDO) emerged to confront a growing operational constraint: the increasing segregation of the land, air, maritime, cyber, and space domains. Whereas three decades ago joint forces could employ capabilities across domains with relative freedom, adversary advances in anti-access/area-denial, electronic warfare, cyber disruption, and space targeting have eroded that flexibility. MDO provides a framework to re-integrate these capabilities; ensuring forces can continue to operate, maneuver, and generate effects despite domain-specific constraints imposed by state and non-state actors.

2. Chinese and Russian doctrinal interpretations introduce additional layers (e.g., cognitive domain, electromagnetic dominance).

3. The relationship between MDO and terrorism should be approached from two complementary perspectives. First, terrorism can disrupt, distract, and degrade a multi-domain force posture. As NATO prioritizes deterrence and defense in the context of great-power competition, the complexity and interdependence of MDO inherently expand the Alliance's attack surface. Terrorist actors, especially those able to exploit cyber, space-enabled systems, or critical infrastructure can target vulnerabilities across domains to create operational friction disproportionate to their size. Second, MDO also provides new opportunities for counterterrorism effectiveness. Integrating capabilities across land, air, maritime, cyber, and space reinforced by data fusion and rapid decision-making architectures can enable more precise and scalable counterterrorism effects, while reducing risk to forces and civilian populations.

4. MDO strains NATO's traditional command-and-control structures designed for hierarchical and slower decision-making cycles.

5. National sovereignty concerns and intelligence classification restrictions hinder real-time cross-domain interoperability.

6. MDO requires advanced digital infrastructure and resilient communications, creating high and recurring cost burdens.

7. Divergent levels of digital maturity among Allies may lead technologically advanced members to operate ahead of others. This might undermine cohesion and interoperability within the Alliance.

8. Rapid technological change can outpace national defence budgets, complicating sustainment over time.

9. Even in regions like the Sahel, where strict domain delineation is less evident, MDO still enhances planning and synchronization.

10. Effective MDO depends on integrating local partners, a continuing gap in crisis and conflict environments.

11. Modern terrorist activity spans cyber, informational, social, and economic domains that lie beyond the military's exclusive remit. Effective MDO therefore requires whole-of-government and whole-of-society integration, expanding CT beyond traditional security actors.

12. CT-focused MDO requires civil–military fusion, expanding operational cooperation beyond purely defence institutions.

Wargaming CT

1. Wargaming is effective for mental flexibility, decision-making, and operator training.

2. Non-state actors can be effectively represented in professional wargames. They can be modelled through distributed cells with distinct behaviors and decision authorities, reflecting the decentralized and adaptive nature of terrorist organizations.

3. Surprise is essential for realistic counterterrorism wargaming. Injecting uncertainty, through fog-of-war mechanics, hidden information, card-based triggers, and facilitator-led shock events better replicates the unpredictability of terrorist tactics and improves training value.

4. AI currently delivers the greatest value in wargaming as a facilitation enabler such as enhancing narrative generation, tracking player actions, maintaining scenario coherence, and dynamically updating the operational environment. Emerging systems already demonstrate strong potential for automating scenario management and producing realistic injects, improving

both scale and effectiveness of wargaming. However, AI as an independent decision-making actor (whether representing state adversaries, non-state cells, or analytical reasoning) remains constrained by structural limitations of current large language models. These include opacity of reasoning ('black-box' dynamics), and instability when ingesting complex datasets at scale. These issues risk undermining analytical rigor and could distort insights drawn from wargame outcomes.

5. Wargaming provides a safe-to-fail environment in which complex CT scenarios can be explored beyond kinetic operations, capturing the interdependence of military, informational, cyber, psychological, and societal domains.

6. Multi-domain CT is shaped as much by information influence, societal resilience, and civilian perceptions as by military force. Wargaming reveals how civilian harm, cultural dynamics, and psychological effects directly influence operational and strategic outcomes.

7. By simulating adversary behavior, institutional constraints, and cross-domain interactions, wargaming exposes capability gaps, organizational blind spots, and unintended consequences well before they materialize in real operations.

8. Including civilian experts, NGOs, and decision-makers in CT wargames improves realism, challenges doctrinal assumptions, and strengthens societal preparedness against hybrid and terrorist threats. Despite its demonstrated value, wargaming is not yet consistently embedded across NATO structures or national CT frameworks, limiting its strategic impact.

AI as a CT Enabler

1. Online recruitment, propaganda, financial transactions, and open-source signals often precede physical attacks. AI-driven analysis of open-source, financial, and behavioural data enables earlier and more preventive intervention than traditional kinetic-focused approaches.

2. The life cycle of a terrorist attack is composed of different stages such as ideation, recruitment to planning, execution, and exploitation. In each and every stage, distinct behavioural and logistical indicators emerge. This staged structure creates recurring opportunities for early detection and disruption.

3. Given the scale, linguistic diversity, and speed of online activity, human monitoring of extremist indicators alone is insufficient. AI enhances analysts' reach by identifying radicalization signals, tracking narratives across platforms, and processing multilingual content at scale.

4. Single indicators rarely reveal an imminent threat. AI is most effective when it integrates anomalies from multiple domains like financial, informational, logistical, and behavioural across time and space to identify emerging attack patterns.

5. The effectiveness and legitimacy of AI-enabled CT is shaped by different constraints like legal, privacy, and ethical restrictions that limit data availability, and also AI systems themselves are vulnerable to bias.

6. Successful AI application depends on leadership support for experimentation, sustained investment in skilled analysts, and institutional willingness to adapt workflows. Technology alone is insufficient without human capital and cultural readiness.

7. There is regulatory divergence on AI-enabled preventive technologies creates operational inconsistencies within the Alliance. While some NATO members possess legal authority to employ AI-driven predictive and preventive tools within counterterrorism operations, others (notably dual EU–NATO members) face restrictions under frameworks such as the EU AI Act. This uneven adoption risks creating capability gaps, complicating

interoperability, and reducing the effectiveness of combined operations in multinational theaters.

Integrating Law Enforcement, Stability Policing and Civilian Capabilities in CT

NATO's operational design has traditionally emphasized military instruments of power in CT settings. However, long-term success against terrorism and violent extremism requires a more holistic approach that fully integrates domestic security expertise, law-enforcement functions, and rule-of-law capabilities. Stability Policing and gendarmerie-type forces, which sit at the critical nexus of military and civilian security, remain under-leveraged in multinational CT efforts, despite their demonstrated role in protecting populations, enabling governance, and preventing insurgent resurgence.

Battlefield Evidence and Biometrics

1. Effective battlefield evidence collection is essential for ensuring accountability for terrorist acts and upholding international legal obligations. While domestic counterterrorism operations often rely on established cooperation between military forces and specialized law enforcement forensic units, such capabilities may be absent in fragile or failed-state environments where NATO forces operate. In these contexts, military units may become the primary collectors of legally relevant evidence. Without standardized procedures, specialized training, and a clear chain of custody, evidentiary integrity can be compromised, reducing admissibility in judicial processes and undermining justice for victims.

2. Effective global counterterrorism cooperation relies on the trusted exchange of sensitive data. Organizations such as Interpol operate on strict principles of data ownership, confidentiality, and controlled dissemination, ensuring that information shared by one nation is not released to others without explicit consent. However, national political sensitivities or bilateral tensions can limit data sharing, reducing the completeness of the international threat picture and potentially constraining timely operational action.

3. Hybrid threats require integrated, cross-domain capabilities. NATO's operational environment increasingly demands forces that can combine military, law enforcement, and specialized technical functions within a single, coherent framework. Hybrid adversaries exploit seams between domains, making fragmented capability structures insufficient.

4. Cross-domain cooperation strengthens both security and legitimacy. Connecting military, police, and judicial information ensures that counter-terrorism efforts contribute not only to defence outcomes but also to rule-of-law objectives and long-term prevention.

5. Bridging military and law enforcement intelligence remains a critical gap. Mechanisms such as Mi-LEx illustrate how battlefield-derived information can support investigations, prosecutions, and prevention, yet such integration is not yet systematic across alliances.

Learning Lessons and Institutionalizing Change

1. While NATO has made significant progress in capturing operational insights from counterterrorism and stabilization missions, persistent challenges remain in translating 'lessons identified' into 'lessons learned'. Complex bureaucratic structures, and competing national priorities can delay the integration of adaptive practices into doctrine, training, and planning cycles. NATO's scale and consensus-driven nature result in slower adaptation and institutionalizing change.

2. Experiences from recent campaigns also highlight that governance fragility and corruption within partner institutions can be more damaging to long-term stability than tactical setbacks alone. Security gains remain fragile without political legitimacy and public trust.

Context Dependence- Tailored Responses

1. Terrorism's drivers differ across societies; 'one-size-fits-all' approaches fail. Terrorism manifests through locally specific political, socioeconomic, cultural, and identity-based grievances. Even when groups share ideological labels, the incentives that motivate radicalization and sustain violence vary significantly across regions and communities. Uniform counterterrorism solutions risk overlooking root causes, and generating unintended consequences. Effective strategies require tailored interventions grounded in contextual understanding, locally informed partnerships, and continuous adaptation to evolving threat dynamics.

2. In Afghanistan, the defeat was political in outcome, but military factors remained decisive. While many ANSF positions collapsed through negotiation rather than direct assault, this does not mean information operations alone determined the outcome. In several cases, Taliban messaging only succeeded after sustained military pressure and the physical overrunning or isolation of key positions, demonstrating that information effects are most effective when paired with credible force.

3. Civilian populations in Afghanistan emerged as a decisive centre of gravity. Local communities, particularly elders and families of ANSF personnel played a critical role in encouraging surrender or withdrawal. Prolonged fighting harmed livelihoods, disrupted commerce and agriculture, and lead many civilians to actively support negotiated exits rather than continued resistance.

4. Signals of external support or the lack it was strategically decisive. The withdrawal of visible international backing significantly strengthened Taliban coercive messaging. Ambiguity surrounding political agreements and reports of orders not to resist eroded confidence within ANSF ranks, reinforcing perceptions that resistance was futile and that surrender was the only rational option.

Countering Terrorism in Sahel and NATO's Potential Role

1. Direct NATO stabilization efforts in the Sahel entail significant strategic risk. While NATO is often viewed as a potential stabilising actor, its involvement would occur in a highly contested environment shaped by the growing influence of Russia and China, actors with whom NATO is unlikely to engage directly. This limits NATO's strategic freedom of action and increases escalation and entanglement risks.

2. External intervention risks generating local backlash and unintended consequences. A visible NATO role could fuel perceptions of external interference, potentially exacerbating anti-Western sentiment. Poorly calibrated engagement could also replicate past intervention failures, increasing instability and contributing to secondary effects such as irregular migration toward Europe. And this could strain European borders and test Alliance solidarity, particularly if affected member states perceive insufficient burden-sharing or guarantees of support.

3. NATO influence is most viable through non-kinetic engagement. Humanitarian assistance, socio-economic support, and capacity-building offer lower-risk pathways to maintain relevance and credibility in the Sahel without provoking confrontation or dependency dynamics. Therefore, **sustained cooperation with regional partners remains essential.** Continued engagement with regional organisations and willing local partners in security and

counter-terrorism domains is critical to mitigating further destabilisation and preserving regional ownership of stability efforts.

4. Regional counterterrorism cooperation can be effective when properly resourced and politically supported. The Multinational Joint Task Force (MNJTF) in the Lake Chad Basin demonstrates that coordinated regional military structures reduce terrorist operational space and civilian harm. Nigeria’s leadership and burden-sharing have been decisive in maintaining force cohesion and operational continuity.

5. International engagement in the Central Sahel remains fragmented and politically constrained. Despite emerging initiatives, such as the proposed Sahel joint force, implementation is hindered by limited external support, political instability, and strategic competition among external actors. NATO’s presence and assistance remain diplomatically challenging in junta-governed states, but more feasible in the Gulf of Guinea states working to contain threat spillover.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR

RECOMMENDATIONS

Terrorist Adaptation, Learning and Evolving Tactics

1. Institutionalize continuous monitoring of global terrorism trends, drawing on sources such as Global Terrorism Index (GTI), United Nations Office of Counter-Terrorism (UNOCT), Europol, Interpol, and national assessments to maintain anticipatory posture and detect emerging modus operandi.

2. Adopt fully integrated, cross-domain counter-terrorism strategies that address the heterogeneous nature of modern terrorist tactics, combining low-cost methods with selective high-tech tools such as drones, cyber intrusions, and encrypted networks.

3. Establish cyber-physical threat fusion centers linking cyber experts, intelligence analysts, and operational units to identify early indicators across online and offline environments.

4. Develop analytic pipelines that integrate OSINT, SIGINT, financial intelligence, and behavioural data to support real-time situational awareness and coordinated response.

5. Improve anticipatory intelligence and adversary modelling that accounts for rapid learning cycles.

6. Enhance layered Counter-UAS and perimeter defences through scalable sensor networks, rapid deployment protocols, and legally grounded rules of engagement aligned with national and international standards.

7. Prioritize the protection of critical infrastructure and high-density civilian spaces against drone-enabled and hybrid cyber-physical attacks.

8. Strengthen international cooperation to prevent the diffusion of innovative terrorist tactics and dismantle transnational financial networks.

9. Reinforce soft-target protection through architectural redesign, controlled access points, traffic-flow optimization, and community-based resilience measures.

10. Promote public awareness and trusted reporting channels to increase early detection of suspicious activity and empower local stakeholders.

11. Implement responsible interventions in the information space, including counter-messaging, coordinated content takedowns, and digital literacy initiatives that reduce susceptibility to manipulation and online radicalization.

12. Recognize that modern terrorist organizations employ nonviolent, sub-threshold activities, from disinformation to diaspora engagement and strategic investments, that must be included in threat assessments.

13. Build holistic terrorist threat profiles grounded in ideology, strategic aims, and organizational behaviour.

Public–Private Cooperation and Governance of Technology

1. NATO and its partners should institutionalize deeper collaboration with the private sector to ensure critical technologies and information ecosystems are effectively governed for counterterrorism. This requires shifting from ad-hoc partnerships to structured, shared-responsibility frameworks that balance innovation, security, and democratic accountability.

2. Formalize joint governance mechanisms: Establish NATO-industry coordination bodies for AI, space-based assets, telecommunications, and digital platforms to align security requirements, crisis response, and responsible innovation.

3. Create secure information-sharing environments: Develop standardized legal and technical pathways for exchanging threat intelligence with technology companies while protecting privacy and commercial sensitivities.

4. Strengthen dual-use technology oversight: Promote 'security-by-design' and ethical compliance standards across emerging technologies to mitigate opportunities for extremist exploitation.

5. Establish international protected environments (like CERN) for safe AI development and testing before global release.

Sovereignty, Data Governance and Private-Sector Power in Modern CT

1. Establish mechanisms that define roles, responsibilities, and ethical standards for private-sector participation in CT and crisis response, including commercial satellite, cloud, and AI operators to develop an Alliance-wide governance framework for security-relevant technologies.

2. Harmonize data-protection and information-sharing rules across Allies through enhancing legal interoperability to prevent regulatory gaps that terrorists can exploit and reduce the ability of corporations to avoid oversight.

3. Create shared decision-making structures with industry and digital platform providers to safeguard critical infrastructure and secure information environments without undermining civil liberties.

4. Introduce incentives and obligations where necessary for companies to prevent harmful use of dual-use technologies and reinforce counter-terrorism safeguards.

5. Expand cooperation between NATO Centres of Excellence, governmental regulators, academia, and technology firms to ensure CT policy evolves with emerging technologies and societal expectations.

Countering Online Terrorist Threat

1. Strengthen and institutionalize cross-platform collaboration mechanisms. States and international organizations should support and engage with multistakeholder platforms that facilitate real-time information sharing, joint analysis, and coordinated responses to terrorist exploitation of digital spaces.

2. Adopt a whole-of-society approach to online counter-terrorism. Countering online extremism should integrate technology companies, governments, civil society, and academic expertise, ensuring that policy responses are informed, proportionate, and adaptable to evolving threat dynamics.

3. Enhance investment in shared technical tools and response frameworks. Tools such as hash-sharing databases and tiered incident response protocols should be expanded and refined to reflect the increasingly complex and cross-platform nature of extremist activity.

4. Prioritize research-driven and evidence-based interventions. Ongoing support for independent research, trend analysis, and practitioner-focused knowledge exchange is essential to anticipate new tactics, technologies, and convergence with other online harms.

5. Strengthening youth-focused digital resilience by investing in comprehensive online literacy programs, school-based prevention initiatives, and targeted outreach in high-risk digital

spaces is critical for preventing extremism and terrorism. Partnerships with social media and gaming companies should prioritize early detection of recruitment behaviours, while ensuring that protective measures respect privacy and fundamental rights. By equipping young people with critical thinking skills, creating trusted online support networks, and reducing the appeal of extremist narratives, states can disrupt recruitment pipelines before they take hold.

Strategic Communication, Information Operations & Public Trust

1. Make communication a core line of effort in CT, not a support function. NATO and partner governments should elevate strategic communication to a primary operational task, planned, resourced, and executed alongside intelligence and kinetic activities. Influence operations must be designed from the outset, not added as an afterthought.

2. Modernize strategic communication doctrines to reflect contemporary information ecosystems.

3. Modernize institutional mind-sets and build communication literacy. Security actors should undergo training to understand digital influence dynamics, behavioural science, youth online culture, and perception management. Communication personnel must be embedded in operational planning cells to enable real-time decision-making.

4. Shift from institutional messaging to population-centric narrative strategies, and reactive messaging to narrative leadership. Instead of focusing on countering extremist propaganda, develop compelling, positive alternative narratives rooted in local identities, community aspirations, and credible governance. This is essential for protecting youth from recruitment by extremists and terrorists.

5. Integrate younger generations and digital-native expertise into strategic communication work.

6. Strengthen crisis communication capabilities to protect legitimacy. Governments should establish rapid response structures, pre-approved messaging protocols, and coordinated information hubs to prevent misinformation vacuums during terrorist incidents or security crises.

7. Create joint information operations with non-military actors. Strategic communication must include whole-of-society partnerships like tech companies, civil society, community leaders, journalists, and international institutions. Shared information standards and synchronized messaging reduce fragmentation and build public trust.

Balancing Hard and Soft Power in CT

Ensure balance between soft and hard power measures. Effective CT necessitates both the use of hard and soft power. NATO and Allies should ensure that soft-power initiatives, including strategic communications, capacity building, and diplomatic engagement are backed by credible deterrence and defence measures. This requires sustained investment in hard-power capabilities, coupled with proactive use of political, economic, and informational tools to reinforce influence, assure partners, and deter adversaries. An integrated approach will enhance the Alliance's ability to shape strategic environments and uphold the rules-based international order.

Enhancing Societal Resilience

Enhance societal resilience through tailored prevention programming is critical. Investing in locally-designed resilience initiatives that reduce vulnerability to radicalization by strengthening community cohesion and individual psychological well-being. Innovative micro-level interventions such as yoga-based rehabilitation with former combatants in Somalia, anonymous support helplines in Finland, and proactive de-radicalization outreach at European cultural events demonstrate measurable success when grounded in local context and trusted community networks. Energy-diversion strategies, including sports, youth-led activities, and accessible community programs, should be scaled as part of a broader preventive architecture. Prioritizing early intervention, cultural relevance, and multi-stakeholder delivery will help inoculate societies against extremist narratives before they take root.

MDO and CT

1. Prioritize MDO as an Alliance-wide synchronization framework. Position MDO not as a purely military construct but as a coordination tool linking political, informational, law enforcement, and civilian instruments of power to counter terrorism across all domains and theatres.

2. Strengthen human capital for MDO-ready force posture. Enhance recruitment, retention, and advanced skill development in critical areas, including cyber, space operations, and AI-enabled decision-support ensuring the Alliance maintains a resilient cadre able to operate across domains.

3. Accelerate training, experimentation, and adaptable doctrine. Invest in iterative wargaming, live exercises, and operational experimentation to refine MDO concepts against real-world terrorist tactics, avoiding excessive theoretical abstraction that outpaces practical capability development.

4. Systematically analyse adversaries' gray-zone application of cross-domain tactics. Monitor and assess how state and non-state actors blend cyber disruption, information operations, and proxy violence to erode stability, using these insights to strengthen NATO counter-strategic design.

5. Integrate terrorism-related risk into MDO force design and readiness. NATO should ensure that multi-domain concepts, capability development, and resilience planning explicitly account for asymmetric threats, particularly those targeting cyber networks, space-enabled services, and critical civilian infrastructure that underpin MDO.

6. Enhance cross-domain situational awareness for counterterrorism missions. Investment in data fusion, Intelligence, Surveillance and Reconnaissance (ISR) integration, and AI-enabled decision support should include CT-specific threat indicators to better detect and anticipate terrorist exploitation of seams between domains.

7. Strengthen civil–military cooperation for infrastructure protection. Coordinated resilience measures with national authorities and private-sector operators are essential to safeguard dual-use systems critical to both MDO and counterterrorism operations.

8. Use MDO to amplify precision and reduce collateral harm in CT operations. Multi-domain capabilities, when paired with strong legal and strategic communication frameworks can generate decisive effects while protecting civilian populations and Alliance legitimacy.

9. Advance training and exercises focused on hybrid terrorist threats. Scenario-based exercises should include terrorist actors demonstrating cross-domain disruption tactics, helping ensure that counterterrorism remains a validated operational requirement within MDO constructs.

10. NATO should continue accelerating the practical integration of MDO across doctrine, force design, and training environments. This includes strengthening cross-domain command-and-control architectures, deepening interoperability with Allies and partners, and prioritizing resilience measures against cyber, space, and electronic warfare disruption. By

institutionalizing MDO-enabled manoeuvre and effects generation, the Alliance can maintain operational freedom in increasingly contested environments and ensure that counterterrorism and deterrence missions remain mutually reinforcing.

Wargaming CT

1. Institutionalize structured methods for representing non-state actors in NATO wargaming. Develop adaptable scenario templates, behaviour models, and decision frameworks for terrorist and insurgent actors that can be applied across exercises and national contexts.

2. Expand the systematic use of surprise mechanisms to stress decision-making and resilience. Incorporate dynamic injects, hidden objectives, and cross-domain disruption effects to ensure wargames meaningfully challenge planning assumptions and expose critical vulnerabilities.

3. Institutional investment should focus on AI capabilities that support scenario management, data integration, and adaptive narrative environments, where benefits are immediate, transparent, and measurable while maintaining human analytical leadership.

4. Establish methodological guidance and validation frameworks to ensure that AI-generated adjudication and injects remain analytically defensible and reproducible.

AI as a CT Enabler

1. Adopt a lifecycle-based approach to AI-enabled CT. NATO and partner institutions should apply AI tools across all stages of terrorist activity, prioritizing early phases such as radicalization, recruitment, and preparation where disruption is most cost-effective and least escalatory.

2. Invest in cross-domain data integration and correlation capabilities. AI systems should be designed to fuse indicators from open-source intelligence, financial data, surveillance inputs, and behavioural patterns.

3. Strengthen partnerships with the commercial sector and academia. Given the pace of AI innovation, NATO should deepen collaboration with private industry and research institutions to accelerate adaptation, and leverage open-source advances.

4. Prioritize open-source intelligence as a strategic enabler. Unclassified and publicly available data represent a growing share of actionable intelligence.

5. Institutionalize safeguards against automation bias and adversarial manipulation. AI outputs must remain subject to human review, continuous model validation, and red-teaming. Training should emphasize critical questioning of AI-generated insights and awareness of system vulnerabilities.

6. Develop robust ethical and legal governance for AI in CT. NATO should pair technological investment with leadership in international norms, legal frameworks, and ethical guidelines governing AI use. Ensuring human accountability and legitimacy is essential to sustaining public trust and Alliance cohesion.

7. Build and retain specialized AI expertise within CT institutions. Sustained effectiveness requires long-term investment in AI-literate analysts, interdisciplinary teams, and dedicated career pathways that integrate technical, operational, and ethical competence.

8. Develop scalable technical solutions such as privacy-preserving machine learning, federated analytics, and controlled-access APIs to enable collaboration without broad data exposure.

Integrating Law Enforcement, Stability Policing and Civilian Capabilities

1. Develop formal mechanisms to integrate law enforcement and stability policing elements into NATO planning and operations where appropriate, ensuring seamless cooperation across domestic and expeditionary CT missions.

2. Prioritize the availability and readiness of gendarmerie-type forces and other public order specialists as part of NATO's force packages, recognizing their critical role in restoring security, protecting populations, and enabling governance.

Battlefield Evidence and Biometrics

1. Support initiatives that strengthen interoperability on evidence collection, biometrics, and information-sharing standards, ensuring lawful and effective counterterrorism outcomes across jurisdictions.

2. Institutionalize joint standards and procedures for battlefield evidence collection, ensuring compatibility with international criminal and human rights law.

3. Develop deployable military forensic capabilities, including trained personnel and technological tools that can operate independently where local law enforcement structures are absent.

4. Formalize rapid cooperation mechanisms with law enforcement agencies, including reach-back forensic support, to preserve evidentiary integrity from collection to prosecution.

5. Develop refined protocols and technical safeguards that allow sensitive law-enforcement and intelligence data to be shared with appropriate partners while respecting national constraints.

6. Expand diplomatic engagement and multilateral dialogue aimed at reducing political inhibitors to sharing information emphasizing shared benefits in preventing terrorist mobility, financing, and operational planning.

Learning Lessons and Institutionalising Change

1. Streamline processes to ensure validated lessons rapidly inform doctrine, capability development, and operational training to accelerate institutional learning mechanisms

2. Expand advisory capacity and assessment tools focused on legitimacy, accountability, and public trust alongside kinetic capabilities for strengthening political and governance support to partners such as strengthening Building Integrity frameworks to address structural vulnerabilities.

3. Use wargaming, pilot programs, and rapid-feedback loops across NATO headquarters and commands to test and adopt emerging CT practices sooner.

4. Use emerging conflicts (e.g., Ukraine) to test and validate adapted doctrines.

5. Improve dissemination of good practices among Allies and Partners, particularly from non-kinetic fields such as stabilization, policing, and strategic communications.

Countering Terrorism in Sahel and NATO's Potential Role

1. Strengthen and sustain successful regional models. NATO and Allies should reinforce initiatives like the Multinational Joint Task Force (MNJTF) through targeted capability development (e.g. interoperable communications, intelligence sharing, mobility, logistics support, and force protection). This would amplify existing gains and bolster regional ownership.

2. Prioritize engagement where conditions allow, especially in the Gulf of Guinea. NATO should deepen partnerships with willing states such as Senegal, Benin, Togo, and Ghana to enhance resilience against Sahel spillover. This can include maritime security cooperation, CT training, and institutional capacity building under existing partnership frameworks.

3. Maintain long-term readiness for future re-engagement in the Central Sahel. As political conditions evolve and democratic governance strengthens, NATO should remain prepared to support a legitimate Sahel joint force, including planning, standardization, and human rights–compliant capability development.

4. Adopt a pragmatic, non-binary engagement posture. To avoid pushing partners toward adversarial actors, NATO should pursue flexible cooperation models that focus on shared security interests rather than 'choose-a-side' paradigms, preserving space for constructive engagement over time.

Holistic Approach

Effective counterterrorism requires a holistic approach that addresses:

- Ideological drivers: Countering extremist narratives, building credible alternative worldviews, and amplifying trusted messengers who can challenge violent ideologies within their cultural context.

- Structural grievances: Tackling governance failures, corruption, security-sector abuses, and socio-economic disparities that fuel recruitment and erode state legitimacy.

- Prevention through resilience: Strengthening community cohesion, cultural and institutional safeguards, and digital literacy to reduce susceptibility to radicalization, both offline and within algorithm-driven digital platforms.

This tri-pillar approach reinforces the principle that defeating terrorism requires more than tactical disruption; it demands shaping environments in which extremist and terrorist movements struggle to take root.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
NATO OTAN
COE-DAT
TERRORISM EXPERTS CONFERENCE & EXECUTIVE LEVEL DEFENCE AGAINST TERRORISM SEMINAR
Ankara/TÜRKİYE
15-16 October 2025
"United Against Terrorism: Securing the Future"
DAY 1 Wrap-Up

Closing Remarks

Dear distinguished guests,

As we bring to a close our Combined Terrorism Experts Conference and the Defense Against Terrorism Executive Level Seminar, I sincerely hope that you have found this activity as inspiring and engaging as I have. It has been both an honor and a pleasure to welcome you here in Ankara.

Over the past two days, we have engaged in constructive dialogue, exchanging knowledge and perspectives on a broad spectrum of terrorism and counter-terrorism issues. Our discussions have highlighted current challenges and future opportunities, as well as the 'unknowns' that remain ahead of us. This shared exploration, I believe, has brought us closer to a common understanding and paved the way for further collaboration.

I extend my sincere gratitude to our distinguished speakers and panelists for their exceptional contributions. Your insights have deepened our understanding of terrorism and provided valuable recommendations for refining our policies and practices.

Equally, I wish to thank all participants for your active engagement. Your diverse expertise, stimulating questions and thought-provoking observations have enriched our dialogue and fostered a spirit of genuine exchange.

I trust that this seminar has been a rewarding experience for you—offering new knowledge, fresh perspectives and opportunities for collaboration. "Beyond the formal presentations and discussions, I hope you also benefited from the informal conversations, the friendships formed, and the cultural connections that make such gatherings truly memorable.

Before concluding, allow me to express my appreciation once again to our academicians for their unwavering support and to the Mercure Grand Hotel for hosting us in such an excellent setting.

Finally, I just wanted to say a massive thank you to everyone for their amazing contributions to this seminar. I wish you a safe journey home and look forward to meeting again at future events.

Together, we have made this seminar a success and with that, we bring it to a close. Thank you.

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

NATO OTAN

NATO OTAN

Centre of Excellence Defense Against Terrorism
COE-DAT