TERRORISM EXPERTS CONFERENCE 2022

Centre of Excellence
Defence Against Terrorism

October 18-19, 2022
Ankara, TÜRKİYE

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 may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the authors are affiliated.

INDEX

Terrorism Experts Conference 2022 Team

Official E-mail of the Conference/Seminar: TEC2022@coedat.nato.int.

Conference Director

Lt.Col. Uwe BERGER (GER A)

Assistant Director

Maj. Ali MAVUŞ (TUR A)

Conference Assistant

Mrs. Özge ERKAN (TUR Civ.)

Speakers & Organizations

Col. Oğuzhan PEHLİVAN, Director of COEDAT

Mr. Lucas COX, US Army War College

Dr. Aleksander OLECH, Institute of New Europe

Mr. Diego OSORIO, NATO Climate Change and Security (COE)

Dr. Gabriel RAICU, Maritime University

Dr. Sarah LOHMANN, US Army War College

Ms. Denise FELDNER, The Globalist

Asst. Prof. Omi HODWITZ, University of Idaho

Dr. Heather GREGG, US Army War College

Prof. Dr. Haldun YALÇINKAYA, TOBB ETÜ

Mr. Ronald BEARSE, Nauset National Security Group, LLC

Dr. Sheelagh BRADY, Security Analysis & Research (SAR) Consultancy

Ms. Liat SHETRET, Elliptic

Dr. Filiz KATMAN, İstanbul Aydın University

Mr. Ivica SIMONOVSKI, Academy of Banking and Information Technology

Rapporteurs

Ms. Elif Merve DUMANKAYA (TUR)

Mr. Taha KALAYCI (TUR)

Biographies of TEC 2022 Speakers

Col. Oğuzhan PEHLİVAN, Director of COEDAT

Colonel Oğuzhan PEHLİVAN (PhD) is the Director and Turkish senior national representative at the NATO Centre of Excellence for the Defence Against Terrorism (COE-DAT) in Ankara, Türkiye. As the Director, Colonel PEHLİVAN leads all aspects supporting the Supreme Allied Commander Transformation in his effort to transform NATO in the field of counterterrorism.

Colonel PEHLİVAN graduated from the Turkish Military Academy as an Infantry Officer in 1996 and from the Infantry School in 1997. He served as platoon leader; company, battalion and deputy brigade commander prior to his assignment at COE-DAT. He also got PhD in Sociology at Hacettepe University in 2017. His studies mainly focus on family sociology, culture, immigration, terrorism, counter terrorism, military decision models. Colonel PEHLİVAN is married to Serpil PEHLİVAN, with a son named Burak Kağan PEHLİVAN.

Mr. Lucas COX, US Army War College

Lucas Cox at the time of writing this publication was an intern with the Strategic Studies Instituteat the United States Army War College and a graduate of the University of Washington's Henry M. Jackson School of International Studies with a degree in International Security, Foreign Policy, Peace, and Diplomacy with a double minor in Political Science and Russian, Eastern European, and Central Asian Studies with a focus on the former Soviet economic and security spheres. He is also the 2023 UW Triana

Deines Rome Center Intern and will begin an internship at NATO's Science and Technology Organization in April 2023.

Dr. Aleksander OLECH, Institute of New Europe

Visiting lecturer at the Baltic Defence College and analyst at the Defence24. Previously, Director of the Security Programme at the Institute of New Europe. Graduate of the European Academy of Diplomacy and War Studies University. He has undertaken research at several international institutions, among others, the Université Jean Moulin III in Lyon, the Institute of International Relations in Prague, the Institute for Peace Support and Conflict Management in Vienna, the NATO Energy Security Centre of Excellence in Vilnius, and the NATO StratCom in Riga. Scholarship holder of the OSCE & UNODA Peace and Security Programme, the NATO 2030 Global Fellowship, and the Casimir Pulaski Foundation. His main research interests include terrorism, energy security, international cooperation for security in Eastern Europe and the role of NATO and the EU with regard to hybrid threats. His scientific publications are available in English, French and Russian.

Mr. Diego OSORIO, NATO Climate Change and Security (COE)

Several years of international multilateral and bilateral experience with an array of humanitarian, development, and diplomatic institutions ranging from the World Bank, UN agencies, NATO and the Canadian foreign service. This is complemented by several languages with various degrees of fluency and a high degree of global mobility and adaptability. Delivered strategic and operational policy analysis and advice on the implementation of diplomatic, humanitarian and development initiatives, both in multilateral and bilateral contexts. Diverse and reliable set of skills in crisis management situations. Conceived and managed humanitarian, civil society support, media development, post-conflict institutional and socio-economic reconstruction projects in challenging development contexts on behalf of bilateral and multilateral agencies. Research fellow and lecturer for master degree's level courses on humanitarian, peace-building, peacekeeping issues, aid and post-conflict reconstruction. Well established record in the development and implementation of capacity building strategies and programmes in a broad range of contexts, covering humanitarian, development, economic, trade issues, and peace building processes. Pro-bono social entrepreneur and youth mentor. Most recent initiatives are the launching of a global youth leadership project with the Club of Madrid, and mentoring Canadian and US undergraduates.

Dr. Gabriel RAICU, Maritime University

Gabriel Raicu is the Vice-Rector for research and innovation at the Maritime University of Constanta (CMU) and the Director of the Center for Excellence in Maritime Cyber Security (MarCySCoE). He coordinated the development of the first maritime cyber security simulator within CMU since 2017, the year when the International Maritime Organization (IMO) took into account for the first time maritime cybersecurity risks. He is the initiator and coordinator of the annual BSCySeC#X conferences series, this year on its sixth edition together with European Security and Defense College (ESDC). He holds a degree in maritime engineering and a PhD in cybernetics. He has contributions in the area of early warning systems for cyber security, in the area of protection of critical maritime systems as well as in the area of development of cyber security infrastructures and logistics. He is also the vice-president of Cyber Security Cluster of Excellence (CYSCOE), an organization that brings together companies, public authorities and academia in order to support the development and integration of cyber security at the level of society as a whole.

Dr. Sarah LOHMANN, US Army War College

Dr. Sarah Lohmann is an Acting Assistant Professor in the Henry M. Jackson School for International Studies and a Visiting Professor at the U.S. Army War College. Her current teaching and research focus is on cyber and energy security and NATO policy, and she is currently a co-lead for a NATO project on "Energy Security in an Era of Hybrid Warfare". She is the author of What Ukraine Taught NATO about Hybrid Warfare (US Army War College Press, 2022) and the editor and co-author of the forthcoming book Countering Terrorism on Tomorrow's Battlefield to be published by the US Army War College Press in collaboration with the NATO Center of Excellence in the Defense Against Terrorism.

Ms. Denise FELDNER, The Globalist

Denise Feldner is Founder of Bridgehead Advisors GmbH, a strategy consulting firm in Germany and co-founder of AECAIR the Asian European Consortium on AI Research. She holds degrees in law, management, and engineering. She was founding managing director of an elite group of German research universities and their representative in the Global Council of Research-Intensive University Networks. She was head of staff to the president of Heidelberg University and legal advisor to the CEO of InnovationLab, a startup and public private partnership for organic electronics. As a lawyer she focused for over ten years on infrastructures, energy law and public economic law. She did her legal traineeship at the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety, focusing on energy law. She is an author and young leader of several young leader conferences, e. g. BDI, and Wilton Park.

Asst. Prof. Omi HODWITZ, University of Idaho

Dr. Omi Hodwitz is a criminologist and Associate Professor in the Department of Culture, Society, and Justice at the University of Idaho. Prior to becoming a professor, Dr. Hodwitz was a researcher at the National Consortium for the Study of Terrorism and Responses to Terrorism (START) Center at the University of Maryland. Dr. Hodwitz specializes in quantitative research examining the influence of policies and practices on violent and extremist behavior. She is the director of the Terrorism Recidivism Study (TRS), a large-scale data project that tracks and reports incidents of terrorist recidivism in select countries around the world. She also directs the Aviation Attack Database (AAD), which records all violent threats and attacks targeting the global aviation industry. Dr. Hodwitz has delivered guest lectures and trainings on data collection, analysis, and policy assessment to academic, practitioner, and military audiences in North America, Europe, MENA, and Asia. She has published an assortment of journal articles, chapters, and research reports on violence and extremism, as well as instructive guides for the counterterrorism community on conducting high quality and ethically sound research.

Dr. Heather GREGG, US Army War College

Heather S. Gregg is professor of Military Strategy and Policy at the U.S. Army War College in the Strategic Studies Institute. Dr. Gregg's academic focus is on irregular warfare, terrorism and counterterrorism, causes of extremism, and leveraging culture in population centric conflicts, including repairing communities and national unity in the wake of war and political instability. Prior to joining the U.S. Army War College, Dr. Gregg was an associate professor at the Naval Postgraduate School in Monterey, California, where she worked primarily with Special Operations Forces. She is the 2017 recipient of the NPS school-wide Hamming Award for excellence in teaching. Dr. Gregg was also an associate political scientist at the RAND Corporation from 2003-2006. She has conducted research for USASOC, OSD, TRADOC, BIMA, NCTC, Department of State, and JIEDDO. Dr. Gregg earned her PhD in Political Science in 2003 from the Massachusetts Institute of Technology. She also holds a Master's degree from Harvard Divinity School, where she studied Islam, and a Bachelor's degree in Cultural Anthropology, with honors, from the University of California, Santa Cruz. In addition to academic experience, Dr. Gregg has spent time in several regions of conflict, including Palestine/West Bank and the former Yugoslavia, in addition to working in Qatar and Japan, and studying in Hungary. From 2013-2015, she was part of teaching and engagement teams in Tajikistan. In 2016, she taught at the Indonesian Defense University on subjects relating to asymmetric warfare. Most recently, she has participated in a series of engagements with NATO's Center of Excellence, Defense Against Terrorism in Ankara, Türkiye. Dr. Gregg has published extensively on irregular warfare, religiously motivated conflict and extremism, including: Religious Terrorism (Cambridge University Press, 2020); "Religiously Motivated Violence" (Oxford University Press 2016); Building the Nation: Missed Opportunities in Iraq and Afghanistan (University of Nebraska 2018); The Path to Salvation: Religious Violence from the Crusades to Jihad (University of Nebraska 2014); and co-editor of The Three Circles of War: Understanding the Dynamics of Modern War in Iraq (Potomac, 2010).

Prof. Dr. Haldun YALÇINKAYA, TOBB ETÜ

Prof. Dr. Haldun YALÇINKAYA is the chair of the Department of Political Science and International Relations at TOBB University of Economics and Technology in Ankara/Türkiye. Professor YALÇINKAYA has been conducting research on Foreign Terrorist Fighters of DAESH and Countering Violent Extremism since 2014 and serving as an academic advisor for the different activities of the NATO Center of Excellence Defence Against Terrorism since 2019. He graduated from Kuleli Military High School and later Turkish Military Academy. During his military service as an officer, he completed his post-graduate studies in International Relations at İstanbul University. Dr. YALÇINKAYA studied "peacekeeping" at MA level and "transformation of war" at Ph.D. level. After earning his Ph.D. degree, he had post-doctoral Research and joined the Changing Character of War Project in Oxford University between 2009-2010. Furthermore, during his military service, he served in Afghanistan in 2005. He published two books on war issues and several academic articles/book chapters on International Security issues focusing on new actors of the battlefields as well as terrorism. After serving more than ten years at Turkish Military Academy he has been Professor in International Relations at TOBB University of Economics and Technology since 2013.

Mr. Ronald BEARSE, Nauset National Security Group, LLC

Ronald BEARSE has been helping organizations manage risk and protect critical infrastructure in an increasingly complex and challenging threat environment for 30 years. He has served in a wide variety of analytical, operational, managerial and senior leadership positions with the U.S. Departments of Defense (DOD), Homeland Security (DHS) and the Treasury (TREA), including positions as: Chairman, US National Security Council's Asset Protection Working Group where he was instrumental in broadening the US Key Asset Protection Program; TREA Liaison to the US Critical Infrastructure Assurance Office, Director, Office of Security and Critical Infrastructure Protection; TREA's first Critical Infrastructure Protection Officer; and Director, Business Continuity and Emergency Preparedness Staff, DHS National Protection Programs Directorate (now the US Cybersecurity and Infrastructure Security Agency). Academically, he has served as: Senior Fellow, George Mason University's Center for Critical structure & Homeland Security; Academic Advisor/Lecturer, NATO, Center of Excellence Defense Against Terrorism (COE-DAT) on critical infrastructure protection against terrorist attacks; and Adjunct Professor in the Emergency Management and Homeland Security Program at the Massachusetts Maritime Academy. BEARSE has an MPA from George Washington University and is a Distinguished Graduate of the US National Defense University

Dr. Sheelagh BRADY, Security Analysis & Research (SAR) Consultancy

Sheelagh Brady has approximately 20 years of experience in policing and security. She began her career An Garda Siochana, the Irish Police Force, where she worked for 14 years. She then moved to the international security arena, holding positions such as, Mission Security Analyst with the European Union Border Assistance Mission in Libya, Senior Security Information Analyst, with UNDSS in Abuja Nigeria, and Analyst with the European Union Police Mission in Bosnia Herzegovina (BiH). Since 2014, she has combined this experience, with her academic knowledge, providing a unique perspective on security and risk. She has a PhD from Dublin City University titled 'PhD Shared cues, different violence organisations – exploring the visual strategies used by extremists, gangs, the military, and private military contractors/mercenaries, Dublin City University, Ireland'. She is also a graduate in theoretical and applied criminal justice studies, from John Jay College of Criminal Justice, New York and University College London, UK.

Ms. Liat SHETRET, Elliptic

Liat Shetret is Director of Global Policy and Regulation at Elliptic. For more than 15 years, she has led global capacity-building and technical assistance programs on AML, countering the financing of terrorism (CFT), financial inclusion, and countering violent extremism. She has formerly worked as Director of Regulatory Affairs & Compliance Policy at Solidus Labs, at the Egmont Group of Financial Intelligence Units, Citigroup Bank, the Global Center on Cooperative Security, and the US House of Representatives Committee for Homeland Security. Liat has extensive experience implementing technical assistance programs, particularly in emerging markets and developing countries across Africa, the Americas, Europe, and the Middle East. She is an Adjunct Instructor at New York University and holds a Master of International Affairs degree from Columbia University's

School of International and Public Affairs (SIPA) and a BA in political science and psychology from the University of Illinois. Liat is also a Certified Anti-Money Laundering Specialist (CAMS).

Dr. Filiz KATMAN, İstanbul Aydın University

Assistant Professor Dr Filiz Katman holds a BA in Economics (in English) from Istanbul University, an MA in Political Science and International Relations (in English) from Marmara University, a PhD in International Security and Terrorism from National Defence University (formerly Turkish Military Academy), certificates from Harvard University Humanitarian Assistance in Conflict and Disaster Program, Oxford University Pembroke College Changing Character of War Programme, Yale University Program on War, Conflict and Order, NATO International School, and NATO Centre of Excellence on Defence Against Terrorism. Currently, Dr Katman is Executive Board President at the Energy Politics and Markets Research Centre (EPPAM) since 2010 (founder of the first research centre on energy politics in Türkiye), Editor-in-Chief at EPPAM Policy Brief, and Erasmus+ Coordinator of Department of Political Science and International Relations (in English) at Istanbul Aydin University. She is Senior Fellow at Centre for Syrian Studies and peer reviewer at Journal for Terrorism Research at University of St Andrews and also Management Committee Member of CA18228-Global Atrocity Justice Constellations COST Action representing Türkiye and also member of working groups in COST Actions of the European Union titled CA16232-European Energy Poverty Agenda Co-Creation and Knowledge Innovation COST Action Working Group 1: Integration - Transformation the state of the art and Working Group 2: Indicators – Developing an operational European energy poverty framework; CA17135-Constitution Making and Deliberative Democracy COST Action Working Group 2: Minority Groups and Deliberative Democracy, Working Group 3: e-Deliberative Democracy, CA19126-Positive Energy Districts European Network COST Action Working Group 1: PED Mapping, Characterisation and Learning, Working Group 2: Guides and Tools, CA18236-Multi-Disciplinary Innovation for Social Change (SHIINE) COST Action and CA15212-The Citizen Science COST Action, CA20107 - Connecting Theory and Practical Issues of Migration and Religious Diversity

Working Group 1: Meta-study on the intersection between Religion and Migration, Working Group 2: Narratives of Migration through the Lenses of Religious/Non-Religious Beliefs, Working Group 3: Design of Practice-Oriented Research Projects, Working Group 4: Migration and Religious Diversity through the lenses of Gender and Age, Working Group 5: Communication and Dissemination, CA20109 -Modular Energy Islands for Sustainability and Resilience, CA20138 - Network on Water-Energy-Food Nexus for a Low-Carbon Economy in Europe and Beyond. She is recipient of several awards and scholarships in both the domestic and international arenas, and has published several articles and books on terrorism, security, political violence, cyber threats, cyber security, countering terrorism financing, energy policy, energy security, Syria, Eurasia and NATO. She is regularly consulted by BBC World News due to her expertise, and is Editor for National Security and Physical Geography at Editorial Advisory Group of Cambridge Scholars Publishing, a Member of TUBITAK Academic Research Funds as Observatory Panelist, TOBB (The Union of Chambers and Commodity Exchanges of Türkiye) Istanbul Women Entrepreneurs Council, Executive Board of Energy Business Council at Foreign Economic Relations Board-DEIK and Honorary Advisory Board Member at Foreign Energy Investors Council.

Mr. Ivica SIMONOVSKI, Academy of Banking and Information Technology

Ivica SIMONOVSKI received his PhD in International Politics at the Faculty of Law, Ss. Cyril and Methodius of Skopje. He is a financial analyst within the Financial Intelligence Office of the Republic of North Macedonia, with 15 years of experience in financial investigation and financial analysis. Since 2018, he is a certified AML/CFT evaluator by Moneyval Committee - Council of Europe. He is a Lecturer at the Academy of Banking and Information Technology in Skopje and Defense Institute for International Legal Studies in New Port, USA. His research areas are money laundering, corruption, serious and organized crime, financing of terrorism and cyber crime. He is the author and co-author of many scientific papers published in international journals, journals and conference books. His first book, “Countering the Financing of Terrorism in the International Community” was published in 2018. The second book “How To Become A Financial Investigator” was published in April 2022. Also, he is the Co-Founder of the Cyber Security, Corporate Security and Crisis Management Initiative (C3I). This non-governmental organization focuses on raising public awareness of phenomena which are related to cyber and human security and privacy, among others money laundering as well as corruption. Since 2021, he is part of the Roster of Experts in Regional Anti-Corruption Initiative in Sarajevo and Council of Europe. Hi is a member of the regional network of Global Initiative against Transnational Organized Crime.

Program of Terrorism Experts Conference 2022

	Conference Program **Terrorism Experts Conference 18-19 OCTOBER 2022**	
October 18, 2022		
14.30 - 15.00	**Communications Check**	
15.00 - 15.02	**Terrorism Experts Conference Video**	
15.02 - 15.05	**Opening Remarks,** Director of Terrorism Experts Conference	
15.05 - 15.10	**Welcome Address,** Director of COE-DAT	
15.10 - 15.15	**COE-DAT Introductory Video**	
15.15 - 15.35	**Session 1: 70th Anniversary of Türkiye's Inauguration to NATO - Contributions of COE-DAT to Counter Terrorism**	**Col. Oğuzhan PEHLİVAN** **COE-DAT Director**
15.35 - 15.40	**Session 2: Critical Infrastructure Security and Resilience Book 2**	**Dr. Sarah LOHMANN** **US Army War College**
15.40 - 16.00	**NATO Mission-Dependent Critical Infrastructure**	**Mr. Lucas COX** **US Army War College**
16.00 - 16.20	**Energy Security as the Crucial for the Safety of Alliance and Partners Nations**	**Dr. Aleksander OLECH** **Baltic Defence College**
16.20 - 16.40	**Climate Change Implicationson the Security of NATO Nations**	**Mr. Diego OSORIO** **NATO Climate Change and Security (COE)**
16.40 - 17.00	**Questions and Discussion**	**Dr. Sarah LOHMANN** **US Army War College**
17.00 - 17.15	***Break***	
17.15 - 17.35	**Session 3: Critical Infrastructure Security and Resilience Book 2**	**Dr. Sarah LOHMANN** **US Army War College**
17.35 - 17.55	**Logistics and Supply Chain Resilience**	**Dr. Gabriel RAICU** **Maritime University**
17.55 - 18.15	**Emerging and Disruptive Technologies**	**Dr. Sarah LOHMANN** **US Army War College**
18.15 - 18.35	**Election Infrastructure as Critical Infrastructure**	**Ms. Denise FELDNER** **Bridgehead Advisors**
18.35 - 18.55	**Questions and Discussion**	**Dr. Sarah LOHMANN** **US Army War College**
18.55 - 20.00	***Ice Breaker***	
20.00	***End Day 1***	

Conference Program
Terrorism Experts Conference 18-19 OCTOBER 2022

October 19, 2022

15.00 - 15.05	Session 1: COE-DAT Research Projects	Col. Shawn YOUNG (USAF) Deputy Director of COEDAT
15.05 - 15.25	Sex Disaggregated Data	Asst.Prof. Omi HODWITZ University of Idaho
15.25 - 15.45	Partnership SOF Crisis Management	Dr. Heather GREGG US Army War College
15.45 - 16.05	Emerging Threats in Terrorism and Counter terrorism	Prof. Dr. Haldun YALÇINKAYA, TOBB ETU
16.05 - 16.25	Critical Infrastructure Security and Resilience (CISR) / Advanced CISR Protection from Terrorist Attacks	Mr. Ronald BEARSE Nauset National Security Group, LLC
16.25 - 16.45	*Questions and Discussion*	Col. Shawn YOUNG (USAF) Deputy Director of COEDAT
16.45 - 17.00	*Break*	
17.00 - 17.05	Session 2 : Countering the Financing of Terrorism	Dr. Sheelagh BRADY, Security Analysis & Research (SAR) Consultancy
17.05 - 17.25	Assessing Opportunity and Innovation in Terrorist Financing in a Post Covid Environment	Dr. Sheelagh BRADY, Security Analysis & Research (SAR) Consultancy
17.25 - 17.45	The Uses of Cryptocurrency in Terrorism Financing and Money Laundering	Ms. Liat SHETRET Elliptic
17.45 - 18.05	Analysis of Countering Terrorism Financing Policy of Türkiye	Dr. Filiz KATMAN İstanbul Aydın University
18.05 - 18.25	Implementation of International Restrictive Measures - An Effective Tool in Prevention of Financing of Terrorism	Mr. Ivica SIMONOVSKI Academy of Banking and Information Technology
18.25 - 18.35	*Questions and Discussion*	Dr. Sheelagh BRADY, Security Analysis & Research (SAR) Consultancy
18.35 - 18.40	*Closing Speech and Final Remarks Dir. COE-DAT*	
18.40	*End Day 2*	

Main Outcomes and Common Points of TEC 2022

- Traditional threats that are secured by traditional security ways now have been replaced by emerging threats of the cyber domain.
- Perceptions of gender roles and the linkage to gender being a women's "issue" creates a "blind spot" in counter terrorism efforts. Gender is more than women and men as gender is a socially constructed phenomenon not a biological one.
- Media is the place for terrorist' recruitment, propaganda and communication. OSINT and analysis of social networks can be effective in detecting terrorist activities. This will only be achieved by the international cooperation of related establishments.
- Pandemics provide some opportunities for terrorists, and provide a "bioterrorism window". States need to intensify cooperation to follow the tracks of terrorist organizations in order to prevent unprecedented risks.
- New approaches to ensure resilience of **military & civilian critical infrastructure** and to maintain the operability and readiness of the alliance is required.
- *Emerging Technologies* threaten international security and the security of NATO partner nations. However, NATO can also harness that same technology to promote defense, deterrence, and resilience.
- NATO can strengthen its **Critical Infrastructure Resilience** through **emphasizing *persistence*** requires continuous assessments of how baseline resilience plans can improve, **capacity consideration** requires a holistic approach that focuses on innovation and collaboration **education** ensures a well-informed public and includes continuously testing resilience **and *furthering* training** requires comprehending all possible risks, and how systems behave when pushed to the point of failure.
- NATO aims to increase its strategic awareness of **energy security** and provide the military with a reliable energy supply. Energy security is a key resilience factor and has become more important since the emergence of cyber and hybrid threats to infrastructure.
- In the future, terrorists may attack not only regions that are rich in natural resources, but also **transport infrastructure**.
- The **resilience of logistics and transport chains** is imperative for an effective defense against any classical or hybrid terrorist threats from previously known terrorist groups

or the hard-to-attribute mix from allegedly liberating actions supported by a rogue state often disguised as hybrid or frozen conflicts.

- **Real time big data analytics** presents big data technology's value in counterterrorism missions.
- While traditional adversaries are making strides in their development, terrorists are also gaining ground in using EDTs in peer-to-peer conflicts.
- **Female extremists** face differential treatment when compared to their male counterparts and this disparity is supported by a narrative that presents females are having reduced agency and accountability.
- Females are treated with leniency at all stages of criminal justice proceedings, including the decision to arrest, the charges laid, the determination of guilt, and the resulting sentence.
- Although the long-term consequences of gender-based disparities is yet to be determined, it is likely that leniency directed towards female extremists will impact the effectiveness of the criminal justice system in protecting the public, deterring current and future terrorists, and rehabilitating those that are already committed to extremist beliefs.
- Much of the development in terrorist financing methods is opportunistic with innovation born out of necessity and in reaction to external forces beyond a group's control, rather than being planned, proactive, or strategic.
- It is still difficult to assess how innovative such terrorist groups are, in their acquisition of finances, given the lack of data.
- COVID-19 has and will continue to create opportunity for terrorist financing, further exacerbated by a convergence of multiple factors, such as the war in Ukraine, possible global recession and increased technological change.
- COE-DAT has committed itself the effort and contributed greatly to CB of NATO in CT. Since the inauguration, COE-DAT has conducted totally 163 courses (including CIED, 28 different types), and in these activities 7807 participants, 1742 lecturers, totally 9549 personnel found a chance to share knowledge, meet together, and augment the organizational capacity of CT. Currently, COE-DAT has executed 8 courses in 2022, and planned 9 courses in 2023. COE-DAT has published 28 activity reports, 21 newsletters, 16 journals, 28 books, and 14 research reports, totally 107 hardcopy products. COE-DAT has conducted 28 Mobile Education in

different 20 countries, and executed 163 courses (excluding CIED) until now. COE-DAT has committed itself the effort and contributed greatly to CB of NATO in CT.

Opening Remarks

Dear Generals, distinguished speakers and participants, ladies and gentlemen,

Good morning or afternoon depending on wherever you are in the world. I am Colonel Oğuzhan Pehlivan, Director of Center of Excellence Defence Against Terrorism. I kindly salute you and express my respects on behalf of all my staff. It is privilege for us to host you in this hybrid conference and seminar here in Ankara. Welcome to the capital city of Türkiye.

I am very pleased with the great interest this activity has received. We have more than 308 participants from 53 countries, across 5 continents and ranging from academia, regional organizations, national war colleges, combatant commands, partner nations, to NATO headquarters. Truly an impressive cluster of knowledge and expertise.

COE-DAT is a hub for counter-terrorism expertise due to its unique role as an independent organization outside of NATO's command structure interacting with universities, think tanks, researchers, international organizations, global partners, and other COE's. Based on the expertise created through interacting with our wide network, COE-DAT is able to provide subject matter expertise and advice to NATO on all counter-terrorism efforts.

The Terrorism Experts Conference is our flagship event and after a two year break, we again find a chance to meet you residentially. The main aim of this conference is to advertise and share the annual products and projects of COE-DAT with our stakeholders. Each year we have executed different kinds of projects according to the new trends in terrorism and counter terrorism, and published our key take aways in our web site. As you scrutinize the program of work of COE-DAT, in 2022 we are very near to finalizing the Critical Infrastructure Security Analysis, Sex-Disaggregated Data, and Countering Terrorist Financing and Emerging Threats projects. Besides these informative and qualified products, we also executed our first SOF Roles in Crisis Management Seminar and Gender in CT workshop for the fourth time. Furthermore, we changed one of our well-known and much requested courses, Critical Infrastructure Protection, to Critical Infrastructure Security and Resilience Against Terrorist Attacks and separated the advanced level as a distinct course in order to update the curriculum. In this conference during these two days, you will obtain more detailed information on these new topics in each session with the contribution of precious scholars.

As stated in NATO Strategic Concept 2022, terrorism, in all its forms and manifestations, is the most direct asymmetric threat to the security of our citizens and to international peace and prosperity. Terrorist organizations seek to attack or inspire attacks against Allies. They have expanded their networks, enhanced their capabilities and invested in new technologies to improve their reach and lethality. Non-state armed groups, including transnational terrorist networks and state supported actors, continue to exploit conflict and weak governance to recruit, mobilize and expand their foothold.[1]

The world is changing day by day, and the only thing that is unchangeable is the changing itself. As COE-DAT, our mission is to provide key decision-makers with a comprehensive understanding to terrorism and CT challenges, in order to transform NATO and nations of interest to meet future security challenges. This transformation is embedded into NATO's three declared core tasks of collective defence, crisis management, and cooperative security. We believe that the world will be a better place with the contribution of all nation states and people. Therefore, these kind of meetings pave the way to share knowledge, understand best practices, and construct mutual understanding.

I see the impatience in your eyes to transition quickly to information bombardment and therefore appreciate your attendance again to Terrorism Experts Conference and Executive Level Seminar. For two years, we have combined both events, however; I hope next year we again separate them.

Ladies and gentlemen, distinguished participants,

To conclude, I would like to wish all of us to have an interesting, challenging, dynamic, and fruitful activity. Prepare yourself to be challenged, excited, and inspired. Your ideas and opinions are valuable for us.

Thanks to those who have already sent questions and comments. We rely on your support. Thank you. Wish you all successful and interesting work.

Oğuzhan PEHLİVAN (PhD)
Colonel (OF-5)
Director of COE-DAT

[1] https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf, Accessed 20 September, 2022.

Closing Remarks

Dear Generals, distinguished speakers and participants, ladies and gentlemen,

As the Terrorism Experts Conference is now drawing to end, I would like to thank you all for your outstanding speeches, distinguished presentations, constructive session discussions, and active participation during two days. I hope you all share my view that the whole conference has been a very stimulating and successful experience. As COE-DAT, within the scope of the projects carrying out in the field of terrorism and counter-terrorism, I believe that we have achieved significant gains with the great contributions of precious scholars.

In the past two days, we received a lot of valuable information, not only from our lecturers but also from our participants. Your contribution and active participation ensured the success of this event. Thus, I do express my sincere thanks to all of you.

On behalf of all participants, I would like to take this opportunity to thank and congratulate the COE-DAT staff specifically TEC Director Ltc. Uwe Berger, TEC Deputy Director Maj. Ali MAVUŞ, and TEC Assistant Mrs. Özge ERKAN for their excellent work in organizing and hosting our flagship event. Also, many thanks to our CIS team. Without you, this challenging but fascinating conference would not be possible.

It has been an honor to host such accomplished individuals and to be able to learn from your knowledge and perspective. We would like to continue to improve the already-existing cooperation and coordination in our future events, so we will be looking forward to hosting you and other people from your institutions in the future.

Thank you very much once again for all your valuable contribution and active participation.

Oğuzhan PEHLİVAN (PhD)
Colonel (OF-5)
Director of COE-DAT

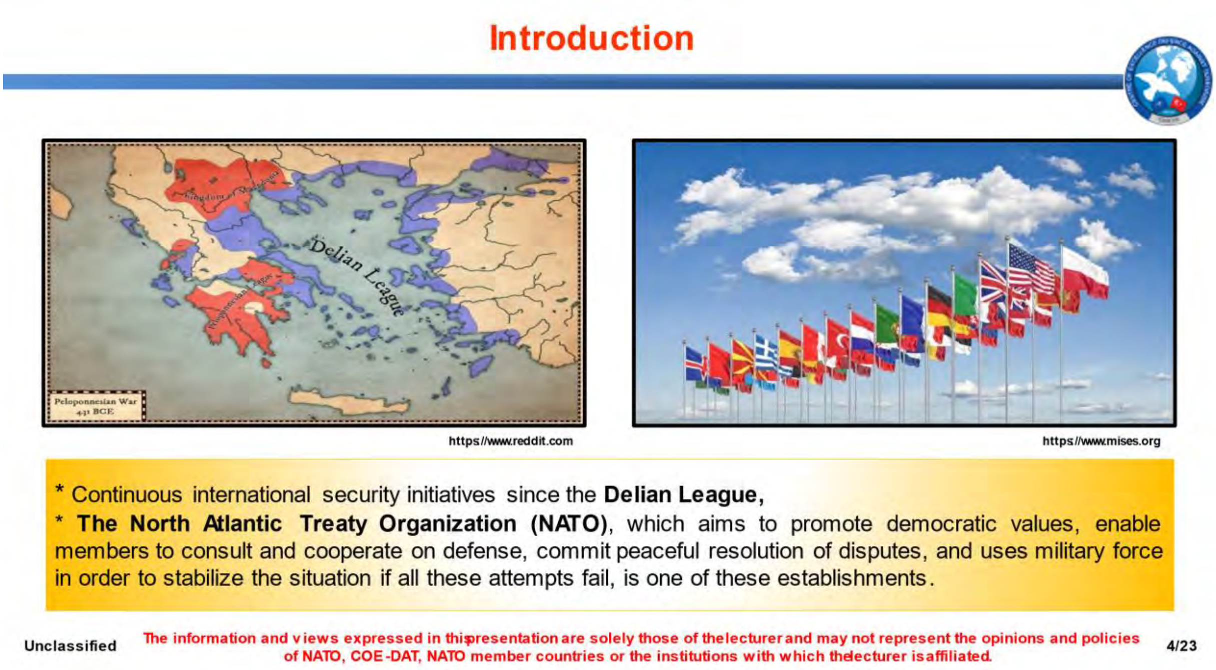
DAY 1

Session 1 – 70th Anniversary of Türkiye's Inaguration to NATO - Contributions of COE-DAT to Counter Terrorism

Col. Oğuzhan PEHLİVAN (PhD)

Dear Generals, Ladies and Gentlemen, Distinguished Visitors,

This year, we celebrated on 18 February the 70th Anniversary of Türkiye's inauguration to NATO. Meantime, 18 also refers to the CEO-DAT anniversary. Today I will present you content analysis main findings of my article for our academic e-journal "***Defense Against Terrorism Review (DATR)".***



Introduction

Kingdom of Macedon
Delian League
Peloponnesian League
Peloponnesian War 431 BCE

https//www.reddit.com

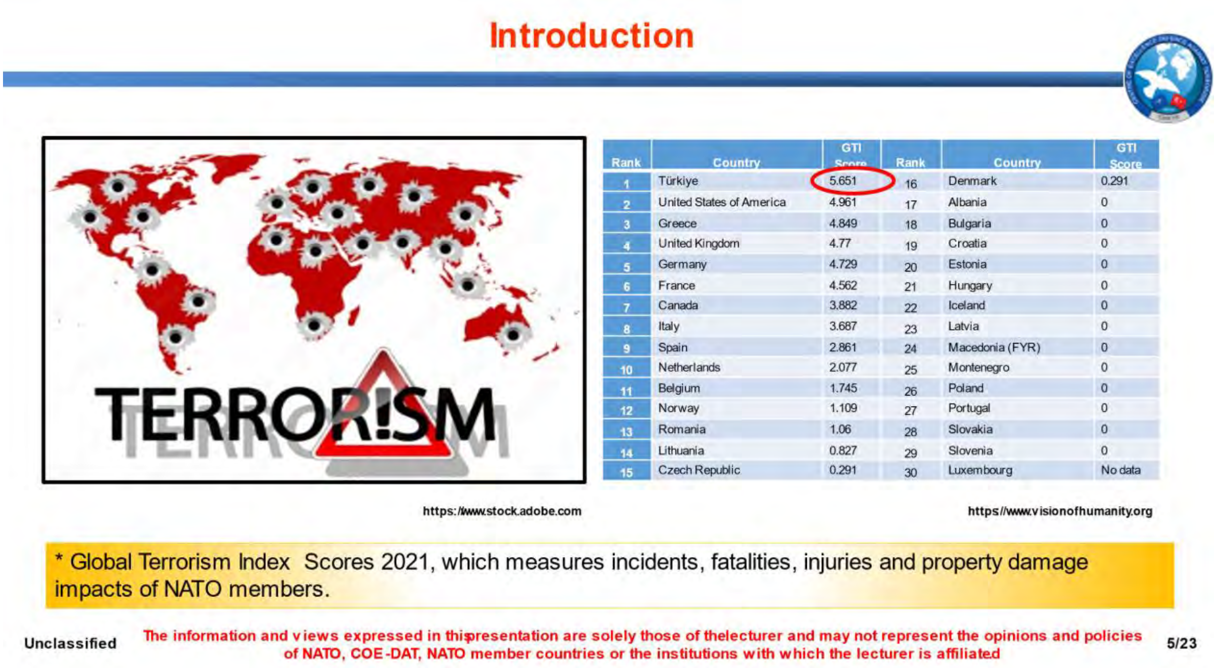
https//www.mises.org

* Continuous international security initiatives since the **Delian League,**
* **The North Atlantic Treaty Organization (NATO)**, which aims to promote democratic values, enable members to consult and cooperate on defense, commit peaceful resolution of disputes, and uses military force in order to stabilize the situation if all these attempts fail, is one of these establishments.

Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated. 4/23

There have always been international security initiatives since the Delian League, which was founded in 478 BC, to prevent conflicts and support peace.

The **North Atlantic Treaty Organization** (NATO), which aims to promote democratic values, enable members to consult and cooperate on defense, commit peaceful resolution of disputes, and uses military force in order to stabilize the situation if all these attempts fail, is one of these establishments.



Introduction

Rank	Country	GTI Score	Rank	Country	GTI Score
1	Türkiye	5.651	16	Denmark	0.291
2	United States of America	4.961	17	Albania	0
3	Greece	4.849	18	Bulgaria	0
4	United Kingdom	4.77	19	Croatia	0
5	Germany	4.729	20	Estonia	0
6	France	4.562	21	Hungary	0
7	Canada	3.882	22	Iceland	0
8	Italy	3.687	23	Latvia	0
9	Spain	2.861	24	Macedonia (FYR)	0
10	Netherlands	2.077	25	Montenegro	0
11	Belgium	1.745	26	Poland	0
12	Norway	1.109	27	Portugal	0
13	Romania	1.06	28	Slovakia	0
14	Lithuania	0.827	29	Slovenia	0
15	Czech Republic	0.291	30	Luxembourg	No data

https://www.stock.adobe.com

https//www.visionofhumanity.org

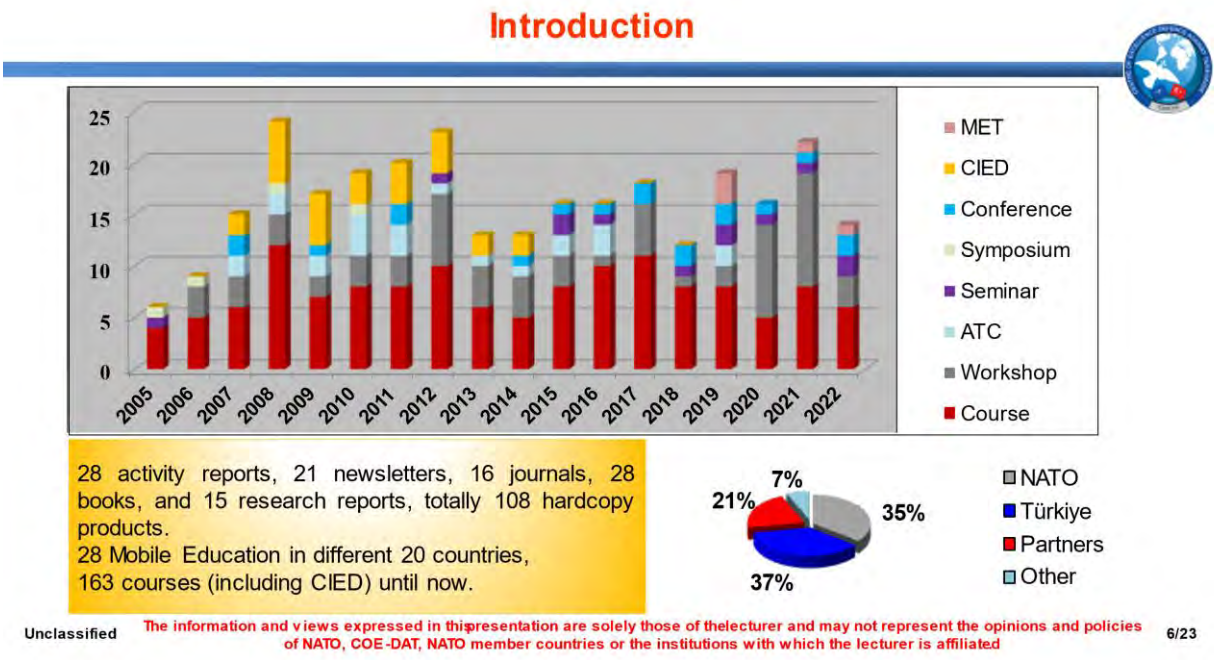
* Global Terrorism Index Scores 2021, which measures incidents, fatalities, injuries and property damage impacts of NATO members.

Unclassified

The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

5/23

Terrorism has been one of the two main security threats of NATO since 9/11 all over the world. Türkiye, when it is compared with other NATO member states, is deemed to be most affected by terrorism according to the Global Terrorism Index (GTI) 2021, which measures incidents, fatalities, injuries and property damage impacts as shown in the slide.



Introduction

28 activity reports, 21 newsletters, 16 journals, 28 books, and 15 research reports, totally 108 hardcopy products.
28 Mobile Education in different 20 countries,
163 courses (including CIED) until now.

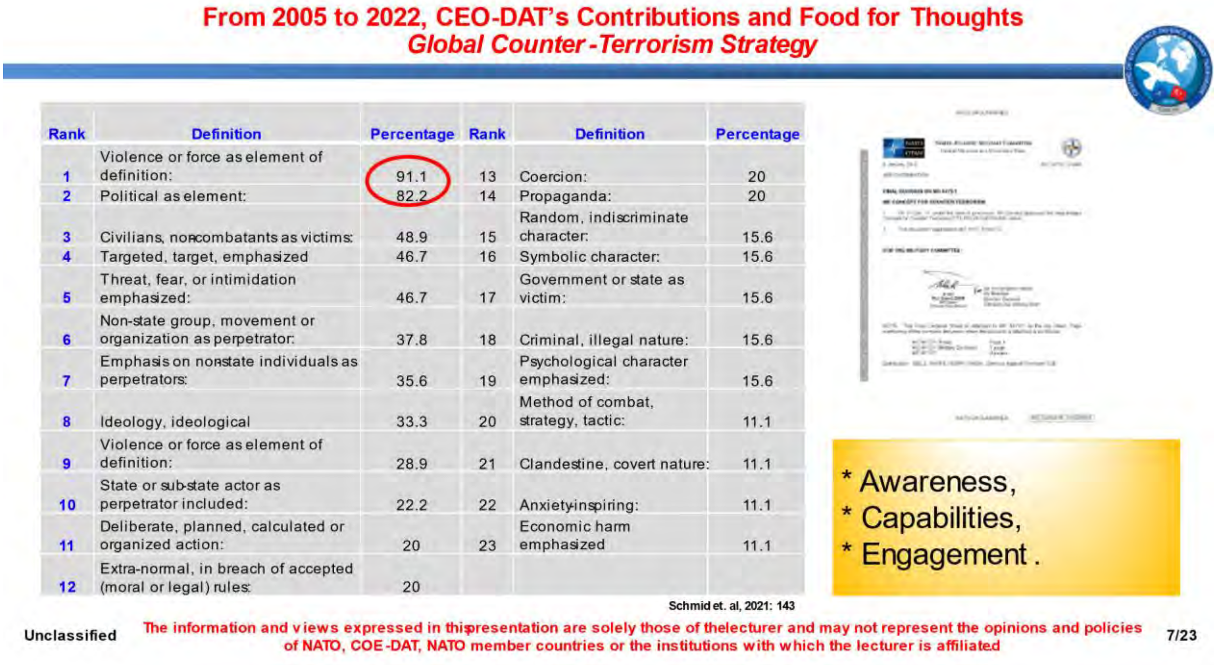
Unclassified

The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

6/23

As the second COE that achieved the accreditation from NATO, COE-DAT received the "**International Military Organization**" status in 2006, and has conducted courses, seminars, workshops, conferences, Mobile Education Teams (MET's) and projects successfully for both NATO and partner nations all over the world.

COE-DAT is a hub for counter-terrorism expertise and interacting with universities, think tanks, researchers, international organizations, global partners, and other COE's. As a result of this fruitful collaboration, COE-DAT has published 28 activity reports, 21 newsletters, 16 journals, 28 books, and 14 research reports, totally 107 hardcopy products. COE-DAT has conducted 28 Mobile Education in different 20 countries, and executed 163 courses (excluding CIED) until now. COE-DAT is additionally appointed as the DH for Alliance CT E&T by Supreme Allied Commander Transformation (SACT).



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Global Counter-Terrorism Strategy

Rank	Definition	Percentage	Rank	Definition	Percentage
1	Violence or force as element of definition:	91.1	13	Coercion:	20
2	Political as element:	82.2	14	Propaganda:	20
3	Civilians, noncombatants as victims:	48.9	15	Random, indiscriminate character:	15.6
4	Targeted, target, emphasized	46.7	16	Symbolic character:	15.6
5	Threat, fear, or intimidation emphasized:	46.7	17	Government or state as victim:	15.6
6	Non-state group, movement or organization as perpetrator:	37.8	18	Criminal, illegal nature:	15.6
7	Emphasis on nonstate individuals as perpetrators:	35.6	19	Psychological character emphasized:	15.6
8	Ideology, ideological	33.3	20	Method of combat, strategy, tactic:	11.1
9	Violence or force as element of definition:	28.9	21	Clandestine, covert nature:	11.1
10	State or sub-state actor as perpetrator included:	22.2	22	Anxiety-inspiring:	11.1
11	Deliberate, planned, calculated or organized action:	20	23	Economic harm emphasized	11.1
12	Extra-normal, in breach of accepted (moral or legal) rules:	20			

Schmid et. al, 2021: 143

* Awareness,
* Capabilities,
* Engagement .

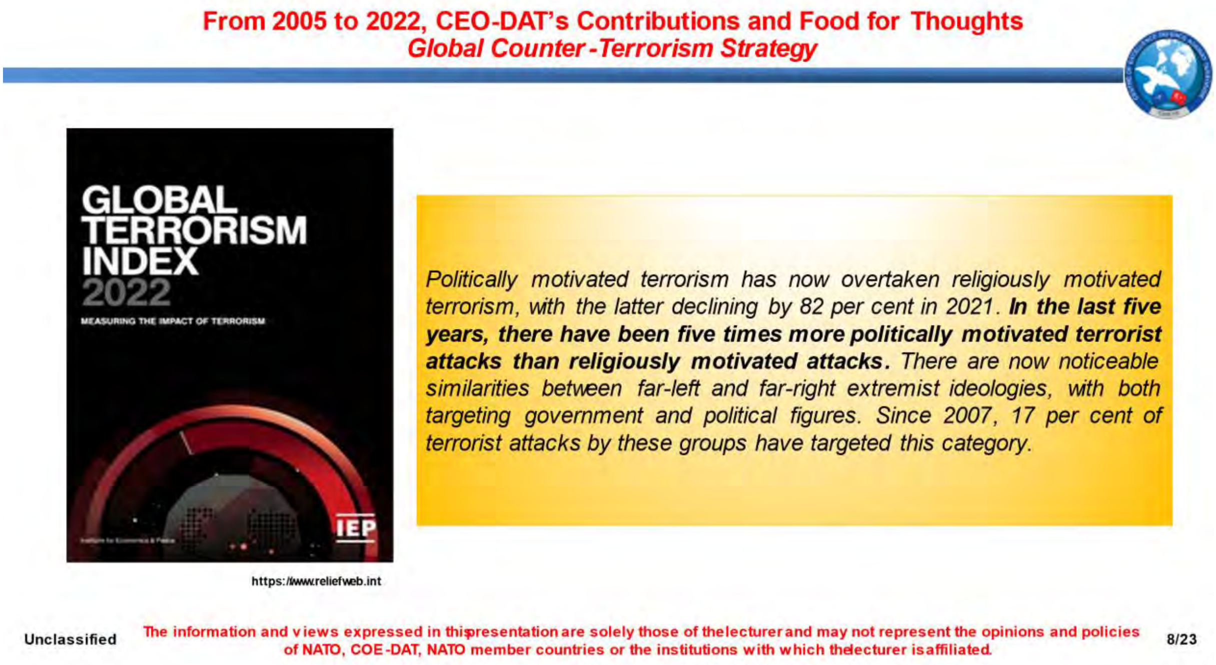
Unclassified

The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

7/23

Today, there is no single definition of Terrorism existing, and its meaning unfortunately changes according to its usage by states and international organizations. One of the recent studies indicated that even though there is a great compromise on the top two items, there has been less agreement on the other terms as shown in the slide.

In order to construct a counter-terrorism strategy, the first step should be to define terrorism and counter terrorism. This is the reason why NATO constituted the **MC0472/1** document in 2016. COE-DAT contributed great effort on the preparation process by focusing on underlying principles and potential initiatives in relation to *Awareness, Capabilities and Engagement* to enhance the Alliance's prevention of, response and resilience to acts of terrorism.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Global Counter-Terrorism Strategy

GLOBAL TERRORISM INDEX 2022
MEASURING THE IMPACT OF TERRORISM
IEP

Politically motivated terrorism has now overtaken religiously motivated terrorism, with the latter declining by 82 per cent in 2021. ***In the last five years, there have been five times more politically motivated terrorist attacks than religiously motivated attacks.*** *There are now noticeable similarities between far-left and far-right extremist ideologies, with both targeting government and political figures. Since 2007, 17 per cent of terrorist attacks by these groups have targeted this category.*

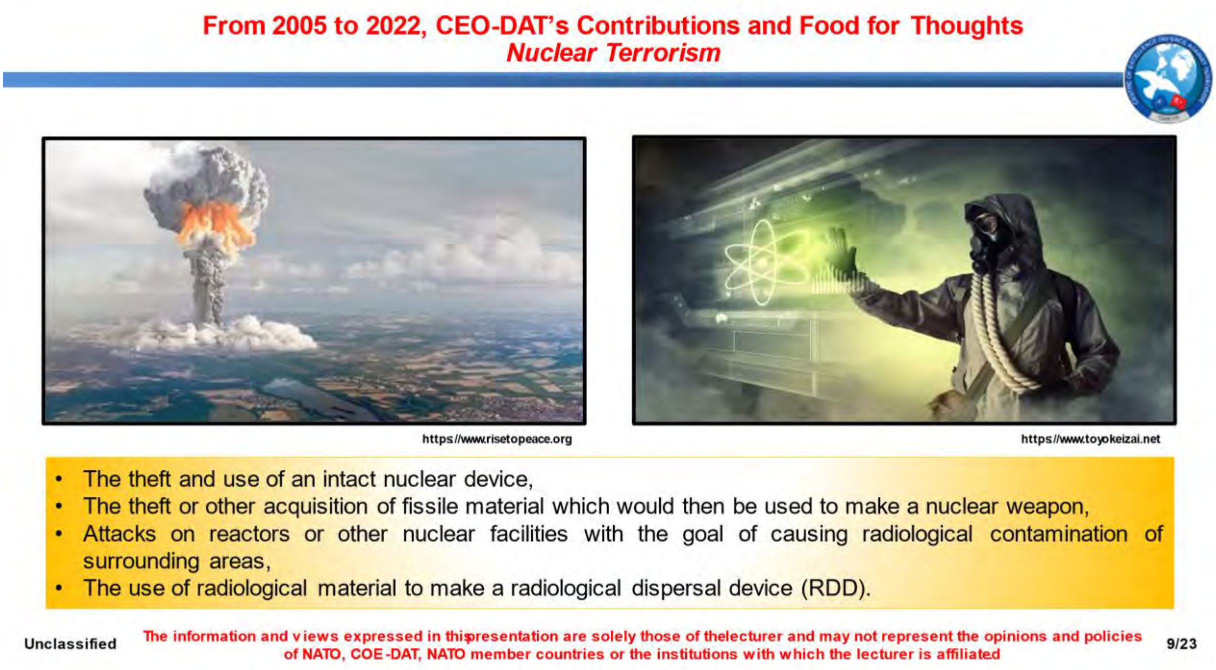
https://www.reliefweb.int

Unclassified The information and views expressed in thispresentation are solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated. 8/23

The Global Terrorism Index (2022) report mentioned that even though religiously motivated terrorism worldwide is dominant, politically motivated terrorism is additionally on the rise. According to this report,

> "*Politically motivated terrorism has now overtaken religiously motivated terrorism, with the latter declining by 82 per cent in 2021. In the last five years, there have been five times more politically motivated terrorist attacks than religiously motivated attacks. There are now noticeable similarities between far-left and far-right extremist ideologies, with both targeting government and political figures. Since 2007, 17 per cent of terrorist attacks by these groups have targeted this category.*"

Therefore, extremism and radicalism also should be handled and examined together with terrorism.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts

Nuclear Terrorism

https//www.risetopeace.org

https//www.toyokeizai.net

- The theft and use of an intact nuclear device,
- The theft or other acquisition of fissile material which would then be used to make a nuclear weapon,
- Attacks on reactors or other nuclear facilities with the goal of causing radiological contamination of surrounding areas,
- The use of radiological material to make a radiological dispersal device (RDD).

Unclassified

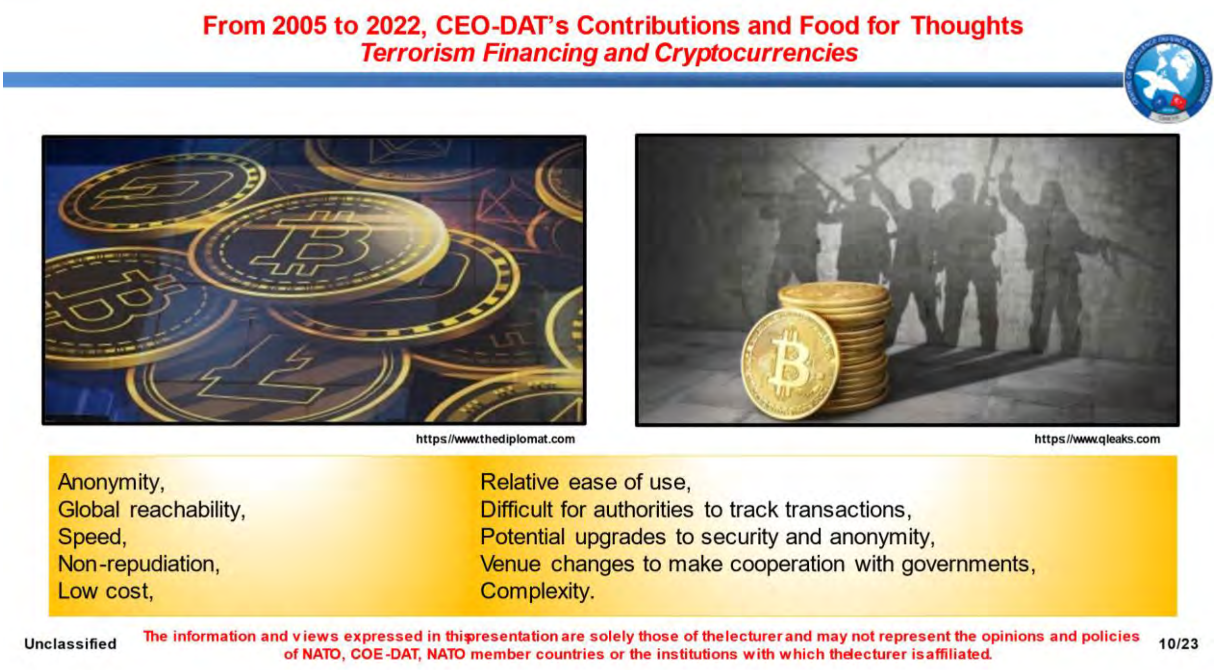
The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated

9/23

Nuclear terrorism combines four main types of terrorist activity. First, the theft and use of an intact nuclear device; second, the theft or other acquisition of fissile material which would then be used to make a nuclear weapon; third, attacks on reactors or other nuclear facilities with the goal of causing radiological contamination of surrounding areas; and last, the use of radiological material to make a radiological dispersal device (RDD).

To counter radiological/nuclear terrorist attacks effectively it requires that standards for securing weapons and materials are set at high level that terrorists simply cannot exploit any compromises or gaps in the defenses.

For the future, in order to prevent nuclear terrorism neural and social networks incorporated with system dynamics, which use data mining systems by cloud computing technology, should be constructed to enable systematic research on cell phones against possible terrorist incidents. I suggest to use big data and artificial intelligence (AI) to provide security and resilience.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts

Terrorism Financing and Cryptocurrencies

https//www.thediplomat.com

https//www.qleaks.com

Anonymity,
Global reachability,
Speed,
Non-repudiation,
Low cost,

Relative ease of use,
Difficult for authorities to track transactions,
Potential upgrades to security and anonymity,
Venue changes to make cooperation with governments,
Complexity.

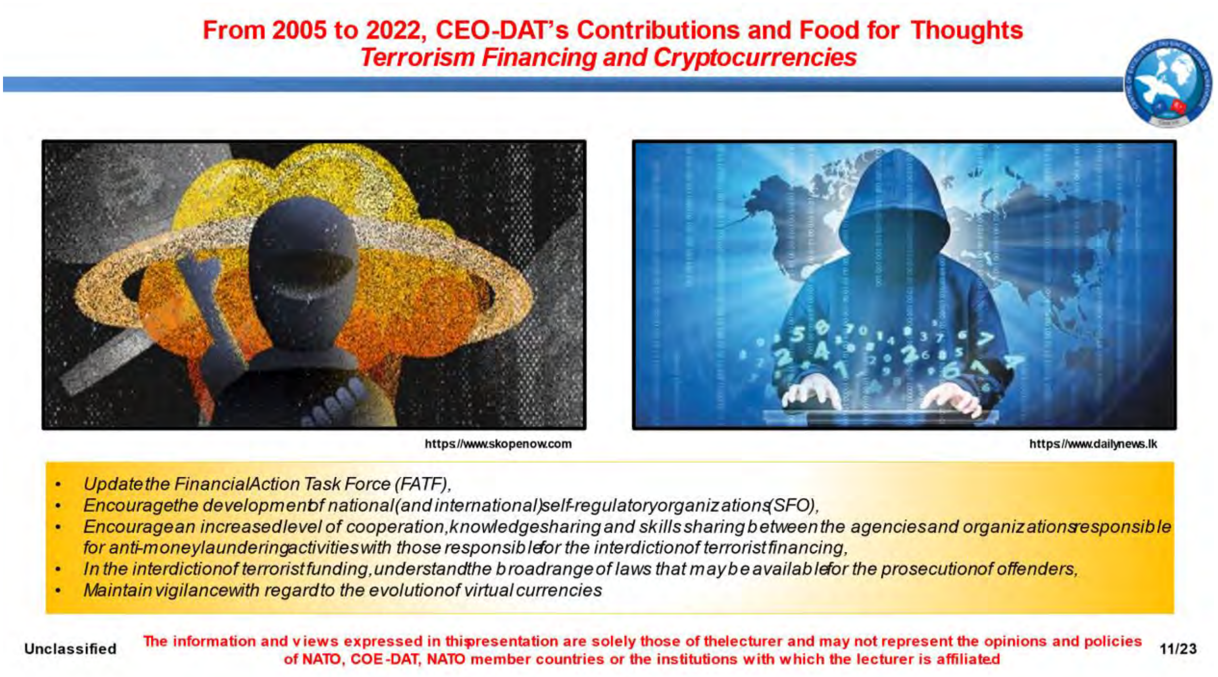
Unclassified

The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.

10/23

Cryptocurrencies are not backed by any government agency. And they have characteristics that make them attractive to those, who might use them for money laundering, for narcotics or human trafficking or even as a vehicle for global terrorist funding.

Cryptocurrencies are created with the help of block chain technology by solving extremely difficult mathematical problems. That is why this new system is attractive for terrorists for mainly ten reasons. First, it is *anonymity*. In this system, nobody has a regulation to show his/her ID card. *Global reachability* is another attractive reason. *Speed* enhances the system to transfer quickly any amount. *Non-repudiation* provides no additional verification. *Low cost to use* makes the system more desirable. *Relative ease of use* mitigates the technical difficulties. *Difficult for authorities to track transactions* is likely the most attractive part that draw attention of terrorists. *Potential upgrades to security and anonymity* cause law enforcement and anti-terrorism agencies to keep theirs weather eye open in order to enhance security. *Venue changes to make cooperation with governments* need collaboration of states and construction of unilateral understanding on terminology. At final stage, *complexity* makes the track of currency nearly impossible.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts

Terrorism Financing and Cryptocurrencies

https://www.skopenow.com

https://www.dailynews.lk

- *Update the Financial Action Task Force (FATF),*
- *Encourage the development of national (and international) self-regulatory organizations (SFO),*
- *Encourage an increased level of cooperation, knowledge sharing and skills sharing between the agencies and organizations responsible for anti-money laundering activities with those responsible for the interdiction of terrorist financing,*
- *In the interdiction of terrorist funding, understand the broad range of laws that may be available for the prosecution of offenders,*
- *Maintain vigilance with regard to the evolution of virtual currencies*

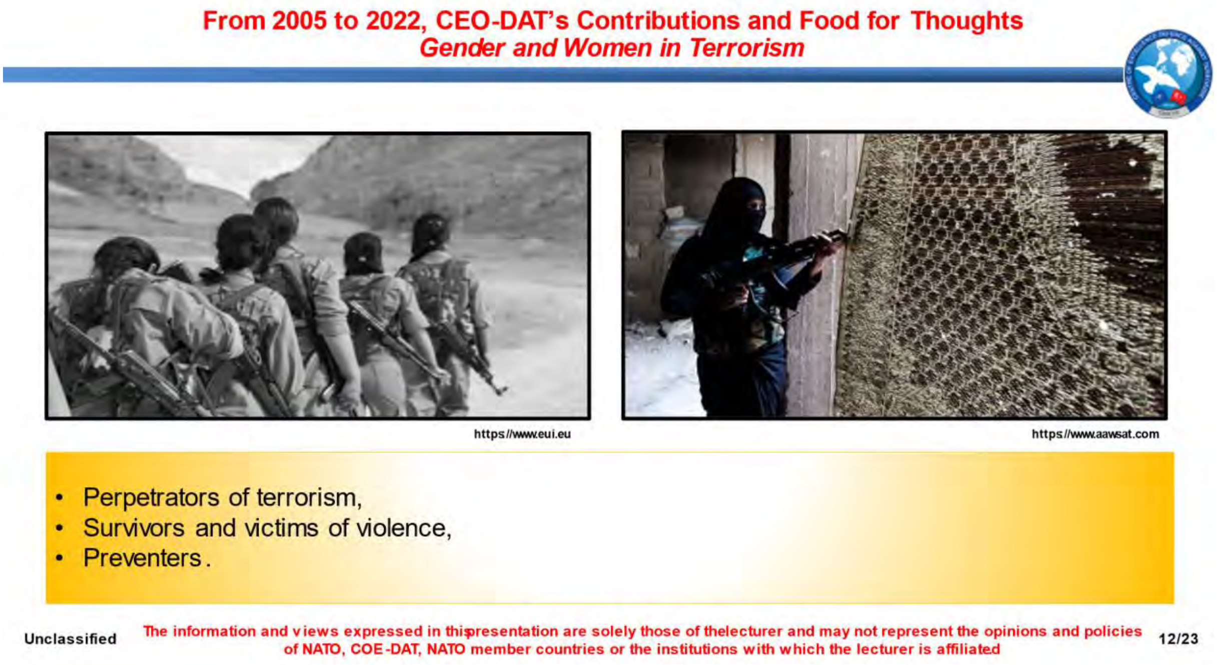
Unclassified

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

11/23

The recommendations and further developments in these topics are listed below.

- *Update the Financial Action Task Force (FATF).*
- *Encourage the development of national (and international) self-regulatory organizations (SFO).*
- *Encourage an increased level of cooperation, knowledge sharing and skills sharing between the agencies and organizations responsible for anti-money laundering activities with those responsible for the interdiction of terrorist financing.*
- *In the interdiction of terrorist funding, understand the broad range of laws that may be available for the prosecution of offenders.*
- *Maintain vigilance with regard to the evolution of virtual currencies.*



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Gender and Women in Terrorism

https://www.eui.eu

https://www.aawsat.com

- Perpetrators of terrorism,
- Survivors and victims of violence,
- Preventers.

Unclassified

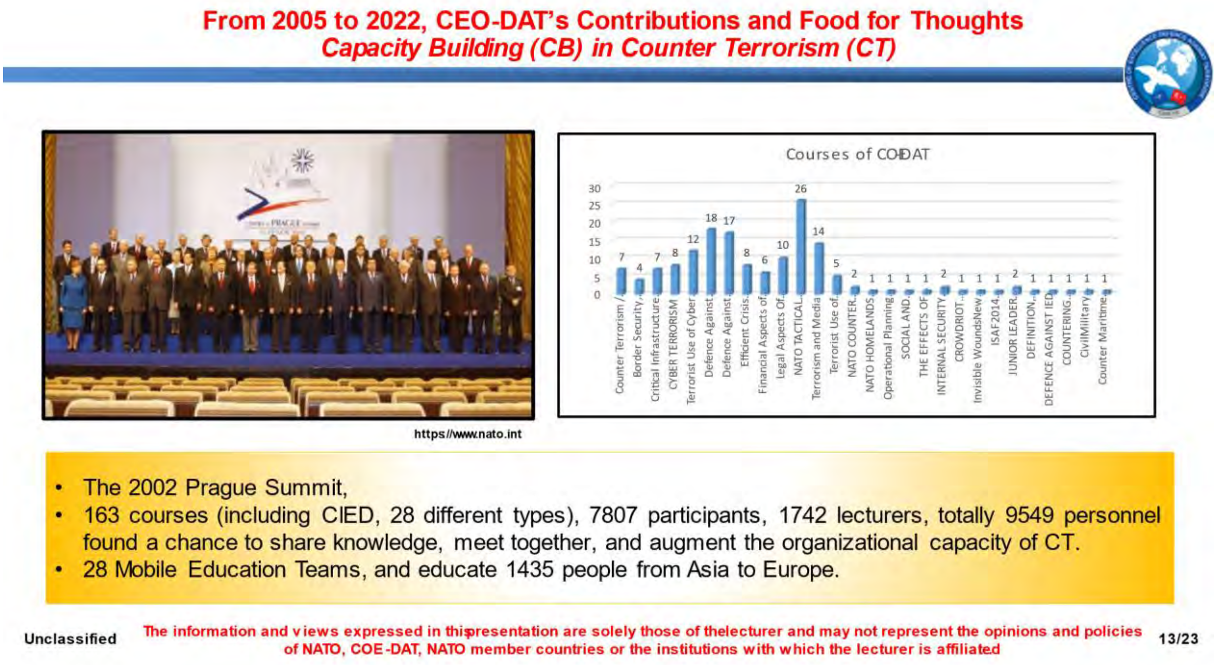
The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

12/23

Perceptions of gender roles and the linkage to gender being a women's "issue" creates a "blind spot" in counter terrorism efforts. Gender is more than women and men as gender is a socially constructed phenomenon not a biological one.

Generally, there is no perceptible disparity between men and women in some motivations, however, when the gender roles are considered it was brought to light or detected that some reasons cannot be same.

Women can play a number of roles. They can be *perpetrators of terrorism*, they can be sympathisers or enablers and they can be mobilisers. They can be **s***urvivors and victims of violence,* and they can be the target of restrictions on women's rights. They can also be *preventers*, peace activists and community leaders. Diyarbakır Mothers is a good example for preventing terrorism.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Capacity Building (CB) in Counter Terrorism (CT)

https//www.nato.int

- The 2002 Prague Summit,
- 163 courses (including CIED, 28 different types), 7807 participants, 1742 lecturers, totally 9549 personnel found a chance to share knowledge, meet together, and augment the organizational capacity of CT.
- 28 Mobile Education Teams, and educate 1435 people from Asia to Europe.

Unclassified

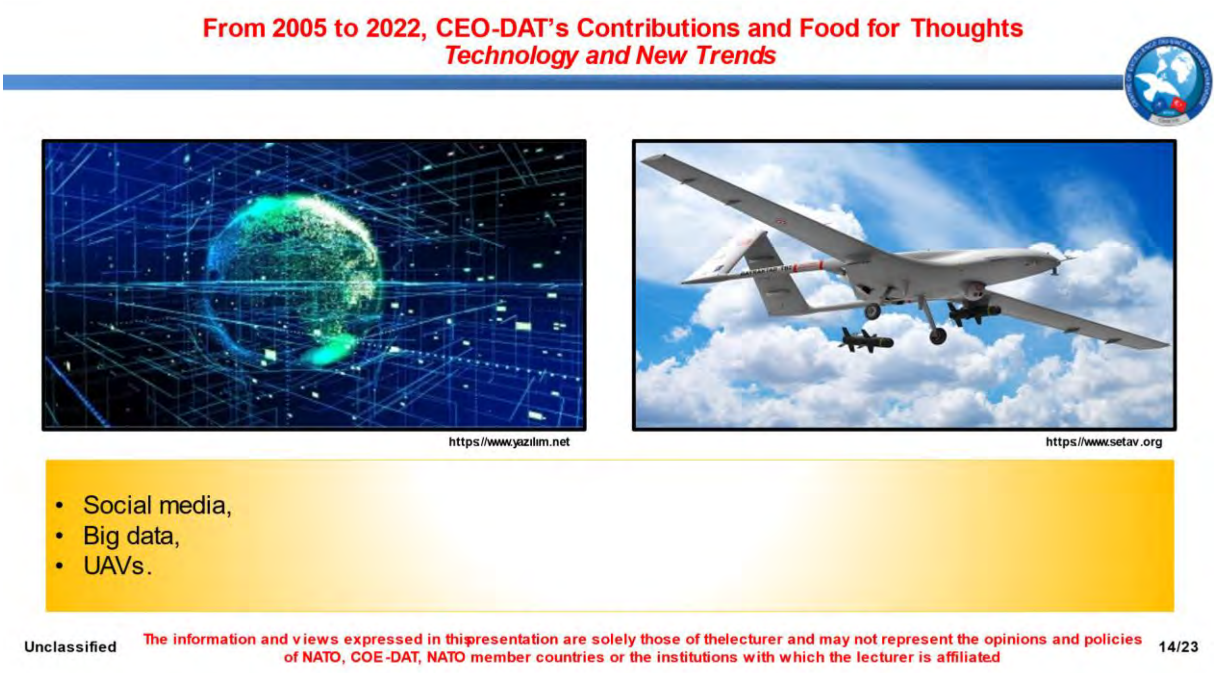
The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

13/23

The 2002 Prague Summit is the milestone for inclusion of CT as a mission within CB.

COE-DAT has committed itself the effort and contributed greatly to CB of NATO in CT. Since the inauguration, COE-DAT has conducted totally 163 courses (including CIED, 28 different types), and in these activities 7807 participants, 1742 lecturers, totally 9549 personnel found a chance to share knowledge, meet together, and augment the organizational capacity of CT. Currently, COE-DAT has executed 8 courses in 2022, and planned 9 courses in 2023. Further, besides residential courses, in order to reach unreachable, COE-DAT has been constructed 28 Mobile Education Teams, and educate **1435** people from Asia to Europe. By the way, these efforts on capacity building also strengthen the bounds with NATO and partner nations.

The workshops, seminars and conferences are additional values that contribute.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Technology and New Trends

https//www.yazılım.net

https//www.setav.org

- Social media,
- Big data,
- UAVs.

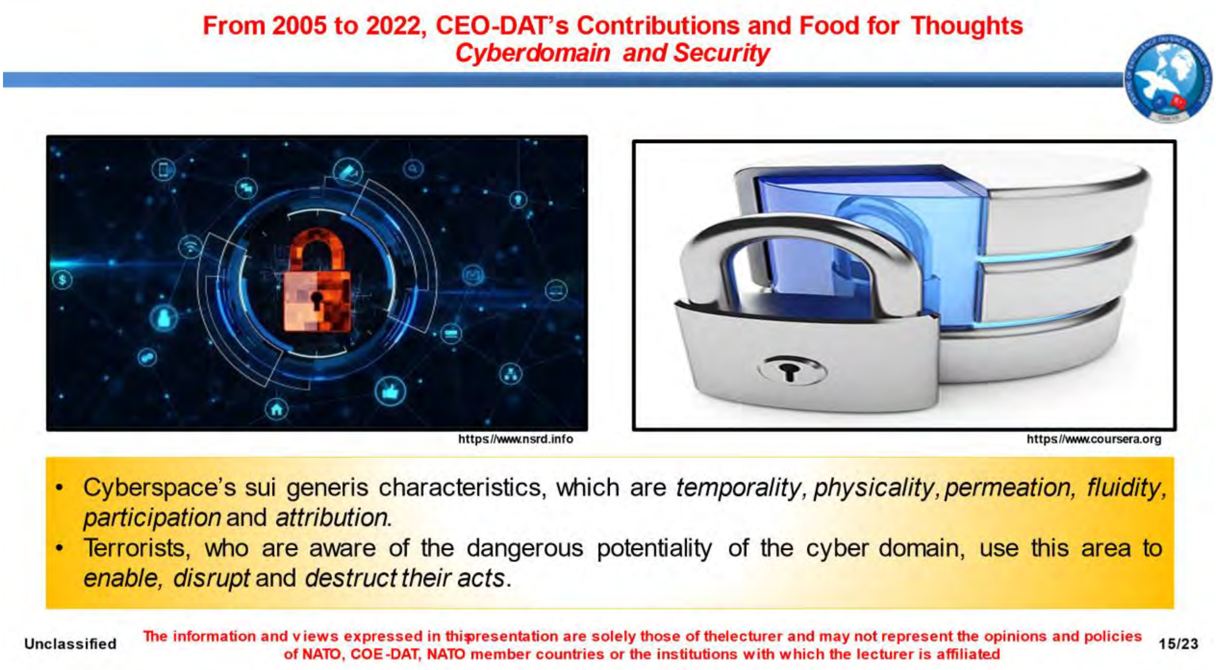
Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated 14/23

Terrorist organizations have exploited technology usage especially in social media.

Exploitation of big data inevitably requires the rapid and accurate sharing of information with appropriate individuals and organizations to make effective use of it. For example, CIA recognized that the pace in the commercial sector of innovation data management was clearly surpassing that of the national agencies.

Unmanned air vehicles (UAV) is another challenge in recent years. Easily accessibility, manufacturability with 3D printer usage and low cost are the main advantages of UAV that make its use attractive for terrorist organisations. There are different categories ranging from mini to decoys, and among these types mass, range, flight altitude and endurance are changed according to the model.

While DAESH used drones for the first time in Syria in August 2014 for propaganda and reconnaissance purposes, PKK/KCK terrorist organization used them for their swarm attack like in November 2018.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts

Cyberdomain and Security

https//www.nsrd.info

https//www.coursera.org

- Cyberspace's sui generis characteristics, which are *temporality, physicality, permeation, fluidity, participation* and *attribution.*
- Terrorists, who are aware of the dangerous potentiality of the cyber domain, use this area to *enable, disrupt* and *destruct their acts*.

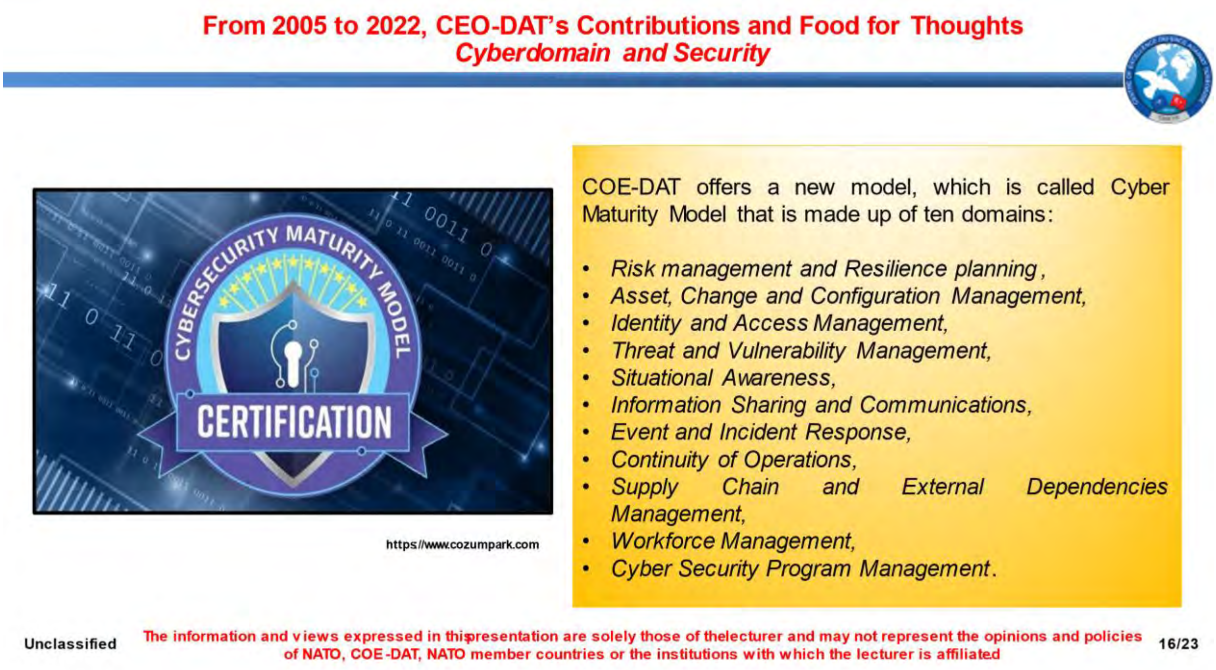
Unclassified

The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated

15/23

Cyberspace's *sui generis* characteristics, which are ***temporality, physicality, permeation, fluidity, participation*** and ***attribution***, have caused unexperienced feelings that people don't have in real world. Traditional threats that are secured by traditional security ways now have been replaced by emerging threats of the cyber domain.

Terrorists, who are aware of the dangerous potentiality of the cyber domain, use this area to *enable*, *disrupt* and *destruct* their acts. In order to provide the sustainability and prevent vulnerability, the cyber domain must be handled with a holistic approach, and besides protection of whole system also resilience must be enhanced.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Cyberdomain and Security

CYBERSECURITY MATURITY MODEL
CERTIFICATION

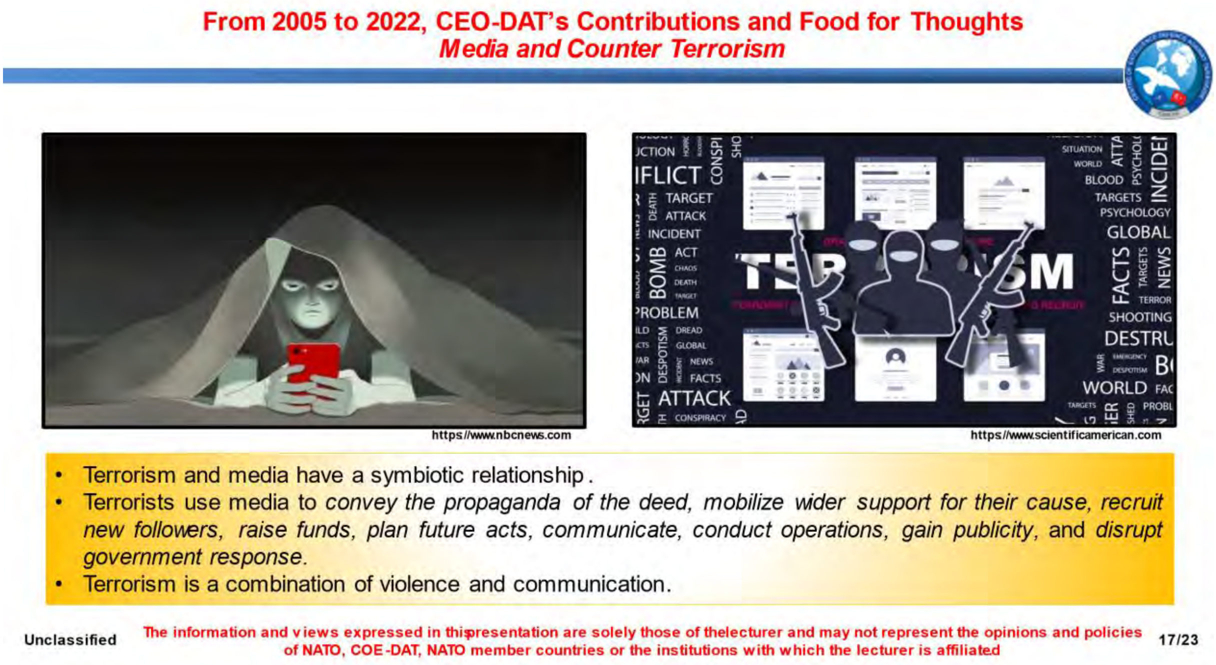
https//www.cozumpark.com

COE-DAT offers a new model, which is called Cyber Maturity Model that is made up of ten domains:

- *Risk management and Resilience planning,*
- *Asset, Change and Configuration Management,*
- *Identity and Access Management,*
- *Threat and Vulnerability Management,*
- *Situational Awareness,*
- *Information Sharing and Communications,*
- *Event and Incident Response,*
- *Continuity of Operations,*
- *Supply Chain and External Dependencies Management,*
- *Workforce Management,*
- *Cyber Security Program Management.*

Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated 16/23

COE-DAT offers a new model, which is called **Cyber Maturity Model**. The cyber maturity model is made up of ten domains as shown in slide. In a nutshell, this new cyber maturity model's implementation on the cyber domain of critical infrastructures should keep the system away from the risks and attacks of terrorists. But it must not be forgotten that the key factor is the people, who use this domain, so the construct of a robust cyber security environment should be tackled in advance.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Media and Counter Terrorism

TERRORISM
CONFLICT
TARGET
ATTACK
INCIDENT
BOMB
PROBLEM
GLOBAL
FACTS
NEWS
SHOOTING
WORLD

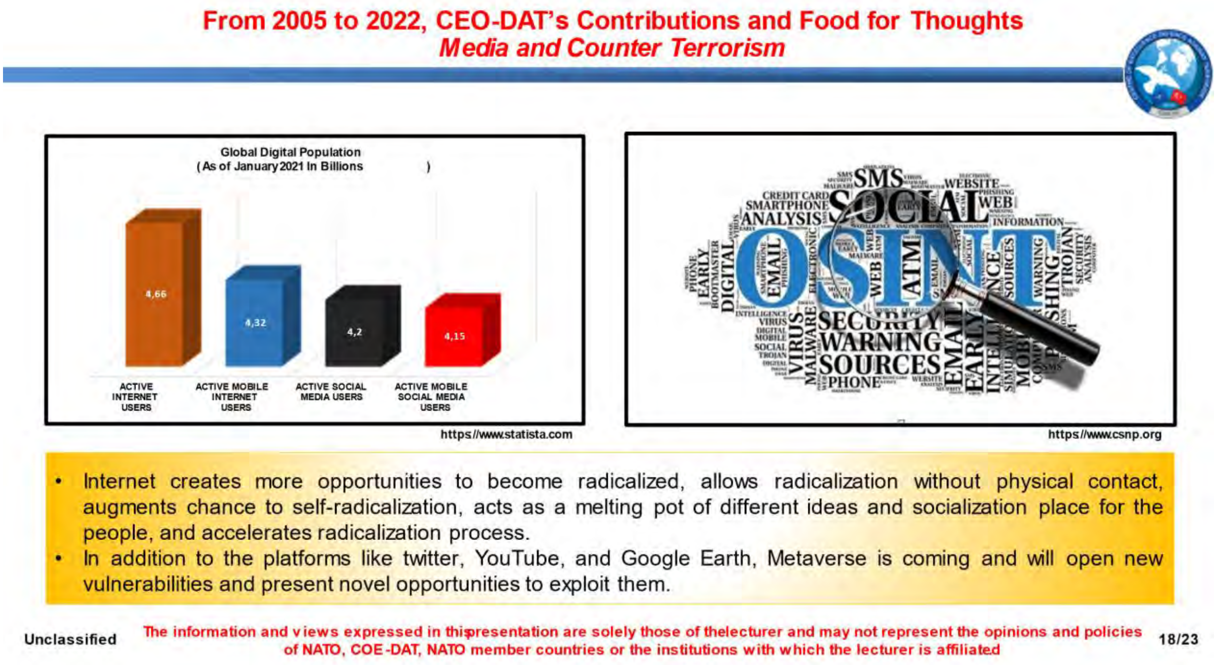
https//www.nbcnews.com

https//www.scientificamerican.com

- Terrorism and media have a symbiotic relationship.
- Terrorists use media to *convey the propaganda of the deed, mobilize wider support for their cause, recruit new followers, raise funds, plan future acts, communicate, conduct operations, gain publicity,* and *disrupt government response.*
- Terrorism is a combination of violence and communication.

Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated 17/23

Terrorism and media have a symbiotic relationship. Terrorists use media to *convey the propaganda of the deed, mobilize wider support for their cause, recruit new followers, raise funds, plan future acts, communicate, conduct operations, gain publicity,* and *disrupt government response.* It has been said that terrorism is a combination of violence and communication.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts
Media and Counter Terrorism

https//www.statista.com

https//www.csnp.org

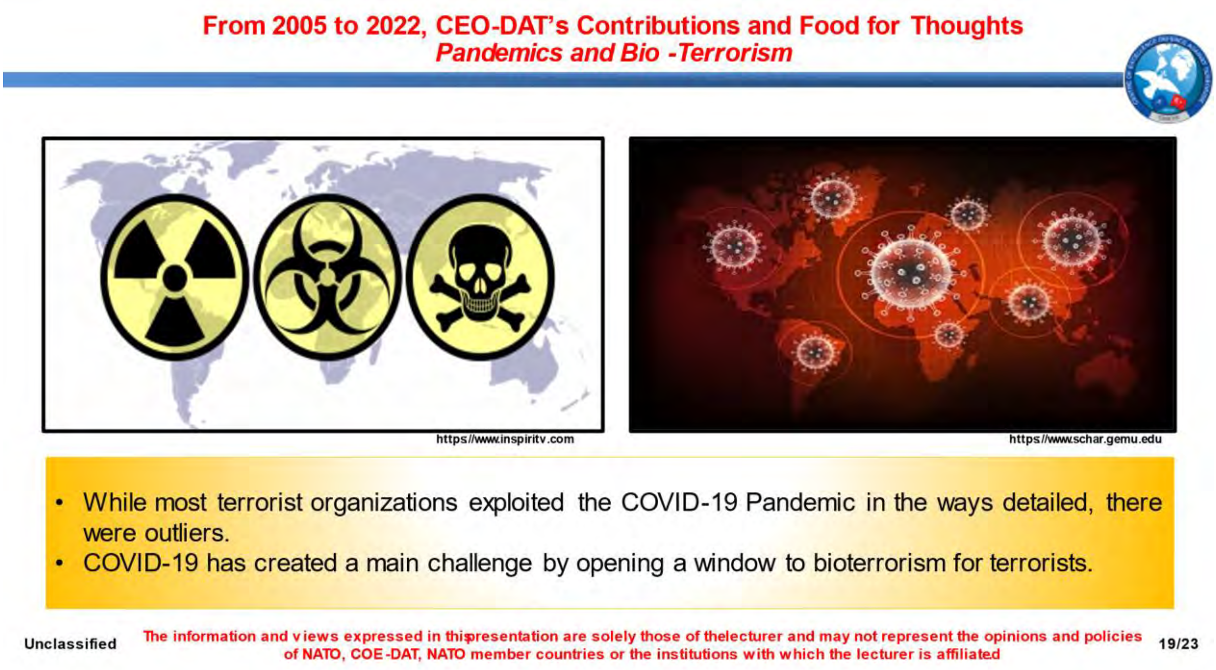
- Internet creates more opportunities to become radicalized, allows radicalization without physical contact, augments chance to self-radicalization, acts as a melting pot of different ideas and socialization place for the people, and accelerates radicalization process.
- In addition to the platforms like twitter, YouTube, and Google Earth, Metaverse is coming and will open new vulnerabilities and present novel opportunities to exploit them.

Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated 18/23

Since the late 1980s, the internet has proven to be a highly dynamic vehicle for communication, reaching now more than half of the global population. Internet usage increase the radicalization at the same time. Internet creates more opportunities to become radicalized, allows radicalization without physical contact, augments chance to self-radicalization, acts as a melting pot of different ideas and socialization place for the people, and accelerates radicalization process.

In addition to the platforms like Twitter, YouTube, and Google Earth, **Metaverse** is coming and will open new vulnerabilities and present novel opportunities to exploit them.

In order to prevent the usage of media platforms by terrorist organizations as a recruitment and communication area, initially states collaborate with each other on constituting establishments to observe and share the data. After 2020's, the new age of web 4.0 has begun, and this age needs advanced software developments techniques based on AI. Open-Source Intelligence (OSINT) is another useful way to detect and deter terrorists.



From 2005 to 2022, CEO-DAT's Contributions and Food for Thoughts

Pandemics and Bio -Terrorism

https//www.inspiritv.com

https//www.schar.gemu.edu

- While most terrorist organizations exploited the COVID-19 Pandemic in the ways detailed, there were outliers.
- COVID-19 has created a main challenge by opening a window to bioterrorism for terrorists.

Unclassified

The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated

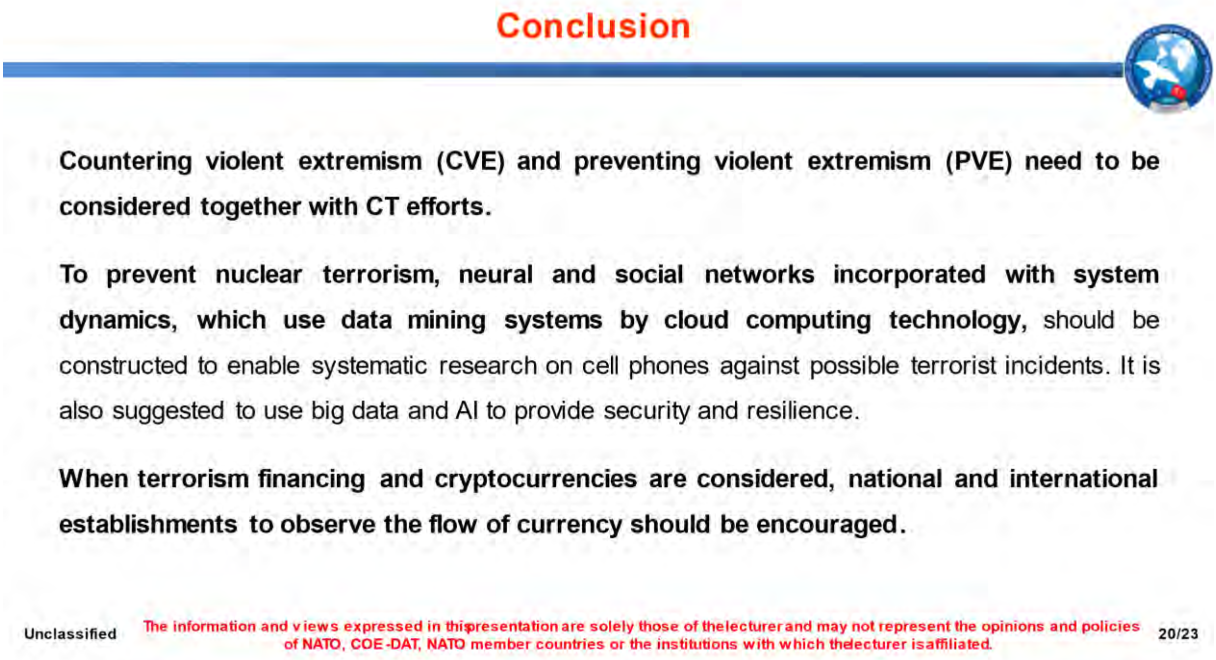
19/23

Bioterrorism is described as the deliberate release of biological agents to produce illness or death in people, animals, and plants.

While most terrorist organizations exploited the COVID-19 Pandemic in the ways detailed, there were outliers. These included the Afghan Taliban who allowed health workers into their areas and, at the other extreme, Racially & Ethnically Motivated Violent Extremist (REMVE) groups who exploited both circumstances and technology on a scale not seen amongst other groups.

COVID-19 has created a main challenge by opening a window to bioterrorism for terrorists.

Bioterrorism, which has low cost, easy obtainability and transferability, huge and invisible impact, has attracted the terrorist groups. In order to fight against terrorism, states need more collaboration than ever before.



Conclusion

Countering violent extremism (CVE) and preventing violent extremism (PVE) need to be considered together with CT efforts.

To prevent nuclear terrorism, neural and social networks incorporated with system dynamics, which use data mining systems by cloud computing technology, should be constructed to enable systematic research on cell phones against possible terrorist incidents. It is also suggested to use big data and AI to provide security and resilience.

When terrorism financing and cryptocurrencies are considered, national and international establishments to observe the flow of currency should be encouraged.

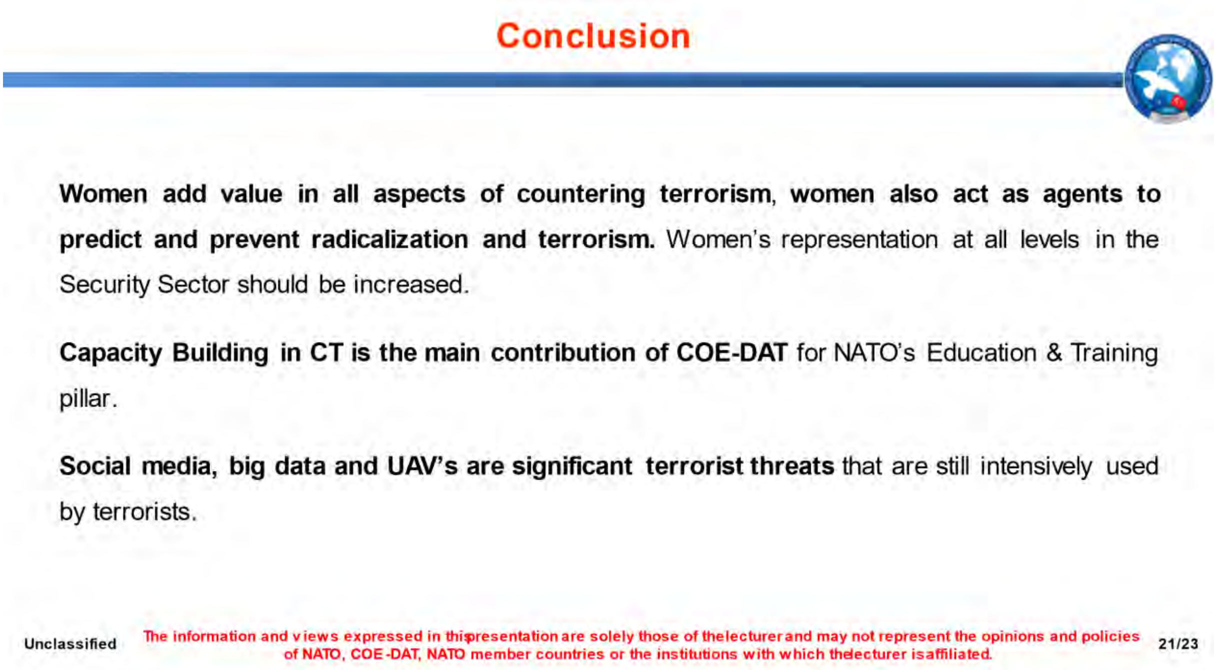
Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated. 20/23

As it is stated before, COE-DAT has added great value on the CT discipline by conducting courses, MET's, seminars, workshops, conferences, and projects. In this study, it is impossible to mention all information that has been collected since 2004. At the same time, while scrutinizing all of the products in advance, it has been found that some of the key findings are obsolete now. Therefore, at the end of the review of all materials, the efforts mainly intensify on nine areas that are mentioned in the second part of the study.

In the "**Global Counter-Terrorism Strategy**" part, it is strongly recommended that countering violent extremism (CVE) and preventing violent extremism (PVE) need to be considered together with CT efforts. Furthermore, radically and ethnically violent extremism (RMVEs), political terrorism, and domestic terrorism are the new challenges in defense against terrorism.

In the nuclear terrorism part, to prevent nuclear terrorism, neural and social networks incorporated with system dynamics, which use data mining systems by cloud computing technology, should be constructed to enable systematic research on cell phones against possible terrorist incidents. It is also suggested to use big data and AI to provide security and resilience.

When terrorism financing and cryptocurrencies are considered, it is revealed to encourage both national and international establishments to observe the flow of currency, to share knowledge, and to collaborate literately.



Conclusion

Women add value in all aspects of countering terrorism, women also act as agents to predict and prevent radicalization and terrorism. Women's representation at all levels in the Security Sector should be increased.

Capacity Building in CT is the main contribution of COE-DAT for NATO's Education & Training pillar.

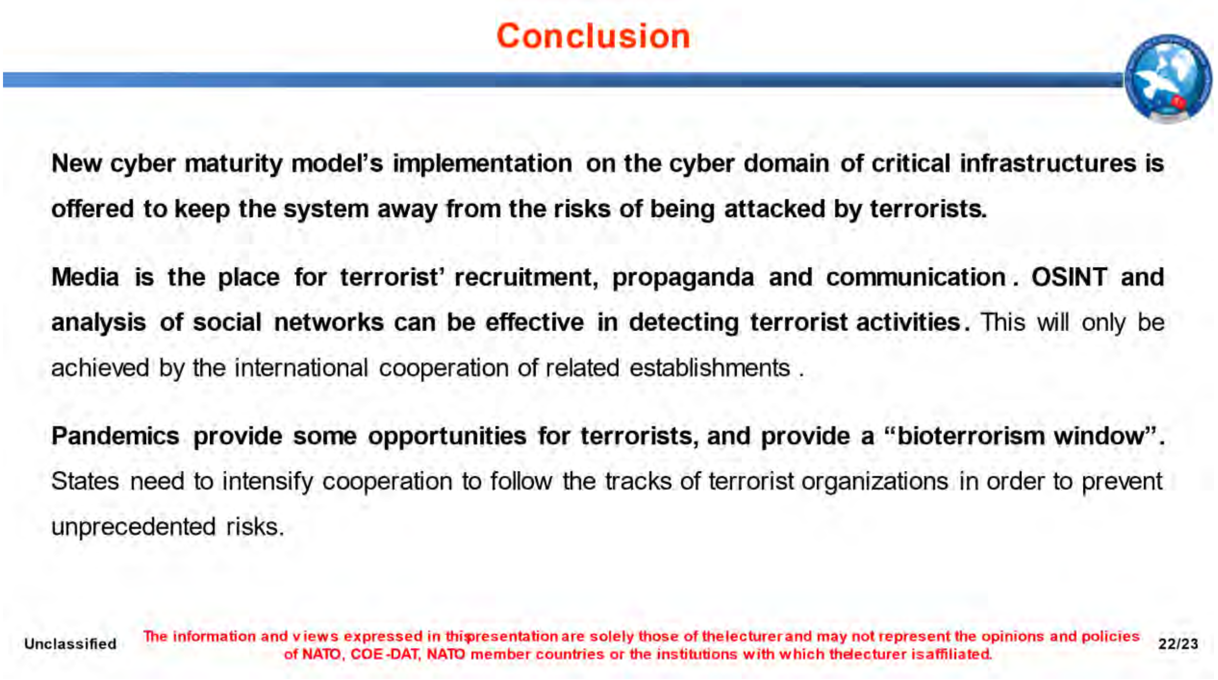
Social media, big data and UAV's are significant terrorist threats that are still intensively used by terrorists.

Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated. 21/23

It is clear that women add value in all aspects of countering terrorism, including analysis, field work, and policy development. In addition, women are involved in the same activities as men such as sympathizers, supporters, radicalizers, recruiters, facilitators, perpetrators, enablers, and combatants. Women also act as agents to predict and prevent radicalization and terrorism as well as are critical security actors that act as force multipliers to build trust and increase security. Women's representation at all levels in the Security Sector should be increased.

Capacity Building in CT is the main contribution of COE-DAT for NATO's Education & Training pillar. COE-DAT has the intention to start a project of "**Terrorism Exercise Scenario and CT Simulation Development**" next year. This project gives COE-DAT the opportunity to develop the skills of participants about applying their knowledge into practice. This project will also enhance the capacity of COE-DAT on writing concepts and doctrine.

Social media, big data and UAVs are significant terrorist threats that are still intensively used by terrorists.



Conclusion

New cyber maturity model's implementation on the cyber domain of critical infrastructures is offered to keep the system away from the risks of being attacked by terrorists.

Media is the place for terrorist' recruitment, propaganda and communication . OSINT and analysis of social networks can be effective in detecting terrorist activities. This will only be achieved by the international cooperation of related establishments .

Pandemics provide some opportunities for terrorists, and provide a "bioterrorism window". States need to intensify cooperation to follow the tracks of terrorist organizations in order to prevent unprecedented risks.

Unclassified The information and views expressed in thispresentation are solely those of thelecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated. 22/23

The Cyber domain seems to be one of the most dangerous parts in defense against terrorism. New cyber maturity model's implementation on the cyber domain of critical infrastructures is offered and it is believed that this model may keep the system away from the risks of being attacked by terrorists.

Media is the place for terrorist' recruitment, propaganda and communication. OSINT and analysis of social networks can be effective in detecting terrorist activities. This will only be achieved by the international cooperation of related establishments.

Pandemics provide some opportunities for terrorists, and provide a "bioterrorism window". States need to intensify cooperation to follow the tracks of terrorist organizations in order to prevent unprecedented risks.

Closing Remarks

You can follow COE -DAT activities by visiting website www.coedat.nato.int

Unclassified

23/23

COE-DAT, as in the past, will keep going on the route with a great determination, and contribute more efforts in the CT domain. The joint intelligence of framework and sponsoring nations of the centre will pave the way for a more safe and secure globe.

You can follow COE-DAT activities by visiting website.

This concludes my brief. Thanks.

Session 2 – Critical Infrastructure Security and Resilience Book 2

NATO Mission-Dependent Critical Infrastructure

Mr. Lucas COX

NATO faces a volatile global security environment. Russia's invasion of Ukraine has disrupted peace in Europe in a way unparalleled in decades. The **COVID-19 Pandemic** reminded the world of the challenge that is responding to **public health emergencies**. *Climate change* will continue to present challenges to international security.

Emergent technologies threaten international security and the security of NATO partner nations. However, NATO can also harness that same technology to promote defense, deterrence, and resilience. And that's what we're here to discuss, starting with the **Critical Infrastructure Resilience.**

Resilience is the capacity to recover quickly from threats. Critical components to strengthen resilience must emphasize building persistence, capacity consideration, education, and further training. In this sense, we also have to talk about **infrastructure,** which is simply "*the basic physical and organizational structures and facilities (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise*." Resilience is a combination of both civil preparedness and military capacity. **At the 2016 Warsaw Summit,** allied leaders committed to striving to achieve **seven baseline requirements for critical infrastructure resilience.** These are as follow:

1. Assured **continuity of government** and **critical government services**
2. Resilient **energy** supplies
3. The ability to deal effectively with **uncontrolled movement of people**
4. Resilient **food and water** resources
5. The ability to deal with **mass casualties**
6. Resilient civil **communications** systems
7. **And** resilient civil **transportation** systems

Many of these areas are codependent and require buy-in from civilian, military, and commercial sectors.

There are for primary means by which NATO can strengthen its resilience:

1. **emphasizing *persistence*** requires continuous assessments of how baseline resilience plans can improve
2. **capacity consideration** requires a holistic approach that focuses on innovation and collaboration
3. **education** ensures a well-informed public and includes continuously testing resilience
4. **and *furthering* training** requires comprehending all possible risks, and how systems behave when pushed to the point of failure.

Over the past months, we've seen **a few critical infrastructure failures** that have let **to deteriorated security situations**. Despite it being out-of-area for NATO, we found it important to use **recent developments in Kazakhstan** as a case study of how **systematic policy failure can lead to Critical Infrastructure failure.**

In January, riots broke out across Kazakhstan, originally in response to the **government lifting price caps on fuel**. The Kazakh government called on the Collective Security Treaty Organization to intervene, leading to the deployment of Russian and other forces into the country. The Kazakh example illustrates **how non-military aspects of critical infrastructure like negative energy supply shocks can really affect NATO security**. A similar situation within NATO territory could be taken advantage of by adversaries to strike during a moment of weakness.We may see this depending on how the situation in Ukraine and its economic consequences develop.

In a changing security environment**, an important step for NATO to strengthen its resilience is to test it.** For instance, the U.S. military has conducted **an energy resilience tests** that involved:

- deliberately **cutting off electricity** supplies to military bases to **test backup generators** and assessing impact on residents, as well as water and energy tests

- In coming years, the U.S. plans to complete **Installation Energy and Water Plans** to **assess any shortcomings** in the military's ability to **provide energy and water** during a crisis.
- The DHS also collaborates with the private sector to test new backup technologies and assess how AI can be used in disaster relief plans

In the cases where member states' infrastructure systems are synchronized, NATO could adopt a some of these frameworks for assessing critical infrastructure resilience. We have identified three main areas where NATO's Critical Infrastructure is most vulnerable:

1. The first is the **interconnectedness of different systems,** where one failure can cascade into system-wide collapse.
    - For example, over **7,000 power plants in the United States are dependent on other facilities and outside supply chains**
    - Transport system failures can debilitate supply chains during emergencies. We have therefore identified that **stable critical infrastructure requires self-reliant facilities.**
        - Current government **efforts** of strengthening resilience often **require voluntary participation from the private sector**, but that participation is **hard to secure**.
2. Which leads to our second vulnerability: **Lack of Voluntary Preparedness.**
    - **Governments offer information** about possible hazards to **incentivize the private sector,** this collaboration is hard to secure, especially against **high-risk, low-probability disasters**, like terrorist attacks.
    - This **lack of preparedness** in the private sector leaves **NATO vulnerable** because of **how much militaries rely** on civil and commercial assets.
3. Finally, the very protocols used to analyze vulnerabilities are not standardize and information is not shared adequately.
    - Some states also lack the funding, technology, or basic expertise required to create of follow preparedness plans.

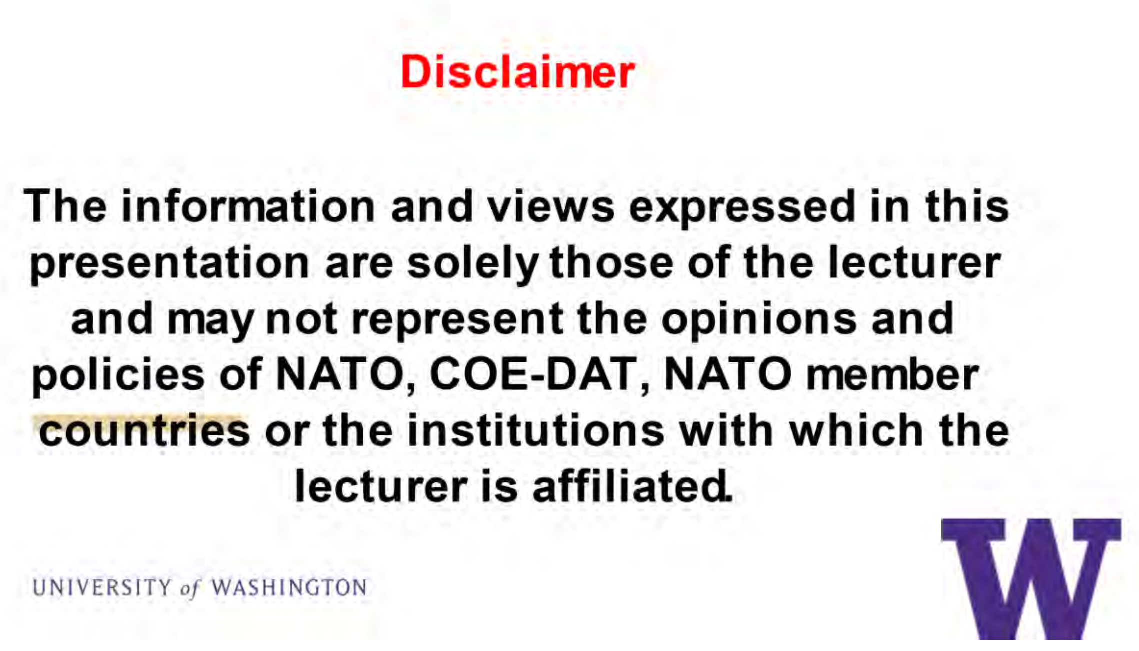
Overall, infrastructural interdependence, especially across border, and a lack preparedness leaves states vulnerable to critical infrastructure failures that can cascade to system-wide failure.

Presentation

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

NATO Critical Infrastructure Security and Resilience

UNIVERSITY of WASHINGTON



Disclaimer

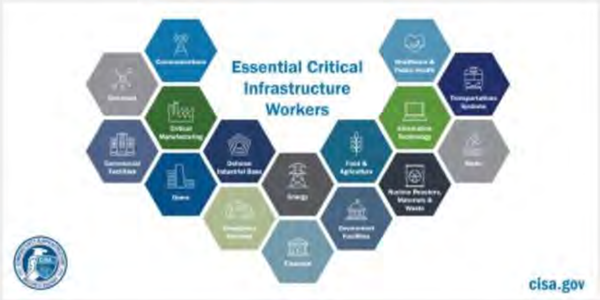
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

UNIVERSITY of WASHINGTON

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY *of* WASHINGTON

Resilience and Critical Infrastructure

Resilience is an alliance capacity that requires complete dedication to preparedness and adaptability to any threat of national security.



- Critical Infrastructure Subcategories
  - Critical National Infrastructure
  - Mission-vital Infrastructure
  - Key Infrastructure

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which the lecturer is affiliated.

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY *of* WASHINGTON

Resilience:

the capacity to recover quickly from threats.

1. Government continuity
2. Energy
3. Uncontrolled movement of people
4. Food and water
5. Mass casualties
6. Telecommunications
7. Transportation

Persistence, capacity consideration, education, and training

Peter Summers/Getty Images

The information and views expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.

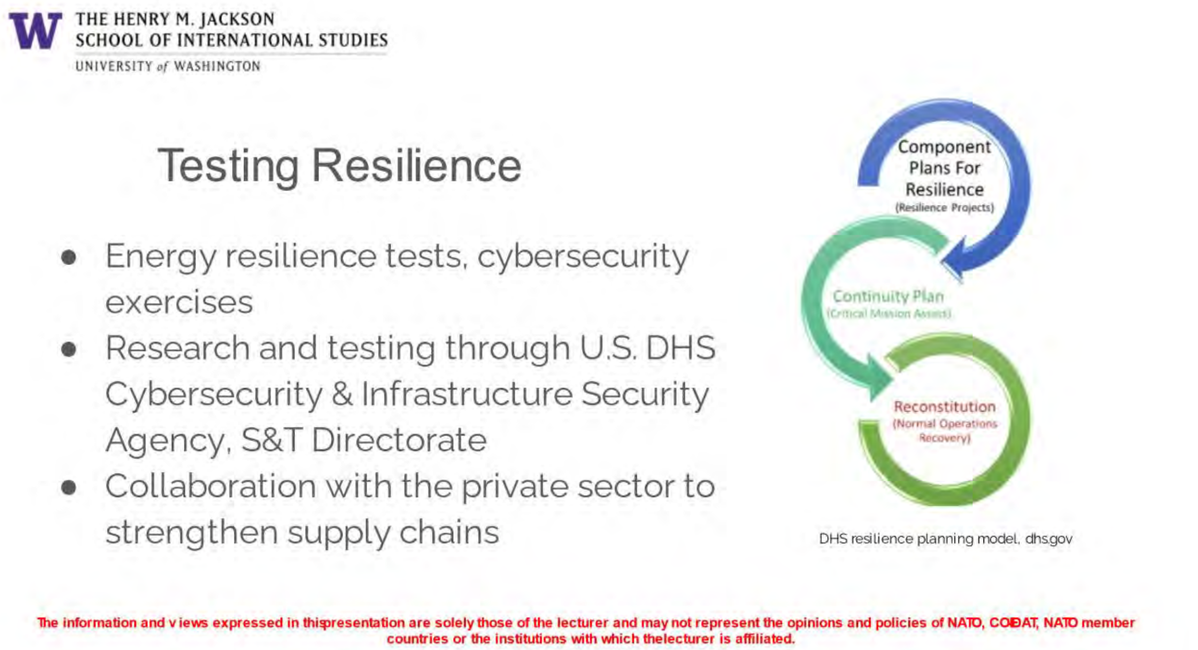
THE HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

Case Study: Kazakhstan and Energy Resilience

- Systematic policy failures can lead to Critical Infrastructure failure
- Public unrest can leave NATO partners vulnerable during turbulent times

Pavel Mikheyev/Reuters

The information and v iews expressed in this presentation are solely those of the lecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer is affiliated.



THE HENRY M. JACKSON SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

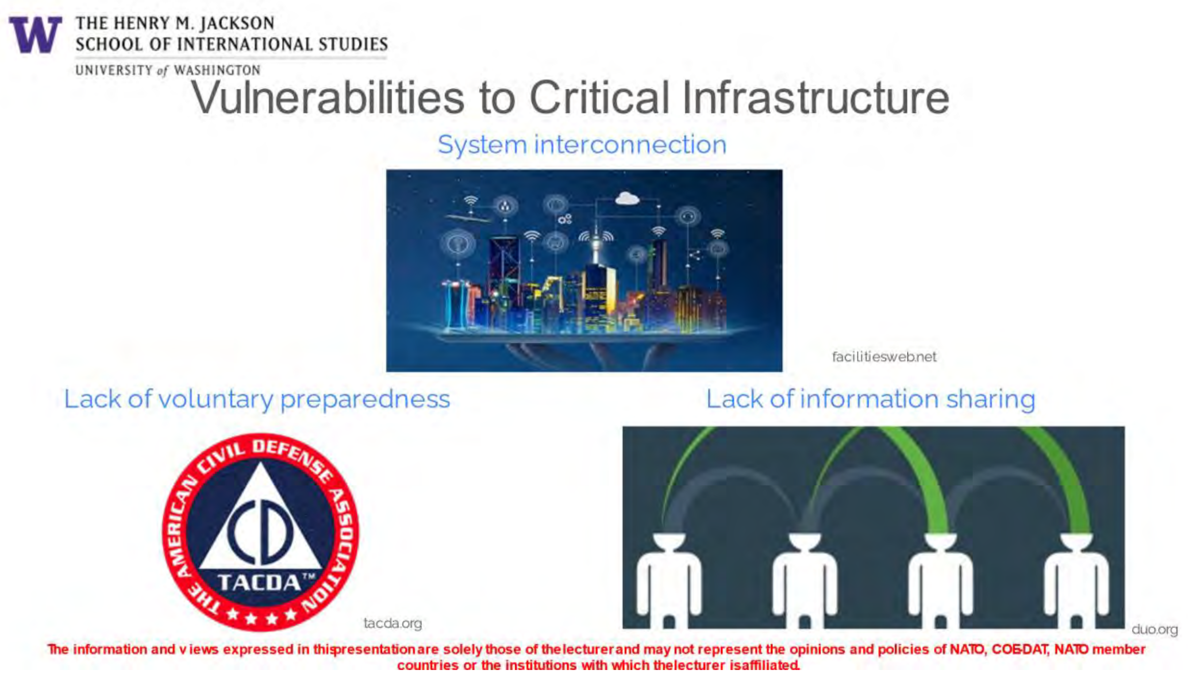
Testing Resilience

- Energy resilience tests, cybersecurity exercises
- Research and testing through U.S. DHS Cybersecurity & Infrastructure Security Agency, S&T Directorate
- Collaboration with the private sector to strengthen supply chains

Component Plans For Resilience
(Resilience Projects)
Continuity Plan
(Critical Mission Assets)
Reconstitution
(Normal Operations Recovery)

DHS resilience planning model, dhs.gov

The information and v iews expressed in thispresentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which thelecturer is affiliated.



THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

Vulnerabilities to Critical Infrastructure

System interconnection

facilitiesweb.net

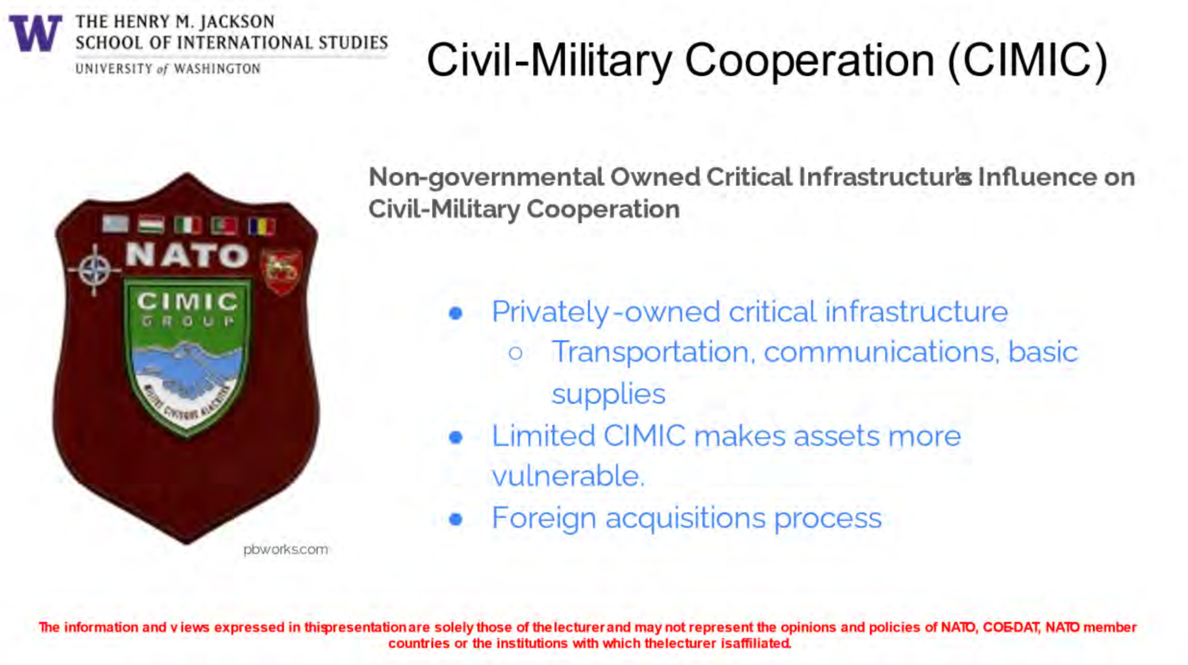
Lack of voluntary preparedness

tacda.org

Lack of information sharing

duo.org

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

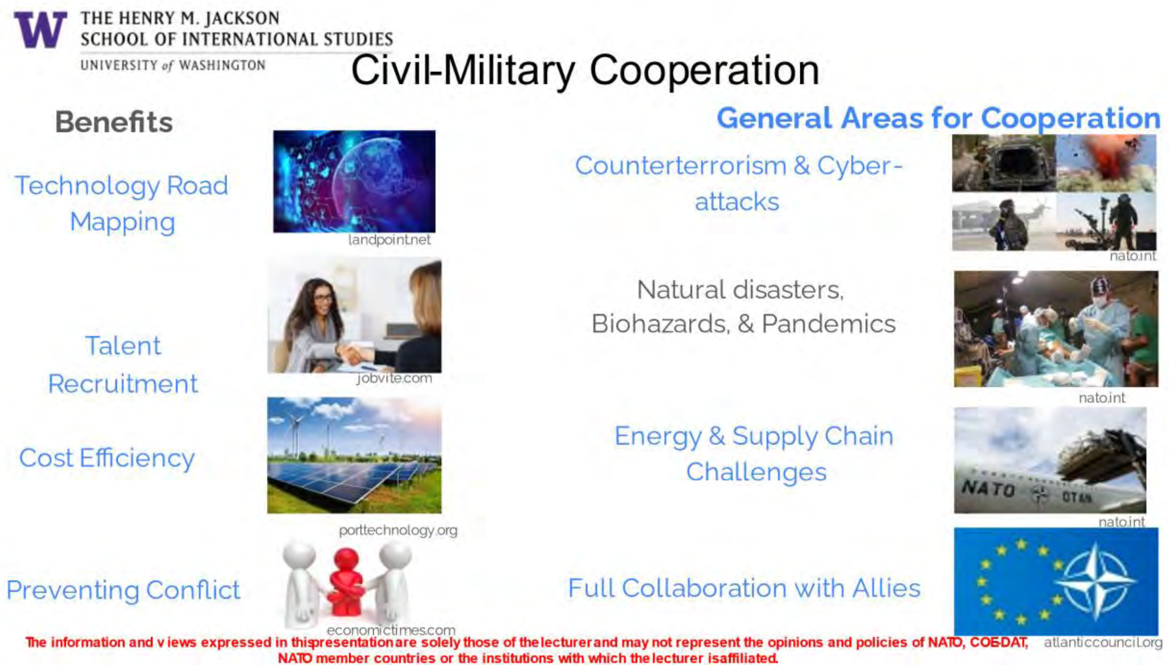
Civil-Military Cooperation (CIMIC)

pbworks.com

Non-governmental Owned Critical Infrastructure's Influence on Civil-Military Cooperation

- Privately-owned critical infrastructure
  - Transportation, communications, basic supplies
- Limited CIMIC makes assets more vulnerable.
- Foreign acquisitions process

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

Civil-Military Cooperation

Benefits

Technology Road Mapping

landpoint.net

Talent Recruitment

jobvite.com

Cost Efficiency

porttechnology.org

Preventing Conflict

economictimes.com

General Areas for Cooperation

Counterterrorism & Cyber-attacks

nato.int

Natural disasters, Biohazards, & Pandemics

nato.int

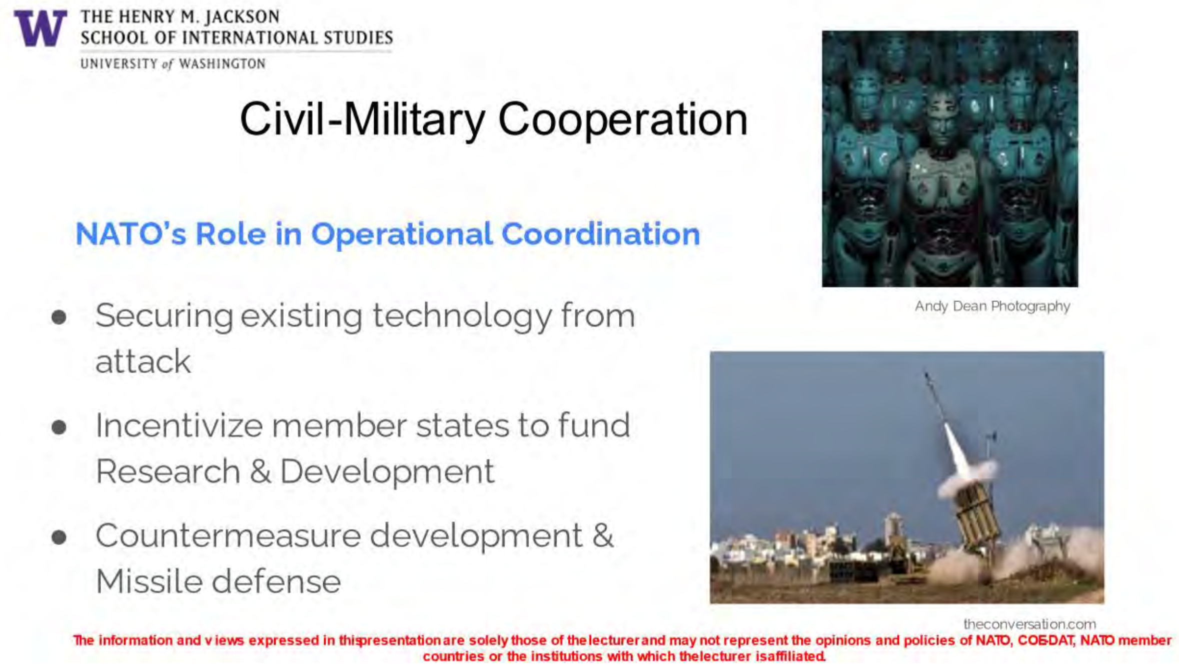
Energy & Supply Chain Challenges

nato.int

Full Collaboration with Allies

atlanticcouncil.org

The information and v iews expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which thelecturer isaffiliated.



THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

Civil-Military Cooperation

NATO's Role in Operational Coordination

- Securing existing technology from attack
- Incentivize member states to fund Research & Development
- Countermeasure development & Missile defense

Andy Dean Photography

theconversation.com

The information and v iews expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which thelecturer isaffiliated.

THE HENRY M. JACKSON
SCHOOL OF INTERNATIONAL STUDIES
UNIVERSITY of WASHINGTON

Vulnerabilities from a Lack of Partnership

- **Interdependencies of national systems**can cause cascading failures
- **Varying standards for**cyber security and data protection leaves the entire alliance insecure

osce.org

Solutions Through Partnership

- **Cross-border research and development** of stable, self-reliant facilities.**CIMIC**
- **Unified standards**for data protection and cyber security

The information and v iews expressed in thispresentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which thelecturer is affiliated.

Energy Security as the Crucial for the Safety of Alliance and Partners Nations

Dr. Aleksander OLECH

Energy security plays a critical role in the common security of the NATO Alliance. NATO's role in energy security was first defined in 2008 at the **Bucharest Summit** and has since been strengthened. Disruption of energy supplies has a significant impact on the safety of NATO members and partner countries and may affect the implementation of military operations. While these topics are primarily the responsibility of the member states, NATO member countries regularly hold consultations on energy security. NATO aims to increase its strategic awareness of energy security and provide the military with a reliable energy supply. Crude oil, as well as gas, are currently the main sources for production of goods, healthcare, transport, and investment in new technologies. Moreover, fuel is indispensable for the sustainment of military operations. The high fuel demand of combat forces must be fulfilled to ensure the effectiveness and safety of the alliance.

The energy sector is vital on two levels, both ***civilian*** and ***military***. Without energy supplies, no NATO members could use either tanks or planes. The disruption of energy supplies would cause insecurity in the societies of member and partner countries of the Alliance and adversely affect NATO military operations. Energy security is a **key resilience factor** and has become more important since the emergence of cyber and hybrid threats to infrastructure. As the energy transition has begun globally, armed forces must adapt to new challenges and maintain operational efficiency by diversifying sources of supplies. Moreover, combat forces have significant fuel needs, and this dependence can affect their performance, increase their vulnerability and force them to reassign part of their personnel to the protection of supply lines.

Any kind of operability of NATO and allied states' troops in Africa and the Middle East using the energy infrastructure of states in the region requires an increased commitment to protect the deposits, pipelines, and transmission routes. NATO, in order to fulfill its potential, needs energy for standard mobility. With the use of local resources, it is much easier to carry out operations in a sustained and efficient manner.

The Russian invasion of Ukraine is also triggering true NATO cohesion and demonstrating reliance of the Alliance on energy imported from Russia. However, differing approaches towards sanctioning and boycotting energy supplies undermine internal cooperation of NATO and shows its vulnerabilities. Even though some countries decided to ban gas and oil from Russia, there are still unwilling to cut the supplies. Moreover, Russian actions, such as attacks on nuclear power plants and destruction of pipelines in Ukraine, must be considered as such war tactics could be used by terrorists and other malign actors.

Russia holds leverage over some European countries because it produces roughly 30% of Europe's natural gas supply. Notwithstanding, in 2019, there were 12 countries exporting LNG to NATO (including Norway and the U.S. which are members of the Alliance). The largest trader of LNG to European NATO members is Qatar, which is responsible for over a quarter of LNG imports. This means that more than 25% of LNG imports are transported through the important straits of Hormuz, Bab el-Mandeb and dangerous waters of the Gulf of Aden. Other important exporters are Algeria, accounting for 13.5%, and Nigeria, constituting 13%; both struggling with terrorist organizations that want to control energy supplies. Furthermore, some LNG which could be rerouted to Europe is exported from Africa and then sold to Asia, the main importer. In December 2021, as much as 2.73 mt of LNG was delivered from Africa to Europe in comparison with Russia that supplied 1.44 mt to Europe.

From 1970–2018, there were almost 2000 terrorist incidents in which **gas or oil facilities were the primary target**. Various African and Middle Eastern countries rely economically on the extraction and processing of crude oil and natural gas. However, production and distribution depend on critical infrastructures such as pipelines, refineries, processing plants, terminals, oil rig substations, pumping stations, ships, and tankers. At the same time, several countries struggle with internal wars and terrorist organizations that attempt to destroy critical infrastructure, threaten to make it their target, or seize it for their purposes and benefits. Between 1999 and 2012, more than 200 attacks on critical infrastructure related to the oil and gas industry in Africa took place. Between 2014 and 2016, al-Qaeda and Daesh alone were responsible for over 70 attacks on the energy sector in North Africa (Algeria, Libya, Egypt).

Terrorism targeting the energy sector is a growing worldwide phenomenon. Back in 2003, such strikes accounted for 25% of terrorist attacks, rising to 35% in 2005. In 2016, there was a 14% increase in terrorist attacks targeted at the oil and gas industry, and these comprised almost 42% of all attacks. They are not limited to physical attacks on power plants, refineries, gas, or oil pipelines, but include other illegal activities such as theft of oil or gas from pipelines, extortion, or sale of raw materials to finance and support groups carrying out the physical attacks.

In the future, terrorists may attack not only regions that are rich in natural resources, but also **transport infrastructure**. In order to undermine NATO countries and their allies carrying out missions in the Middle East and Africa, terrorists will seek to cut off energy sources. Moreover, by taking control of the sale of energy resources, they will be able to finance terrorist activities, manipulate the market through overpricing and cut off certain consumers from resources. The provision of training and logistics support, as well as a gradual move towards cooperation with countries that have a smaller share of the energy market but a large potential, is crucial for NATO members. The main objective is not only to sustain military activity, but also to ensure development for countries that rely on imports. Therefore, taking action to eliminate terrorist attacks in the energy sector should provide the basis for developing anti-terrorist strategies and increasing the Alliance's resilience.

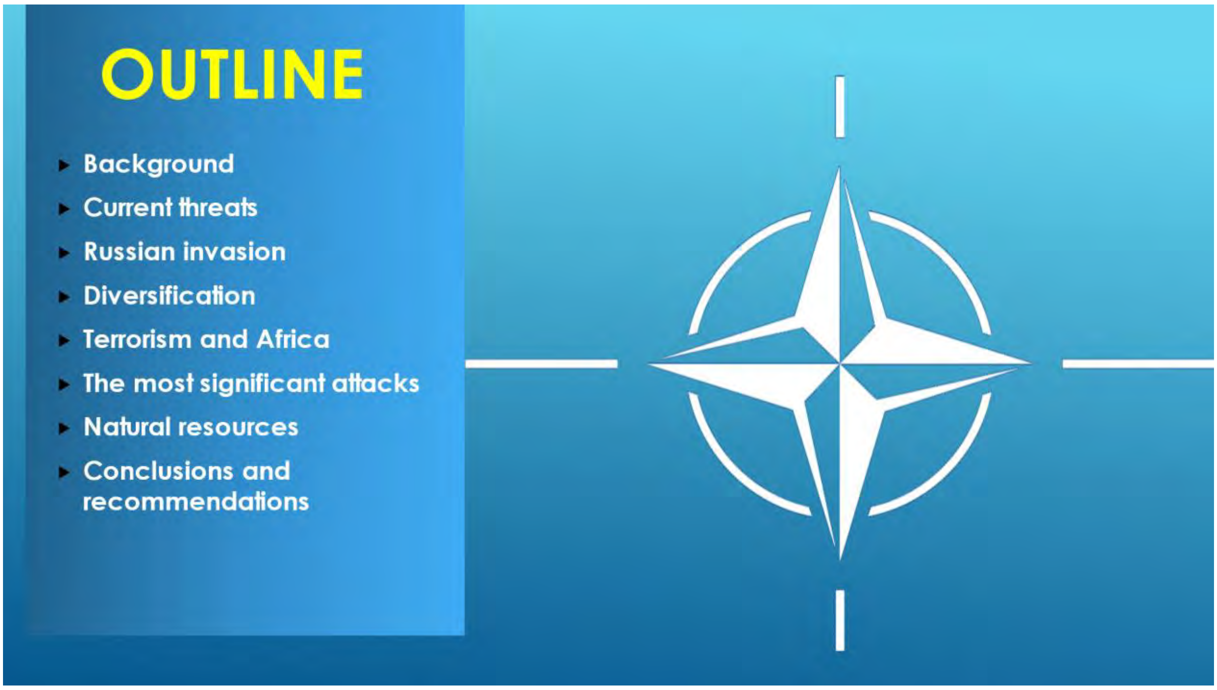
Presentation

ENERGY SECURITY
AS THE CRUCIAL FOR THE SAFETY
OF ALLIANCE AND
PARTNERS NATIONS

Aleksander Olech, PhD

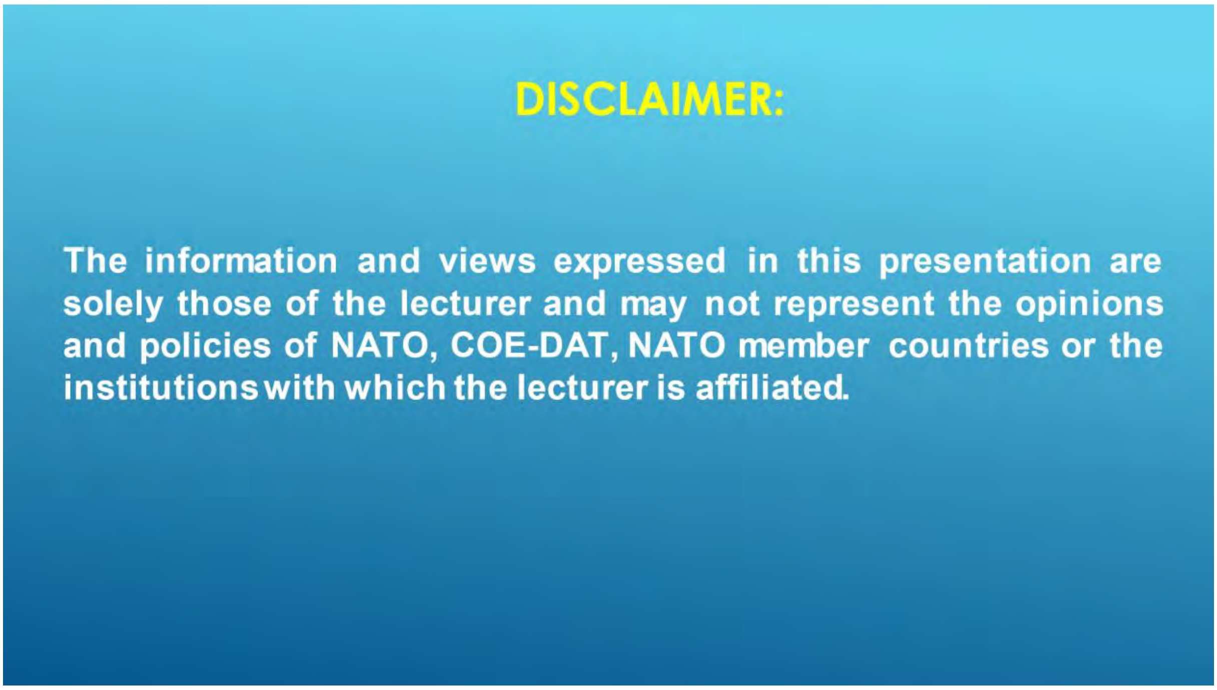
Baltic Defence College, Defence24

Centre of Excellence Defence Against Terrorism
Ankara, October 18, 2022



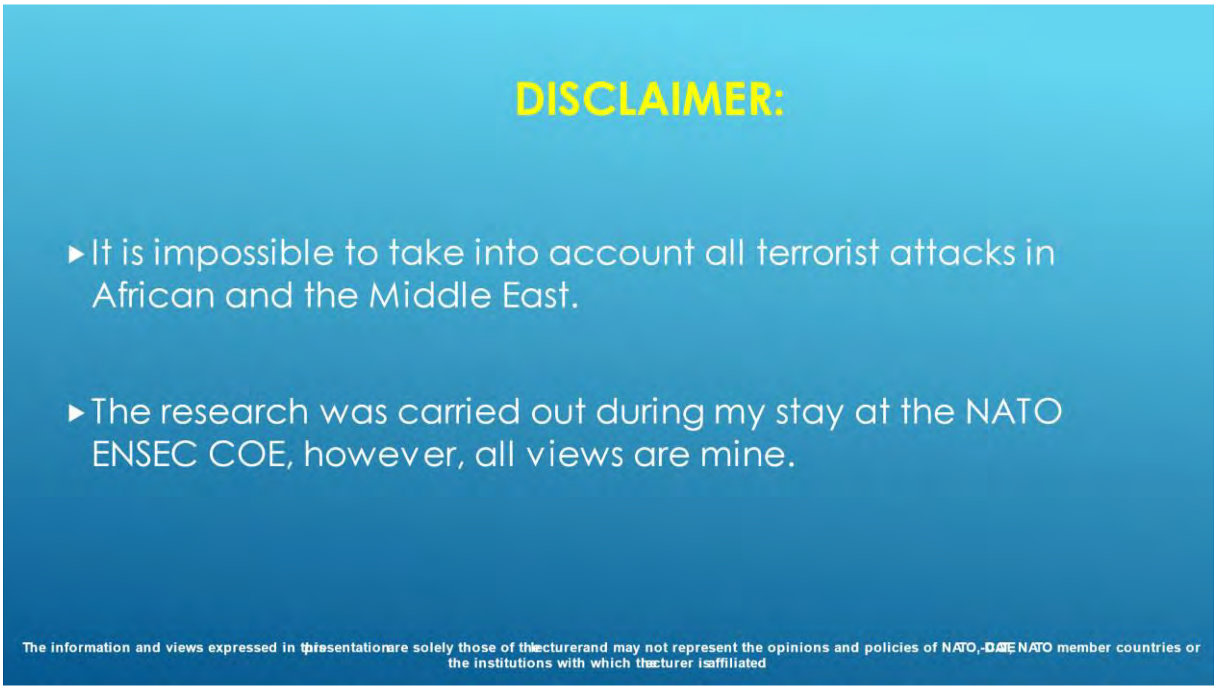
OUTLINE

- Background
- Current threats
- Russian invasion
- Diversification
- Terrorism and Africa
- The most significant attacks
- Natural resources
- Conclusions and recommendations



DISCLAIMER:

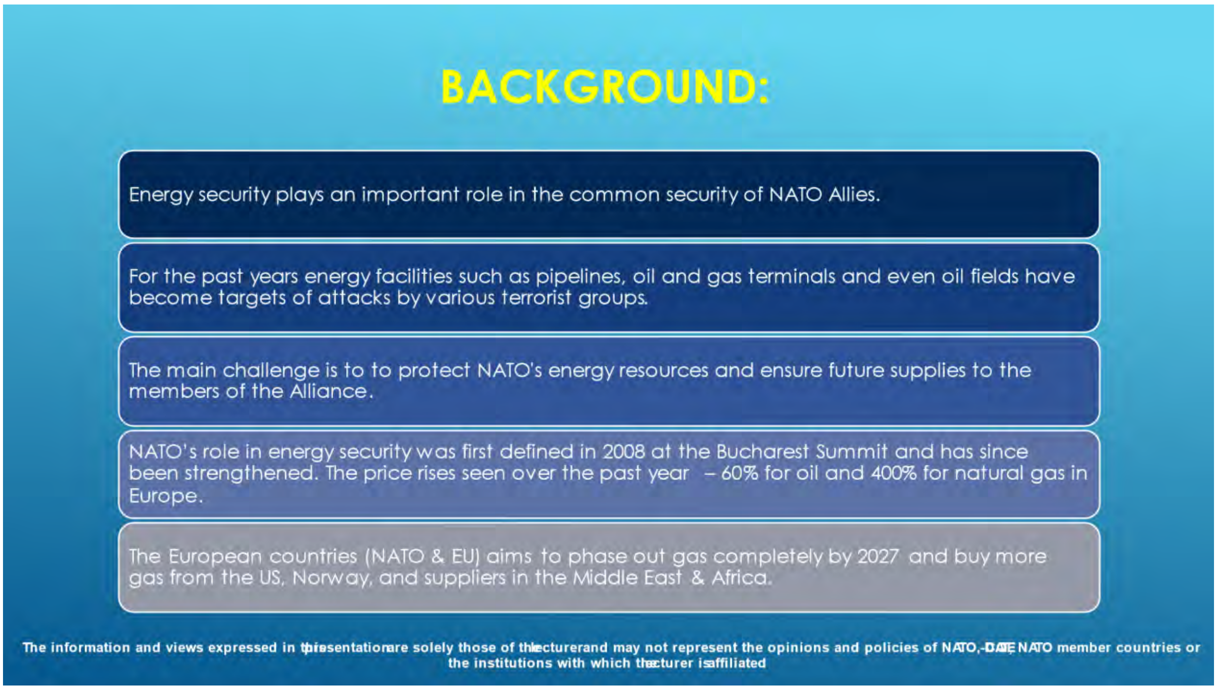
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



DISCLAIMER:

- It is impossible to take into account all terrorist attacks in African and the Middle East.
- The research was carried out during my stay at the NATO ENSEC COE, however, all views are mine.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, ENSEC COE, NATO member countries or the institutions with which the lecturer is affiliated



BACKGROUND:

Energy security plays an important role in the common security of NATO Allies.

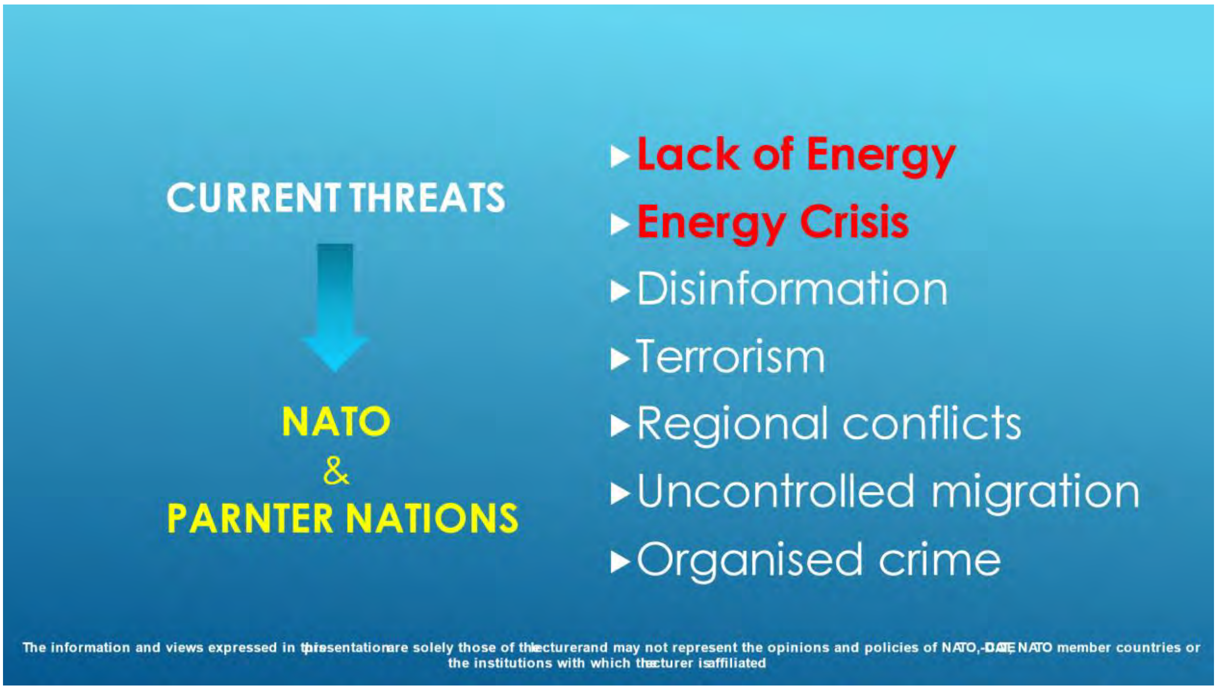
For the past years energy facilities such as pipelines, oil and gas terminals and even oil fields have become targets of attacks by various terrorist groups.

The main challenge is to to protect NATO's energy resources and ensure future supplies to the members of the Alliance.

NATO's role in energy security was first defined in 2008 at the Bucharest Summit and has since been strengthened. The price rises seen over the past year – 60% for oil and 400% for natural gas in Europe.

The European countries (NATO & EU) aims to phase out gas completely by 2027 and buy more gas from the US, Norway, and suppliers in the Middle East & Africa.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, ENSEC COE, NATO member countries or the institutions with which the lecturer is affiliated

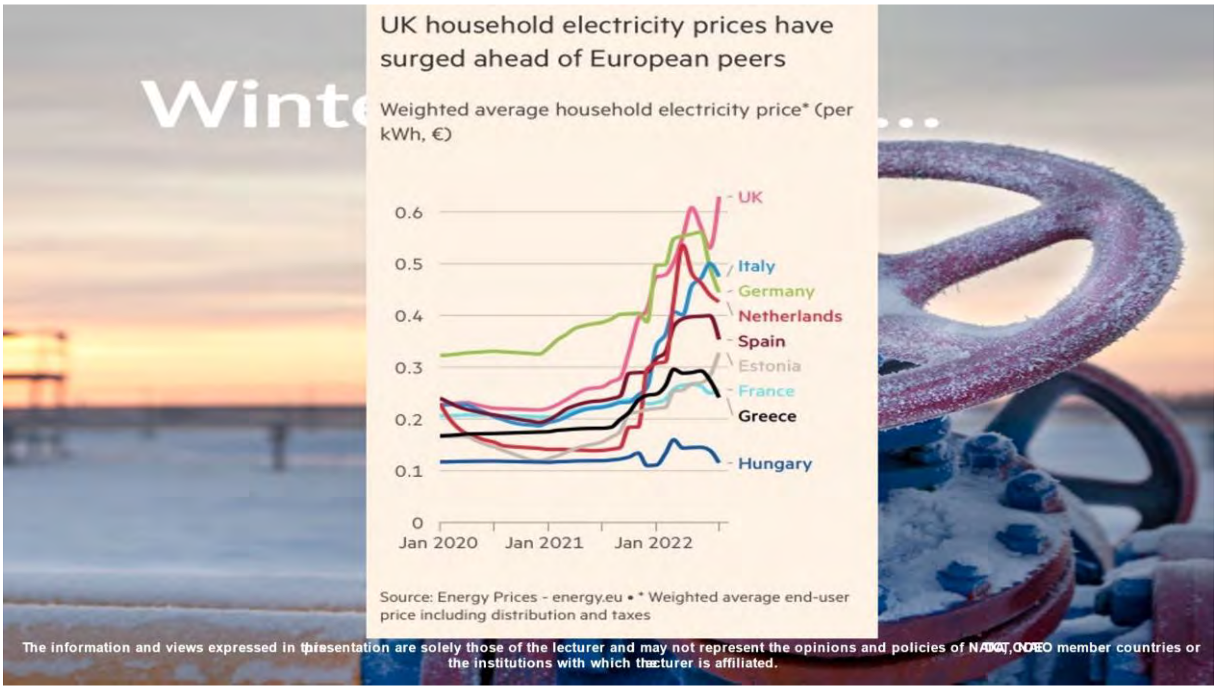


CURRENT THREATS

NATO
&
PARNTER NATIONS

- Lack of Energy
- Energy Crisis
- Disinformation
- Terrorism
- Regional conflicts
- Uncontrolled migration
- Organised crime

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

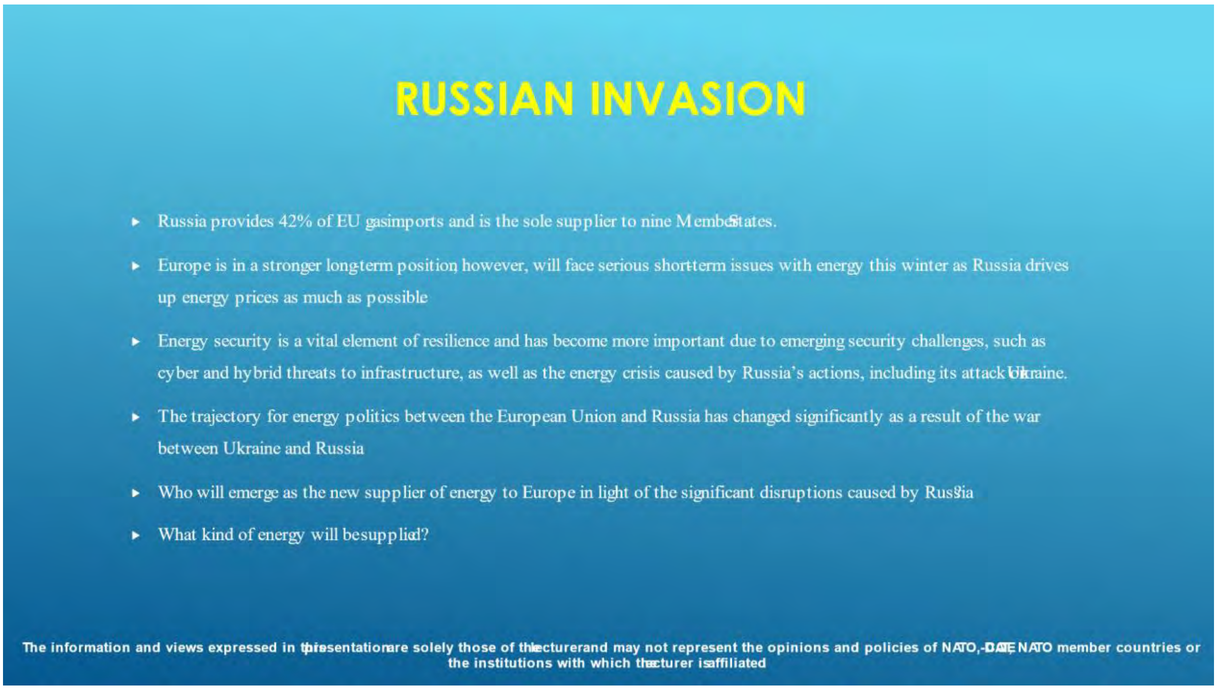


UK household electricity prices have surged ahead of European peers

Weighted average household electricity price* (per kWh, €)

Source: Energy Prices - energy.eu • * Weighted average end-user price including distribution and taxes

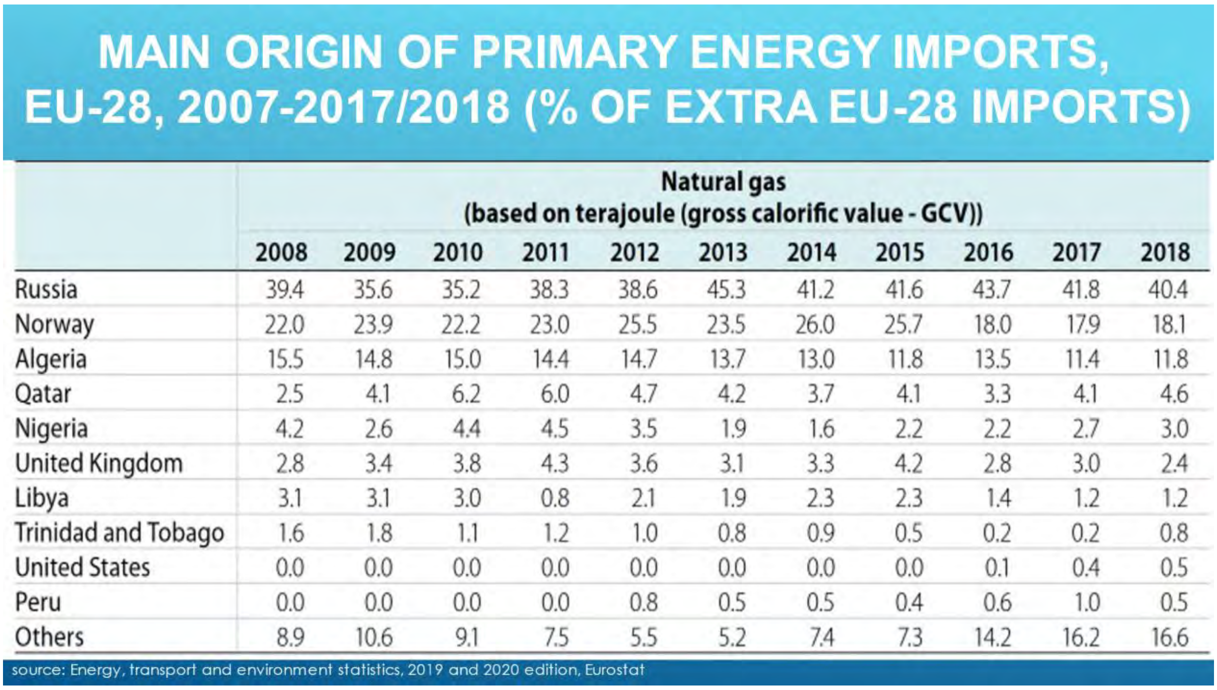
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



RUSSIAN INVASION

- Russia provides 42% of EU gasimports and is the sole supplier to nine MemberStates.
- Europe is in a stronger longterm position, however, will face serious shortterm issues with energy this winter as Russia drives up energy prices as much as possible
- Energy security is a vital element of resilience and has become more important due to emerging security challenges, such as cyber and hybrid threats to infrastructure, as well as the energy crisis caused by Russia's actions, including its attack on Ukraine.
- The trajectory for energy politics between the European Union and Russia has changed significantly as a result of the war between Ukraine and Russia
- Who will emerge as the new supplier of energy to Europe in light of the significant disruptions caused by Russia?
- What kind of energy will besupplied?

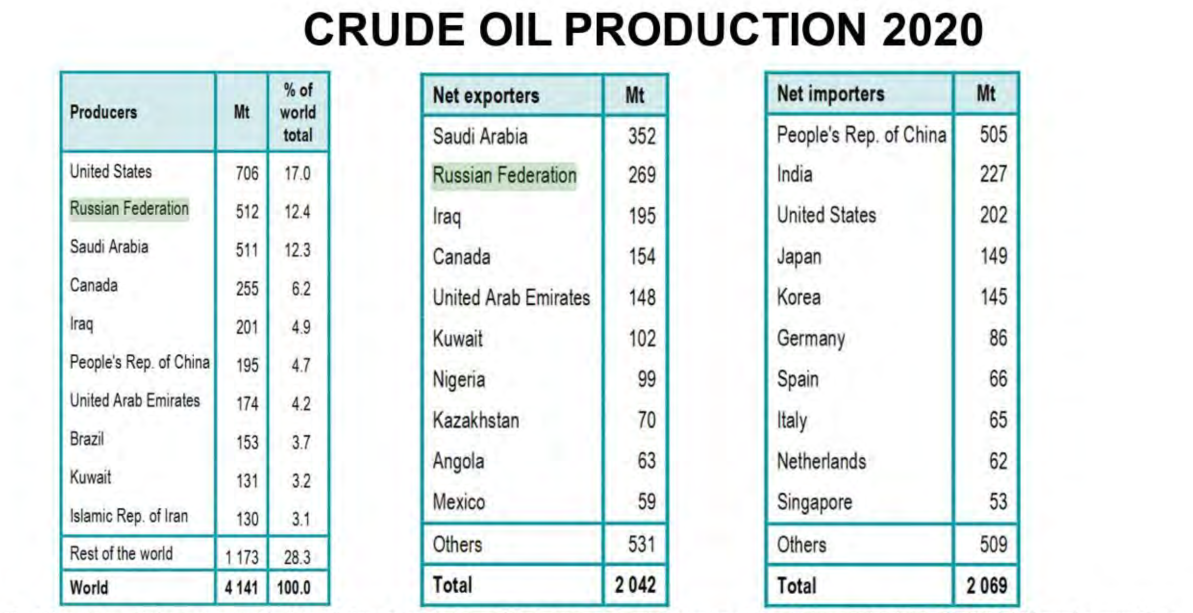
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, DAT COE, NATO member countries or the institutions with which the lecturer is affiliated



MAIN ORIGIN OF PRIMARY ENERGY IMPORTS, EU-28, 2007-2017/2018 (% OF EXTRA EU-28 IMPORTS)

	Natural gas (based on terajoule (gross calorific value - GCV))										
	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Russia	39.4	35.6	35.2	38.3	38.6	45.3	41.2	41.6	43.7	41.8	40.4
Norway	22.0	23.9	22.2	23.0	25.5	23.5	26.0	25.7	18.0	17.9	18.1
Algeria	15.5	14.8	15.0	14.4	14.7	13.7	13.0	11.8	13.5	11.4	11.8
Qatar	2.5	4.1	6.2	6.0	4.7	4.2	3.7	4.1	3.3	4.1	4.6
Nigeria	4.2	2.6	4.4	4.5	3.5	1.9	1.6	2.2	2.2	2.7	3.0
United Kingdom	2.8	3.4	3.8	4.3	3.6	3.1	3.3	4.2	2.8	3.0	2.4
Libya	3.1	3.1	3.0	0.8	2.1	1.9	2.3	2.3	1.4	1.2	1.2
Trinidad and Tobago	1.6	1.8	1.1	1.2	1.0	0.8	0.9	0.5	0.2	0.2	0.8
United States	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.1	0.4	0.5
Peru	0.0	0.0	0.0	0.0	0.8	0.5	0.5	0.4	0.6	1.0	0.5
Others	8.9	10.6	9.1	7.5	5.5	5.2	7.4	7.3	14.2	16.2	16.6

source: Energy, transport and environment statistics, 2019 and 2020 edition, Eurostat



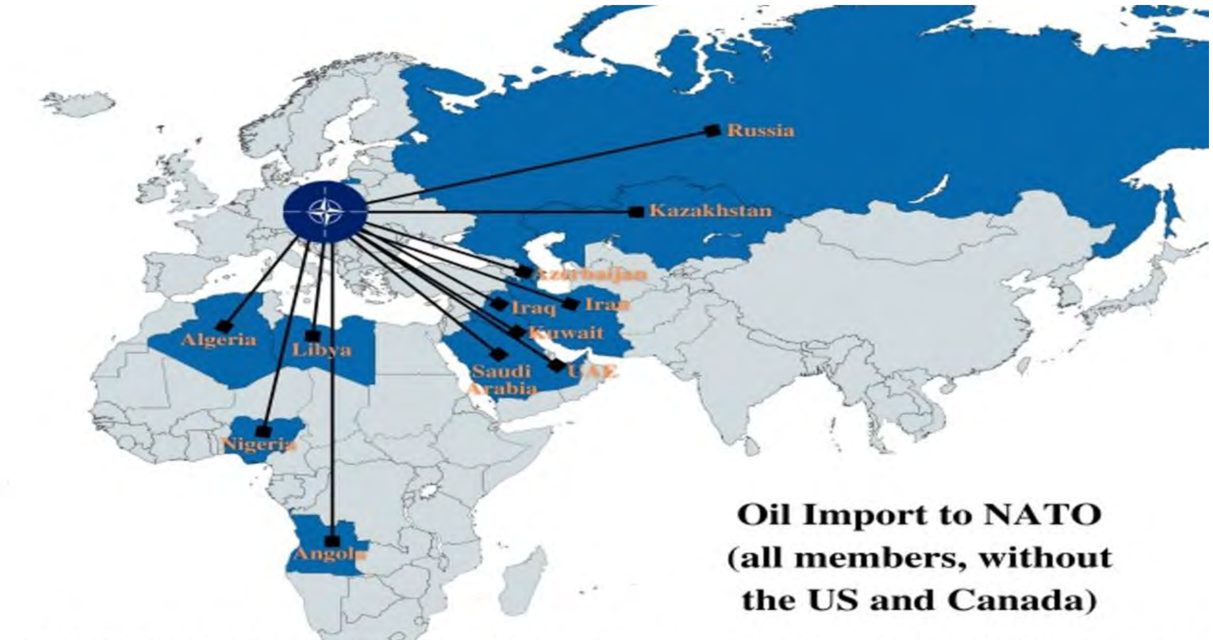
CRUDE OIL PRODUCTION 2020

Producers	Mt	% of world total
United States	706	17.0
Russian Federation	512	12.4
Saudi Arabia	511	12.3
Canada	255	6.2
Iraq	201	4.9
People's Rep. of China	195	4.7
United Arab Emirates	174	4.2
Brazil	153	3.7
Kuwait	131	3.2
Islamic Rep. of Iran	130	3.1
Rest of the world	1 173	28.3
World	**4 141**	**100.0**

Net exporters	Mt
Saudi Arabia	352
Russian Federation	269
Iraq	195
Canada	154
United Arab Emirates	148
Kuwait	102
Nigeria	99
Kazakhstan	70
Angola	63
Mexico	59
Others	531
Total	**2 042**

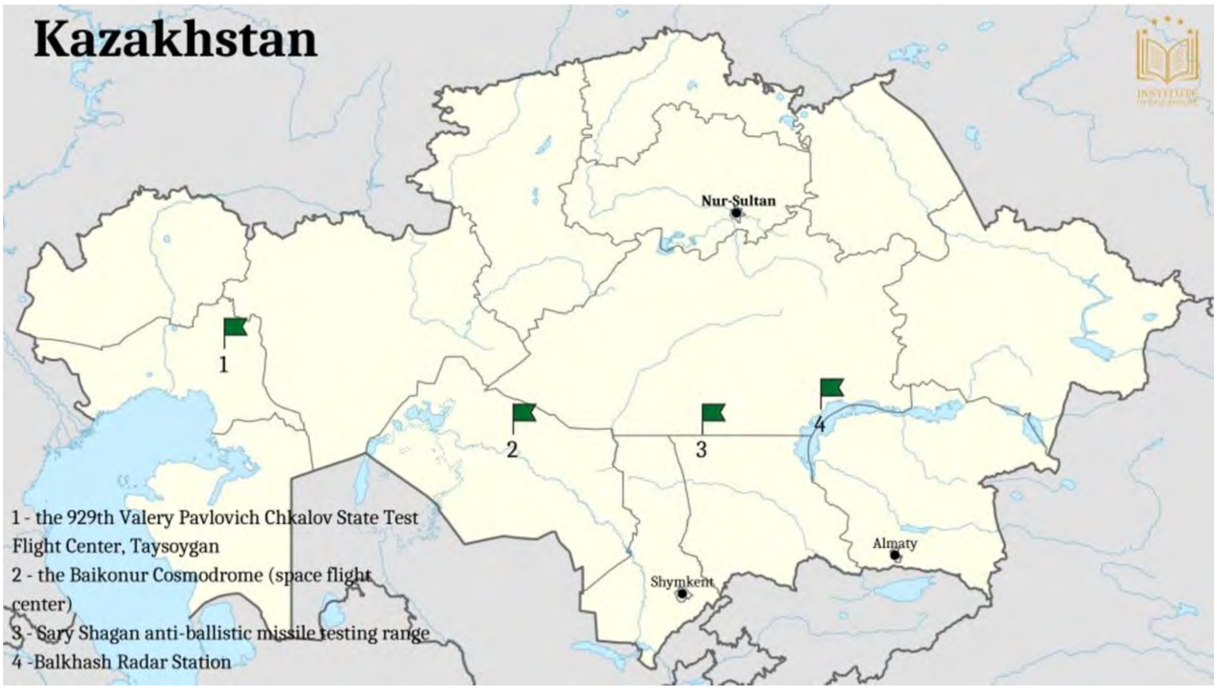
Net importers	Mt
People's Rep. of China	505
India	227
United States	202
Japan	149
Korea	145
Germany	86
Spain	66
Italy	65
Netherlands	62
Singapore	53
Others	509
Total	**2 069**

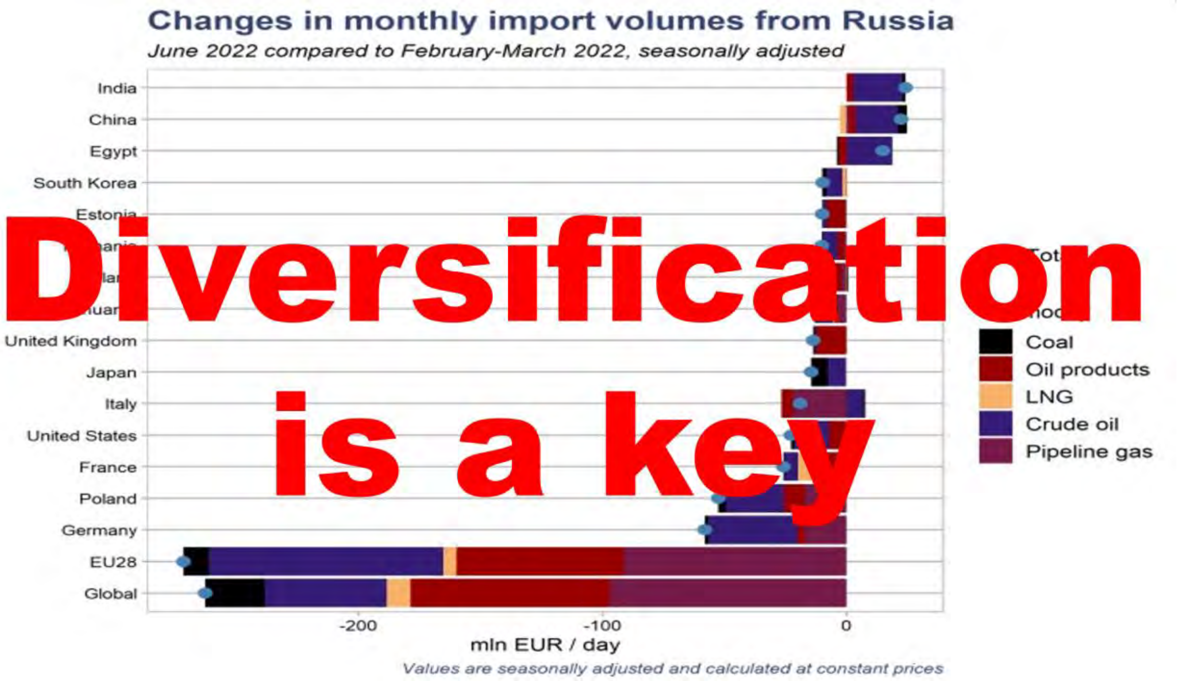
The information and views expressed in thpiresentation are solely those of the lecturer and may not represent the opinions and policies of NADCO, NATO member countries or the institutions with which thelecturer is affiliated.



Oil Import to NATO (all members, without the US and Canada)

The information and views expressed in thpiresentationare solely those of thlecturerand may not represent the opinions and policies of NATO,-DATE NATO member countries or the institutions with which thelecturer is affiliated.


Kazakhstan
Nur-Sultan
1
2
3
4
Almaty
Shymkent
1 - the 929th Valery Pavlovich Chkalov State Test Flight Center, Taysoygan
2 - the Baikonur Cosmodrome (space flight center)
3 - Sary Shagan anti-ballistic missile testing range
4 -Balkhash Radar Station

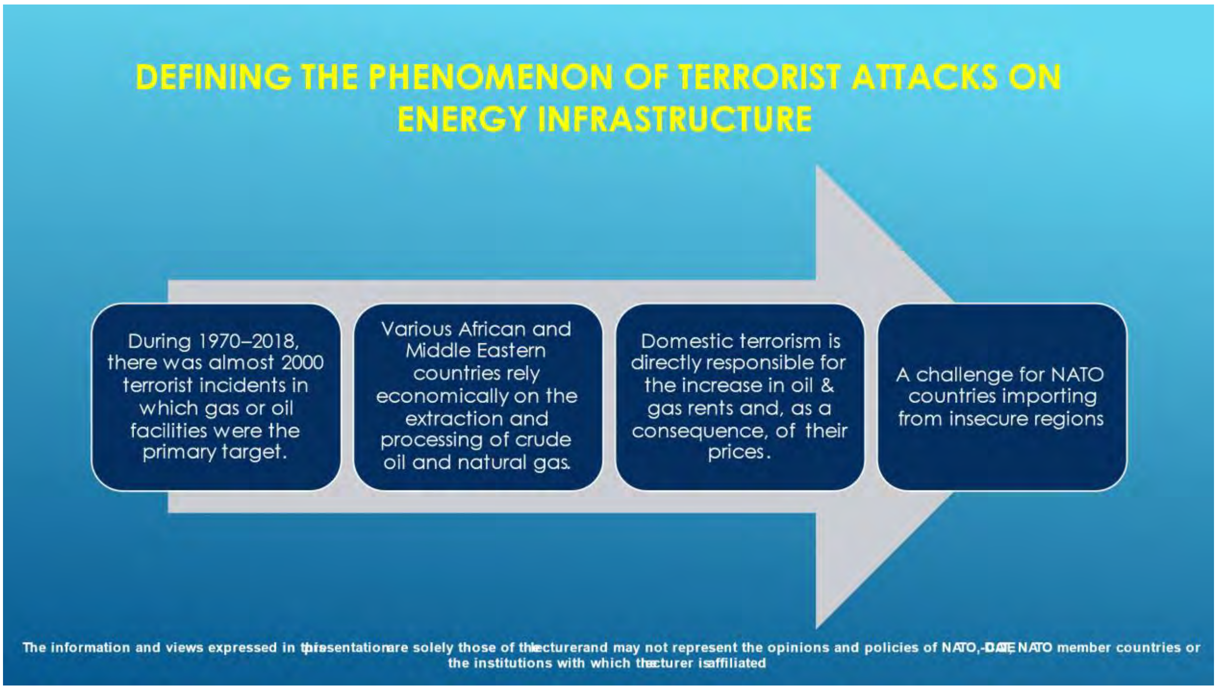

Changes in monthly import volumes from Russia
June 2022 compared to February-March 2022, seasonally adjusted
India
China
Egypt
South Korea
Estonia
United Kingdom
Japan
Italy
United States
France
Poland
Germany
EU28
Global
-200
-100
0
mln EUR / day
Values are seasonally adjusted and calculated at constant prices
Coal
Oil products
LNG
Crude oil
Pipeline gas
Diversification is a key

AFRICA? THE MIDDLE EAST?

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

TERRORISM

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated



DEFINING THE PHENOMENON OF TERRORIST ATTACKS ON ENERGY INFRASTRUCTURE

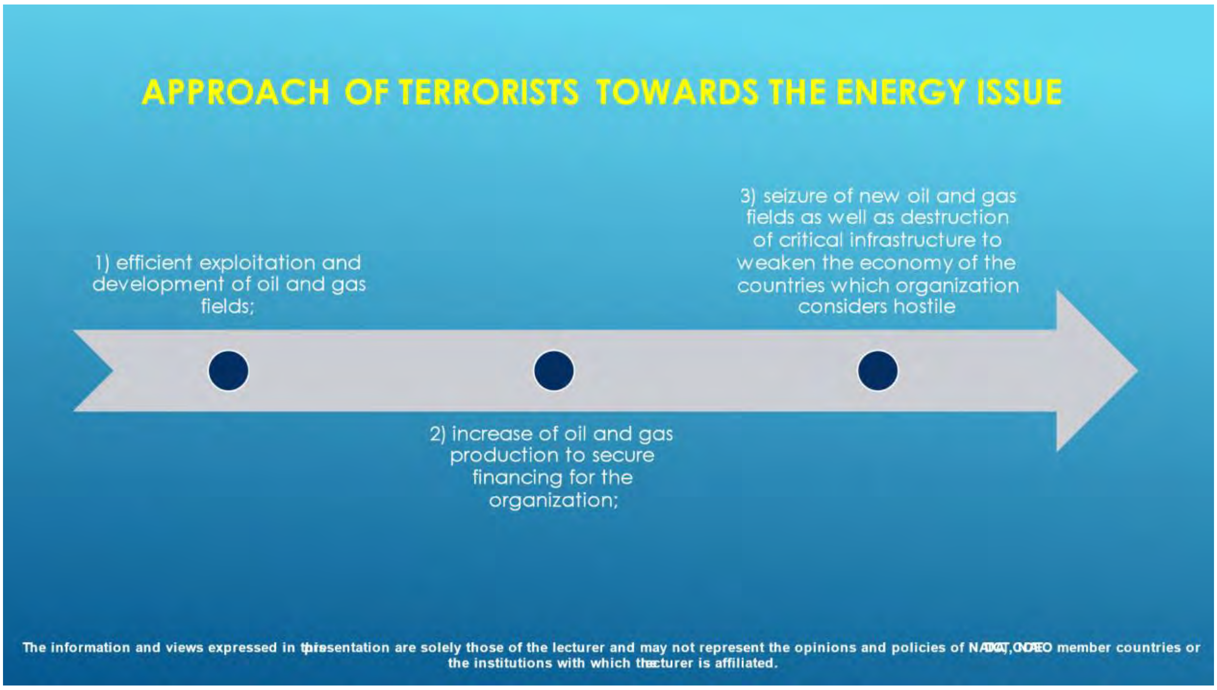
During 1970–2018, there was almost 2000 terrorist incidents in which gas or oil facilities were the primary target.

Various African and Middle Eastern countries rely economically on the extraction and processing of crude oil and natural gas.

Domestic terrorism is directly responsible for the increase in oil & gas rents and, as a consequence, of their prices.

A challenge for NATO countries importing from insecure regions

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated



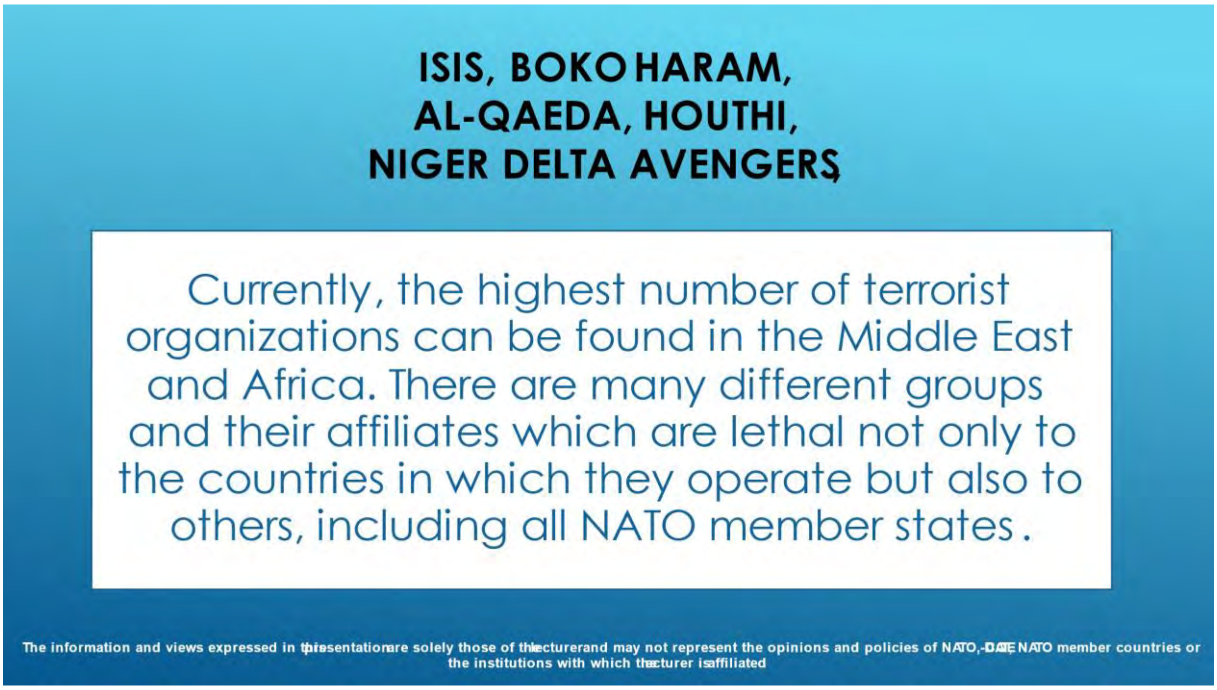
APPROACH OF TERRORISTS TOWARDS THE ENERGY ISSUE

1) efficient exploitation and development of oil and gas fields;

2) increase of oil and gas production to secure financing for the organization;

3) seizure of new oil and gas fields as well as destruction of critical infrastructure to weaken the economy of the countries which organization considers hostile

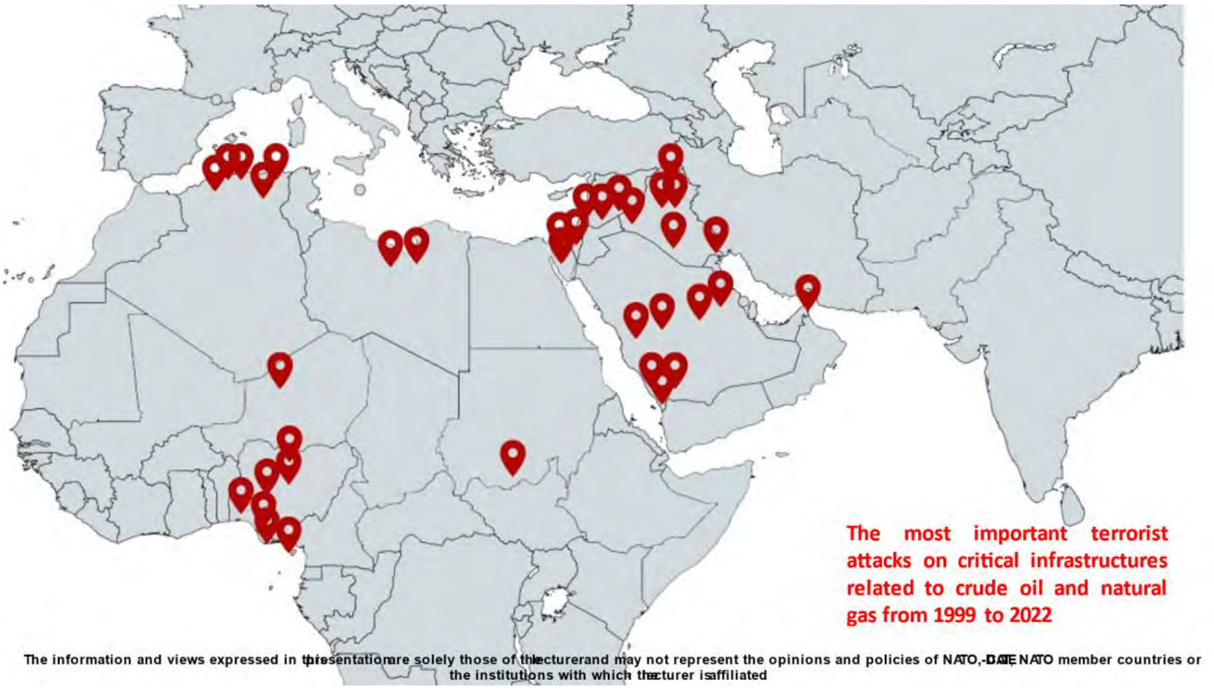
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



ISIS, BOKO HARAM, AL-QAEDA, HOUTHI, NIGER DELTA AVENGERS,

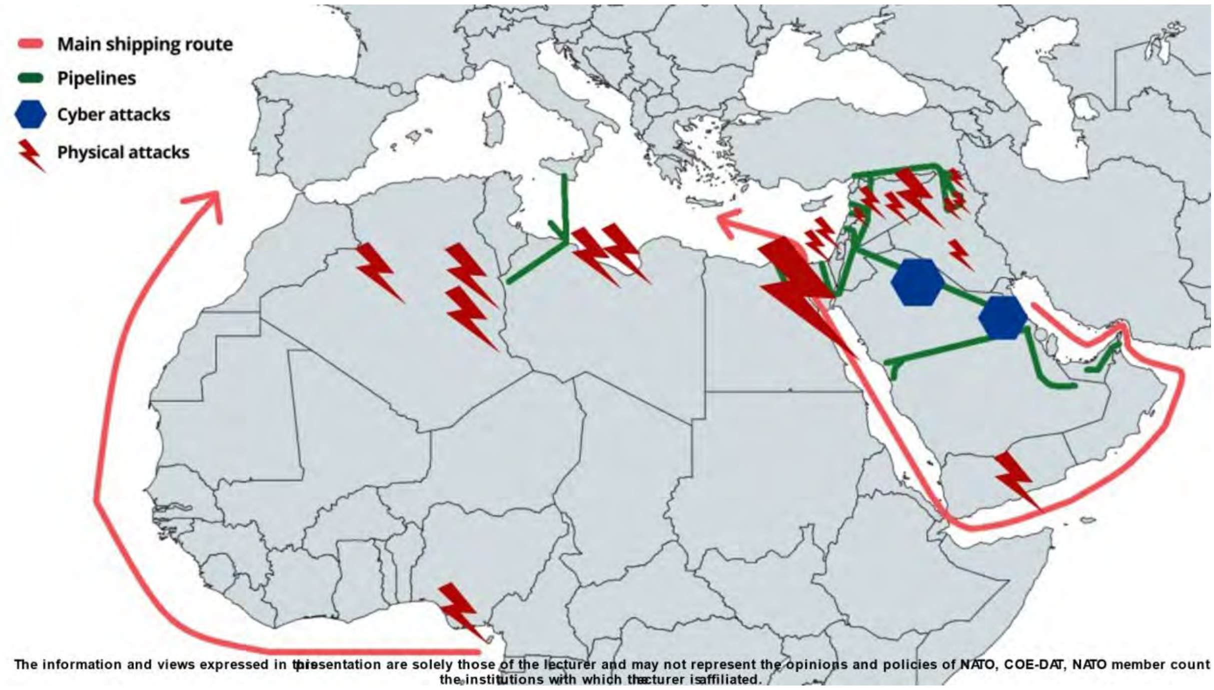
Currently, the highest number of terrorist organizations can be found in the Middle East and Africa. There are many different groups and their affiliates which are lethal not only to the countries in which they operate but also to others, including all NATO member states.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO,-DAT, NATO member countries or the institutions with which the lecturer is affiliated

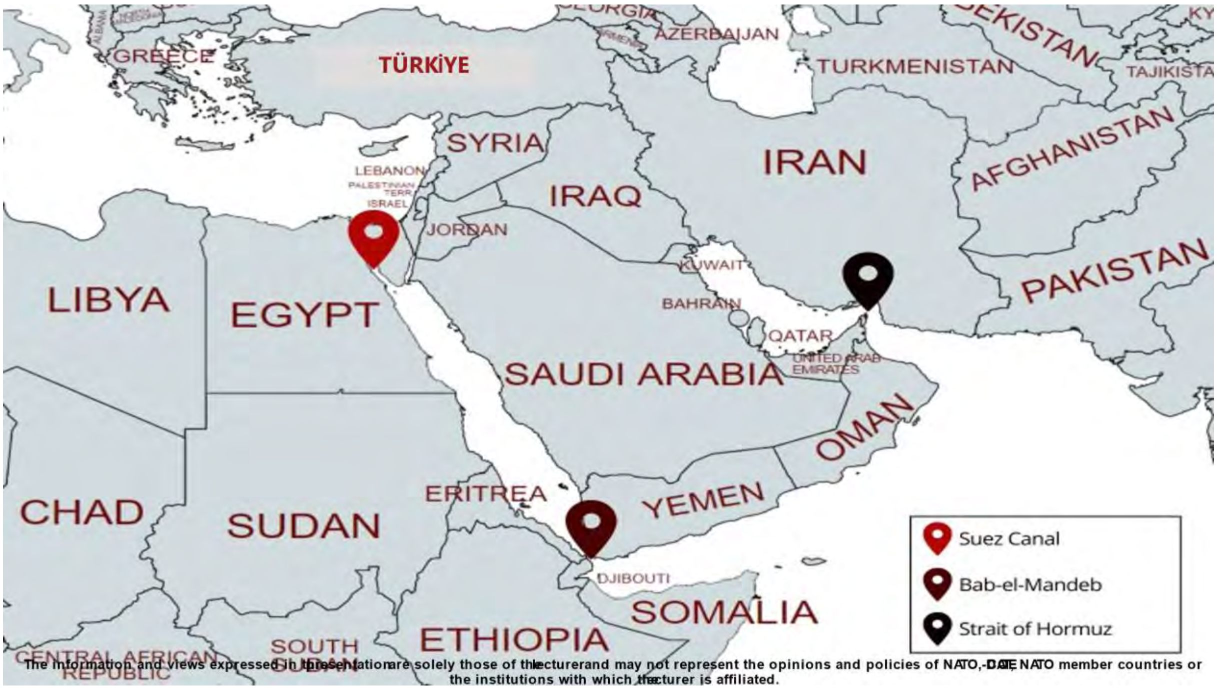


The most important terrorist attacks on critical infrastructures related to crude oil and natural gas from 1999 to 2022

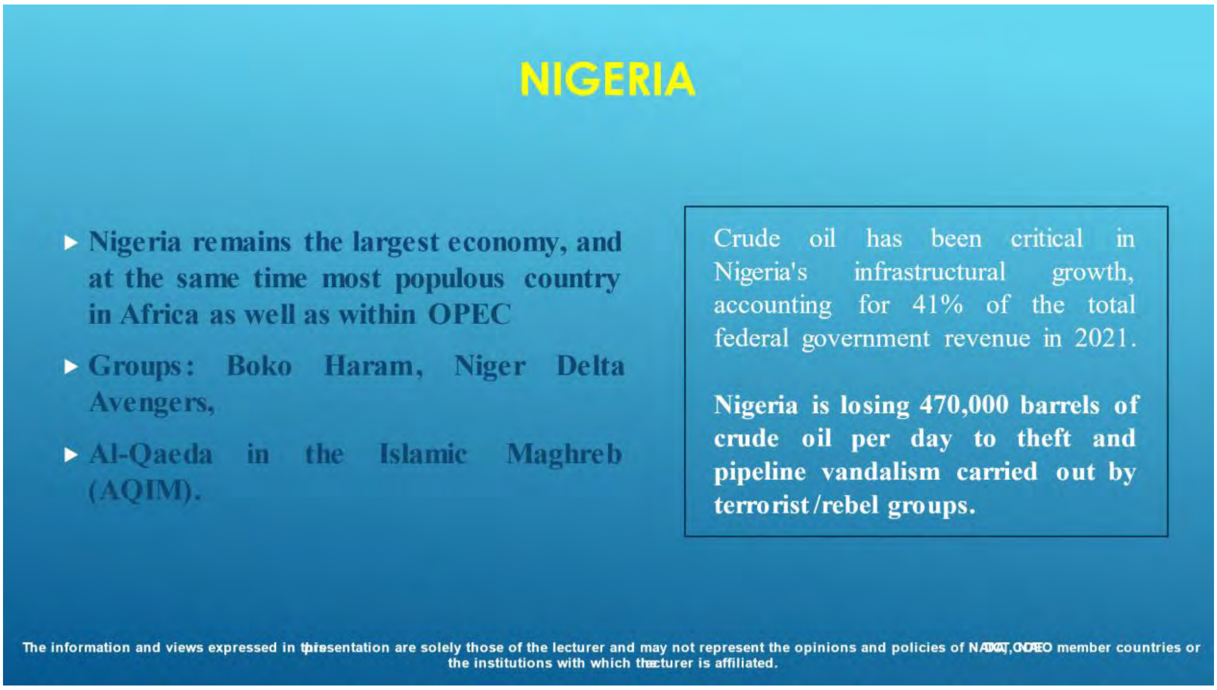
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO,-DAT, NATO member countries or the institutions with which the lecturer is affiliated



The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member count the institutions with which the lecturer is affiliated.



The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



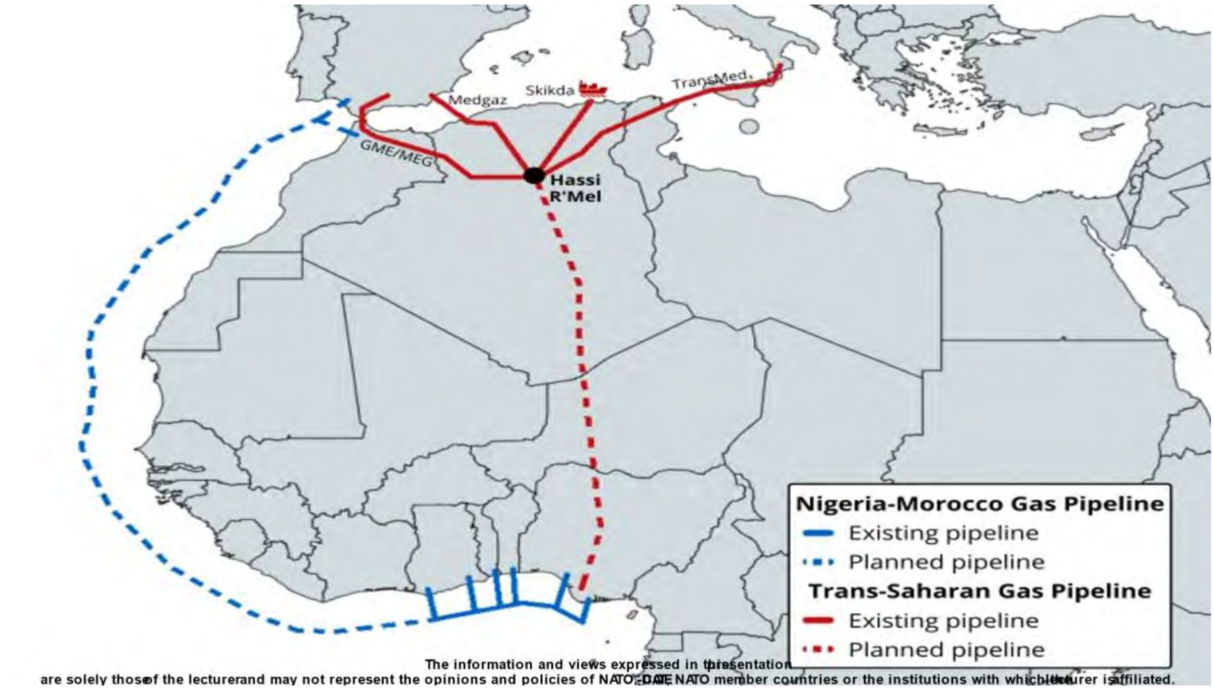
NIGERIA

- Nigeria remains the largest economy, and at the same time most populous country in Africa as well as within OPEC
- Groups: Boko Haram, Niger Delta Avengers,
- Al-Qaeda in the Islamic Maghreb (AQIM).

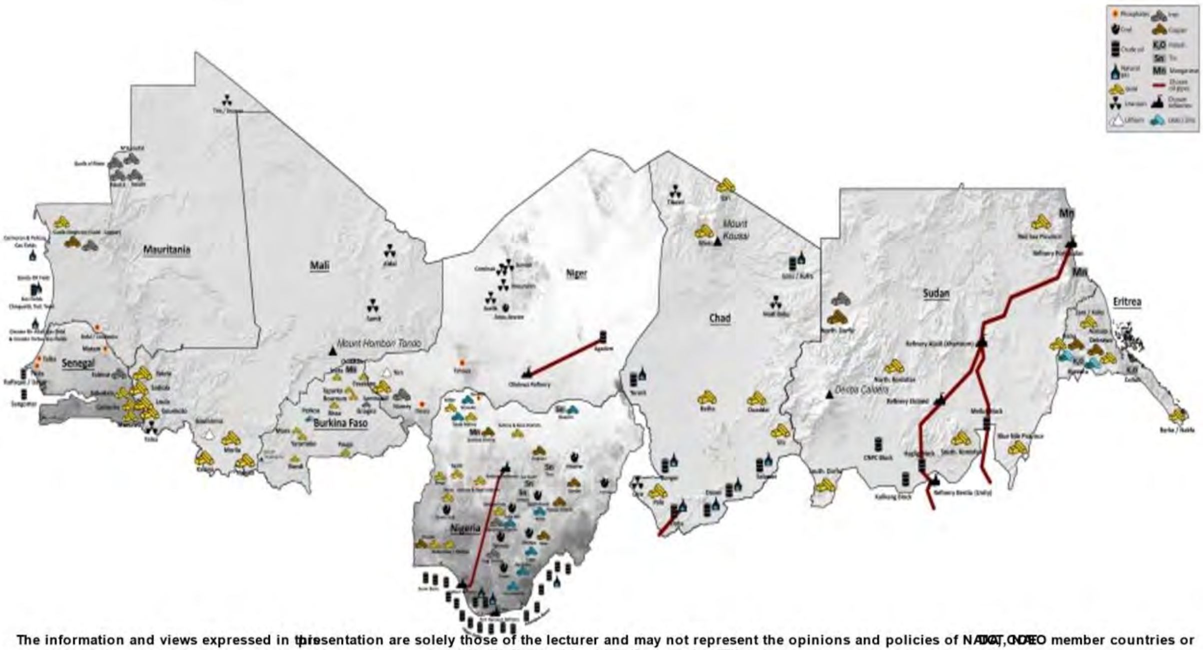
Crude oil has been critical in Nigeria's infrastructural growth, accounting for 41% of the total federal government revenue in 2021.

Nigeria is losing 470,000 barrels of crude oil per day to theft and pipeline vandalism carried out by terrorist/rebel groups.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

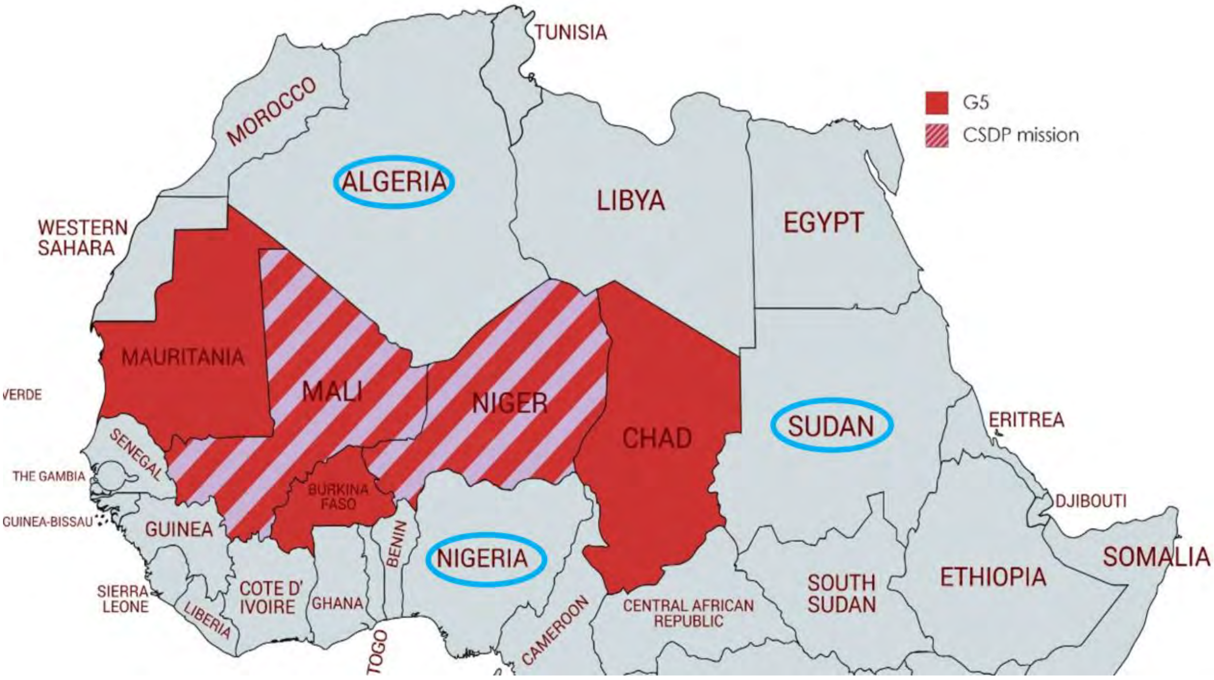


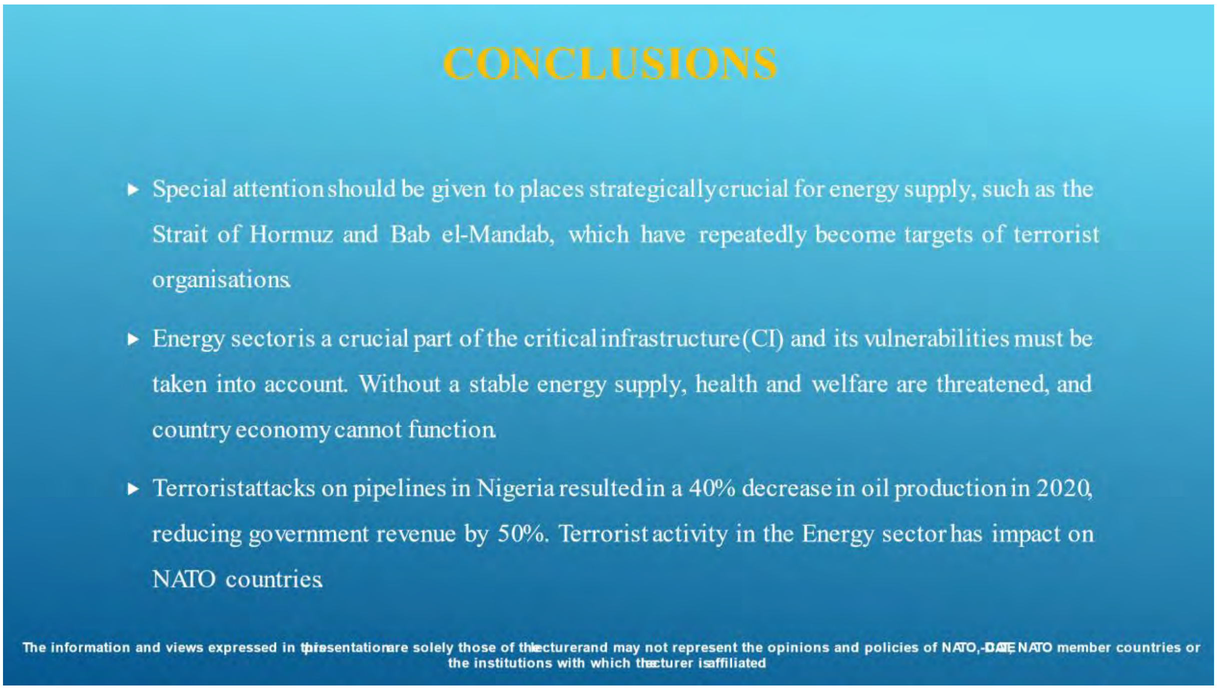
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, NDC, NATO member countries or the institutions with which the lecturer is affiliated.

Authors: A.H., B.W.

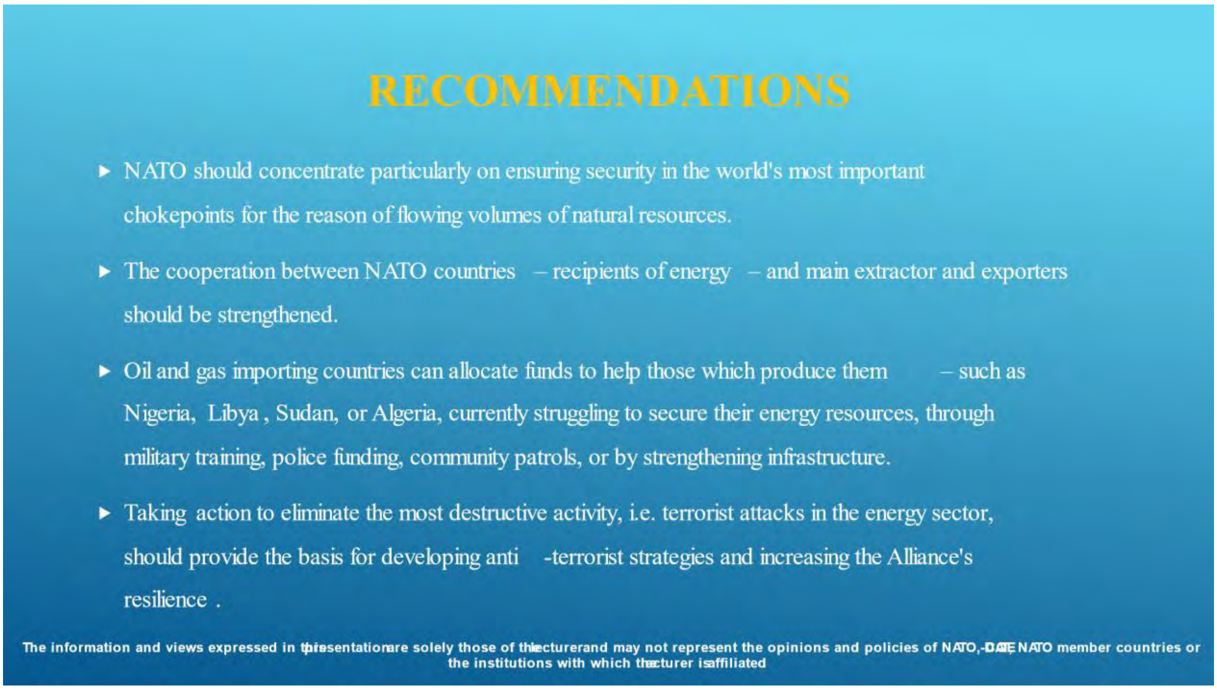




CONCLUSIONS

- Special attention should be given to places strategically crucial for energy supply, such as the Strait of Hormuz and Bab el-Mandab, which have repeatedly become targets of terrorist organisations.
- Energy sector is a crucial part of the critical infrastructure (CI) and its vulnerabilities must be taken into account. Without a stable energy supply, health and welfare are threatened, and country economy cannot function.
- Terrorist attacks on pipelines in Nigeria resulted in a 40% decrease in oil production in 2020, reducing government revenue by 50%. Terrorist activity in the Energy sector has impact on NATO countries.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated



RECOMMENDATIONS

- NATO should concentrate particularly on ensuring security in the world's most important chokepoints for the reason of flowing volumes of natural resources.
- The cooperation between NATO countries – recipients of energy – and main extractor and exporters should be strengthened.
- Oil and gas importing countries can allocate funds to help those which produce them – such as Nigeria, Libya , Sudan, or Algeria, currently struggling to secure their energy resources, through military training, police funding, community patrols, or by strengthening infrastructure.
- Taking action to eliminate the most destructive activity, i.e. terrorist attacks in the energy sector, should provide the basis for developing anti-terrorist strategies and increasing the Alliance's resilience .

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

REFERENCES:

- Russia's fossil fuel export volumes continued to fall in July, but revenue rose due to higher fossil gas prices, https://energyandcleanair.org/russia-fossil-fuel-exports-july.
- Key World Energy Statistics 2021, https://iea.blob.core.windows.net/assets/52f66a88-0b63-4ad2-94a5-29d36e864b82/KeyWorldEnergyStatistics2021.pdf
- Primary energy consumption in selected EU Countries compared to global, the https://www.degruyter.com/document/doi/10.1515/cdem-2020-0046/html?lang=en
- European Energy Security Post-Russia, https://cepa.org/european-energy-security-post-russia/
- Chia-yi Lee, "Why do terrorists target the energy industry? A review of kidnapping, violence and attacks against energy infrastructure", Energy Research & Social Science 87 (2022).
- Salem Alelyani and Harish Kumar, "Overview of Cyberattack on Saudi Institutions," Journal of Information Security and Cybercrimes Research 1, no. 1 (2018): 1-9.
- Lukáš Tichý, "The Islamic State oil and gas strategy in North Africa," Energy Strategy Reviews 24 (2019): 254-260, https://doi.org/10.1016/j.esr.2019.04.001.
- Jamie Shea, "Energy Security: NATO's potential role," NATO Review, September 1, 2006, https://www.nato.int/docu/review/articles/2006/09/01/energy-security-natos-potential-role/index.html.
- Rim Berahab, "Global trends in the energy sector and their implication on energy security in NATO's southern neighbourhood," Policy Center for the New South, ARI 103/2020, September 8, (2020), https://media.realinstitutoelcano.org/wp content/uploads/2021/10/ari103-2020-berahab-global-trends-energy-sector-and-implication-on-energy-security-in-natos-southern-neighbourhood.pdf.
- Karen Smith Stegen, Patrick Gilmartin and Janetta Carlucci, "Terrorists versus the Sun: Desertec in North Africa as a case study for assessing risks to energy infrastructure," Risk Management 14, no. 1 (February 2012): 3-26.
- United Nations High Commissioner for Refugees, Nigeria Situation 2017 Funding Update as of 28 November 2017, https://data2.unhcr.org/fr/documents/download/60938
- United Nations High Commissioner for Refugees, Tendances des réfugiés maliens depuis 2012,
- Source: CMAIS- Compagnie Méditerranéenne d'Analyse et d'Intelligence Stratégique, Les sources du financement des bandes armées au Sahel, Rabat 2013, p. 4-5
- http://data2.unhcr.org/fr/situations/malisituation
- https://ec.europa.eu/eurostat/documents/2995521/9333488/8-02012018-AP-EN.pdf/3fa5fa53-0764a5f8bb5a8075f639167
- University of Maryland National Consortium for the Study of Terrorism and Responses to Terrorism's Global Terrorism Database
- Szkurłat I., *Terroryzm a polityka bezpieczeństwa państw Europy Zachodniej na przełomie XX i XXI w*, Akademia Pomorska w Słupsku, Słupsk 2018.
- Townshend Ch. *Terroryzm*, Wydawnictwo Uniwersytetu Łódzkiego, Lodż 2017.
- Truchan R., Zubrzycki W., Włodarz-Podgórska K. *Wybrane aspekty zwalczania terroryzmu*, Wyższa Szkoła Policji w Szczytni, Szczytno 2017.
- Vincent Nouzille, *Erreurs fatales: Comment nos présidents ont failli face au terrorisme*, Fayard, Paris 2017, ISBN-10: 2213693986.
- Wejkszner A., *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej*, Difin, Warszawa 2018.
- William Bourdon, *Les dérives de l'état d'urgence*, Plon, Paris 2017, ISBN-10: 225925215X.
- Jean Guisnel, David Korn-Brzoza, *Au service secret de la France. Les maîtres de l'espionnage se livrent enfin*, Éditions Points, Paris 2016, ISBN-10: 2757855093.
- Jean-François Gayraud, David Sénat, *Le terrorisme*, PUF, Paris 2006.
- Jean-Michel Fauvergue, *Patron du RAID. Face aux attentats terroristes*, Mareuil Éditions, Paris 2018, ISBN-10: 2372540688.
- Kepel G., Jardin A., *Terror we Francji : geneza francuskiego dżihadu*, Wydawnictwo Akademickie Dialog, Warszawa 2017.
- Laurent Bonelli, Fabien Carrié, *La fabrique de la radicalité. Une sociologie des jeunes djihadistes français*, Le Seuil, Paris 2018, ISBN-10: 2021397939.

Aleksander Olech, PhD

Baltic Defence College,
Defence24

akolech@wp.pl

THANK YOU FOR YOUR ATTENTION !

Climate Change Implications on the Security of NATO Nations
Mr. Diego OSORIO

Mr. Diego Osorio presented his work with Dr. Sabrina Schulz and Dr. Marcus Mohlin. His presentation focused on impacts of the climate change on the military infrastructure and operations of NATO. He reiterated that climate change was acknowledged as a "***threat multiplier***" in NATO Climate Change and Security Action Plan in 2021. He stated that climate change is a crucial challenge and threat multiplier for the member countries' security and also in the Alliance's neighbourhood. Osorio argued that climate change is related to **Article 3** and **Article 5** the North Atlantic Treaty. He stated that NATO needs to adapt in strategic and operational terms.

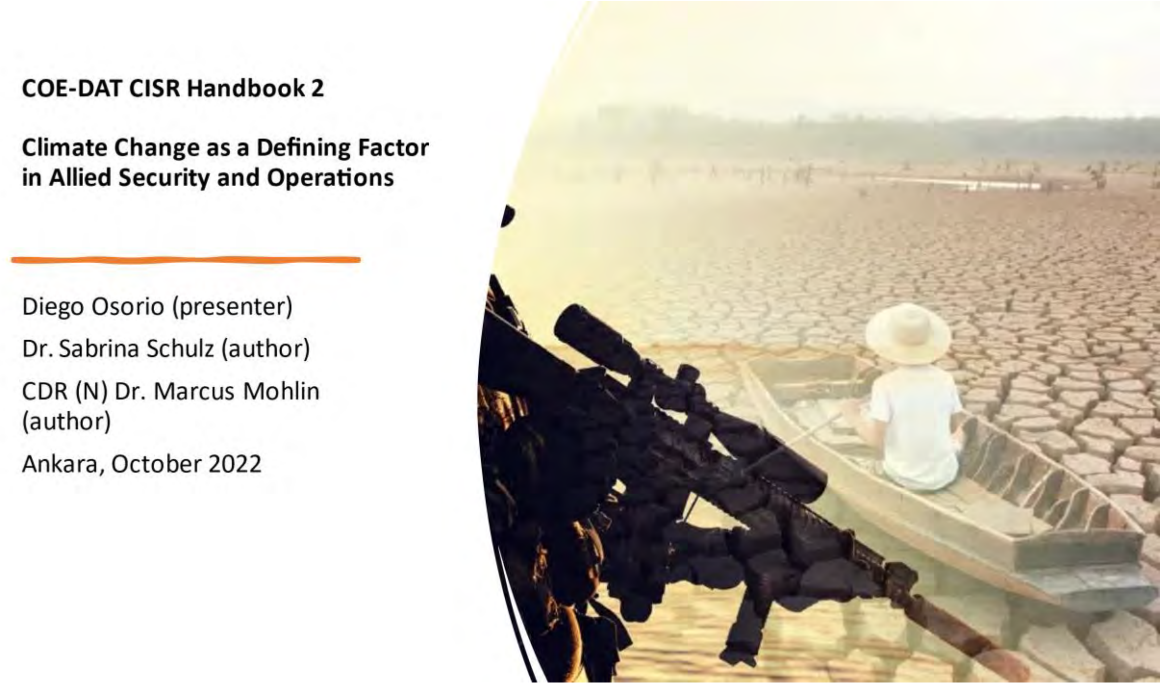
Diego Osorio claims that there are direct and indirect security impacts, on critical infrastructure and armed forces. He indicates that literature on climate impacts on military infrastructure and operations still insufficient despite their significance. Osorio mentions that military operations which focus on humanitarian aid and disaster relief (HA/DR) in regions of the world where climate change impacts are increasing. He reminds that this comes with consequences for military planning and the role of Armed Forces. Osorio argues that NATO needs to adapt to the new challenges arising from climate change both in strategic and in operational terms. In his presentation Diego Osorio mentions three dimensions of climate change on the allied countries. First dimension is about direct impacts of climate change. These direct dimensions are climate change impacts such as rising temperatures in air and water, rising sea levels and changing weather patterns. He states that these impacts require **new approaches to ensure resilience of military & civilian critical infrastructure** and **to maintain the operability and readiness of the alliance**. Notably, non-state armed groups and terrorists may try to take advantage of weather-related instability and chaos. Second dimension that speaker mentions is about fossil fuels. In this regard, He states that **allied forces are transitioning from traditional fossil fuels to green alternatives (RES)** in an effort to reduce their carbon footprint and to strengthen their strategic and tactical independence from fossil fuels. Developments are likely to be driven by both markets and government regulation. Last dimension that Osorio mentions are indirect impacts and cascading effects of climate change. Conflicts in regions of the world are affected by climate change. He emphasizes long-term impacts on the physical natural environment, e.g. when ice shields in the Arctic are melting at an accelerated pace. Socio-economic and geostrategic nature of climate-linked conflicts require a completely new toolkit for prevention, management, and response.

Diego Osorio mentions NATO’s seven baseline requirements for national resilience are key guidelines for a new definition of resilience in the face of climate impacts: Assured continuity of government and critical government services, resilient energy supplies, ability to deal effectively with uncontrolled movement of people, resilient food and water resources, ability to deal with mass casualties, resilient civil communication systems, resilient civil transportation system.

The presenter states that geographical occurrence of the most climate impacts are largely concentrated in Global South and areas of low resilience. 10 out of 21 UN peace operations in countries ranked as most exposed to climate change as of December 2020. He recommends that member states need to prepare for these scenarios: Sea level rise or drought-related harvest failures, people in the affected regions might be displaced/forced to migrate, increase of “climate refugees”, social unrest due to food insecurity and hunger when agricultural land is not arable any longer, failure of governments to address these challenges can lead to hunger crises, violent conflict and political instability, emerging governance vacuum can make it easier for armed criminal and extremist groups, including terrorists, to radicalize parts of society and recruit fighters.

The speaker demonstrates the case studies in the last part of his presentation. Case studies include the places most affected by climate change. In the Mediterranean, factors such as temperature increase, drought, sea-level rise, extreme weather events lead to food and water scarcity and jeopardizes fragile stability. These negative impacts also lead migration from Southern to Northern shore. In Ethiopia and Horn of Africa, climate impacts further exacerbate existing tensions such as hunger. In the West Africa, climate impacts further contribute to the destabilization of the region and aggravates effects of existing security risks. In Mali MINUSMA addresses climate impacts and at the same time climate impacts undermines MINUSMA’s efforts to support peace and stability. In the Arctic, there are direct climate impacts through accelerated rate of warming creates second/third order effects such as geopolitical risks, competition over resources and trafficking. Lastly, Osorio mentions the dry corridor in Central America. The second case study that the speaker mentioned is Nord Stream 2. He argues that Nord Stream 2 at the center of tensions with Russia even before war of aggression in Ukraine. Osorio stated that Nord Stream 2 would have meant increased strategic dependence on Russia. For Diego Osorio, Nord Stream 2 has serious risks for Europe such as energy security risks for Europe, climate security risks due to higher emissions and geopolitical risks as Russia could have used Nord Stream 2 as a weapon against Eastern Europe, especially Ukraine. He argues that strategic energy independence can only be achieved through reliance on domestic energy sources, i.e. renewables.

Presentation



COE-DAT CISR Handbook 2

Climate Change as a Defining Factor in Allied Security and Operations

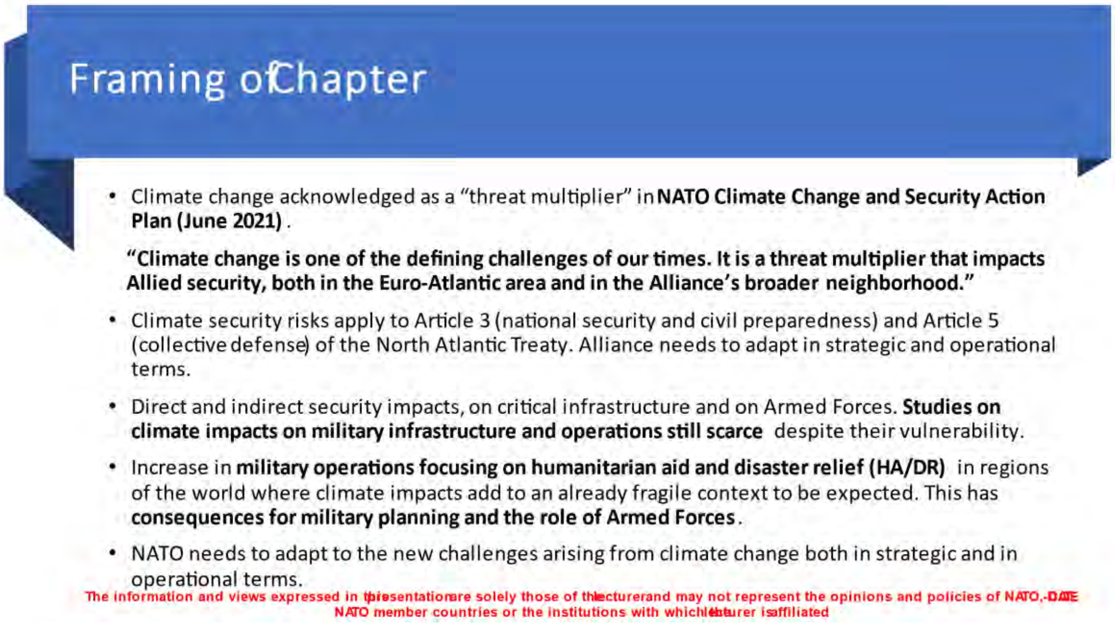
Diego Osorio (presenter)
Dr. Sabrina Schulz (author)
CDR (N) Dr. Marcus Mohlin (author)
Ankara, October 2022

Disclaimer and Public Statement

The content and opinions provided in this presentation reflect **only** <u>the personal views</u> of the speaker and do not engage in any way Her Majesty the Queen in right of Canada, or any instance of the Canadian Government.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

- Diego Osorio 11-11-2022 2



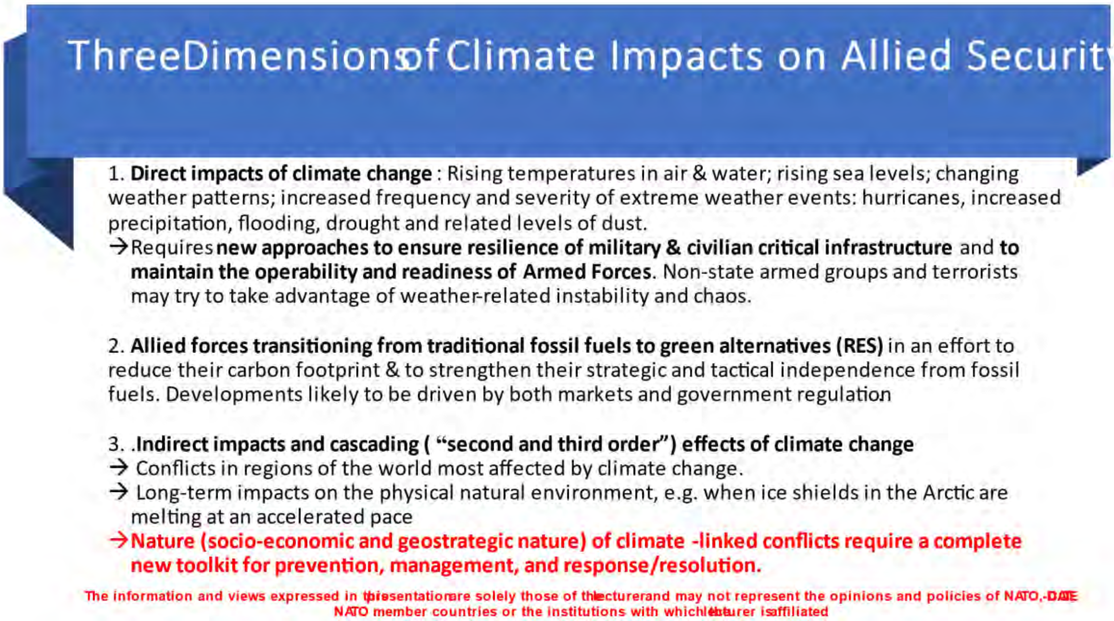
Framing of Chapter

- Climate change acknowledged as a "threat multiplier" in **NATO Climate Change and Security Action Plan (June 2021)**.

"Climate change is one of the defining challenges of our times. It is a threat multiplier that impacts Allied security, both in the Euro-Atlantic area and in the Alliance's broader neighborhood."

- Climate security risks apply to Article 3 (national security and civil preparedness) and Article 5 (collective defense) of the North Atlantic Treaty. Alliance needs to adapt in strategic and operational terms.
- Direct and indirect security impacts, on critical infrastructure and on Armed Forces. **Studies on climate impacts on military infrastructure and operations still scarce** despite their vulnerability.
- Increase in **military operations focusing on humanitarian aid and disaster relief (HA/DR)** in regions of the world where climate impacts add to an already fragile context to be expected. This has **consequences for military planning and the role of Armed Forces**.
- NATO needs to adapt to the new challenges arising from climate change both in strategic and in operational terms.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated



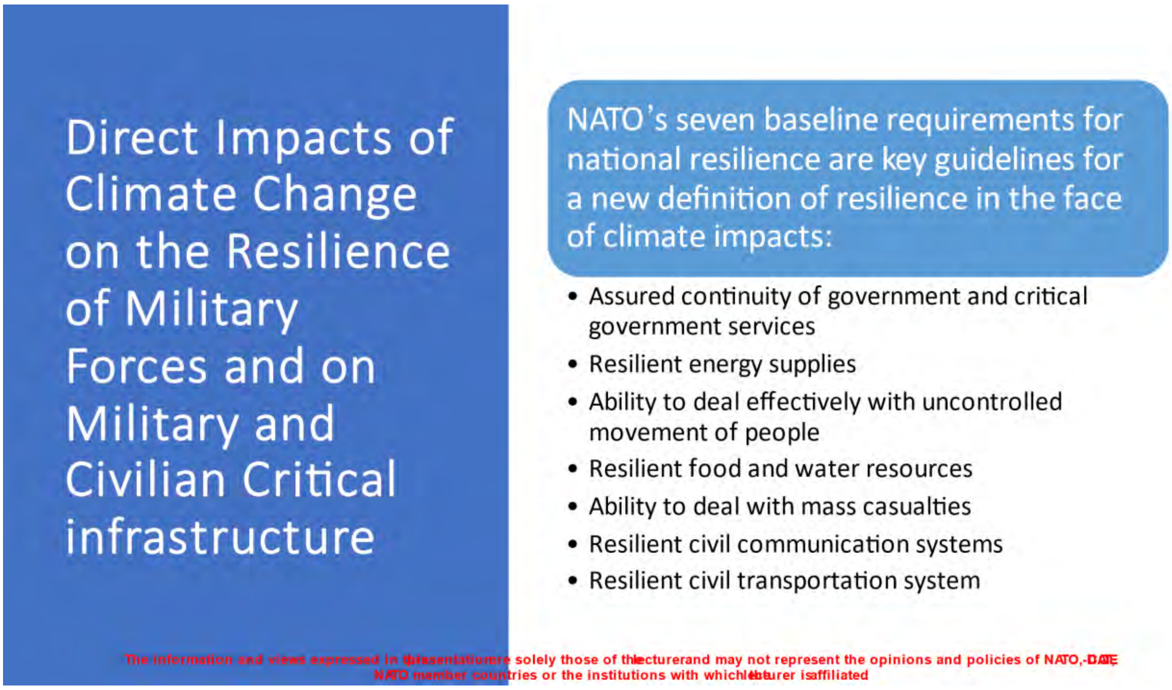
Three Dimensions of Climate Impacts on Allied Securit

1. **Direct impacts of climate change** : Rising temperatures in air & water; rising sea levels; changing weather patterns; increased frequency and severity of extreme weather events: hurricanes, increased precipitation, flooding, drought and related levels of dust.
→Requires **new approaches to ensure resilience of military & civilian critical infrastructure** and **to maintain the operability and readiness of Armed Forces**. Non-state armed groups and terrorists may try to take advantage of weather-related instability and chaos.

2. **Allied forces transitioning from traditional fossil fuels to green alternatives (RES)** in an effort to reduce their carbon footprint & to strengthen their strategic and tactical independence from fossil fuels. Developments likely to be driven by both markets and government regulation.

3. .**Indirect impacts and cascading ("second and third order") effects of climate change**
→ Conflicts in regions of the world most affected by climate change.
→ Long-term impacts on the physical natural environment, e.g. when ice shields in the Arctic are melting at an accelerated pace
→**Nature (socio-economic and geostrategic nature) of climate -linked conflicts require a complete new toolkit for prevention, management, and response/resolution.**

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated

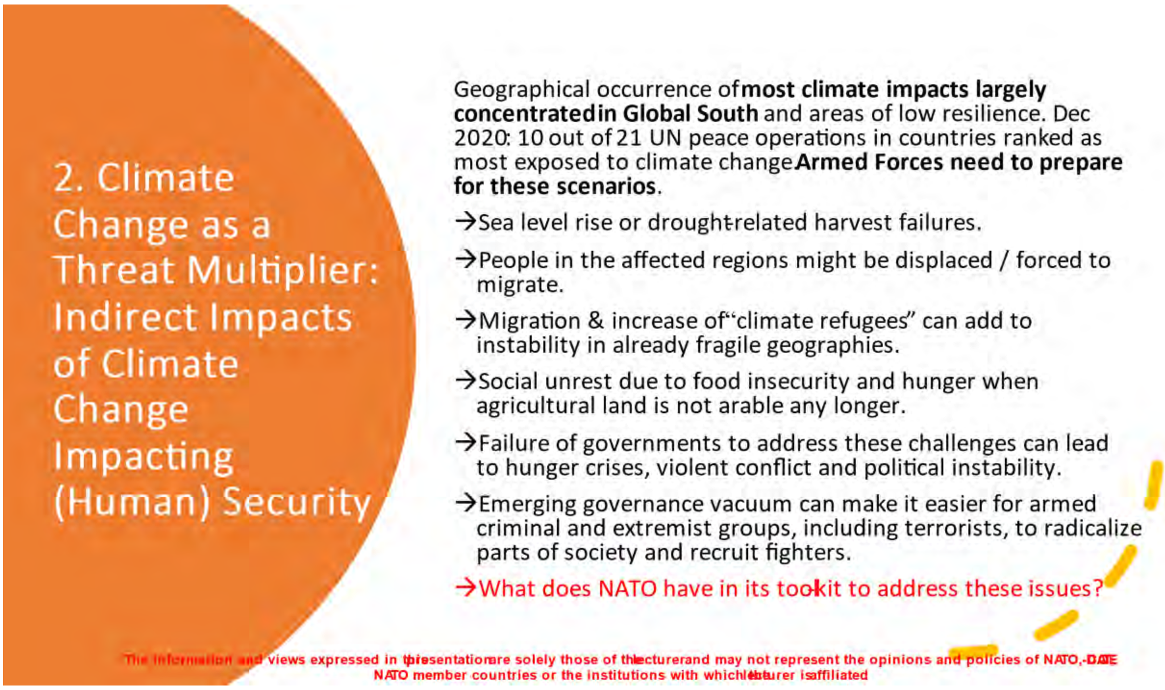


Direct Impacts of Climate Change on the Resilience of Military Forces and on Military and Civilian Critical infrastructure

NATO's seven baseline requirements for national resilience are key guidelines for a new definition of resilience in the face of climate impacts:

- Assured continuity of government and critical government services
- Resilient energy supplies
- Ability to deal effectively with uncontrolled movement of people
- Resilient food and water resources
- Ability to deal with mass casualties
- Resilient civil communication systems
- Resilient civil transportation system

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated



2. Climate Change as a Threat Multiplier: Indirect Impacts of Climate Change Impacting (Human) Security

Geographical occurrence of **most climate impacts largely concentrated in Global South** and areas of low resilience. Dec 2020: 10 out of 21 UN peace operations in countries ranked as most exposed to climate change. **Armed Forces need to prepare for these scenarios**.

→Sea level rise or drought-related harvest failures.

→People in the affected regions might be displaced / forced to migrate.

→Migration & increase of "climate refugees" can add to instability in already fragile geographies.

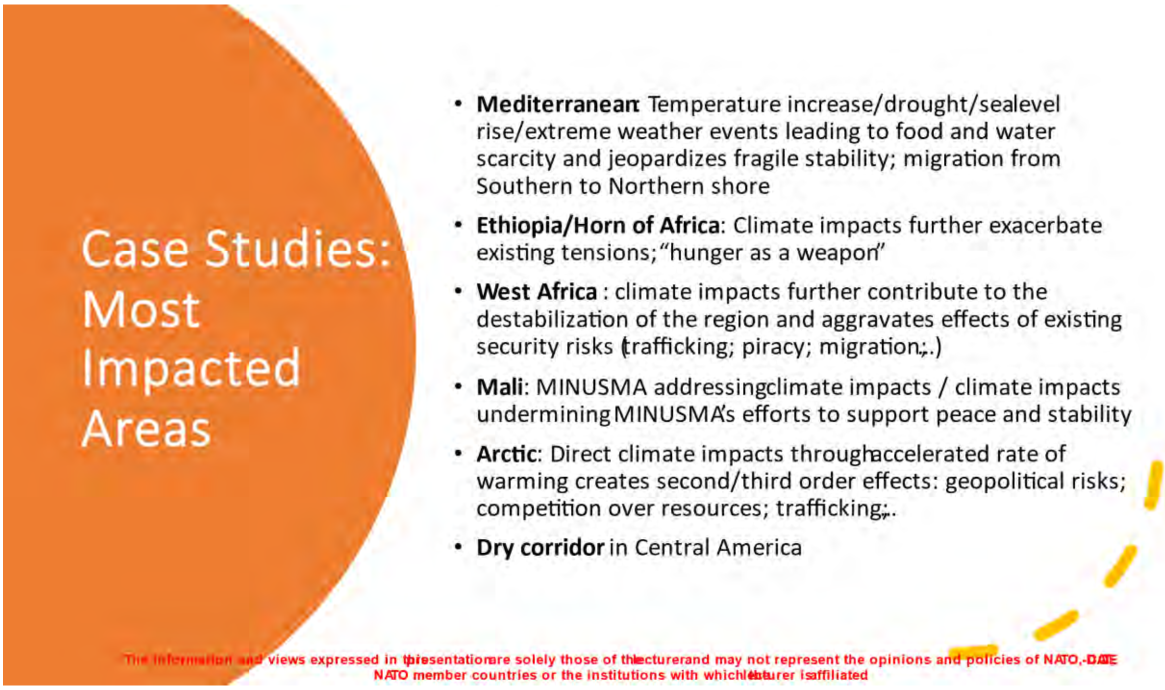
→Social unrest due to food insecurity and hunger when agricultural land is not arable any longer.

→Failure of governments to address these challenges can lead to hunger crises, violent conflict and political instability.

→Emerging governance vacuum can make it easier for armed criminal and extremist groups, including terrorists, to radicalize parts of society and recruit fighters.

→What does NATO have in its toolkit to address these issues?

The information and views expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, DATE NATO member countries or the institutions with whichlecturer isaffiliated



Case Studies: Most Impacted Areas

- **Mediterranean**: Temperature increase/drought/sealevel rise/extreme weather events leading to food and water scarcity and jeopardizes fragile stability; migration from Southern to Northern shore
- **Ethiopia/Horn of Africa**: Climate impacts further exacerbate existing tensions; "hunger as a weapon"
- **West Africa** : climate impacts further contribute to the destabilization of the region and aggravates effects of existing security risks (trafficking; piracy; migration;..)
- **Mali**: MINUSMA addressingclimate impacts / climate impacts undermining MINUSMA's efforts to support peace and stability
- **Arctic**: Direct climate impacts throughaccelerated rate of warming creates second/third order effects: geopolitical risks; competition over resources; trafficking;..
- **Dry corridor** in Central America

The information and views expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, DATE NATO member countries or the institutions with whichlecturer isaffiliated

3. Going green – Effects on Operations in the Transition Away from Fossil Fuels

- Energy resilience in military operations
- Energy logistics and smart energy
- Joint implementation
- Compatibility between civilian and military solutions
- Case Studies: Offshore Wind Power; Renewable Energy Sources on Forward and Rear Operating Bases

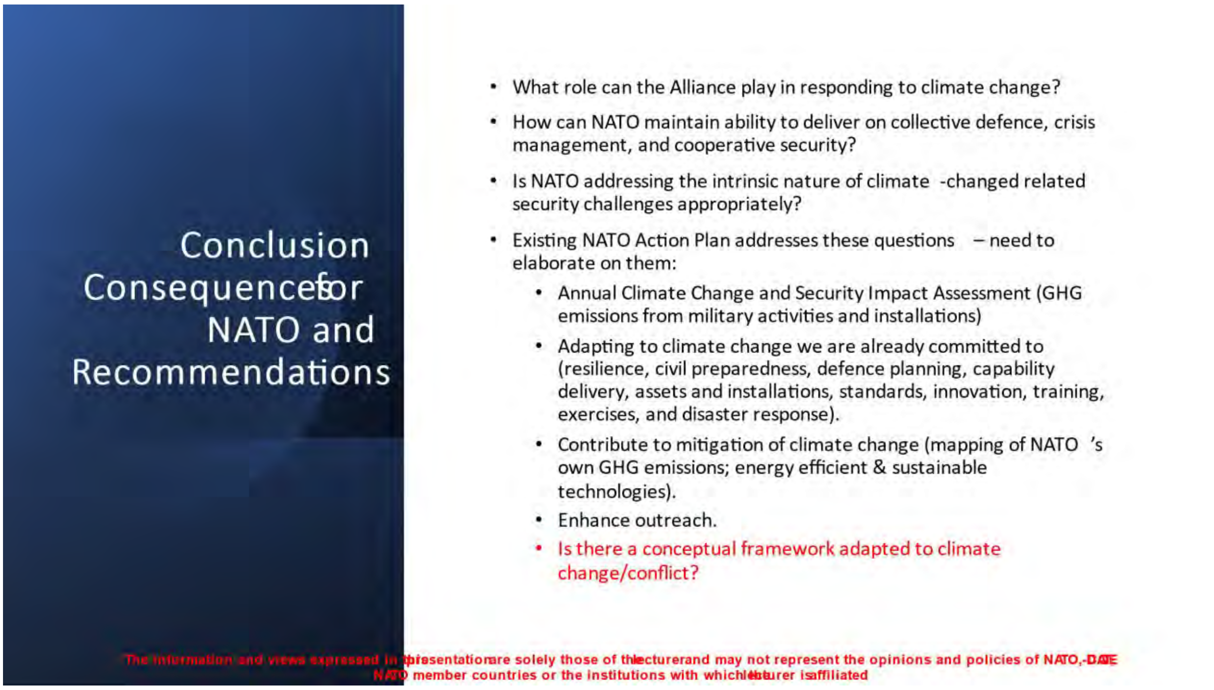
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, DATE, NATO member countries or the institutions with which the lecturer is affiliated

Case Study: Nord Stream2

- Nord Stream2 at the centre of tensions with Russia even before war of aggression in Ukraine
- NS2 would have meant increased strategic dependence on Russia
- **NS2 showed risks:**
  - Energy security risks for Europe;
  - Climate security risks due to higher emissions;
  - Geopolitical risks as Russia could have used NS2 as a weapon against Eastern Europe, esp. Ukraine.

Strategic energy independence only through reliance on domestic energy sources, i.e. renewables.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, DATE, NATO member countries or the institutions with which the lecturer is affiliated



Conclusion Consequences for NATO and Recommendations

- What role can the Alliance play in responding to climate change?
- How can NATO maintain ability to deliver on collective defence, crisis management, and cooperative security?
- Is NATO addressing the intrinsic nature of climate -changed related security challenges appropriately?
- Existing NATO Action Plan addresses these questions – need to elaborate on them:
  - Annual Climate Change and Security Impact Assessment (GHG emissions from military activities and installations)
  - Adapting to climate change we are already committed to (resilience, civil preparedness, defence planning, capability delivery, assets and installations, standards, innovation, training, exercises, and disaster response).
  - Contribute to mitigation of climate change (mapping of NATO 's own GHG emissions; energy efficient & sustainable technologies).
  - Enhance outreach.
  - Is there a conceptual framework adapted to climate change/conflict?

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, DATE, NATO member countries or the institutions with which the lecturer is affiliated

For contact

- Diego Osorio, BA, MILE, MPA, PhD (Cand).
- E-mail: **diego_osorio_un@outlook.com**
- Canada:+1 (581) 317-6168
- **https://ca.linkedin.com/in/diegoosoriocanada**

DAY I

SESSION 2: Questions and Answers

Questions to Mr. Lucas COX

1. *Could you give more information about the consequences of the Crimean Incident?*

   We have seen the secondary effects of the invasion. But the fact that NATO partner allies are so closely economically connected, I think it shows the challenge of being able to respond as one as an alliance. It shows economics and the supply chain is a front center military issue. But this is ignored by some governments. It is the reason of increase in prices energy. 400% increase in gas prices are due to military situation. I think that are learned are that NATO alliance can take more supervisory role when it comes supervising governments how they source critical infrastructure. There may be more cooperation in this regard.

Questions to Dr. Aleksander OLECH

1. *If we are looking the Middle East North Africa region which actors should be most concerned about, especially now as we turn from Russia as major energy supplier to the Middle East and North Africa as major energy supplier?*

   If we are looking at energy supplies firstly, there's the challenge forward as I said that covers the area and the situation has been released with Iran and there are problems with straits of Hormuz and Bab el-Mandab. Most countries can cope with the terrorist challenges but Nigeria cannot. There are first Boko Haram and then Niger Delta Avengers in Nigeria. These organizations constrain the energy sector. We switched from challenging or facing the government and these organizations decided to earn money by having an impact on the energy sector. On the other hand, the largest port for energy transportation was built by China. In addition, China invests in critical infrastructure in African countries. China also invests in the sports industry in the region. Why? Because people are interested in sports, that's why China is building sports facilities. It also builds buildings such as hospitals and schools. Just to finish, terrorist groups and rebel groups always aim to change something in the country. The most important sector that these organizations can impact is the *energy* *sector*. The most valuable property is energy in the region. For some countries the threat might be Boko Haram as in Nigeria, for Poland and Ukraine it might be Russia, or for some countries it might be Iran.

DAY I

SESSION 3 – Critical Infrastructure Security and Resilience Book

Logistics and Supply Chain Resilience

Dr. Gabriel RAICU

The resilience of logistics and transport chains is imperative for an effective defense against any classical or hybrid terrorist threats from previously known terrorist groups or the hard-to-attribute mix from allegedly liberating actions supported by a rogue state often disguised as hybrid or frozen conflicts.

During the Cold War, NATO logistics was limited to the North Atlantic area with a planned linear defense of Western Europe with national corps supported by national support elements.

Aspects of threats and the complexity of the supply chain

Supply process can be considered as system of systems aggregated activity were supplying the military with everything from food to equipment is a part of each NATO operation. It is a complex process, creating new LOCs far more complex than finding roads, airports and rail networks, or ports to dock ships.

A major challenge in terms of supply chain security is its dependence on the private sector, which raises several risks for various reasons, ranging from the company's own operational limitations to the related interest given by political affiliation or confusing geostrategic interest, which the owner of a logistics node may have.

Supply chain and collective logistics

Sharing the provision and use of logistic capabilities between nations is one of the key logistics principles driving all related support in NATO. There must be a flexible ability to move forces in an efficient manner in and between operational theatres. The complete spectrum of NATO roles and missions also needs advanced logistical support.

The current strategic logistics guidance consisting of the revised vision statement provides effective logistical support and broadens the Logistics Vision to give NATO commanders the greatest flexibility in current and future missions promoting the pursuit of collective logistics within the Alliance.

Supply efficiency and operational consolidation

NATO has no direct access to all the necessary supply-chain capabilities and logistics, even in its primary military defense responsibility. NATO's assets and capabilities belong to its members states, with few exceptions, most notably for political consultations and command and control.

Through the NATO Defence Planning Process (NDPP), nations coordinate and distribute their capabilities at the Alliance level. The Transfer of Authority (ToA) mechanism allows national forces to fall under the control of NATO's Supreme Commander if needed.

Threats complexity and their interrelation

Threats can come from state and non-state actors in the form of terrorist attacks, cyberattacks, or combined in a form of hybrid warfare, with faint delineations between conventional and unconventional forms of conflict. There is a Strengthened Resilience Commitment reiterated in 2021 by the Heads of State and Government of the North Atlantic Alliance to address this issue.

Non-physical & advanced (cyber) threats to logistical chain

Any kinetic action in any field can involve attacks in cyberspace, although cyber warfare can exist mainly in virtual space. Escalation of conflicts and the potential to be used for terrorist purposes, if cyber conflicts escalate, inevitably attracts the targeting of railways, roads, airports and sea and river ports, as well as connecting infrastructure such as bridges and ferryboats. There is a close logical connection within the civilian domains that can be constituted in real areas of disruption of the supply chain. Cyberattacks on the transport system can block the industry due to a ripple effect in the supply chain. As a sample entry level scenario, a cyberattack against maritime facilities could disrupt the customs approval process or facilitate the import of illegal goods or the proliferation of dangerous operations. Threat actors may also have a bigger target in their sights if a cyber threat can proliferate from a port to other interconnected systems like airports or railways.

Case studies:

- Logistical challenges of relocating NATO capabilities on the Eastern Flank: Russia - Ukraine War
- Major logistical vulnerabilities and defences of the Alliance weakest points - Suwalki Corridor

Pillars of supply chain resilience - Resiliency building by managing supply chain risks

- Increasing the ability to absorb shocks by minimizing the risk of disrupting the supply chain and other severe impacts, for example, by flexibly switching from primary to secondary supply routes, rebalancing the worldwide supply, or switching suppliers.
- Redesigning the Global Network by increasing flexibility by using dual-source redundancy or using approaches that include nearshoring to reduce dependence on complex global logistics and vertical integration to bring production to critical components including semiconductors or other in-house IT elements.
- New parameters for supply chain buffers when the organization needs to develop an effective multi-tier inventory strategy, which tends to generate new stock targets in the high volatility nodes of the supply chain.
- Managing suppliers proactively by assessing the criticality of suppliers and adjusting relationships with all of them to ensure the availability of resources.
- Reaction speed when disruption occurs is needed in order to manage normal volatility and to avoid interruptions, as well as to increase resilience. They must apply agile ways of working in different functions and regions where the logistics system operates.
    - Any deviation must be managed transparently and develop a forward-looking view of risks and opportunities through simulation.
    - The rapid response should support multi-enterprise supply chain management, end-to-end risk management, and planning scenarios based on anticipation and simulation.

Logistics Cybersecurity & Energy Security interlinks

There is a close logical connection with the civil domains that can be constituted in real areas of disruption of the supply chain. Examples can be cited in many areas, aviation maritime and railways being a major logistics component that has been subjected to multiple types of attacks.

There are limits, at least in Europe, where ownership of the energy resources that power the NATO operations belong to states and regional actors that can become hostile at any time.

Main topics covered in Logistic Chapter

Logistics and supply chain in the NATO context

- Complexity of the supply chain
- Supply chain and collective logistics
- Supply efficiency and operational consolidation

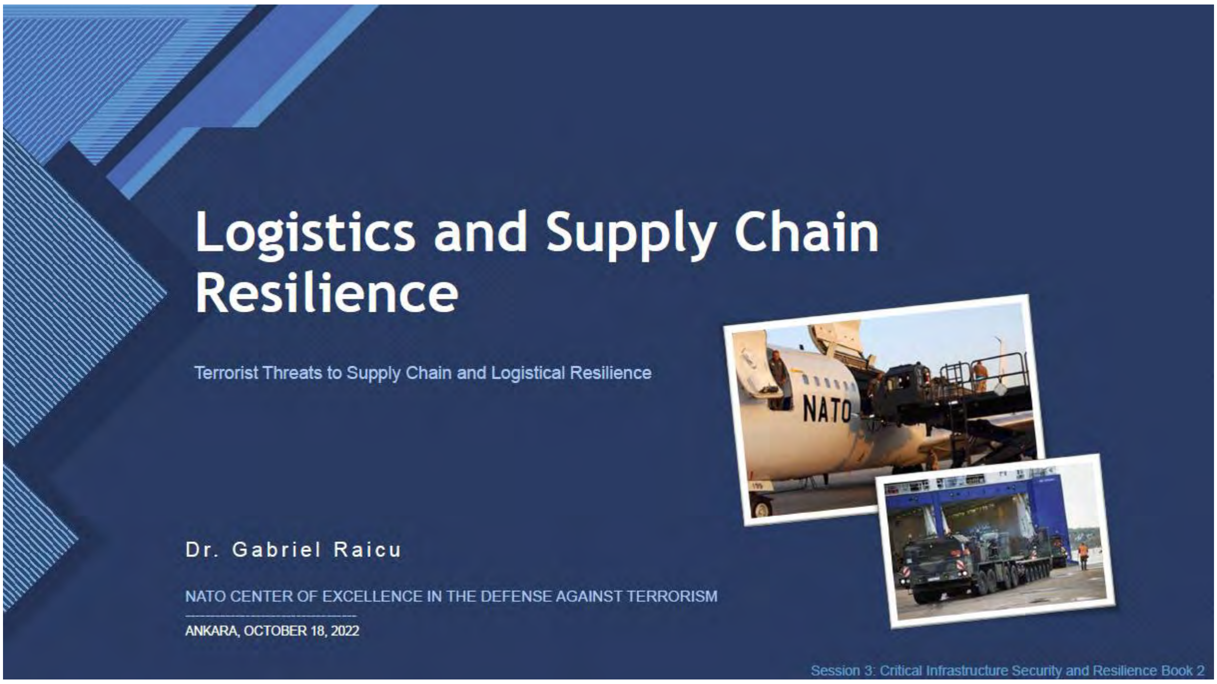
Logistics and supply chain threats aspects

- Threats complexity and their interrelation
- Non-physical & advanced (cyber) threats to logistical chain
- Multinational interaction mechanisms
- Complex risks for critical logistic infrastructure
- Major logistical vulnerabilities and defenses of the weakest points – the **Suwalki Gap** case study
- Logistical challenges of relocating NATO capabilities on the Eastern Flank: Russia - Ukraine War case study

Supply chain resilience

- Interoperability context and operating principles
- Changes triggered by threats and incidents
- Resilience commitment and logistics
- Pillars of supply chain resilience

Presentation



Logistics and Supply Chain Resilience

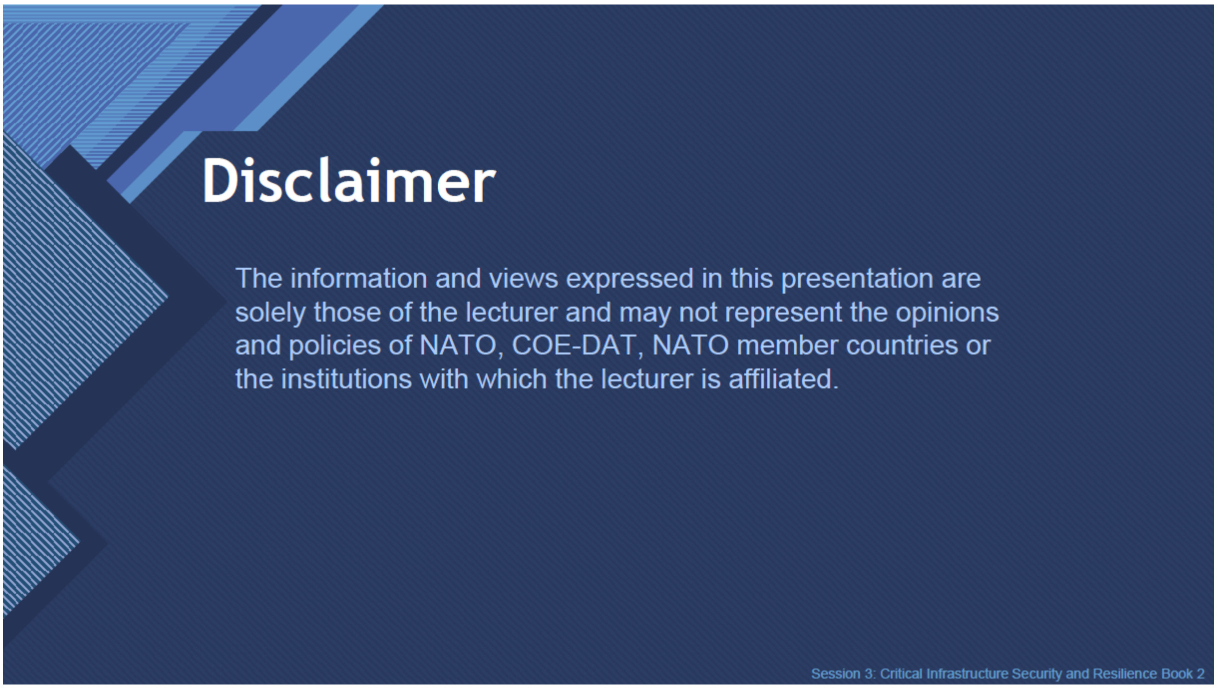
Terrorist Threats to Supply Chain and Logistical Resilience

Dr. Gabriel Raicu

NATO CENTER OF EXCELLENCE IN THE DEFENSE AGAINST TERRORISM

ANKARA, OCTOBER 18, 2022

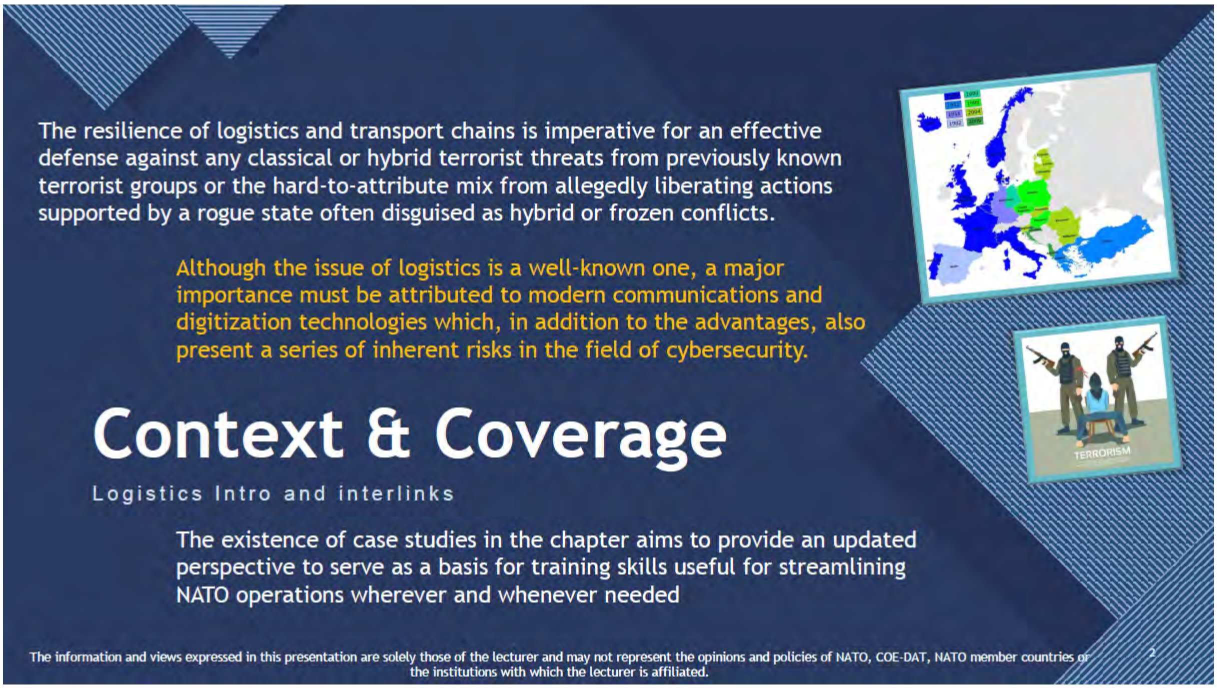
Session 3: Critical Infrastructure Security and Resilience Book 2



Disclaimer

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Session 3: Critical Infrastructure Security and Resilience Book 2



The resilience of logistics and transport chains is imperative for an effective defense against any classical or hybrid terrorist threats from previously known terrorist groups or the hard-to-attribute mix from allegedly liberating actions supported by a rogue state often disguised as hybrid or frozen conflicts.

Although the issue of logistics is a well-known one, a major importance must be attributed to modern communications and digitization technologies which, in addition to the advantages, also present a series of inherent risks in the field of cybersecurity.

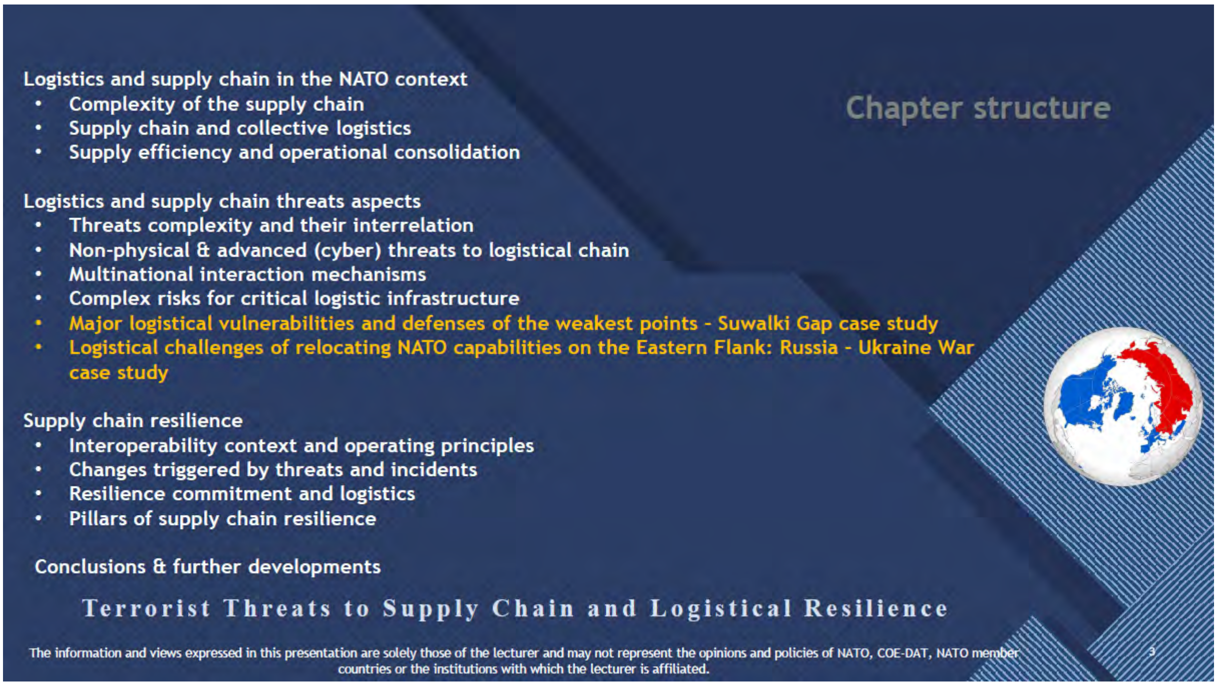
Context & Coverage

Logistics Intro and interlinks

The existence of case studies in the chapter aims to provide an updated perspective to serve as a basis for training skills useful for streamlining NATO operations wherever and whenever needed

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

2



Chapter structure

Logistics and supply chain in the NATO context

- Complexity of the supply chain
- Supply chain and collective logistics
- Supply efficiency and operational consolidation

Logistics and supply chain threats aspects

- Threats complexity and their interrelation
- Non-physical & advanced (cyber) threats to logistical chain
- Multinational interaction mechanisms
- Complex risks for critical logistic infrastructure
- Major logistical vulnerabilities and defenses of the weakest points - Suwalki Gap case study
- Logistical challenges of relocating NATO capabilities on the Eastern Flank: Russia - Ukraine War case study

Supply chain resilience

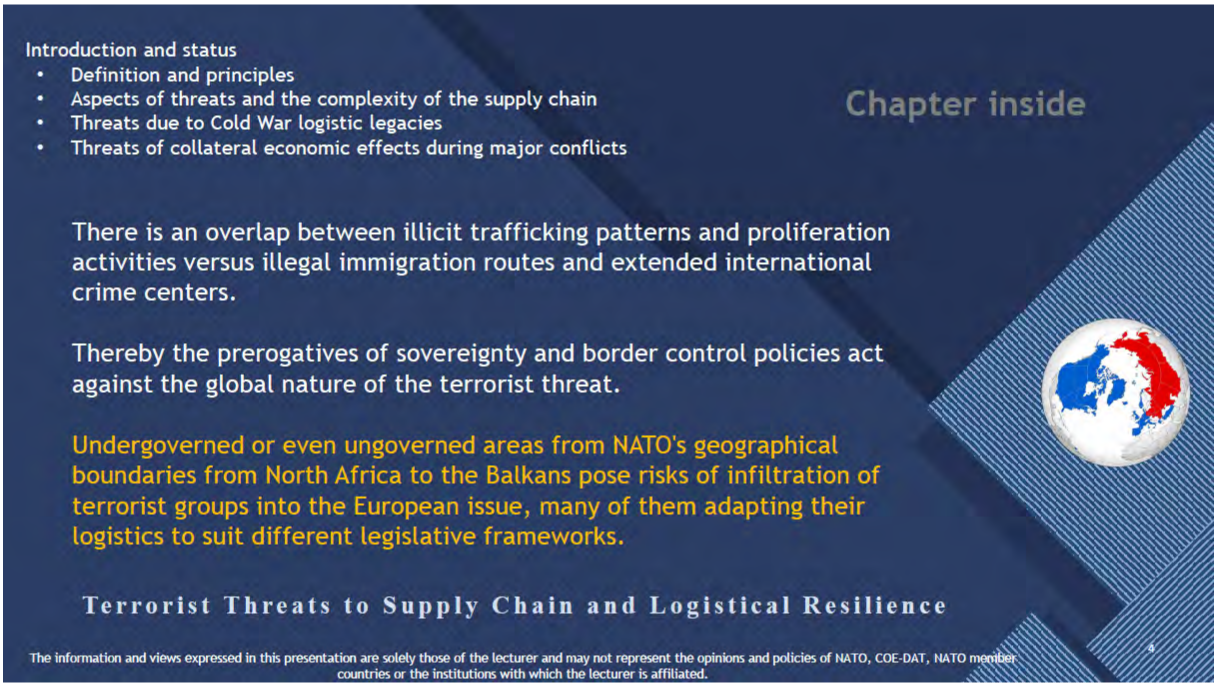
- Interoperability context and operating principles
- Changes triggered by threats and incidents
- Resilience commitment and logistics
- Pillars of supply chain resilience

Conclusions & further developments

Terrorist Threats to Supply Chain and Logistical Resilience

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

3



Introduction and status

- Definition and principles
- Aspects of threats and the complexity of the supply chain
- Threats due to Cold War logistic legacies
- Threats of collateral economic effects during major conflicts

Chapter inside

There is an overlap between illicit trafficking patterns and proliferation activities versus illegal immigration routes and extended international crime centers.

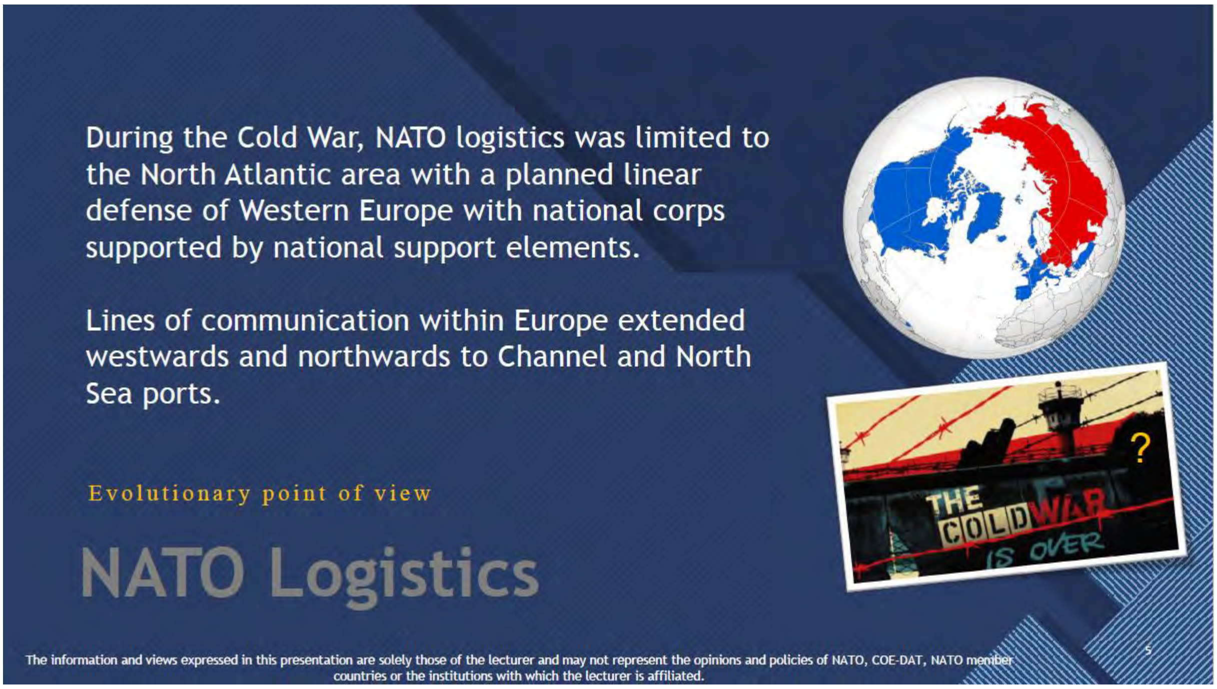
Thereby the prerogatives of sovereignty and border control policies act against the global nature of the terrorist threat.

Undergoverned or even ungoverned areas from NATO's geographical boundaries from North Africa to the Balkans pose risks of infiltration of terrorist groups into the European issue, many of them adapting their logistics to suit different legislative frameworks.

Terrorist Threats to Supply Chain and Logistical Resilience

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

4



During the Cold War, NATO logistics was limited to the North Atlantic area with a planned linear defense of Western Europe with national corps supported by national support elements.

Lines of communication within Europe extended westwards and northwards to Channel and North Sea ports.

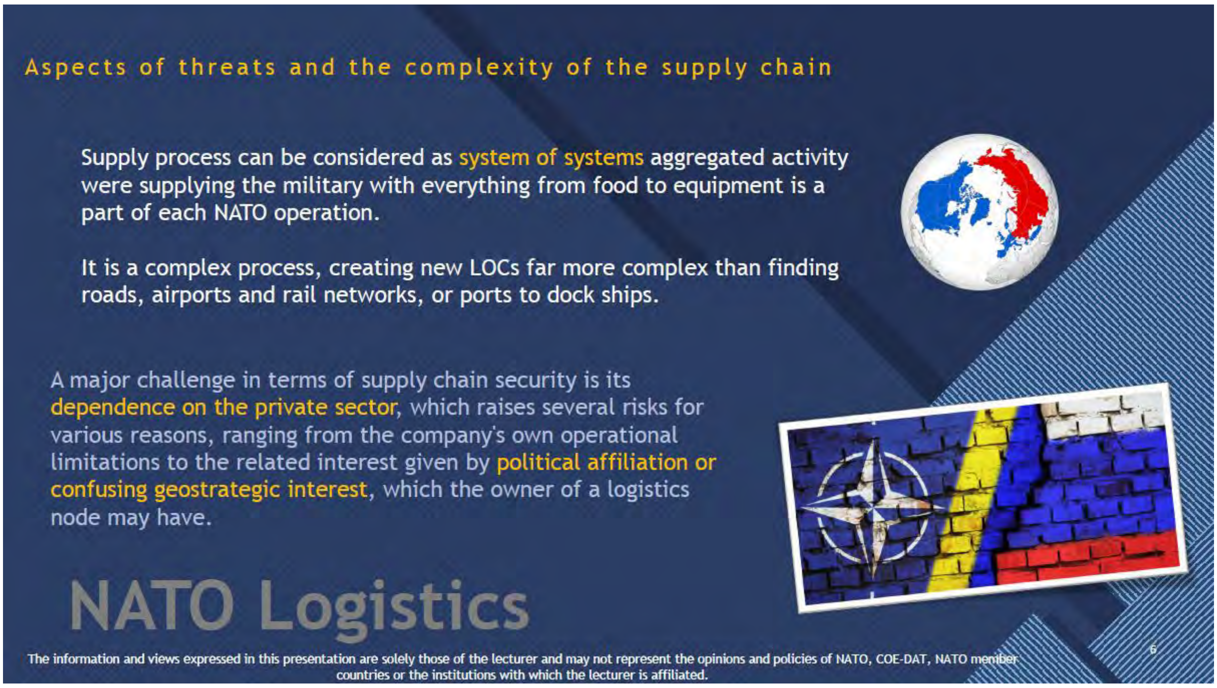
Evolutionary point of view

NATO Logistics

THE COLD WAR IS OVER
?

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

5



Aspects of threats and the complexity of the supply chain

Supply process can be considered as system of systems aggregated activity were supplying the military with everything from food to equipment is a part of each NATO operation.

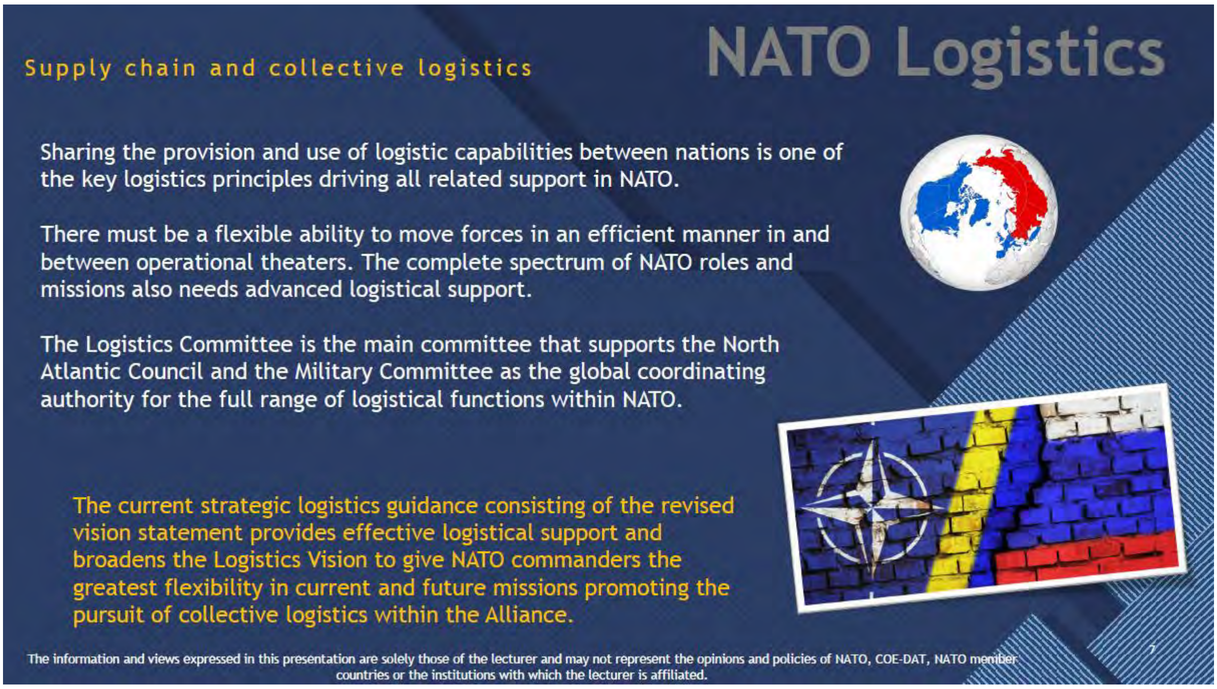
It is a complex process, creating new LOCs far more complex than finding roads, airports and rail networks, or ports to dock ships.

A major challenge in terms of supply chain security is its dependence on the private sector, which raises several risks for various reasons, ranging from the company's own operational limitations to the related interest given by political affiliation or confusing geostrategic interest, which the owner of a logistics node may have.

NATO Logistics

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

6



Supply chain and collective logistics

NATO Logistics

Sharing the provision and use of logistic capabilities between nations is one of the key logistics principles driving all related support in NATO.

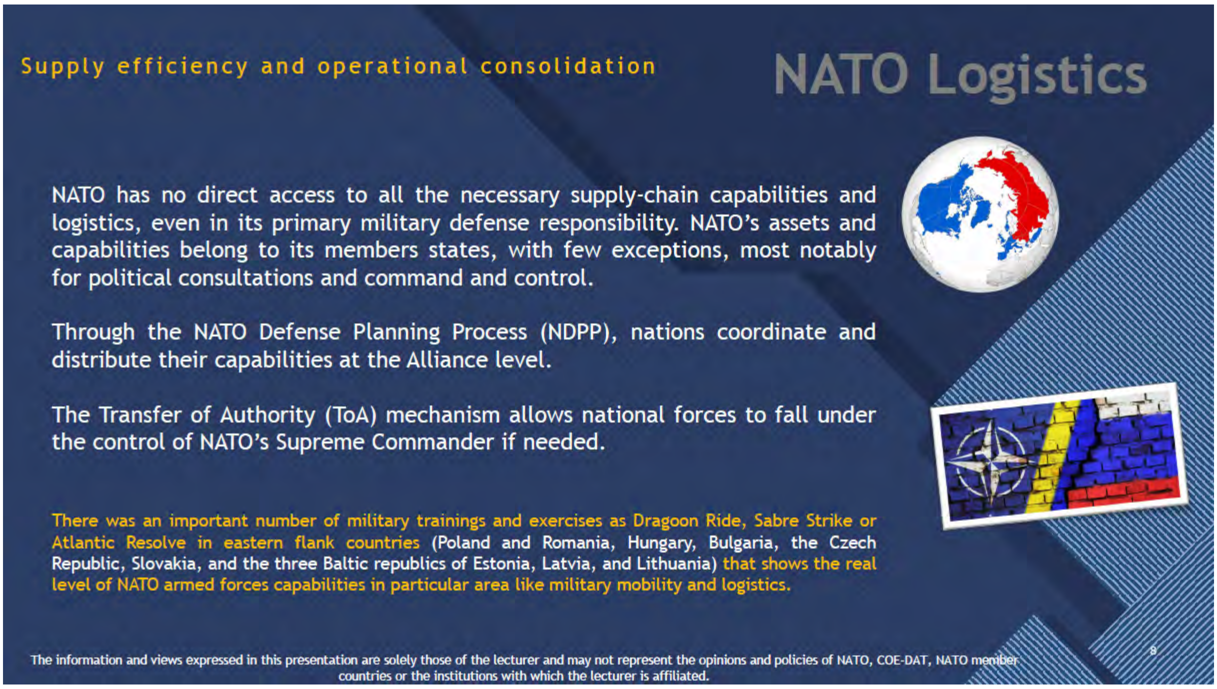
There must be a flexible ability to move forces in an efficient manner in and between operational theaters. The complete spectrum of NATO roles and missions also needs advanced logistical support.

The Logistics Committee is the main committee that supports the North Atlantic Council and the Military Committee as the global coordinating authority for the full range of logistical functions within NATO.

The current strategic logistics guidance consisting of the revised vision statement provides effective logistical support and broadens the Logistics Vision to give NATO commanders the greatest flexibility in current and future missions promoting the pursuit of collective logistics within the Alliance.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

7



Supply efficiency and operational consolidation

NATO Logistics

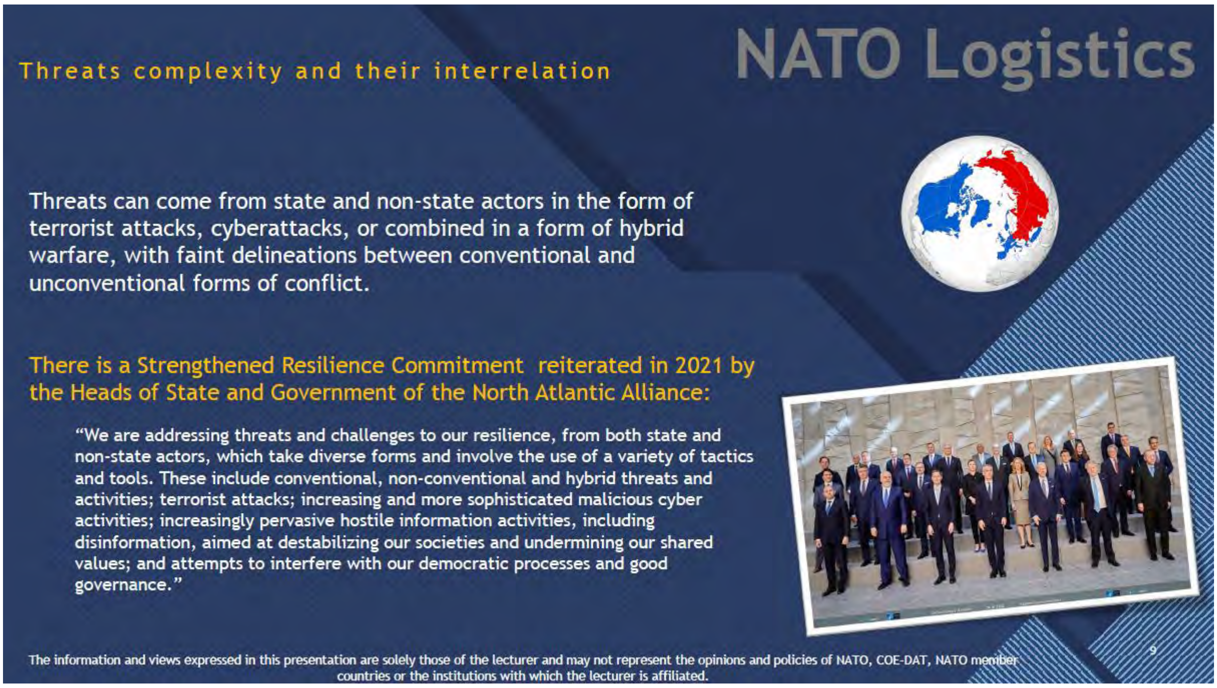
NATO has no direct access to all the necessary supply-chain capabilities and logistics, even in its primary military defense responsibility. NATO's assets and capabilities belong to its members states, with few exceptions, most notably for political consultations and command and control.

Through the NATO Defense Planning Process (NDPP), nations coordinate and distribute their capabilities at the Alliance level.

The Transfer of Authority (ToA) mechanism allows national forces to fall under the control of NATO's Supreme Commander if needed.

There was an important number of military trainings and exercises as Dragoon Ride, Sabre Strike or Atlantic Resolve in eastern flank countries (Poland and Romania, Hungary, Bulgaria, the Czech Republic, Slovakia, and the three Baltic republics of Estonia, Latvia, and Lithuania) that shows the real level of NATO armed forces capabilities in particular area like military mobility and logistics.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Threats complexity and their interrelation

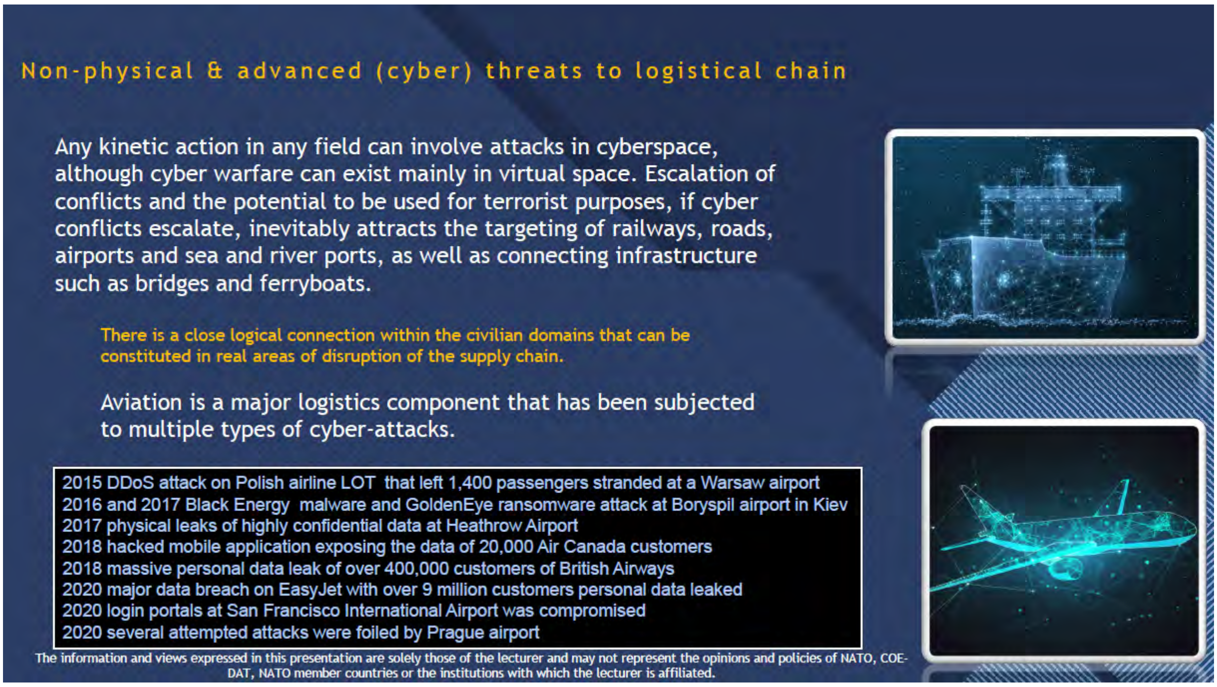
NATO Logistics

Threats can come from state and non-state actors in the form of terrorist attacks, cyberattacks, or combined in a form of hybrid warfare, with faint delineations between conventional and unconventional forms of conflict.

There is a Strengthened Resilience Commitment reiterated in 2021 by the Heads of State and Government of the North Atlantic Alliance:

> "We are addressing threats and challenges to our resilience, from both state and non-state actors, which take diverse forms and involve the use of a variety of tactics and tools. These include conventional, non-conventional and hybrid threats and activities; terrorist attacks; increasing and more sophisticated malicious cyber activities; increasingly pervasive hostile information activities, including disinformation, aimed at destabilizing our societies and undermining our shared values; and attempts to interfere with our democratic processes and good governance."

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Non-physical & advanced (cyber) threats to logistical chain

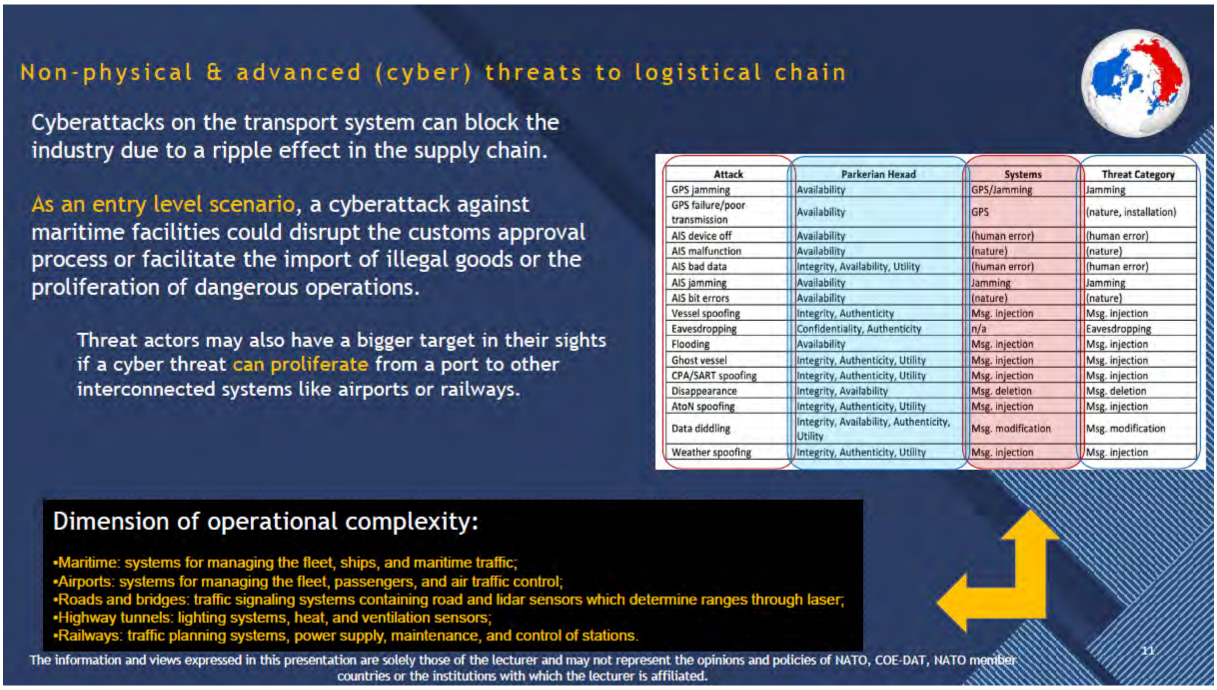
Any kinetic action in any field can involve attacks in cyberspace, although cyber warfare can exist mainly in virtual space. Escalation of conflicts and the potential to be used for terrorist purposes, if cyber conflicts escalate, inevitably attracts the targeting of railways, roads, airports and sea and river ports, as well as connecting infrastructure such as bridges and ferryboats.

There is a close logical connection within the civilian domains that can be constituted in real areas of disruption of the supply chain.

Aviation is a major logistics component that has been subjected to multiple types of cyber-attacks.

2015 DDoS attack on Polish airline LOT that left 1,400 passengers stranded at a Warsaw airport
2016 and 2017 Black Energy malware and GoldenEye ransomware attack at Boryspil airport in Kiev
2017 physical leaks of highly confidential data at Heathrow Airport
2018 hacked mobile application exposing the data of 20,000 Air Canada customers
2018 massive personal data leak of over 400,000 customers of British Airways
2020 major data breach on EasyJet with over 9 million customers personal data leaked
2020 login portals at San Francisco International Airport was compromised
2020 several attempted attacks were foiled by Prague airport

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Non-physical & advanced (cyber) threats to logistical chain

Cyberattacks on the transport system can block the industry due to a ripple effect in the supply chain.

As an entry level scenario, a cyberattack against maritime facilities could disrupt the customs approval process or facilitate the import of illegal goods or the proliferation of dangerous operations.

Threat actors may also have a bigger target in their sights if a cyber threat can proliferate from a port to other interconnected systems like airports or railways.

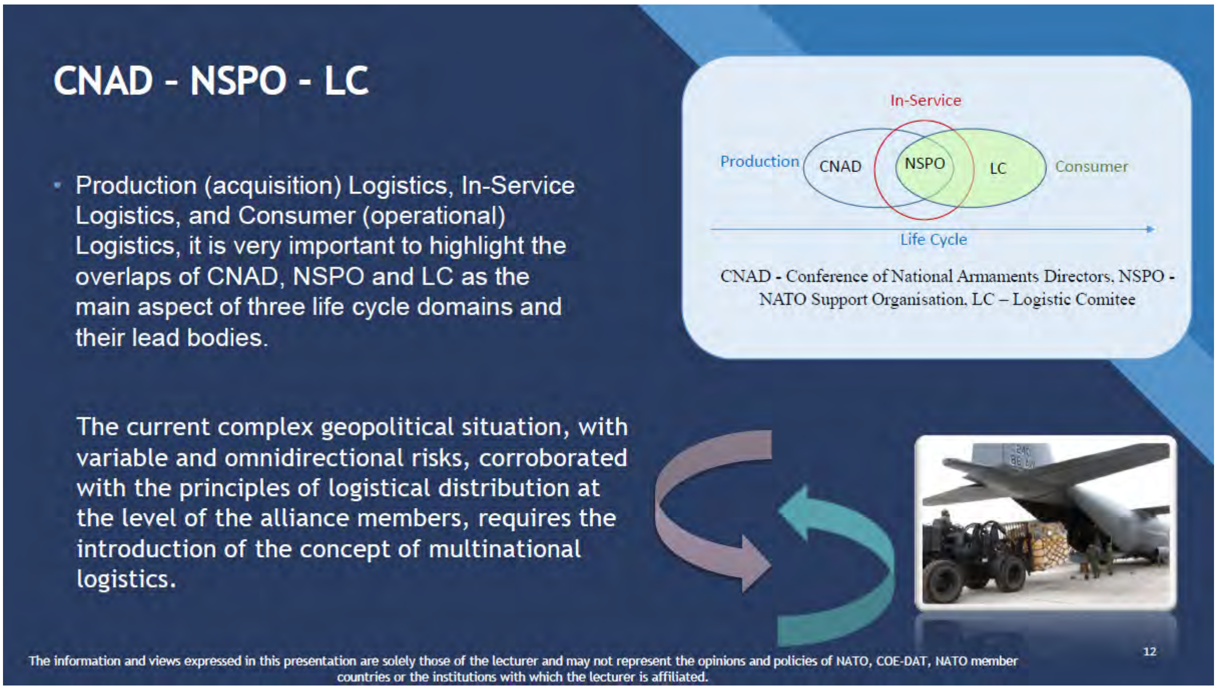
Attack	Parkerian Hexad	Systems	Threat Category
GPS jamming	Availability	GPS/Jamming	Jamming
GPS failure/poor transmission	Availability	GPS	(nature, installation)
AIS device off	Availability	(human error)	(human error)
AIS malfunction	Availability	(nature)	(nature)
AIS bad data	Integrity, Availability, Utility	(human error)	(human error)
AIS jamming	Availability	Jamming	Jamming
AIS bit errors	Availability	(nature)	(nature)
Vessel spoofing	Integrity, Authenticity	Msg. injection	Msg. injection
Eavesdropping	Confidentiality, Authenticity	n/a	Eavesdropping
Flooding	Availability	Msg. injection	Msg. injection
Ghost vessel	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
CPA/SART spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Disappearance	Integrity, Availability	Msg. deletion	Msg. deletion
AtoN spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection
Data diddling	Integrity, Availability, Authenticity, Utility	Msg. modification	Msg. modification
Weather spoofing	Integrity, Authenticity, Utility	Msg. injection	Msg. injection

Dimension of operational complexity:

- Maritime: systems for managing the fleet, ships, and maritime traffic;
- Airports: systems for managing the fleet, passengers, and air traffic control;
- Roads and bridges: traffic signaling systems containing road and lidar sensors which determine ranges through laser;
- Highway tunnels: lighting systems, heat, and ventilation sensors;
- Railways: traffic planning systems, power supply, maintenance, and control of stations.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

11



CNAD - NSPO - LC

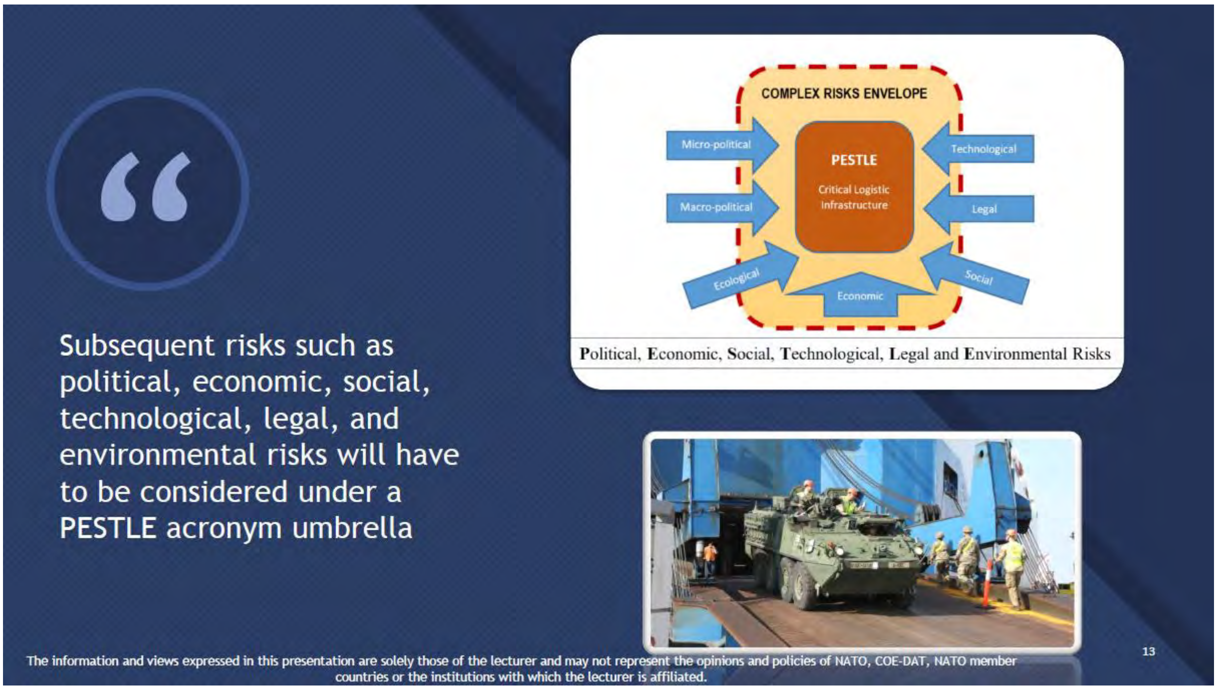
- Production (acquisition) Logistics, In-Service Logistics, and Consumer (operational) Logistics, it is very important to highlight the overlaps of CNAD, NSPO and LC as the main aspect of three life cycle domains and their lead bodies.

CNAD - Conference of National Armaments Directors, NSPO - NATO Support Organisation, LC – Logistic Comitee

The current complex geopolitical situation, with variable and omnidirectional risks, corroborated with the principles of logistical distribution at the level of the alliance members, requires the introduction of the concept of multinational logistics.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

12

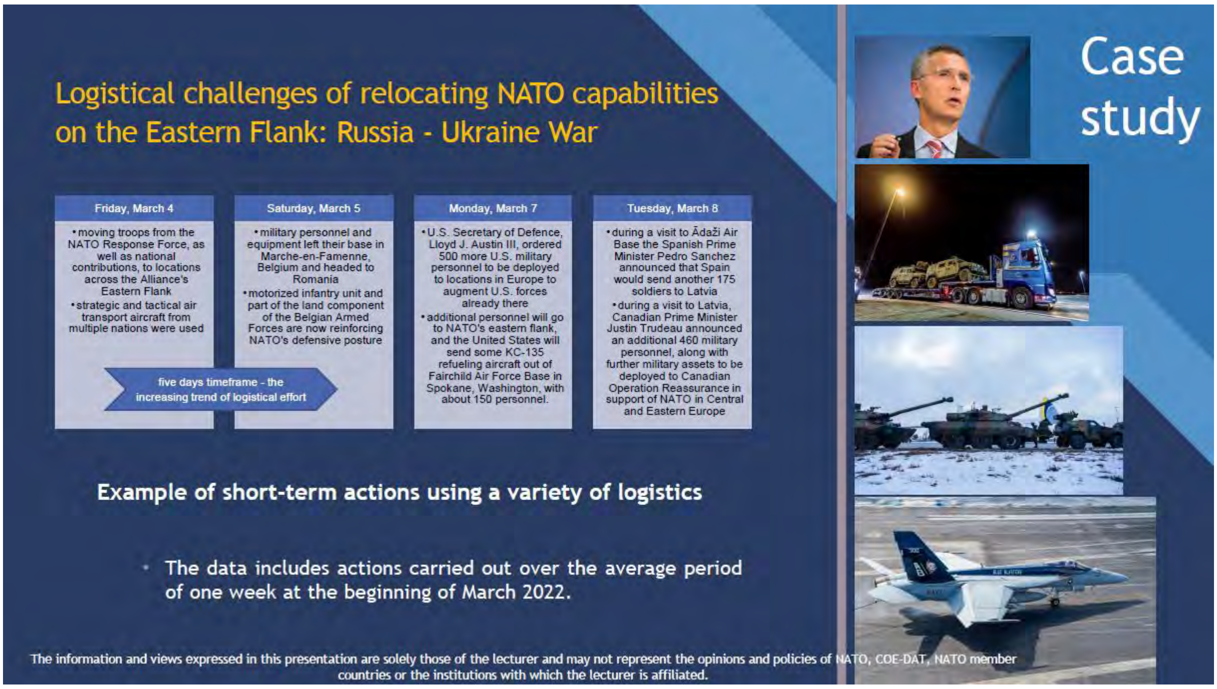


Political, Economic, Social, Technological, Legal and Environmental Risks

Subsequent risks such as political, economic, social, technological, legal, and environmental risks will have to be considered under a PESTLE acronym umbrella

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

13



Case study

Logistical challenges of relocating NATO capabilities on the Eastern Flank: Russia - Ukraine War

Friday, March 4

- moving troops from the NATO Response Force, as well as national contributions, to locations across the Alliance's Eastern Flank
- strategic and tactical air transport aircraft from multiple nations were used

Saturday, March 5

- military personnel and equipment left their base in Marche-en-Famenne, Belgium and headed to Romania
- motorized infantry unit and part of the land component of the Belgian Armed Forces are now reinforcing NATO's defensive posture

Monday, March 7

- U.S. Secretary of Defence, Lloyd J. Austin III, ordered 500 more U.S. military personnel to be deployed to locations in Europe to augment U.S. forces already there
- additional personnel will go to NATO's eastern flank, and the United States will send some KC-135 refueling aircraft out of Fairchild Air Force Base in Spokane, Washington, with about 150 personnel.

Tuesday, March 8

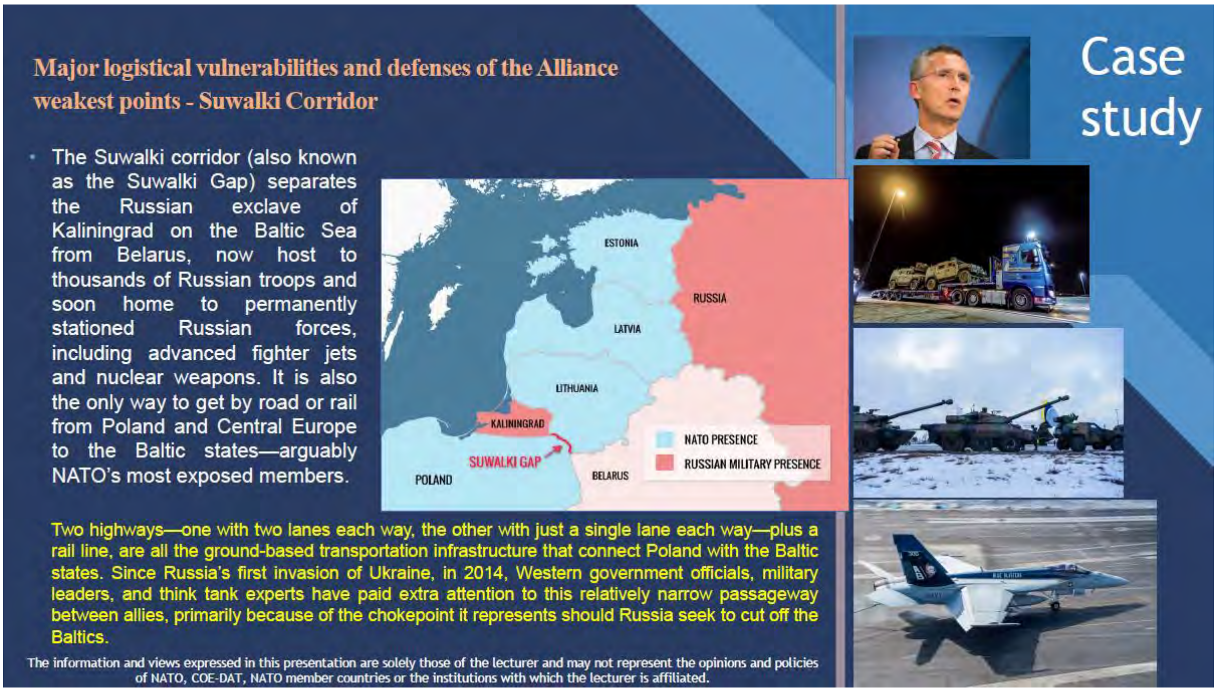
- during a visit to Ādaži Air Base the Spanish Prime Minister Pedro Sanchez announced that Spain would send another 175 soldiers to Latvia
- during a visit to Latvia, Canadian Prime Minister Justin Trudeau announced an additional 460 military personnel, along with further military assets to be deployed to Canadian Operation Reassurance in support of NATO in Central and Eastern Europe

five days timeframe - the increasing trend of logistical effort

Example of short-term actions using a variety of logistics

- The data includes actions carried out over the average period of one week at the beginning of March 2022.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



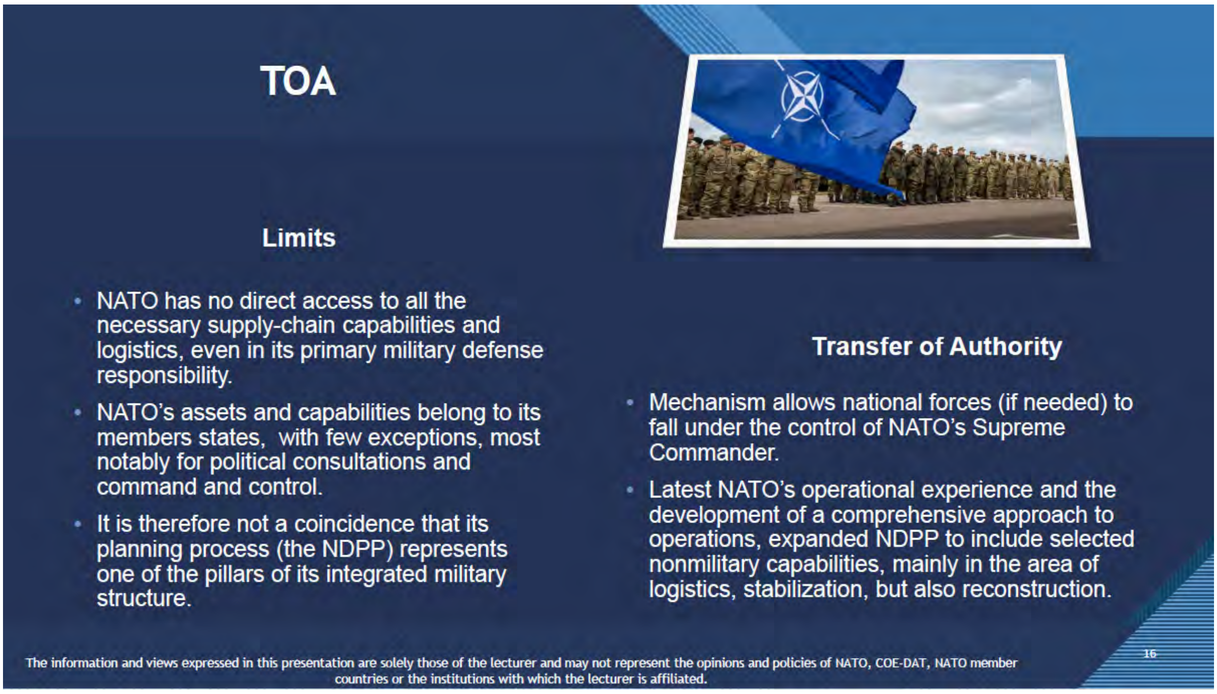
Case study

Major logistical vulnerabilities and defenses of the Alliance weakest points - Suwalki Corridor

- The Suwalki corridor (also known as the Suwalki Gap) separates the Russian exclave of Kaliningrad on the Baltic Sea from Belarus, now host to thousands of Russian troops and soon home to permanently stationed Russian forces, including advanced fighter jets and nuclear weapons. It is also the only way to get by road or rail from Poland and Central Europe to the Baltic states—arguably NATO's most exposed members.

Two highways—one with two lanes each way, the other with just a single lane each way—plus a rail line, are all the ground-based transportation infrastructure that connect Poland with the Baltic states. Since Russia's first invasion of Ukraine, in 2014, Western government officials, military leaders, and think tank experts have paid extra attention to this relatively narrow passageway between allies, primarily because of the chokepoint it represents should Russia seek to cut off the Baltics.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



TOA

Limits

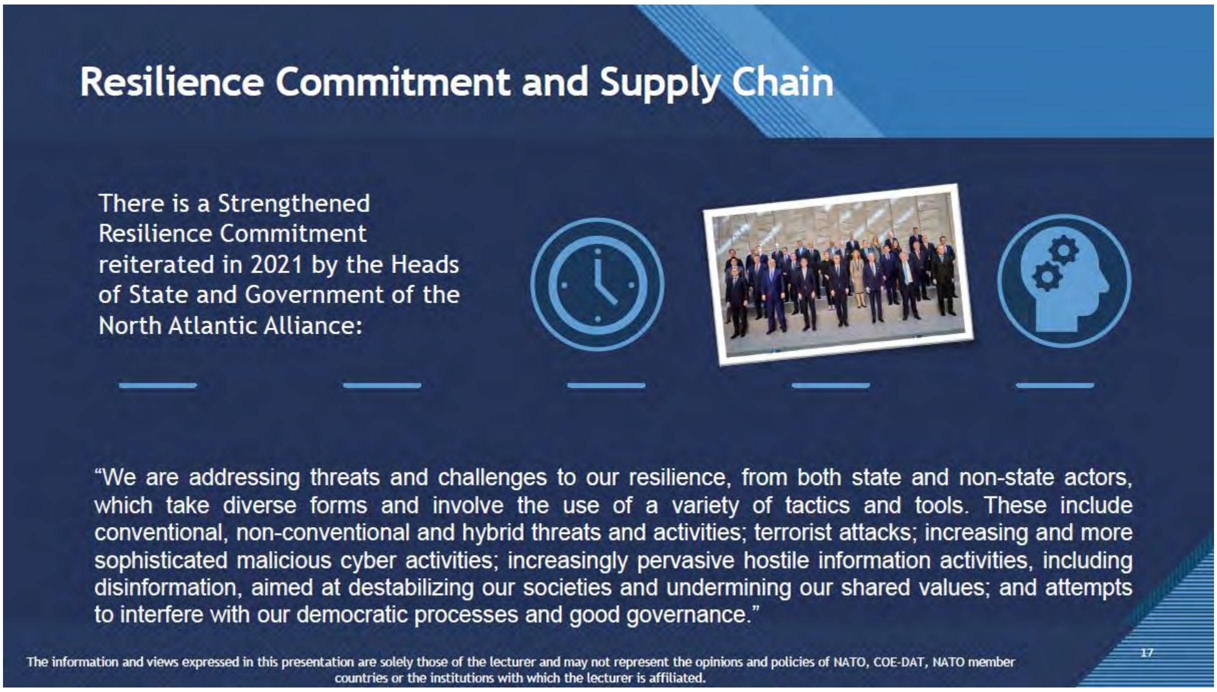
- NATO has no direct access to all the necessary supply-chain capabilities and logistics, even in its primary military defense responsibility.
- NATO's assets and capabilities belong to its members states, with few exceptions, most notably for political consultations and command and control.
- It is therefore not a coincidence that its planning process (the NDPP) represents one of the pillars of its integrated military structure.

Transfer of Authority

- Mechanism allows national forces (if needed) to fall under the control of NATO's Supreme Commander.
- Latest NATO's operational experience and the development of a comprehensive approach to operations, expanded NDPP to include selected nonmilitary capabilities, mainly in the area of logistics, stabilization, but also reconstruction.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

16



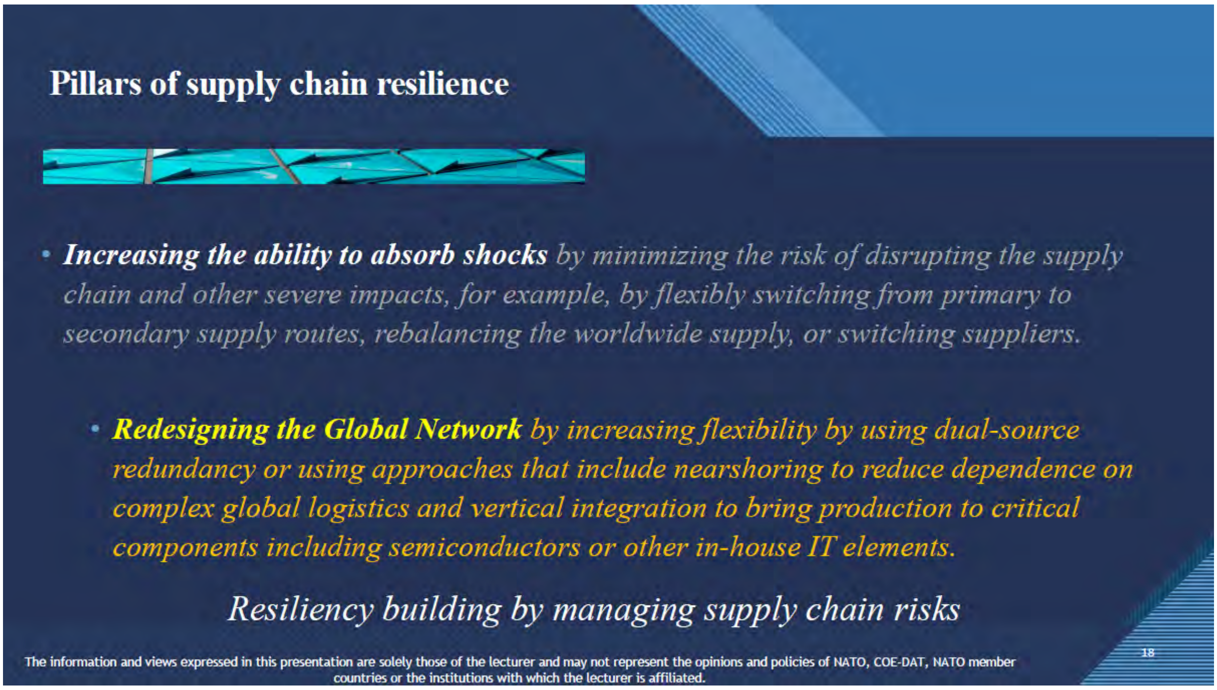
Resilience Commitment and Supply Chain

There is a Strengthened Resilience Commitment reiterated in 2021 by the Heads of State and Government of the North Atlantic Alliance:

"We are addressing threats and challenges to our resilience, from both state and non-state actors, which take diverse forms and involve the use of a variety of tactics and tools. These include conventional, non-conventional and hybrid threats and activities; terrorist attacks; increasing and more sophisticated malicious cyber activities; increasingly pervasive hostile information activities, including disinformation, aimed at destabilizing our societies and undermining our shared values; and attempts to interfere with our democratic processes and good governance."

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

17



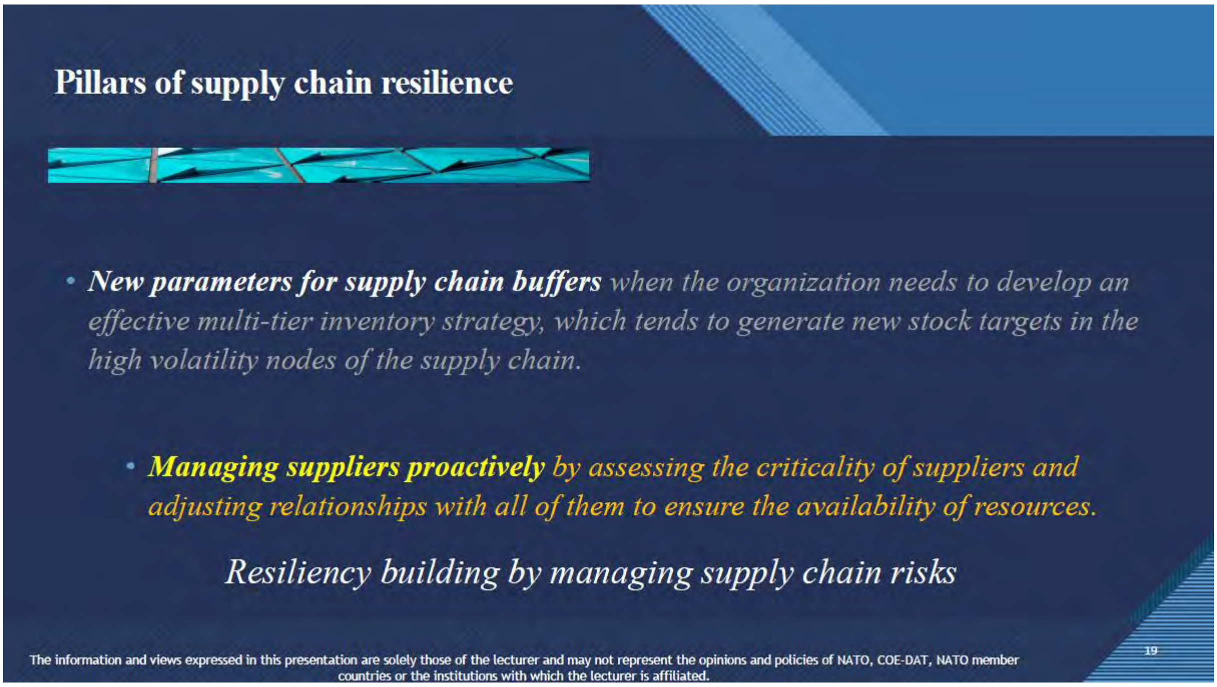
Pillars of supply chain resilience

- ***Increasing the ability to absorb shocks*** *by minimizing the risk of disrupting the supply chain and other severe impacts, for example, by flexibly switching from primary to secondary supply routes, rebalancing the worldwide supply, or switching suppliers.*
  - ***Redesigning the Global Network*** *by increasing flexibility by using dual-source redundancy or using approaches that include nearshoring to reduce dependence on complex global logistics and vertical integration to bring production to critical components including semiconductors or other in-house IT elements.*

Resiliency building by managing supply chain risks

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

18



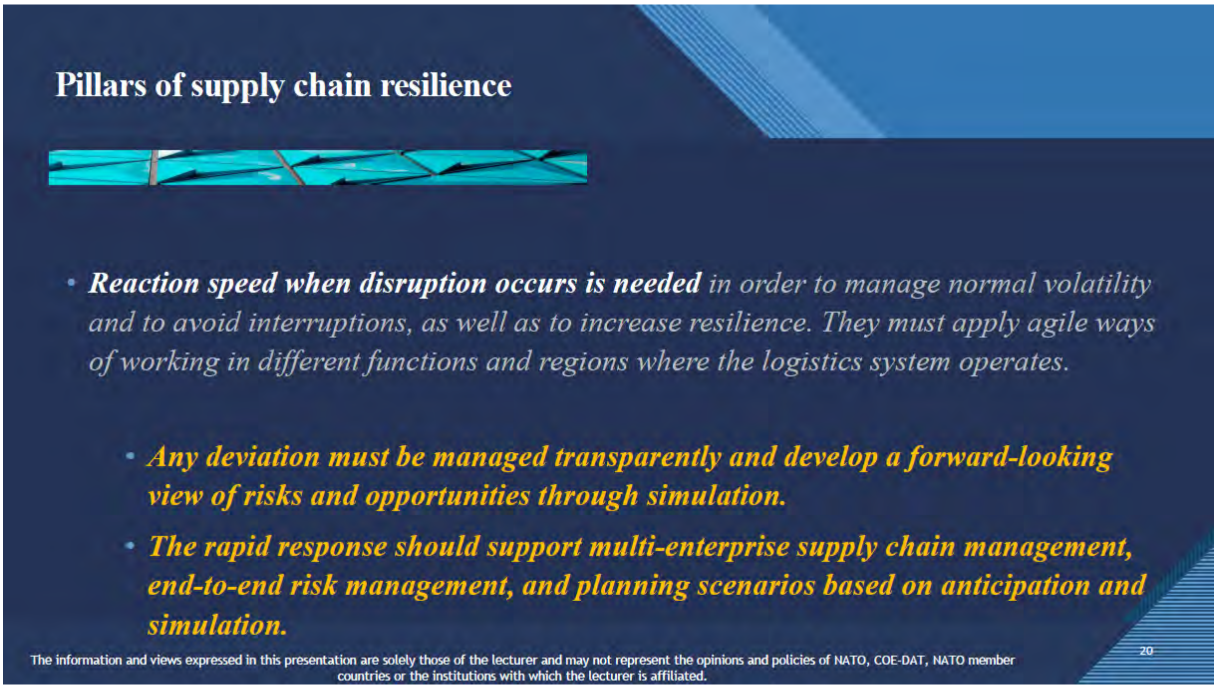
Pillars of supply chain resilience

- ***New parameters for supply chain buffers*** *when the organization needs to develop an effective multi-tier inventory strategy, which tends to generate new stock targets in the high volatility nodes of the supply chain.*
  - ***Managing suppliers proactively*** *by assessing the criticality of suppliers and adjusting relationships with all of them to ensure the availability of resources.*

Resiliency building by managing supply chain risks

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

19

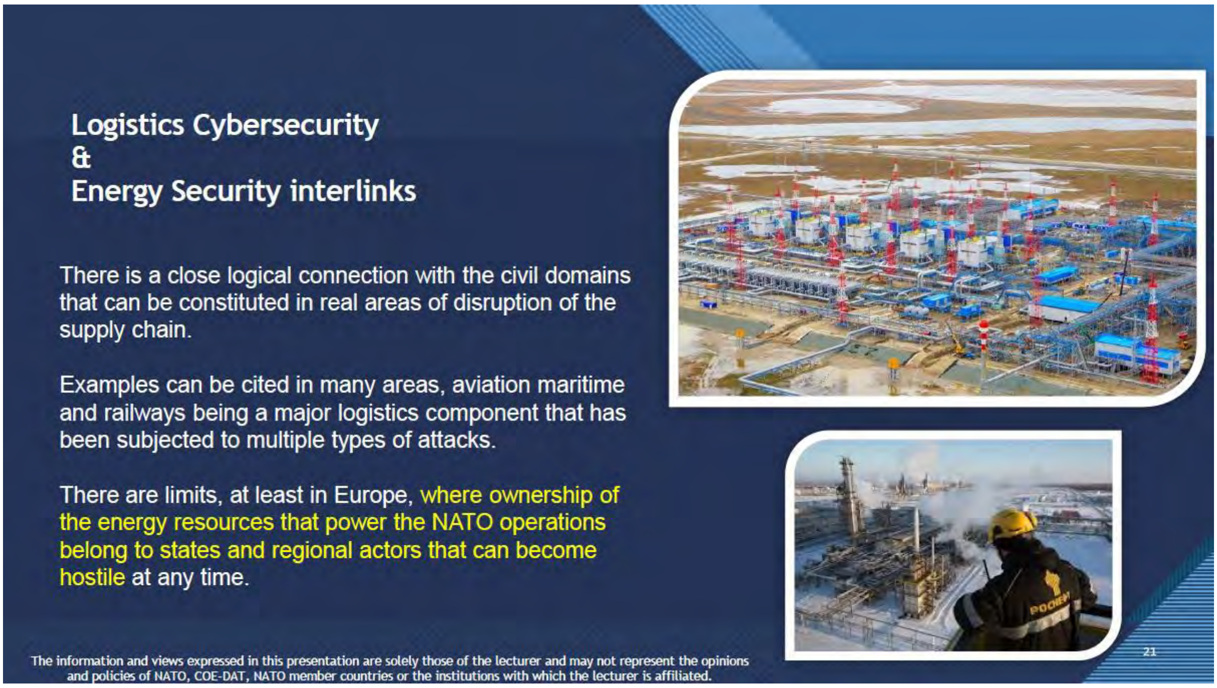


Pillars of supply chain resilience

- ***Reaction speed when disruption occurs is needed*** *in order to manage normal volatility and to avoid interruptions, as well as to increase resilience. They must apply agile ways of working in different functions and regions where the logistics system operates.*
  - ***Any deviation must be managed transparently and develop a forward-looking view of risks and opportunities through simulation.***
  - ***The rapid response should support multi-enterprise supply chain management, end-to-end risk management, and planning scenarios based on anticipation and simulation.***

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

20



Logistics Cybersecurity & Energy Security interlinks

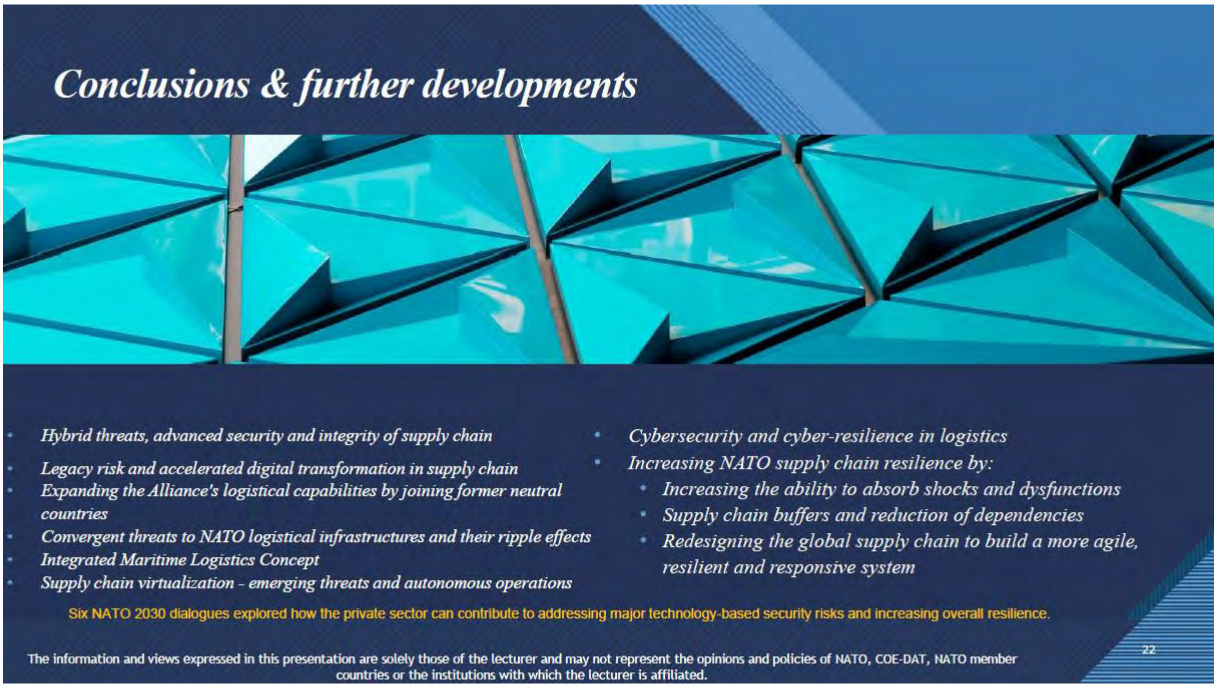
There is a close logical connection with the civil domains that can be constituted in real areas of disruption of the supply chain.

Examples can be cited in many areas, aviation maritime and railways being a major logistics component that has been subjected to multiple types of attacks.

There are limits, at least in Europe, where ownership of the energy resources that power the NATO operations belong to states and regional actors that can become hostile at any time.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

21



Conclusions & further developments

- *Hybrid threats, advanced security and integrity of supply chain*
- *Legacy risk and accelerated digital transformation in supply chain*
- *Expanding the Alliance's logistical capabilities by joining former neutral countries*
- *Convergent threats to NATO logistical infrastructures and their ripple effects*
- *Integrated Maritime Logistics Concept*
- *Supply chain virtualization - emerging threats and autonomous operations*
- *Cybersecurity and cyber-resilience in logistics*
- *Increasing NATO supply chain resilience by:*
  - *Increasing the ability to absorb shocks and dysfunctions*
  - *Supply chain buffers and reduction of dependencies*
  - *Redesigning the global supply chain to build a more agile, resilient and responsive system*

Six NATO 2030 dialogues explored how the private sector can contribute to addressing major technology-based security risks and increasing overall resilience.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

22

Logistics and Supply Chain Resilience

Terrorist Threats to Supply Chain and Logistical Resilience

Thank You!

DR. GABRIEL RAICU

NATO CENTER OF EXCELLENCE IN THE DEFENSE AGAINST TERRORISM

ANKARA, OCTOBER 18, 2022

SESSION 3: CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE BOOK 2

Emerging and Disruptive Technologies

Dr. Sarah LOHMANN

"Future conflicts will be fought not just with bullets and bombs, but also with bytes and big data. We see authoritarian regimes racing to develop new technologies, from artificial intelligence to autonomous systems. So we are taking further steps to future-proof the alliance."

NATO Secretary-General Jens Stoltenberg, Oct. 20, 2021

NATO's defense methods are being drastically changed by the emerging technologies used to threaten its member states and allies across the globe. For the first time, **hypersonics** has been used as a weapon of war on the battlefield in Ukraine. Drones have given a once-small terrorist resistance force in Yemen fire power, and the Taliban have harnessed big data intended for counterterrorism purposes to carry out their own terror. At the same time, critical infrastructure connected to emerging technology is creating new vulnerabilities and national security concerns.

NATO's **Science for Peace and Security Program** defines emerging and disruptive technologies (EDTs) as "*technologies that undergo rapid development and can be disruptive to existing systems such as critical infrastructure, supply chains, data networks*". NATO has identified seven key areas for cooperation on innovation and defense within the Alliance as it pertains to EDTs: **Artificial intelligence, data and computing, autonomous weapons, quantum-enabled technologies, biotechnology and human enhancements, hypersonic technologies, and space.**

In this seminar, three of those technologies are examined, as well as how they are being used to counter terrorism: autonomous weapons such as drones, technologies using big data, and hypersonic weapons. Likewise, each technology is analyzed for how it has been used by terrorists or state actors to threaten security and leave critical infrastructure vulnerable.

NATO defines "**autonomy**" as: "*A system's ability to function, within parameters established by programming and without outside intervention, in accordance with desired* *goals, based on acquired knowledge and an evolving situational awareness*."[2] An unmanned aerial vehicle (UAV) is often referred to as a drone and is an aircraft without a pilot or human life onboard.[3]

While international law prevents the use of fully autonomous drones, NATO's Science and Technology Organization (STO) predicts that "*semi-autonomous systems will have more impact on operations*" for the Alliance in the near term.[4] There, the warfighter remains the final decision maker, while Artificial Intelligence and other emerging technologies allow the drone to respond to numbers of adversaries or new obstacles autonomously, while seeking out preprogrammed targets.

The danger that is posed by drones used by terrorists, nation-states, and non-state actors is assessed in the seminar, as are current counter-UAV efforts within NATO nations. How drones are changing the battlefield is analyzed in case studies such as the Houthi's attack on the United Arab Emirates' critical infrastructure in 2022 and NATO partner Azerbaijan's use of drones in the Nagorno-Karabakh war in 2020. There are also examples mentioned of how drones are being used, and tracked, in the Ukraine conflict.

Real time big data analytics presents big data technology's value in counterterrorism missions. Here, there is also discussion of how the Taliban captured US biometric devices, and ways to secure the technology so that it cannot be used if it falls into the hands of bad actors.

Finally, the hypersonics analysis examines NATO's changing posture as it faces gains made by China, Russia, and North Korea, and how it is harnessing hypersonic technology for deterrence in this adversarial environment.

The NATO Context

In December of 2019, NATO leaders agreed on an **Emerging and Disruptive Technology Implementation Roadmap**, which helped the Alliance to coordinate its work around emerging

[2] North Atlantic Treaty Organization NATO Standardization Office, NATO Glossary of Terms and Definitions, AAP-06, Edition 2019.

[3] Hu, J., Lanzon, A. (2018). "An innovative trirotor drone and associated distributed aerial drone swarm control". Robotics and Autonomous Systems. 103: 162-174. Doi:10.1016/j.robot2018.02.019. See also: US Army, UAS Center of Excellence, US Army Roadmap for UAS 2010-2035, Alabama, 2010.

[4] NATO Science and Technology Organization, NATO Science and Technology Trends 2020-2040, Exploring the S&T Edge, 2020.

technology in the areas of defense, deterrence, and capabilities. Emerging technologies were having an increasing impact on NATO's task of defending its member states, while also creating new challenges from adversaries. By July of 2020, NATO Secretary General Jens Stoltenberg had created an Advisory Group on Emerging and Disruptive Technologies, made up of a dozen private sector and academic experts, who provide NATO with advice on the adoption of EDT in its mission. By September of 2020, these experts had provided NATO with recommendations for technologies on which to focus, and by March 2021, their first annual report.

In February 2021, Defense Ministers endorsed a strategy focusing on military and civilian dual-use technology that can improve NATO's defense advantage, while also creating a forum for best practices. These goals were made tangible through the creation of a NATO Innovation Fund at the 2021 Brussels Summit in June to support the development of and guidance on such technology.

Real-time data analytics and autonomous weapons have a history of dual use. This can create both greater competition for the creation of quality defense products, and greater risk when the technology is available to adversaries of democratic states. As the example of the capture of biometric devices in Afghanistan shows, technology used by the military must be hardened to ensure dual-use technology vital to mission does not become compromised.

Thus, this seminar explores how member states future-proof the way they develop emerging technology used for NATO missions. As critical national infrastructure is shaped or challenged by innovators or malicious actors using emerging technology, NATO is repositioning itself to create a **coordinated response**. The analysis in this seminar documents that journey and identifies areas under development.

Recommendations

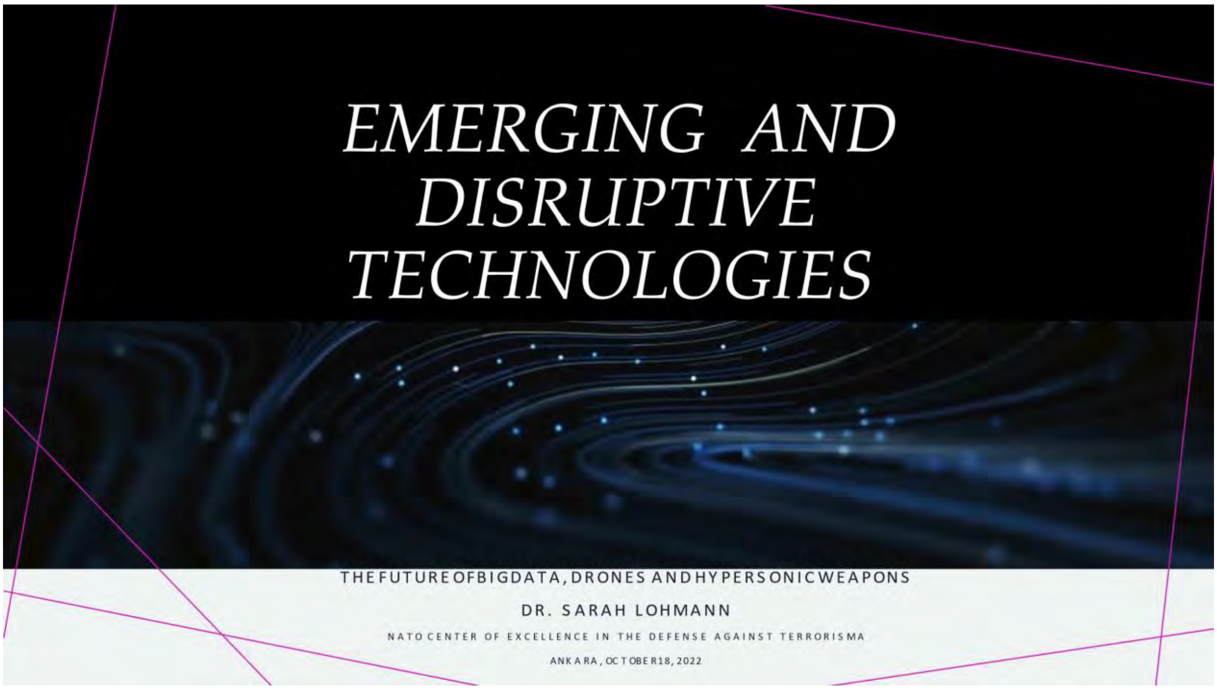
As NATO looks ahead to preparing for the emerging technology challenges to critical infrastructure resilience for the next two decades, its member states must be prepared to counter EDTs on two fronts. While traditional adversaries are making strides in their development, terrorists are also gaining ground in using EDTs in peer-to-peer conflicts.

NATO has made initial strides in expanding its innovation and joint defense in this rapidly changing environment, there is much room for improvement. In the area of autonomous weapons, countermeasures and innovation are already being developed in a coordinated way. Exercises, a whole of government approach and interoperability strategies are being incorporated across the Alliance to both operations and technology to hold terrorists and rogue actors at bay. As NATO nations continue to work together to develop and improve the performance of both autonomous weapons and counter-UAV technology for the battlefield, they will be able to better protect critical infrastructure and national security of member states.

The collection of big data and the process that makes it useful – big data analytics – is changing NATO's preparedness and the way it protects critical infrastructure. Analytics helps to target terrorists and receive early warning of armed conflict, transportation or communication vulnerabilities, nuclear threats or pandemics more accurately. NATO is just in the nascent stages of fully harnessing the advantages of using this data and exploring how to share it with nation states within the Alliance in a secure way that does not harm national security on the one hand, or civil liberties on the other. While proposals exist for doing this more effectively, creating common standards across the Alliance for secure storage, jurisdiction, access and cybersecurity will remain an important strategic task for nation states in the future. In addition, NATO nation states should continue to develop and invest in early warning systems using big data analytics and machine learning to receive foresight on where and when terrorists and malicious actors could escalate armed violence or threaten critical infrastructure.

Finally, as NATO considers its new posture in the hypersonic arms race, it will need to make a strategic decision about the most effective deterrence methods. This will include whether its nation states should invest in offensive or defensive weapons, and how to best counter adversary's new hypersonic technology. A coordinated approach among nuclear powers and using civil-military cooperation on hypersonic development and countermeasures will ensure NATO can defend its nation states in a way that maximizes innovation while considering escalation impacts.

Presentation



EMERGING AND DISRUPTIVE TECHNOLOGIES

THE FUTURE OF BIG DATA, DRONES AND HYPERSONIC WEAPONS

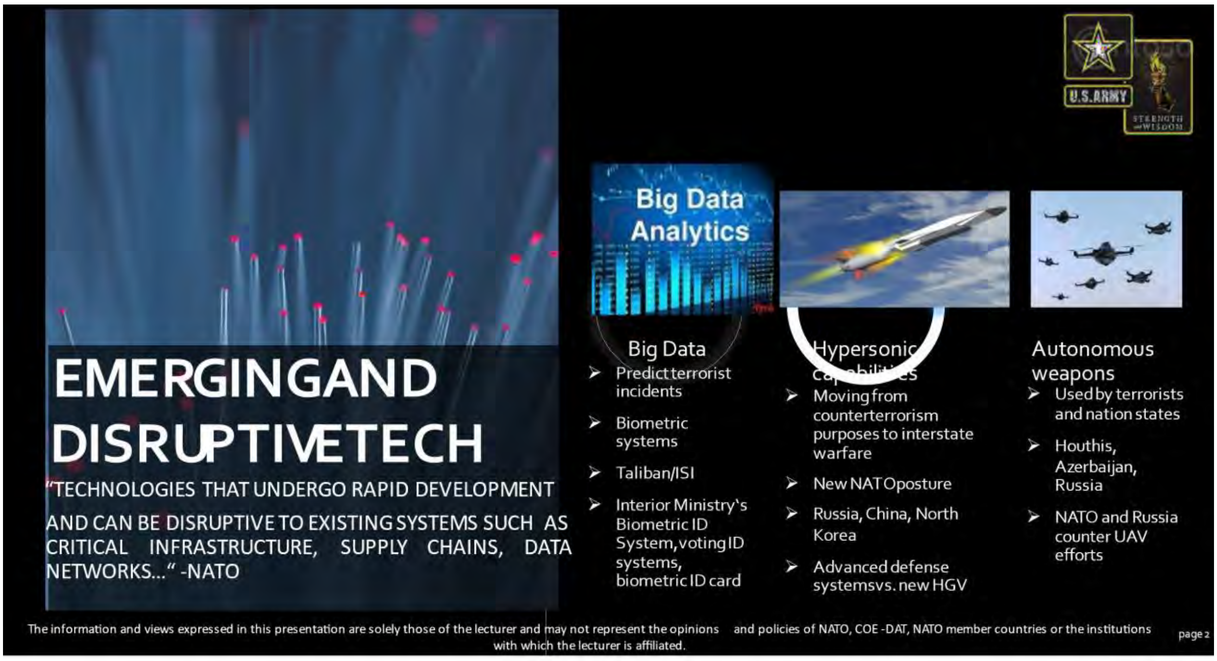
DR. SARAH LOHMANN

NATO CENTER OF EXCELLENCE IN THE DEFENSE AGAINST TERRORISMA

ANKARA, OCTOBER 18, 2022

DISCLAIMER

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



EMERGINGAND DISRUPTIVETECH

"TECHNOLOGIES THAT UNDERGO RAPID DEVELOPMENT AND CAN BE DISRUPTIVE TO EXISTING SYSTEMS SUCH AS CRITICAL INFRASTRUCTURE, SUPPLY CHAINS, DATA NETWORKS…" -NATO

Big Data
Analytics
U.S.ARMY

Big Data

- Predictterrorist incidents
- Biometric systems
- Taliban/ISI
- Interior Ministry's Biometric ID System,votingID systems, biometricID card

Hypersonic capabilities

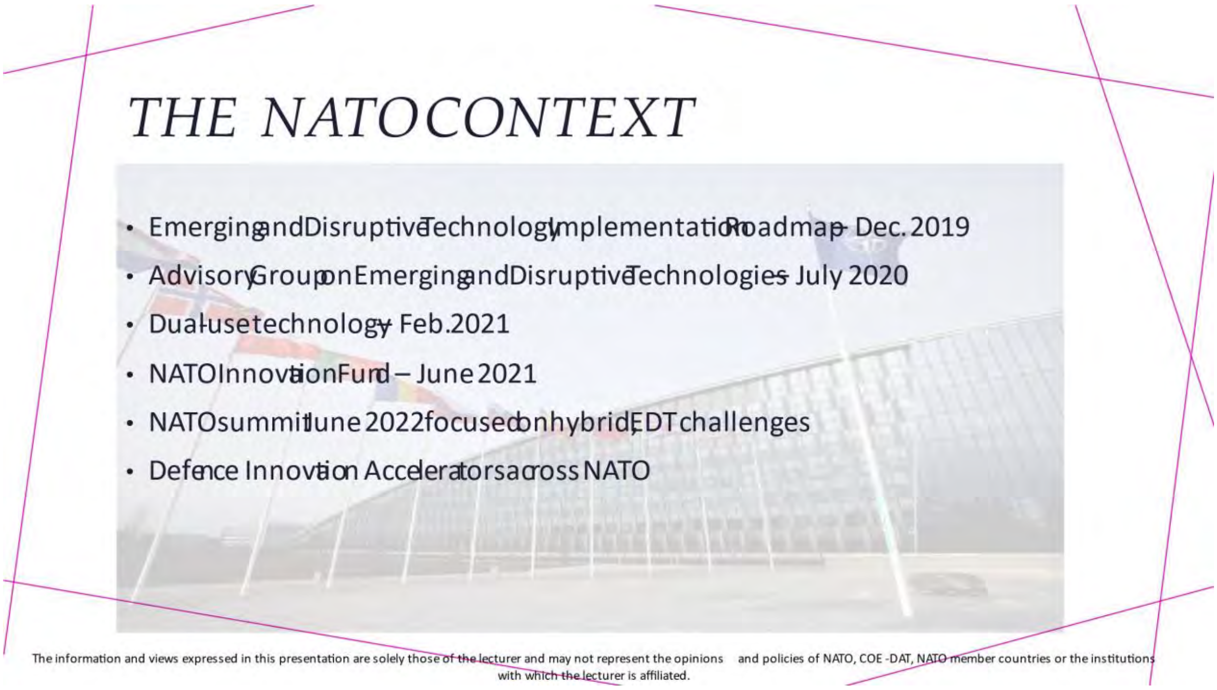
- Moving from counterterrorism purposes to interstate warfare
- New NATOposture
- Russia, China, North Korea
- Advanced defense systemsvs. new HGV

Autonomous weapons

- Usedby terrorists and nation states
- Houthis, Azerbaijan, Russia
- NATO and Russia counter UAV efforts

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

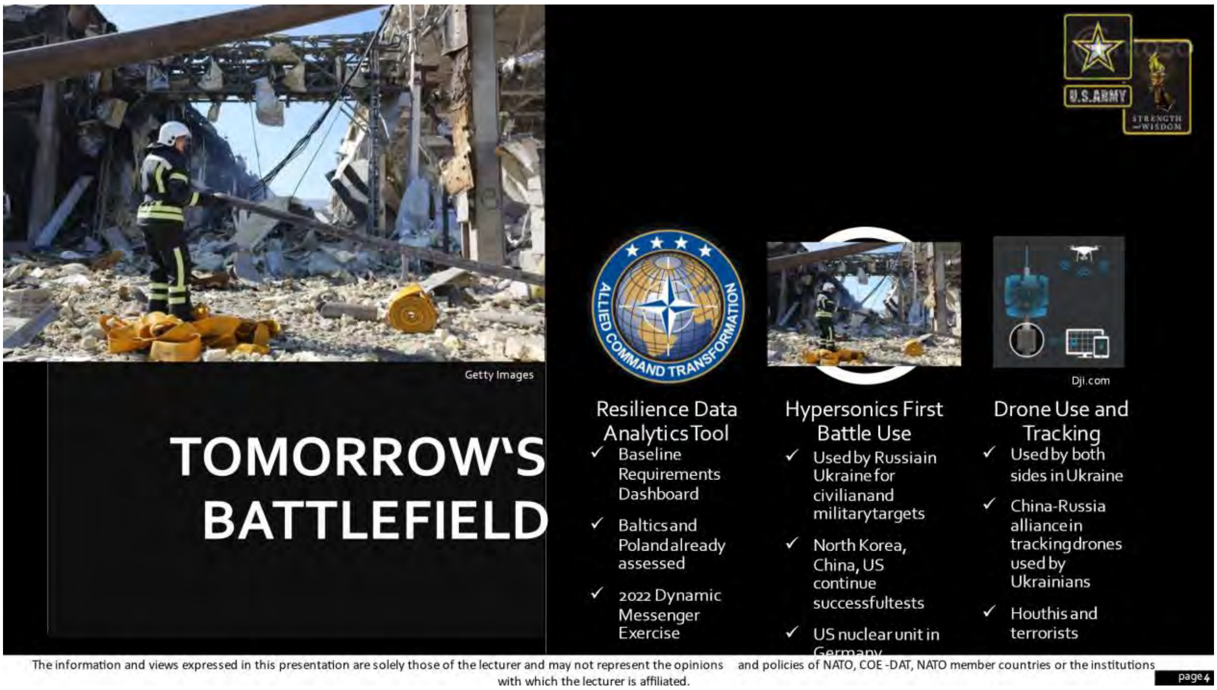
page 2



THE NATOCONTEXT

- EmergingandDisruptiveTechnologyImplementationRoadmap- Dec.2019
- AdvisoryGrouponEmergingandDisruptiveTechnologies- July 2020
- Dual-usetechnology- Feb.2021
- NATOInnovationFund – June2021
- NATOsummitJune 2022focusedonhybridEDTchallenges
- Defence Innovation AcceleratorsacrossNATO

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Getty Images

TOMORROW'S BATTLEFIELD

Dji.com

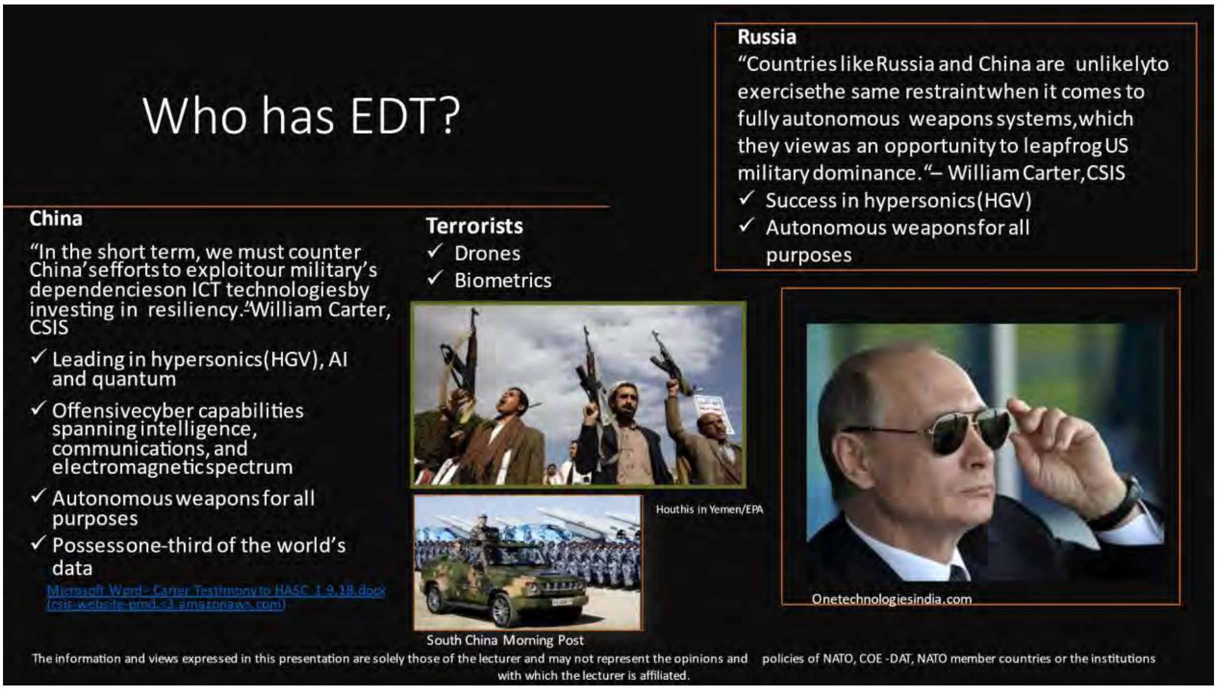
Resilience Data Analytics Tool
- ✓ Baseline Requirements Dashboard
- ✓ Baltics and Poland already assessed
- ✓ 2022 Dynamic Messenger Exercise

Hypersonics First Battle Use
- ✓ Used by Russian Ukraine for civilian and military targets
- ✓ North Korea, China, US continue successful tests
- ✓ US nuclear unit in Germany

Drone Use and Tracking
- ✓ Used by both sides in Ukraine
- ✓ China-Russia alliance in tracking drones used by Ukrainians
- ✓ Houthis and terrorists

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

page 4



Who has EDT?

China

"In the short term, we must counter China's efforts to exploit our military's dependencies on ICT technologies by investing in resiliency."William Carter, CSIS

- ✓ Leading in hypersonics(HGV), AI and quantum
- ✓ Offensive cyber capabilities spanning intelligence, communications, and electromagnetic spectrum
- ✓ Autonomous weapons for all purposes
- ✓ Possess one-third of the world's data

Microsoft Word - Carter Testimony to HASC 1.9.18.docx (csis-website-prod.s3.amazonaws.com)

Terrorists
- ✓ Drones
- ✓ Biometrics

Houthis in Yemen/EPA

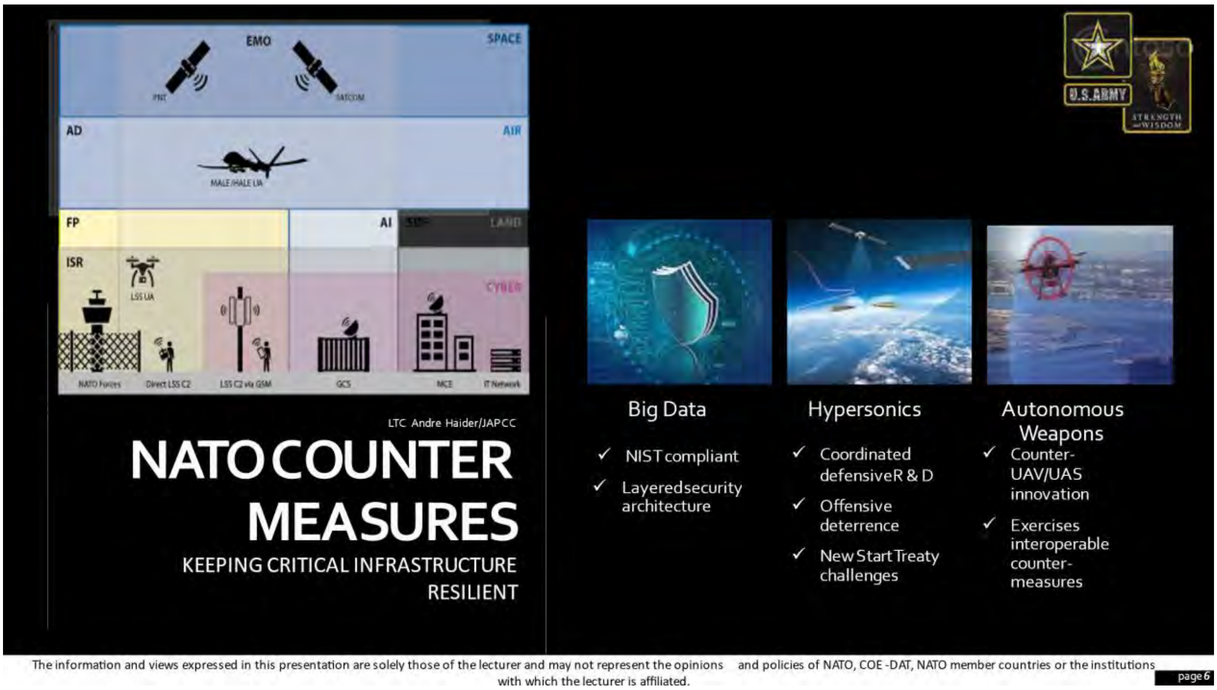
South China Morning Post

Russia

"Countries like Russia and China are unlikely to exercise the same restraint when it comes to fully autonomous weapons systems, which they view as an opportunity to leapfrog US military dominance."– William Carter, CSIS
- ✓ Success in hypersonics(HGV)
- ✓ Autonomous weapons for all purposes

Onetechnologiesindia.com

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.


EMO
SPACE
PNT
SATCOM
AD
AIR
MALE/HALE UA
FP
AI
SDP
LAND
ISR
LSS UA
CYBER
NATO Forces
Direct LSS C2
LSS C2 via GSM
GCS
MCE
IT Network
U.S.ARMY
STRENGTH and WISDOM

LTC Andre Haider/JAPCC

NATO COUNTER MEASURES

KEEPING CRITICAL INFRASTRUCTURE RESILIENT

Big Data

- ✓ NIST compliant
- ✓ Layeredsecurity architecture

Hypersonics

- ✓ Coordinated defensiveR & D
- ✓ Offensive deterrence
- ✓ New Start Treaty challenges

Autonomous Weapons

- ✓ Counter-UAV/UAS innovation
- ✓ Exercises interoperable counter-measures

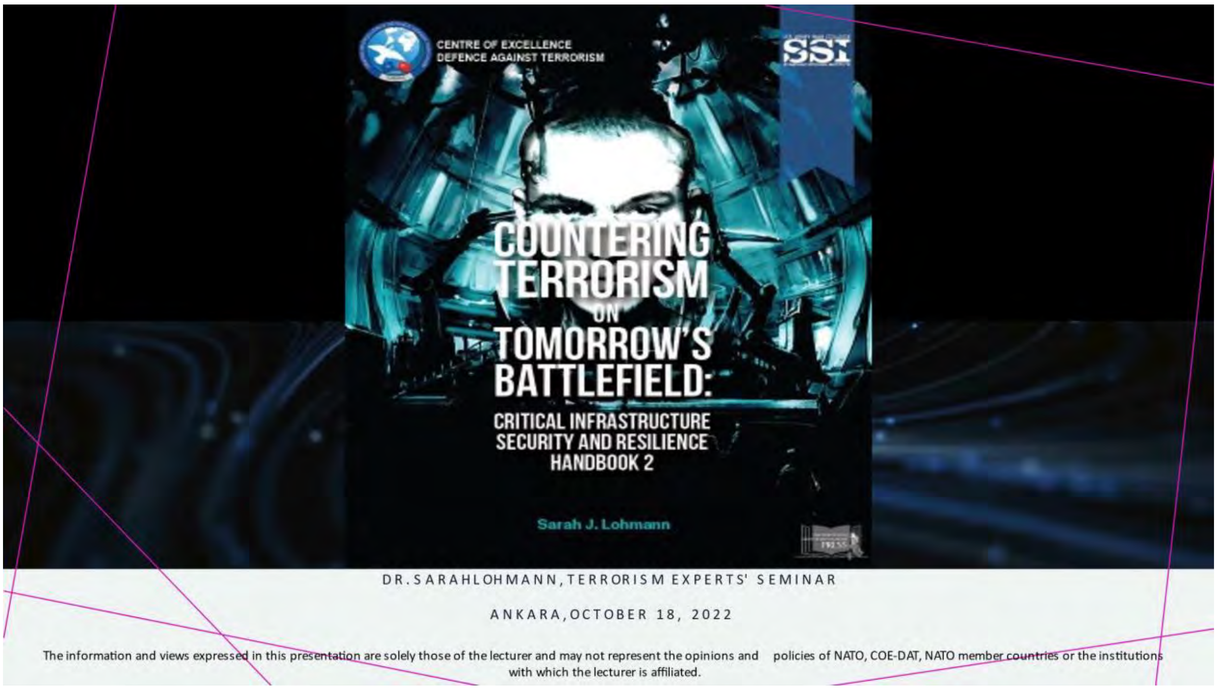
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

PREPARING FOR EDT THREATS

- ✓ Big dataanalytics:Use of nationaldatabases,big datasourcesforcounterterrorism,early warning purposes across NATO
- ✓ Hypersonics:NATO'spostureas offensive/defensive.Coordinationbetweennuclearpowersand civil-militarycooperationonhypersonicdevelopmentandcountermeasures
- ✓ Autonomousweapons:Exercises,a wholeof governmentapproachandinteroperability strategies.Awarenessof alliancesin counter-UAV strategies

A CONTINUOUS PROCESS

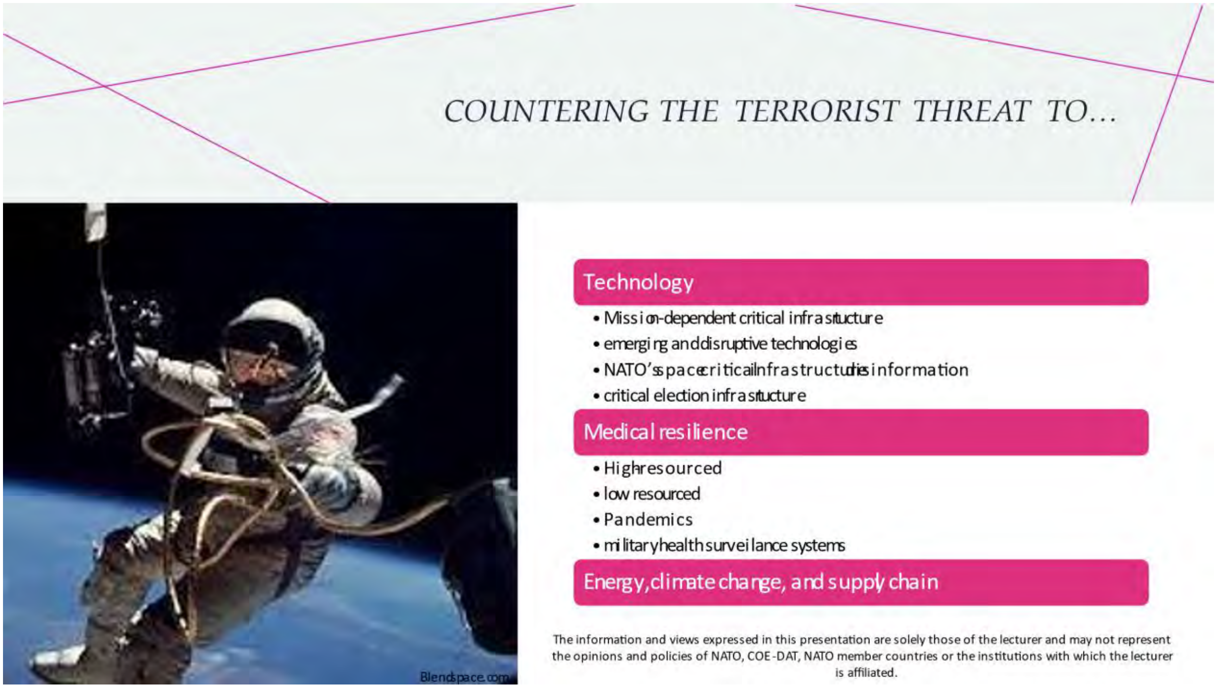
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.


CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM
SSI
COUNTERING TERRORISM ON TOMORROW'S BATTLEFIELD:
CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE HANDBOOK 2
Sarah J. Lohmann
PRESS

DR. SARAH LOHMANN, TERRORISM EXPERTS' SEMINAR

ANKARA, OCTOBER 18, 2022

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



COUNTERING THE TERRORIST THREAT TO…

Technology

- Mission-dependent critical infrastructure
- emerging and disruptive technologies
- NATO's space critical infrastructure is information
- critical election infrastructure

Medical resilience

- High resourced
- low resourced
- Pandemics
- military health surveillance systems

Energy, climate change, and supply chain

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Blendspace.com

Election Infrastructure as Critical Infrastructure

Ms. Denise FELDNER

Democratic resilience and election integrity are foundational to NATO's future success as a military alliance. The Alliance – a military and political alliance – underlined in the new 2022 Strategic Concept the members intend to reinforce political unity and deepen consultations to address all matters that affect security—including democratic resilience.

With election infrastructures being the backbone of liberal democracies, they are critical to NATOs futures successes—with all due respect to national sovereignty. And they stand at the epicenter of NATO adversaries' activities against the Alliance's stability. One weak democracy in NATO can weaken the Alliance. NATO's active role as a political alliance in creating defense and democratic resilience against disruptions to critical societal functions such as elections and cohesion is therefore central to a prosperous future of liberal democracies and the unity of member states.

In the last years the discussions within and among member states centered around:

1. Competition among states of "great power" as a reason for election interferences;
2. Election integrity and critical election infrastructures being weaponized to fight liberal democracies;
3. Specific and new types of adversaries.

Why elections are critical to the success of the Alliance

People's trust that their votes will be counted, that they will be counted correctly, and that they will not be manipulated is a critical pillar of democratic stability in a democracy as it is defined today. The trust of the people in institutions, be they infrastructures, processes, or political organizations is of utmost importance to the stability of NATO as a military and political alliance.

The US solution for safeguarding critical election infrastructures

Based on the experience of election interferences, the United States of America introduced a new type of critical infrastructure in 2017. Today, election infrastructures are referred to as critical infrastructures, which means that more money and attention is available to support them and ensure they are functioning properly.

The question that arises and should be discussed is whether other NATO members or allies should apply a definition of critical election infrastructures in their countries and take care of these infrastructures as threatened infrastructures. The topic is difficult to address within NATO because of the national responsibility for critical infrastructure.

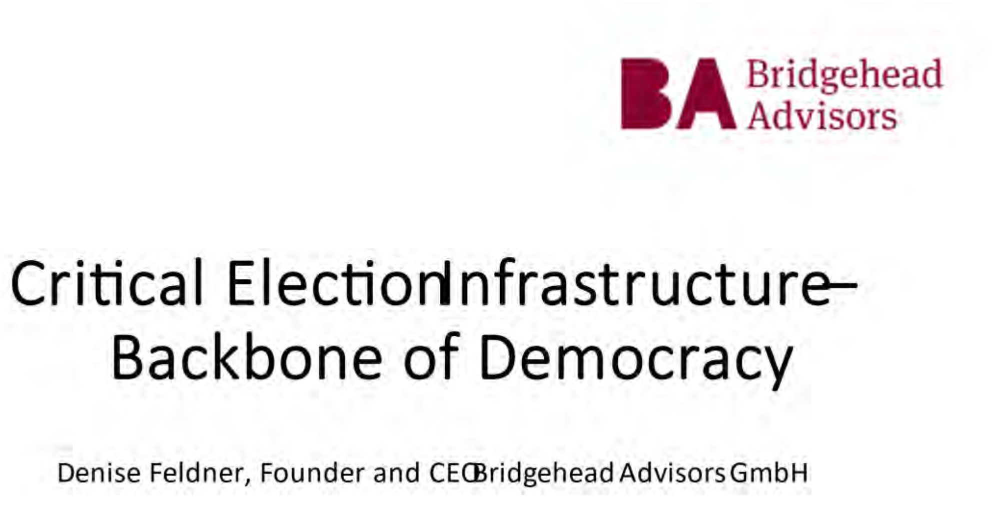
Possible reactions within NATO / among NATO member states

However, some actions and possible institutions under the Alliance umbrella could be tasked with this topic and help finding a common sense among member states to implement Article 2 of the NATO Treaty.

For example:

- Forming a Democratic Resilience Center as proposed by the president of NATO Parliamentary Assembly and member states of NATO PA.
- Creating a new thematic framework nation concept (FNC) focusing on election security and enabling multinational cooperation among member states. It could be based on the work of existing NATO COE's: NATO COE DAT in Ankara, Türkiye, NATO CCD COE in Tallinn, Estonia, and NATO StratCom COE in Riga, Latvia.
- Drafting and discussing guidelines that can be followed but must not be followed by members states.

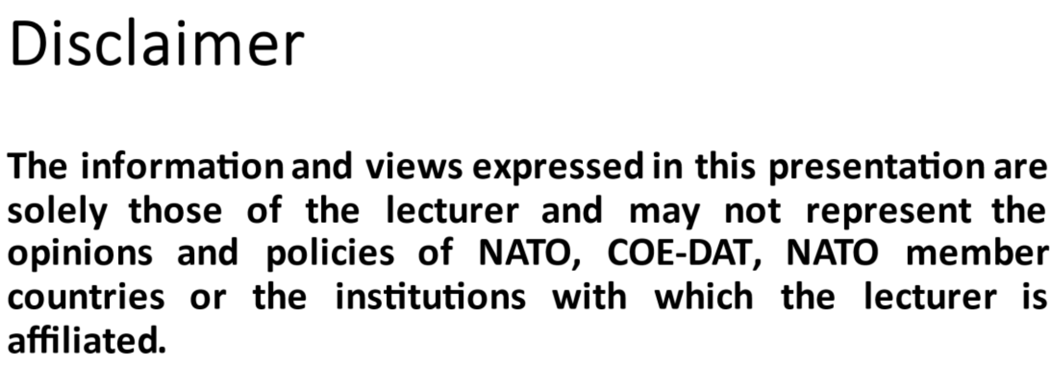
Presentation



BA Bridgehead Advisors

Critical Election Infrastructure – Backbone of Democracy

Denise Feldner, Founder and CEO Bridgehead Advisors GmbH



Disclaimer

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Elections: „Backbone of Democracies“

- Democracy is inconceivable without free elections. They are an important form of democratic control for individual citizens of a democracy:
- **In elections, the people transfer the power to rule to their representatives for a defined period of time.**
- The people’s trust in their votes to be counted, to be counted correctly, and not to be manipulated is a critical pillar of democratic stability.
- The trust of the people in institutions, be they infrastructures, processes, or political organizations is of utmost importance to the stability of NATO as an alliance.

The information and views expressed in thispresentation are solelythose of the lecturer and maynot represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which the lecturer is affiliated.

Elections: „Backbone of Democracies“

© Yasuyoshi Chiba/AFP

- It is now commonplace that every election in any developing country is a defining moment for state-building or a potential source of conflict – and for countries coming out of civil war, the stakes are even higher.
- Therefore, systems and structures must be operationalized as a catalyst to prevent or avert political violence in times of elections.

The information and views expressed in thispresentationare solelythose of thelecturer and maynot represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which the lecturer is affiliated.

Criticalelectioninfrastructures: „Backbone of secureelections“

- Definition of critical election infrastructurein the United States

✓ Based on experiences with election interferences starting between 2014 and 2016 and continuing further

- Other rising threats with impact on security of critical election infrastructure

✓ New technologies
✓ Influence industry
✓ Uncertain and destabilized situations and area referenda

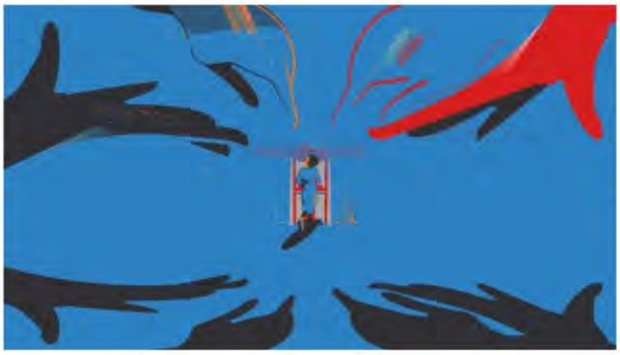
The information and views expressed in thispresentation are solelythose of the lecturer and maynot represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

US definitionof criticalelectioninfrastructure

- Voter registration databases and associated IT-systems
- IT infrastructure and systems used to manage elections (such as the counting, auditing, and displaying of election results, and post election reporting to certify and validate results)
- Voting systems and associated infrastructure
- Storage facilities for election and voting system infrastructure
- Polling places, to include early voting locations

The information and views expressed in thispresentation are solelythose of the lecturer and maynot represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

WhyshouldNATO care?



- NATO is an outcomeof political cohesion and a source of it, but:
- The alliance is threatened internally
- External threats in third countries / developing and young democracies
- Relevant because every election in any (developing) country is now a defining moment for rising conflicts in established democracies, state-building or a potential source of new conflict(s).

The information and views expressed in thispresentation are solelythose of the lecturer and maynot represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Internalthreats

- Threat actors

✓ Actors using religiousidentity to fuel the rise of illiberal,nationalist or populist democracies

✓ Left-wing and right-wing terrorism

✓ Ethno nationalism

- Adversariesusing differentmethods to weaponize election infrastructures:

✓ Cyber attacks and other forms of sabotage

✓ Surveillance,scanning for vulnerabilitiesand exploitations

✓ Targeting measures related to an election, e.g. the will to vote

✓ Foreign and direct investmentsin critical infrastructures (e.g. telecommunication systems)

The information and views expressed in thispresentation are solelythose of the lecturer and maynot represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Terroristsexploitingpowervoids

- Power voids enable smaller groups / terroriststo step in powerful positions in a society
- Deliver their messages
- Destabilize a stable society
- Hand over power from one group / party to another
- Disrupt a society and cause a system change
- Anything from destabilization until chaos is possible depending on the specific circumstances where such activities are taking place

The information and views expressed in thispresentationare solely those of the lecturer and may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which the lecturer is affiliated.

Holisticapproachto electionsecurity

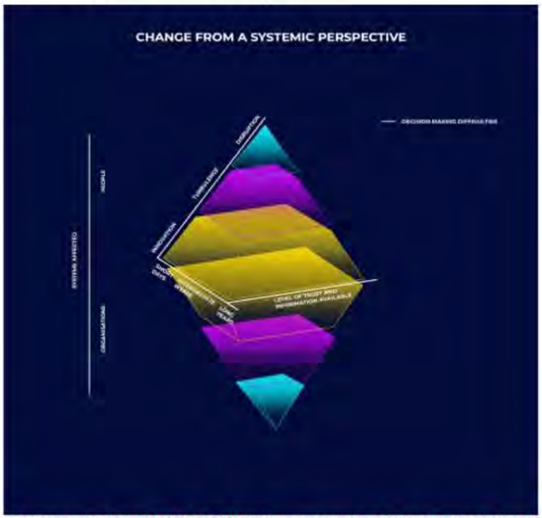
✓ Regarding time and technological developments

✓ Regarding involved actors and affected groups and people

✓ Regarding involved institutions, e. g. states as well as non-state actors

1. Elections and election processes are interrelated
(a) physical as well as
(b) social processes and systems considered to be vital to the running of a democratic country.

2. Threats are rising, and elections became more important in the competition between political philosophies.


CHANGE FROM A SYSTEMIC PERSPECTIVE
DECISION MAKING DIFFICULTIES
SYSTEMS AFFECTED
PEOPLE
ORGANISATIONS
DISRUPTION
TURBULENCE
INNOVATION
SHORT DAYS
WEEKS
LONG YEARS
LEVEL OF TRUST AND INFORMATION AVAILABLE

The information and views expressed in thispresentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which the lecturer is affiliated.

Risingthreats

- Metaverse and the Internet of Behaviors
- AI
- Influence industry, data-analytics
- Competing political philosophies
- In war-situations

The information and views expressed in thispresentationare solely those of the lecturer and may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which the lecturer is affiliated.

Recommendationsand Solutions

- Critical election infrastructuredefinition to be applied across NATO members
- Facing and reacting actively to threats and the competition between different political systemsand philosophies
- Recognizing the Metaverseas a rising threat
- Using measures in NATOto strenghten elections (e.g. creating a framwork, Democratic Resilience Center,resilience objectives)
- Using cutting-edge technologies to secure elections, e.g. precise real-time location tracking of movable election infrastructures

The information and views expressed in thispresentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COEDAT, NATO member countries or the institutions with which the lecturer is affiliated.

BA Bridgehead Advisors

Ass. jur. Denise Feldner, M. B. L.

feldner@bridgeheadadvisors.com

DAY I

SESSION 3: Questions and Answers

Questions to Dr. Gabriel RAICU

1. *The private sector is fully involved in the supply chain even in the defense supply chain. Do you believe NATO should affirm or ask for basic rules for the defense industry from private sector in order to be resilient when they're under cyber-attack?*

   It is a very interesting question and very comprehensive. Because it is very important to have cyber security, if possible, from the design phase. Unfortunately, not every element in supply chain was designed with cyber security in the primary idea. For this reason, today we can experience different kinds of attacks with different degree of success. Nevertheless, with the proper rules and the proper activities will be possible in the future to include more resilience technology using that leverage to start to create to build to putting practice the good cybersecurity things. There are a lot of private companies here and I think it will be possible to even increase their capacities in terms of cyber security and also will be very interesting to put everything in the good place from start from drafting new technology from drafting a new supply chain and from drafting a new manageable situation and the interfacing in this regard.

2. *In your opinion what provides more resiliency to main operations? Is it assurance of military power to the specific nodes in a transportation network or is it to having multiple and separate logistic routes?*

   It is a very comprehensive question. Because it asks about two different pathways. One is to increase the security of each node. The second is to diversify, to have different meanings different resources to obtain. I think both are important and we need to find a balance between them. Because this is a practice demonstrates until now it is very important to have a very secure intermediary nodes but also, it's very important to have different resources. As you can see today we are living in very unprecise from logistics point of view at the global level not entirely related to NATO. NATO is more stable here but different ways from different corners could appear and they could generate different repulse. if we cannot have alternatives. Therefore, both are important. Both are very for the resilience on long term.

3. *What are the major factors NATO should keep in mind which influence logistic system development for an ideal level of sustainment to the systems in the context of new consideration?*

   I think it is very important for all developments to become sustainable in medium and long term. It is very important because in that time, we have to make a lot of considerations, a lot of corrections. The NATO staff sustain very well design approach in the future. For this reason, I think it is necessary to develop everything in a sort of very tight integration between new technology and existing technology but taking in consideration all new developments started this year and maybe we need to make new adaptation at least in short term.

<u>Questions to Dr. Sarah LOHMANN</u>

1. *In your presentation, you did not mention about the where you place the autonomous weapons probably. But I think that the Internet of Things (IoT) can be turned to a weapon in the hands of the terrorists. What do you think about this issue? Because we may be witnessing an era in which we see hacker terrorists. Would you agree?*

   In terms of the question about terrorist use of the Internet, to actually interfere with our both UAS and UAV systems we are already seeing that now. In my 7th presentation, you can see how the cybersphere see in the in the right-hand corner actually plays a key role in as well as space as well as the airfield so terrorists can use all of this. We've seen them use space to counter GPS. We have seen them use cyber to hack both our communications as well as operations in in the field for both UAS and UAB. Therefore, this is a field that terrorists are using now but we expect them to become increasingly sophisticated and to use this in the future.

2. *You mentioned in your briefing about emerging and disruptive technologies autonomous weapon systems. To my understanding, autonomous systems are those that basically choose and attack targets without human interference or human manipulation.*

To the best of my knowledge, currently there is no such a technology or there is no such use of that. Do you also use that definition the way I explain or you know of event where those systems are used in current battlefield by either a nation states or a terrorist group?

Actually, I do start the chapter with the definitions, and I defined specifically that at this point that technology is not to that point of development where there is complete autonomy. Therefore, though the term exists we are not to the point where there is absolute operation on every front without any human programing. So, I agree with your definition.

<u>Questions to Ms. Denise FELDNER</u>

1. *Actually, it is so confusing to understand to connect NATO with the elections. Because just intervening elections for NATO could not be accepted as a good point. Especially for Europe, there is a special organization for this, you might know, OSCE, and they care about democracies and elections, they send observers to the elections, if we just need to discover any international organization for election safety or security OSCE would be more appropriate to my understanding. NATO would be controversial in terms of political thought, just the position of NATO and its connotation with elections especially for the public opinion would be higher reaction from society to NATO.*

   You are absolutely right and it is highly controversial. I think that's why the NATO summit in 2020 did not decide to set up the Democracy Center which was promoted by the president of the parliamentary assembly. I think there is a critical group of nations already under the umbrella of NATO and on the sidelines discussing those topics and I see a possibility where nations can exchange knowledge. This is the primary goal here, exchanging knowledge and experience about critical election infrastructure and countries may help the others to be more stable in their societies. Yet again, it is highly controversial.

2. *Could you clarify the definition of Metaverse that you are using and how you would interlink that with NATO? I would like to know more about how Metaverse should be treated as a rising threat or risk. I do not really see anything different from other areas or tools or opportunities online.*

Let me take the social media platforms as they are today. In Metaverse, people and their specific behavior will be much more involved than it is now and that is why I think it is a kind of Second World. We know that there was a Second World existing on the Internet but at this time is different and I would put it on the top of the list of emerging technologies which are of importance to security. Because people basically walk through the Internet and they live their daily lives in the metaverse or they will do that. I think this is a major difference compared to what we have today and how we see it today and how we experience it today. Furthermore, you will see elections in the metaverse, as well.

3. *In your presentation, you generally touch upon the technical points of the election system but what do you think about the disinformation? In addition, this can be a turned to a tool in the hands of the terrorists and they can affect the people and they can impact the elections.*

There was one thing on my slides which was named "***influence industry***" and behind the influence industry, all social media activities in these fields are hidden somehow. What I meant by that the influence industry was coined during the Cambridge Analytica scandal that came up in the elections in US. This exactly was one reason for the US coming up with it with the definition of critical election infrastructure. After the Cambridge Analytica scandal, the influence industry companies, data analytics companies and strategic communication companies used the tool of social media platforms to influence or possibly influence the vote of people and of citizens. This is a huge field and is of highest importance. I did not shed much light in more article on that because I thought there will be another article focusing directly on social media platforms and so it was not my scope but it is of highest importance to the fear of election security. But the same counts for all other topics in my article we could dig keeper in all of those topics. The social media platforms have the highest importance because they can be used and exploited and the people acting on those platforms also in signal groups. They can just gather and do some things together and it is a new space for people to behave and that is why they are of such great importance and that is why I came up with a metaverse and internet of behavior which is a kind of second name for the metaverse.

I believe it is the for me the social media platform 2.0 when it comes to the effects it could have or it will have from my perspective.

4. *You mentioned about the inner threats to election infrastructure and the right-wing terrorists and left-wing terrorists but also, we see there is a rise in racism and also a will to vote for the right-wing parties as well as a rise in the governing right-wing parties which are against some nations in NATO or in the EU. Therefore, do you think that's also a threat to NATO's unity and integrity and also to the EU and what's the border between the bill of citizens and the threat to NATO or EU*?

Your question has a very broad scope. I tried to narrow it down and that is why I only came up with two slides and I said I see internal threats and external threats and the internal threats there we see threat actors, and these are left-wing and right-wing threat actors. I avoided specifically speaking about specific cases. I have shown on my slides one of them was the *Querdenken* group in Germany. They are also on the rise and I think although the state is looking at what they are doing and it is absolutely a threat inside the European Union and in the US.

The last question was the effect on the citizens. That is actually a very difficult question. However, when it comes to democracy, I would say, democracy lives when everybody can discuss and make a decision and the majority will succeed in an election and in the discussion that would be my answer to your question.

DAY II

SESSION 1: COE-DAT Research Projects

Gender Sex Disaggregated Data

Asst. Prof. Omi HODWITZ

Countering terrorism requires both **proactive** and **reactive** measures. The former, which traditionally fall under the auspices of the military model, have been studied extensively while the latter, usually housed in the criminal justice model, are underexplored. Despite the limited research in this area, studies that examine the intersection between extremism and the criminal justice system offer promising results, suggesting the model may be effective at rehabilitating or deterring former terrorists. This is particularly evident when criminal proceedings are perceived as fair, consistent, and legitimate. This research, however, tends to focus primarily on male samples, overlooking the possibility that female extremists might have different outcomes.

Recognizing the deficit in the research, COE-DAT partnered with researchers from the University of Idaho, the Counter Extremism Project, and John Carrol University, to explore the intersection between gender, extremism, and criminal justice response. Specifically, the research team focused on using sex-disaggregated data to address two questions:

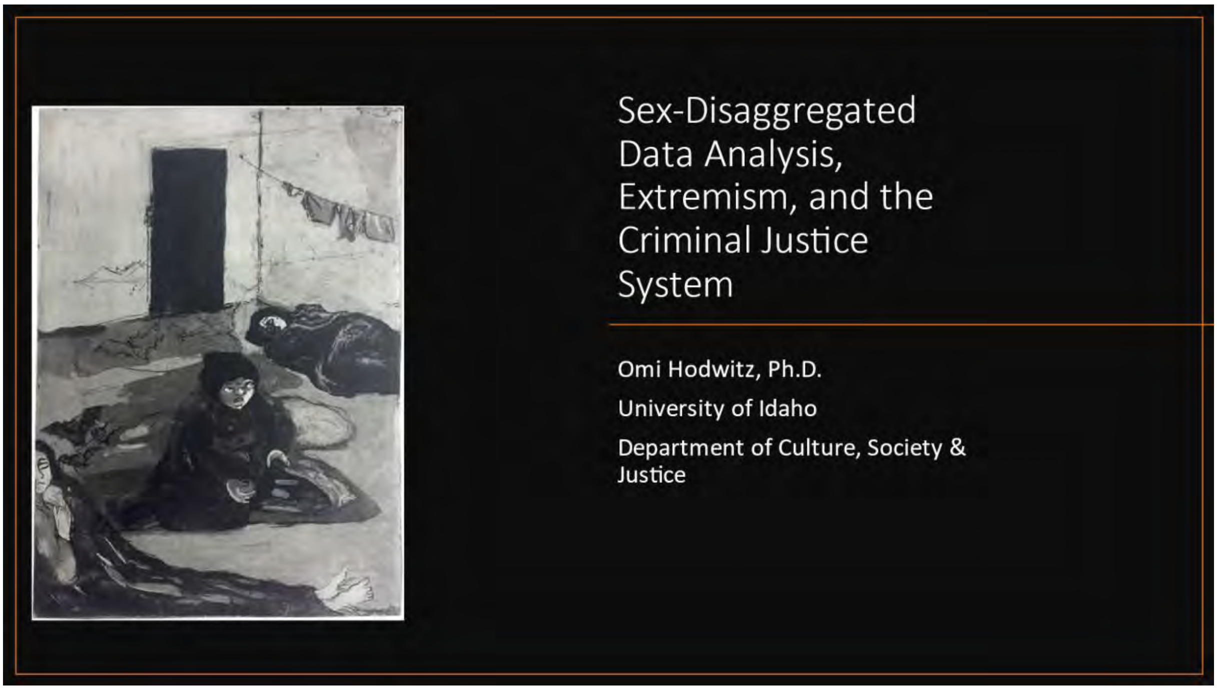
1) Does the criminal justice system respond differently to female extremists when compared to their male counterparts?

2) If there are disparities in criminal justice proceedings, what form do they take?

Using **sex-disaggregated data** and a variety of qualitative and quantitative techniques, the research team examined criminal justice responses to male and female extremists in the Western Balkans, Germany, Canada, and the United States. Each country or region of study focused on a different stage of criminal justice proceedings, thus providing a more complete assessment of potential points of differential treatment. Data for the **Western Balkans**, for example, revealed an interesting anomaly at the arrest stage of the criminal justice process: a lack of female representation. Content analysis and database comparison confirmed a clear disparity: in the Western Balkans, it appears that most female extremists are not arrested and charged with extremist-related behaviors. This appears to be driven, at least in part, by the belief that females have reduced agency and accountability and thus prosecution is likely to fail. In **Germany**, on the other hand, female Daesh returnees may be arrested, but the arrest patterns are different for males and females, as are the charges that each group is likely to face. Females are either under- or over-indicted when compared to their male counterparts and, when they are indicted, they tend to incur "private sphere" offenses, reflecting the perspective that women function primarily in a domestic capacity. The Canadian dataset presented gender-based disparities in conviction and sentence rates. Content analysis of media and legal documents illustrated that these discrepancies are likely due to a social and legalistic narrative that presents female extremists as desperate, easily coerced, and more sympathetic than their male counterparts. Lastly, the data from the United States support the Canadian findings, demonstrating disparities in sentencing outcomes. This finding remains even when other factors or explanations are considered and seems to be focused primarily on women who engage in gender atypical offenses.

In summary, research results indicate that female extremists face differential treatment when compared to their male counterparts and this disparity is supported by a narrative that presents females are having reduced agency and accountability. As such, females are treated with leniency at all stages of criminal justice proceedings, including the decision to arrest, the charges laid, the determination of guilt, and the resulting sentence. These disparities are concerning for several reasons, not the least of which relates to the overall goals of the criminal justice model. This model is driven by an allegiance to deterrence, rehabilitation, and social defense. At every stage of the criminal justice process, female extremists are being excluded and/or offered leniency, which compromises the ability of the system to meet each of these goals. Although the long-term consequences of gender-based disparities is yet to be determined, it is likely that leniency directed towards female extremists will impact the effectiveness of the criminal justice system in protecting the public, deterring current and future terrorists, and rehabilitating those that are already committed to extremist beliefs.

Presentation

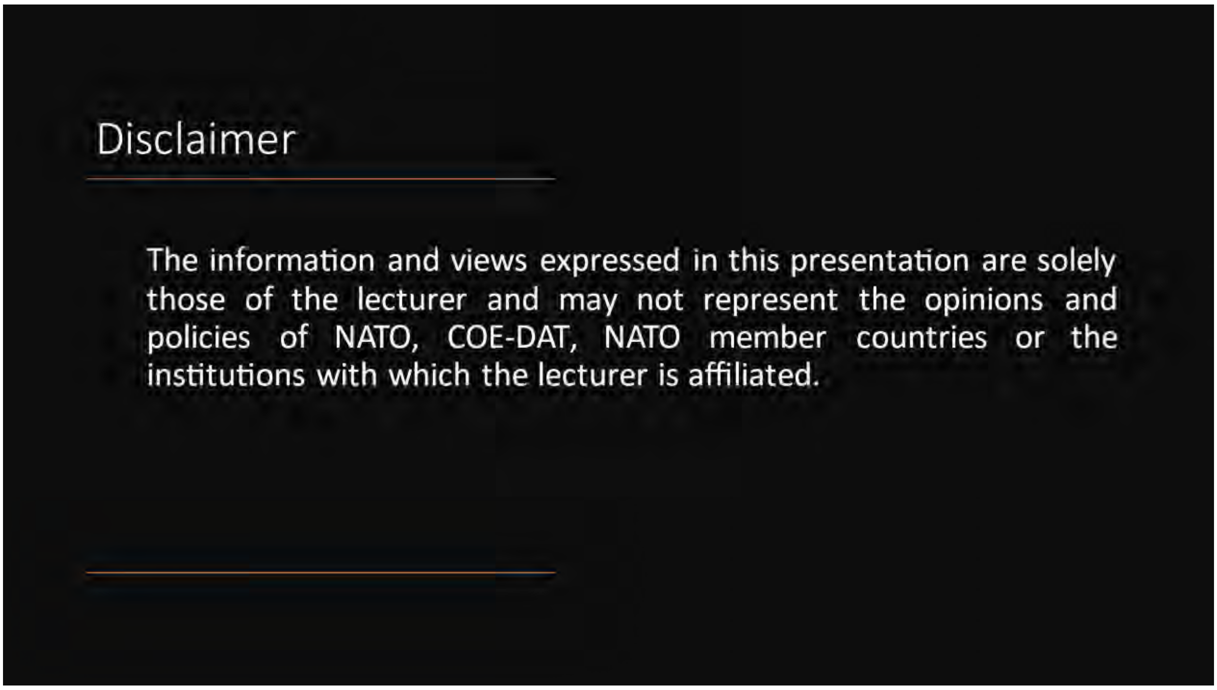


Sex-Disaggregated Data Analysis, Extremism, and the Criminal Justice System

Omi Hodwitz, Ph.D.

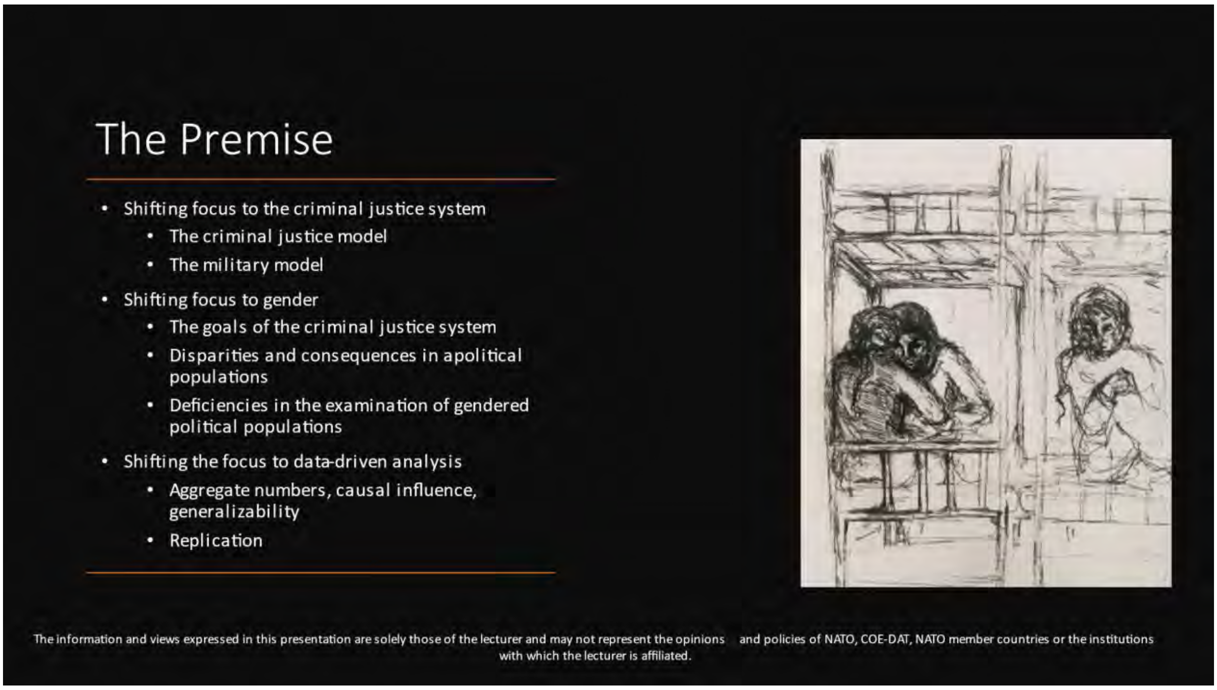
University of Idaho

Department of Culture, Society & Justice



Disclaimer

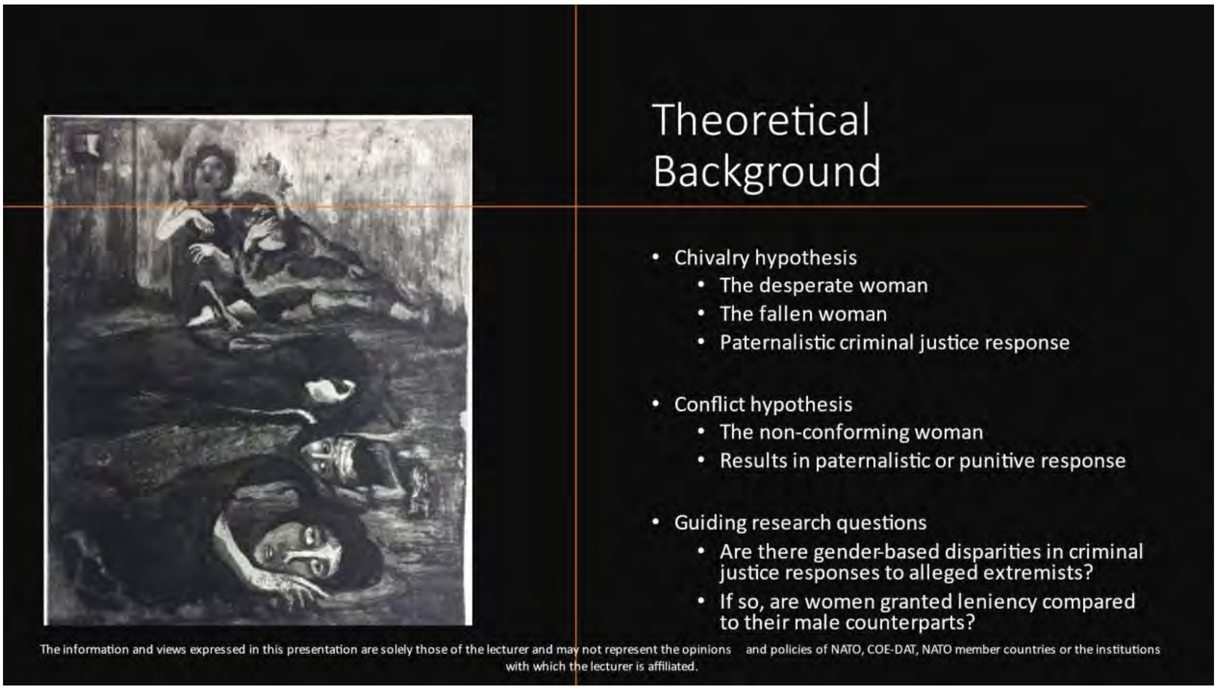
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



The Premise

- Shifting focus to the criminal justice system
  - The criminal justice model
  - The military model
- Shifting focus to gender
  - The goals of the criminal justice system
  - Disparities and consequences in apolitical populations
  - Deficiencies in the examination of gendered political populations
- Shifting the focus to data-driven analysis
  - Aggregate numbers, causal influence, generalizability
  - Replication

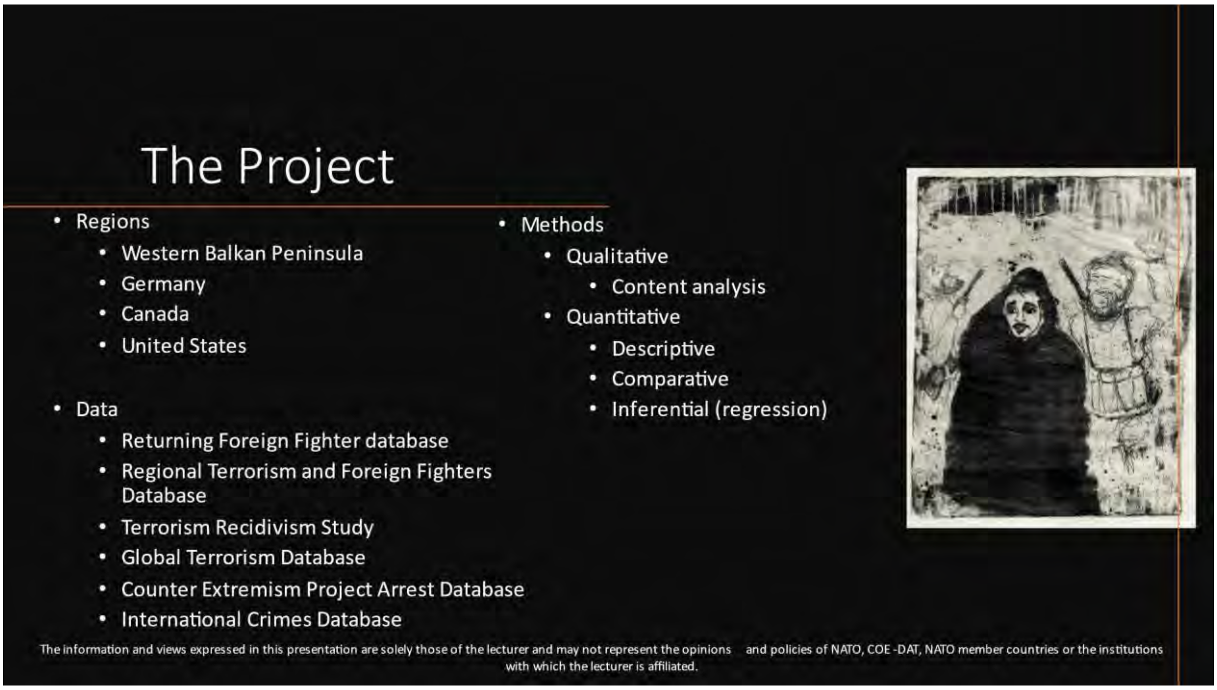
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Theoretical Background

- Chivalry hypothesis
  - The desperate woman
  - The fallen woman
  - Paternalistic criminal justice response
- Conflict hypothesis
  - The non-conforming woman
  - Results in paternalistic or punitive response
- Guiding research questions
  - Are there gender-based disparities in criminal justice responses to alleged extremists?
  - If so, are women granted leniency compared to their male counterparts?

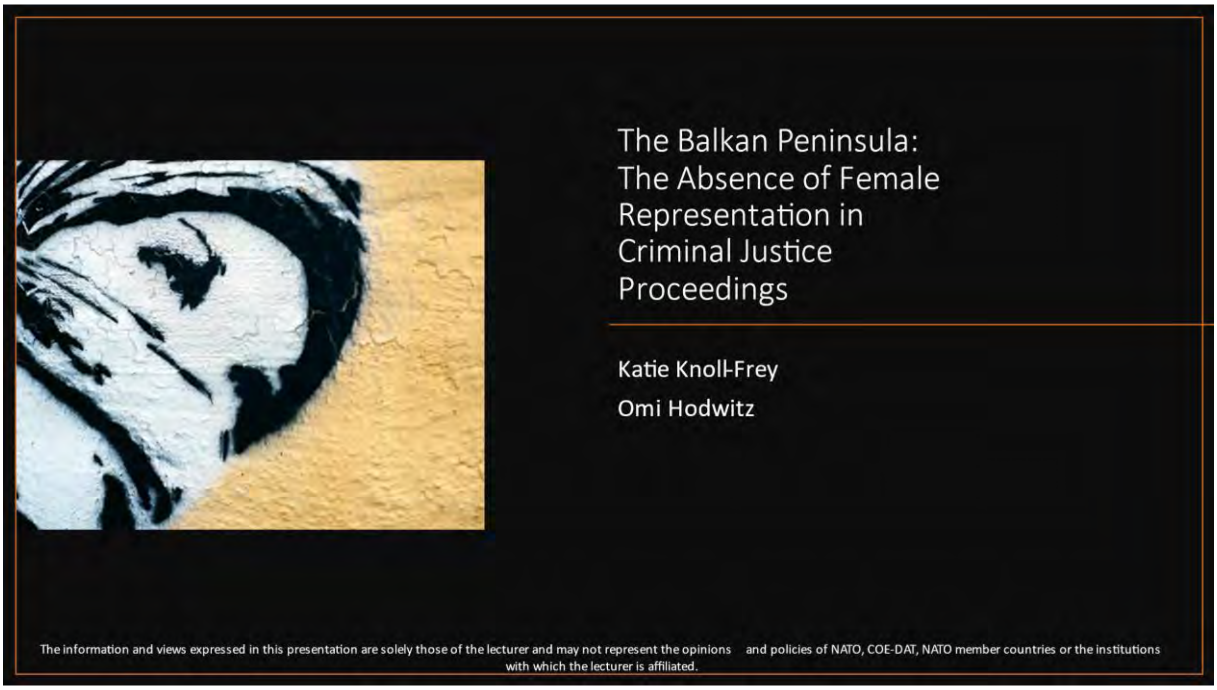
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



The Project

- Regions
  - Western Balkan Peninsula
  - Germany
  - Canada
  - United States
- Data
  - Returning Foreign Fighter database
  - Regional Terrorism and Foreign Fighters Database
  - Terrorism Recidivism Study
  - Global Terrorism Database
  - Counter Extremism Project Arrest Database
  - International Crimes Database
- Methods
  - Qualitative
    - Content analysis
  - Quantitative
    - Descriptive
    - Comparative
    - Inferential (regression)

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

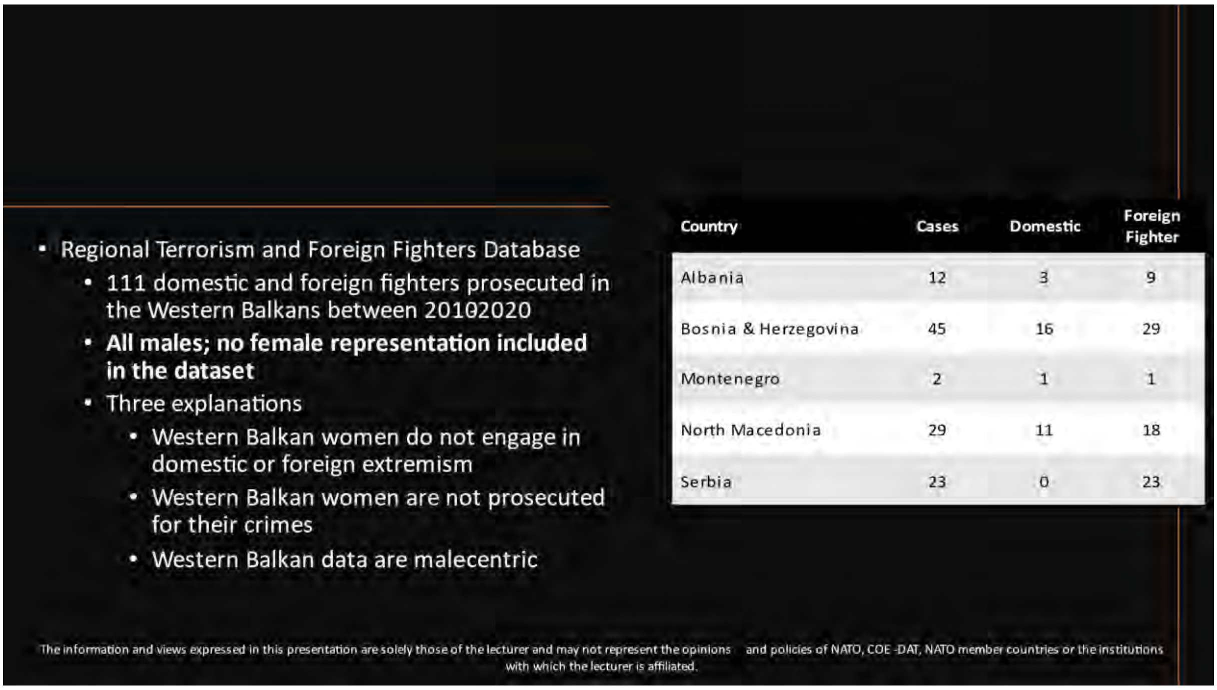


The Balkan Peninsula: The Absence of Female Representation in Criminal Justice Proceedings

Katie Knoll-Frey

Omi Hodwitz

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



- Regional Terrorism and Foreign Fighters Database
  - 111 domestic and foreign fighters prosecuted in the Western Balkans between 20102020
  - **All males; no female representation included in the dataset**
  - Three explanations
    - Western Balkan women do not engage in domestic or foreign extremism
    - Western Balkan women are not prosecuted for their crimes
    - Western Balkan data are malecentric

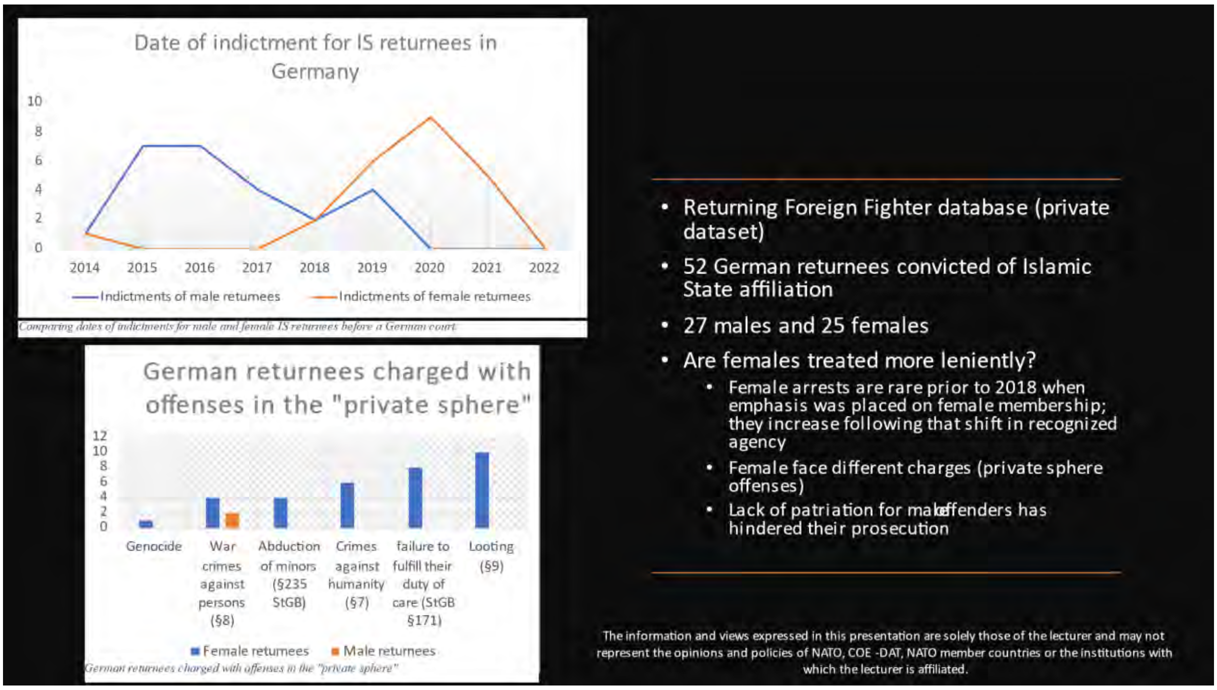
Country	Cases	Domestic	Foreign Fighter
Albania	12	3	9
Bosnia & Herzegovina	45	16	29
Montenegro	2	1	1
North Macedonia	29	11	18
Serbia	23	0	23

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Germany: Differential Prosecution of Male and Female Daesh returnees

Sofia Koller

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

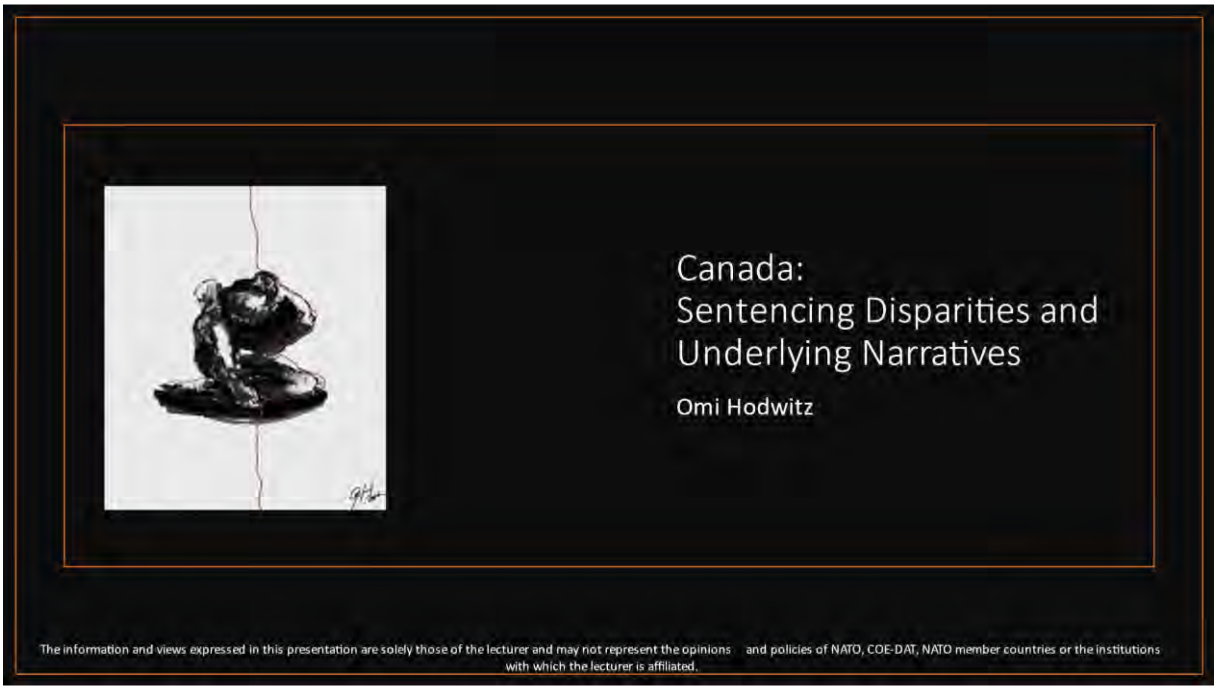


Comparing dates of indictments for male and female IS returnees before a German court

German returnees charged with offenses in the "private sphere"

- Returning Foreign Fighter database (private dataset)
- 52 German returnees convicted of Islamic State affiliation
- 27 males and 25 females
- Are females treated more leniently?
  - Female arrests are rare prior to 2018 when emphasis was placed on female membership; they increase following that shift in recognized agency
  - Female face different charges (private sphere offenses)
  - Lack of patriation for maleoffenders has hindered their prosecution

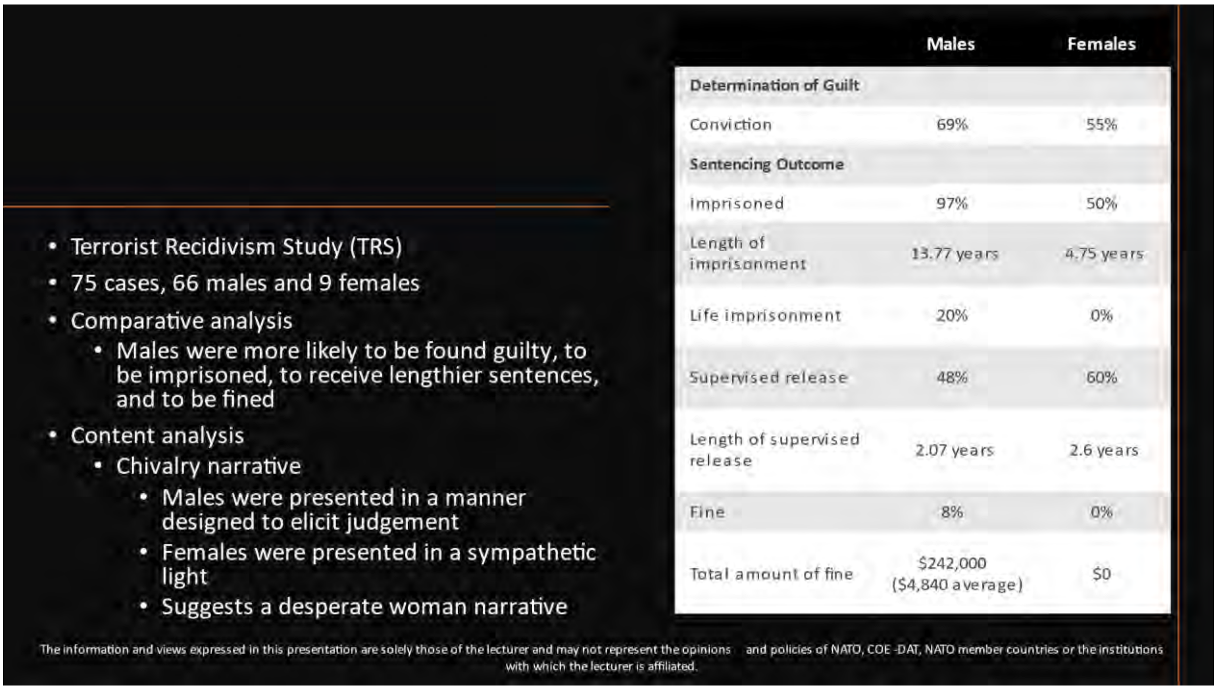
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Canada: Sentencing Disparities and Underlying Narratives

Omi Hodwitz

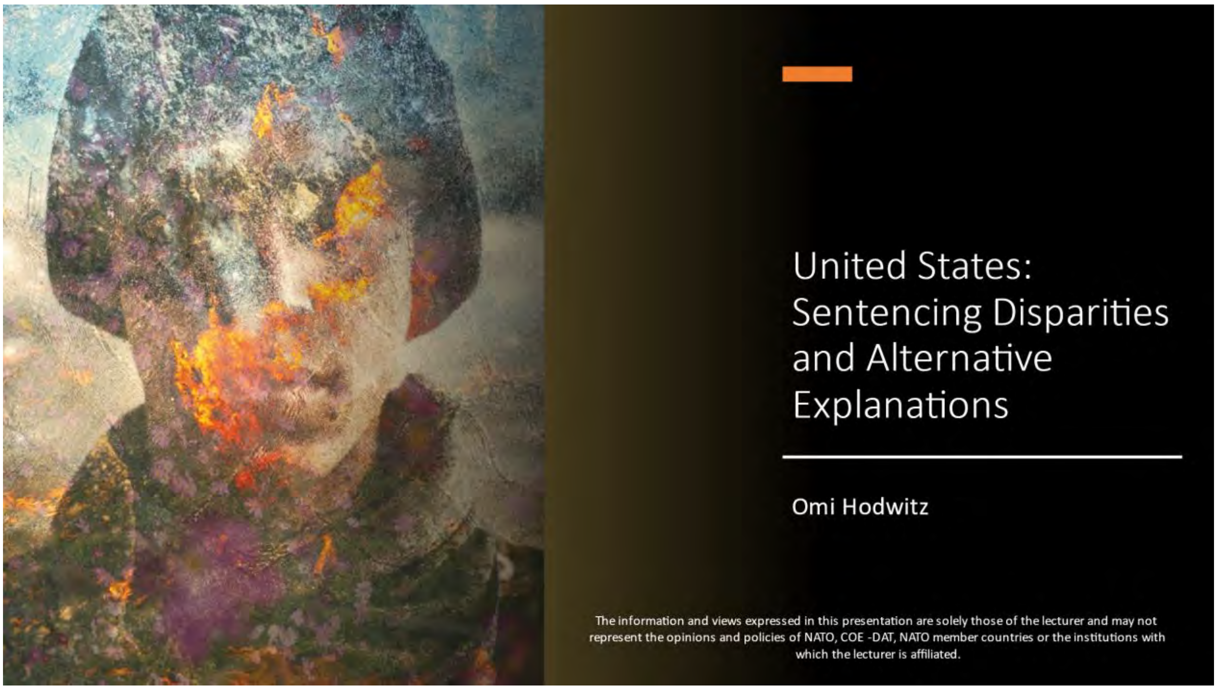
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



- Terrorist Recidivism Study (TRS)
- 75 cases, 66 males and 9 females
- Comparative analysis
  - Males were more likely to be found guilty, to be imprisoned, to receive lengthier sentences, and to be fined
- Content analysis
  - Chivalry narrative
    - Males were presented in a manner designed to elicit judgement
    - Females were presented in a sympathetic light
    - Suggests a desperate woman narrative

	Males	Females
Determination of Guilt		
Conviction	69%	55%
Sentencing Outcome		
Imprisoned	97%	50%
Length of imprisonment	13.77 years	4.75 years
Life imprisonment	20%	0%
Supervised release	48%	60%
Length of supervised release	2.07 years	2.6 years
Fine	8%	0%
Total amount of fine	$242,000 ($4,840 average)	$0

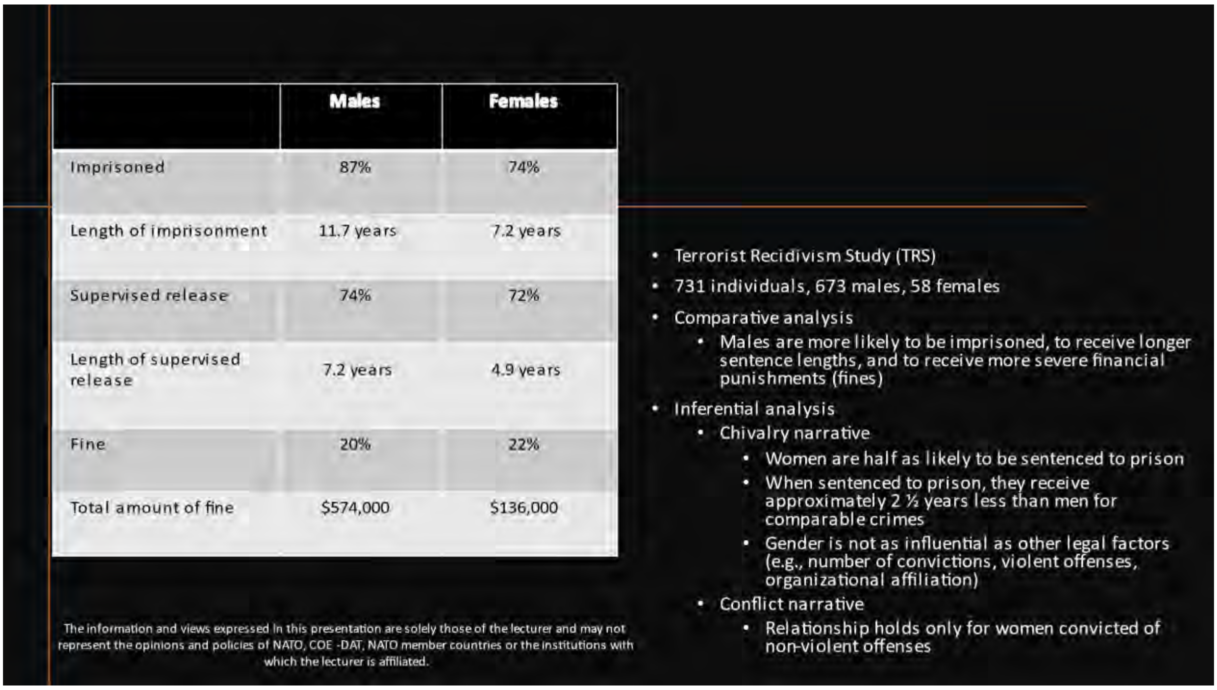
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



United States: Sentencing Disparities and Alternative Explanations

Omi Hodwitz

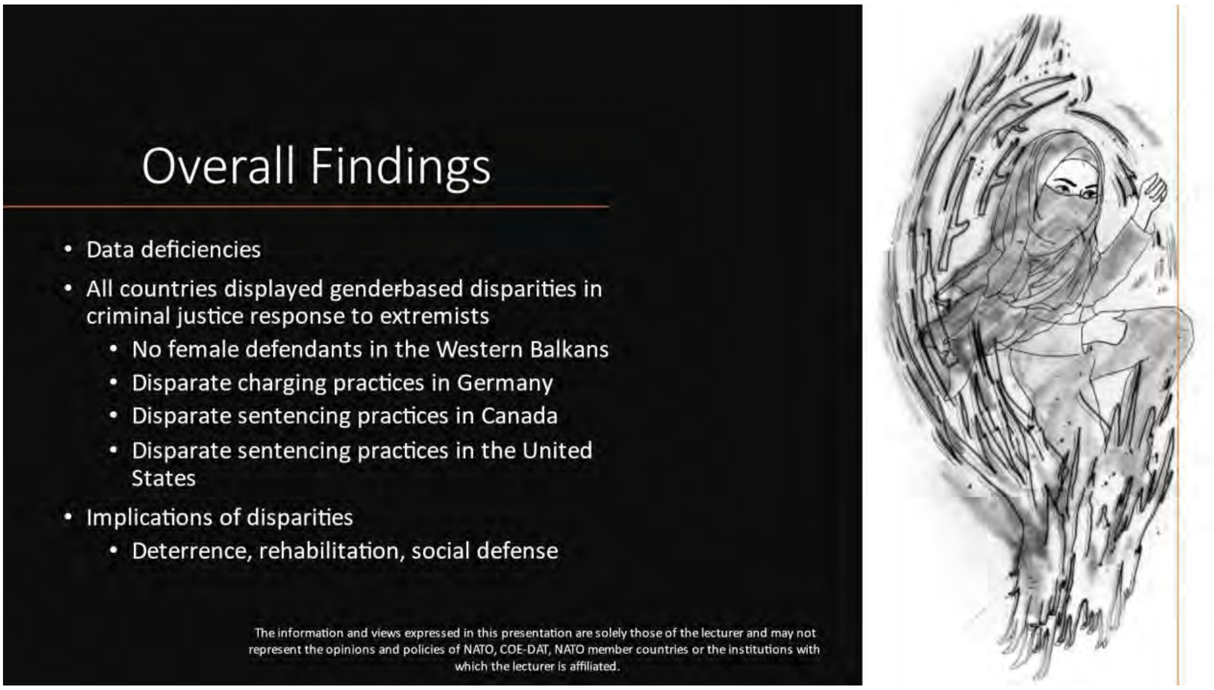
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



	Males	Females
Imprisoned	87%	74%
Length of imprisonment	11.7 years	7.2 years
Supervised release	74%	72%
Length of supervised release	7.2 years	4.9 years
Fine	20%	22%
Total amount of fine	$574,000	$136,000

- Terrorist Recidivism Study (TRS)
- 731 individuals, 673 males, 58 females
- Comparative analysis
  - Males are more likely to be imprisoned, to receive longer sentence lengths, and to receive more severe financial punishments (fines)
- Inferential analysis
  - Chivalry narrative
    - Women are half as likely to be sentenced to prison
    - When sentenced to prison, they receive approximately 2 ½ years less than men for comparable crimes
    - Gender is not as influential as other legal factors (e.g., number of convictions, violent offenses, organizational affiliation)
  - Conflict narrative
    - Relationship holds only for women convicted of non-violent offenses

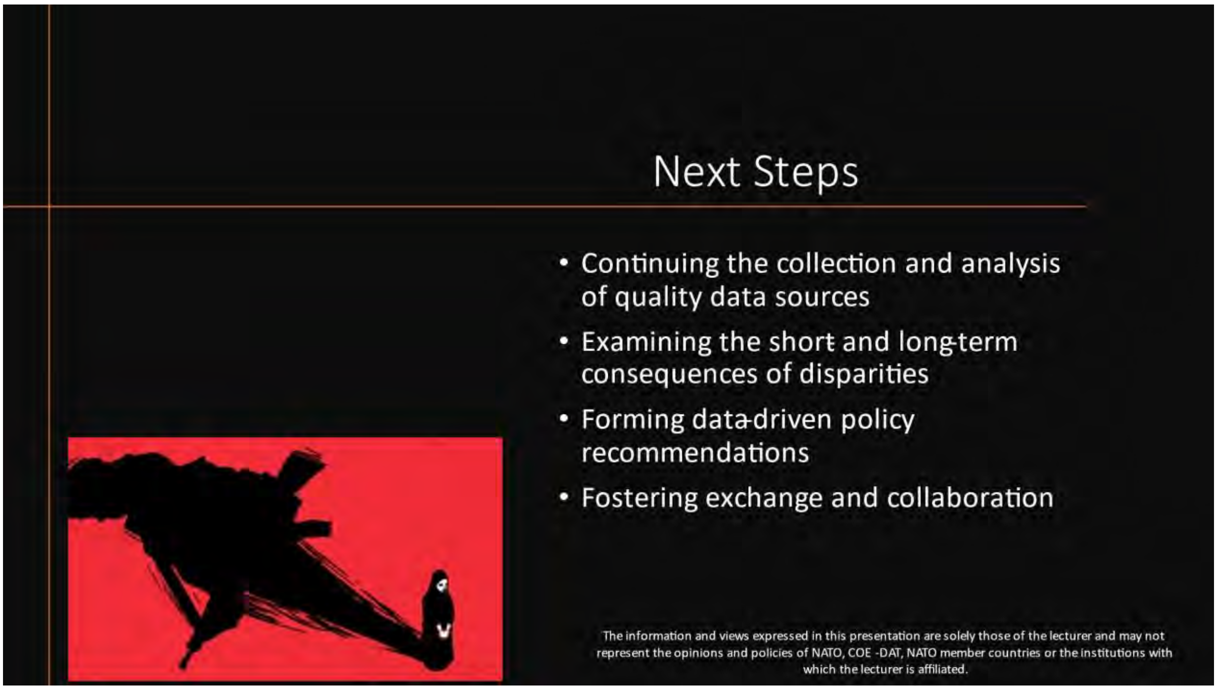
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Overall Findings

- Data deficiencies
- All countries displayed genderbased disparities in criminal justice response to extremists
  - No female defendants in the Western Balkans
  - Disparate charging practices in Germany
  - Disparate sentencing practices in Canada
  - Disparate sentencing practices in the United States
- Implications of disparities
  - Deterrence, rehabilitation, social defense

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Next Steps

- Continuing the collection and analysis of quality data sources
- Examining the short and long-term consequences of disparities
- Forming data-driven policy recommendations
- Fostering exchange and collaboration

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Partnership SOF Crisis Management
Dr. Heather GREGG

This presentation summarized the first iteration of the SOF Roles in Crisis/CT seminar, which was a three-day workshop held from 6-8 July 2022 in Ankara, Türkiye, at NATO COE-DAT's headquarters.

This workshop was a collaborative effort between NATO SOF Headquarters (NSHQ) in Brussels, Belgium; the NATO COE DAT in Ankara, Türkiye; and the U.S. Army War College's Strategic Study Institute. Together these stakeholders developed three broad goals for the workshop: to engage NATO SOF partner nations and emerging partner nations; to provide an opportunity for NATO SOF allies, partner nations, and emerging partner nations to network and build relationships; and to share best practices in crisis responses to terrorist incidents and explore how SOF can help inform these responses, including the roles that SOF may—or may not—play in the actual response.

Twenty-five individuals from eleven countries—Algeria, Australia, Egypt, France, Hungary, India, Slovakia, Tunisia, Türkiye, United Kingdom, and the United States—attended the workshop, representing a range of military ranks and civilians focused on counter-terrorism (CT) at the tactical, operational, and strategic levels.

Day one of the workshop included a comparison case study between two attacks perpetrated by al-Shabaab in Kenya and the crisis response—the 2013 Westgate Shopping Mall siege and the 2019 DusitD2 Complex attack—followed by breakout sessions to discuss lessons learned from these attacks. Day two began with a presentation on nine lessons learned in CT, followed by a scenario exercise in which participants had to formulate a response to a multi-pronged terrorist attack on a hotel, including building a crisis response team, discussing what actions should be taken, formulating a media response, and debating how to conduct an After Action Review (AAR) of the attack. Day three concluded the workshop with summary points of lessons learned and a discussion on possible topics for the next iteration of the workshop.

Drawing from the report of the workshop, the key takeaways included:

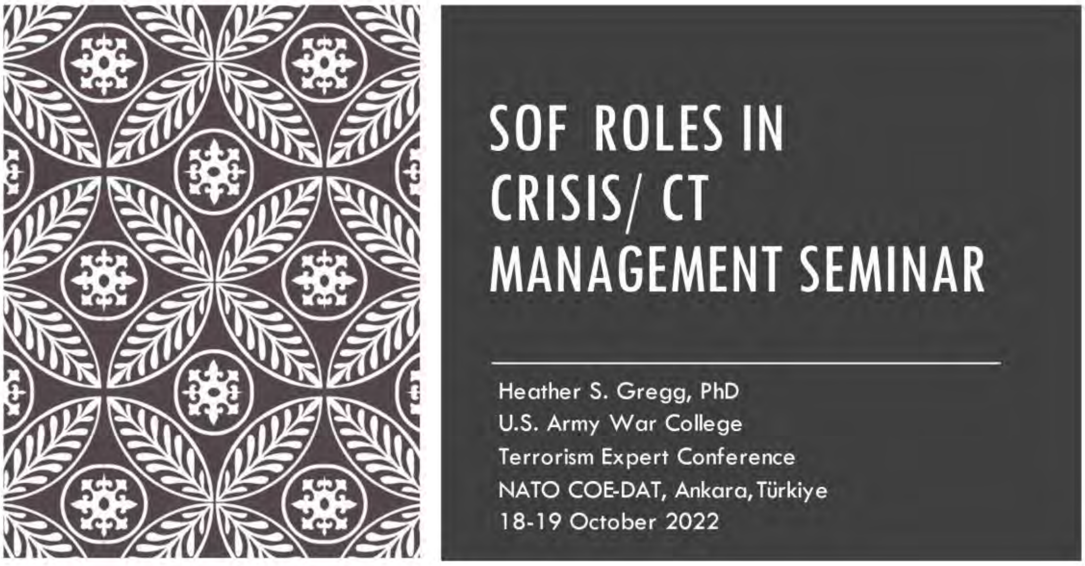
- The critical importance of coordination and achieving interoperability between security forces in crisis management—including equipment and particularly communications equipment—but also the need for training and doctrine; the creation of a coordinating structure, such as a fusion cell; intelligence sharing; and pre-crisis designation of who is in charge based on the type of crisis
- The need for a whole of government approach. CT is not just a law enforcement task or a military operation; it requires multiple departments, ministries, and agencies in a country to effectively deter and respond to terrorist attacks
- Achieving coordination and interoperability are extremely difficult on an ad hoc basis; rather, pre-attack planning and training between stakeholders for a coordinated, whole of government approach is usually more successful. However, often the impetus for this planning is a failed CT crisis response, making preemption very difficult. Sharing best practices and learning from other countries' CT plans may be a way to address this dilemma, including through MSATs (Multinational SOF Advisory Teams)
- The importance of laws that delineate authorities, roles, responsibilities, and limits of various security forces in a domestic CT response, as well as who should be in charge and under which circumstances
- The importance of a whole of society approach to CT. This includes creating resilience in the population, including preparing the population for the possibility of attacks, leveraging the population for intelligence and help with CT ("If you see something, say something"); and possibly creating a form of Comprehensive Defense as a CT strategy and using SOF to coordinate these efforts. This is a whole of society approach
- The need to have a media strategy as part of the crisis response to inform the public and ensure that terrorists do not control the narrative
- The role that SOF Liaison Officers could play at the highest levels of government to help advise on CT matters (*SOF Roles in CT/Crisis Management*, 3-4).

The full report can be read here: https://www.tmmm.tsk.tr/SOF_Roles_inCT_Crisis_ManagementReport.pdf

The next iteration of the workshop will be held from May 2-5, 2023, in Ankara, Türkiye, at NATO COE-DAT's headquarters. It will focus on the same goals of building partnerships between NATO SOF members, partner nations and emerging partner nations. The stakeholders aim to broaden the scope of participants for the next iteration of the workshop to include law enforcement, government officials, media, and the private sector.

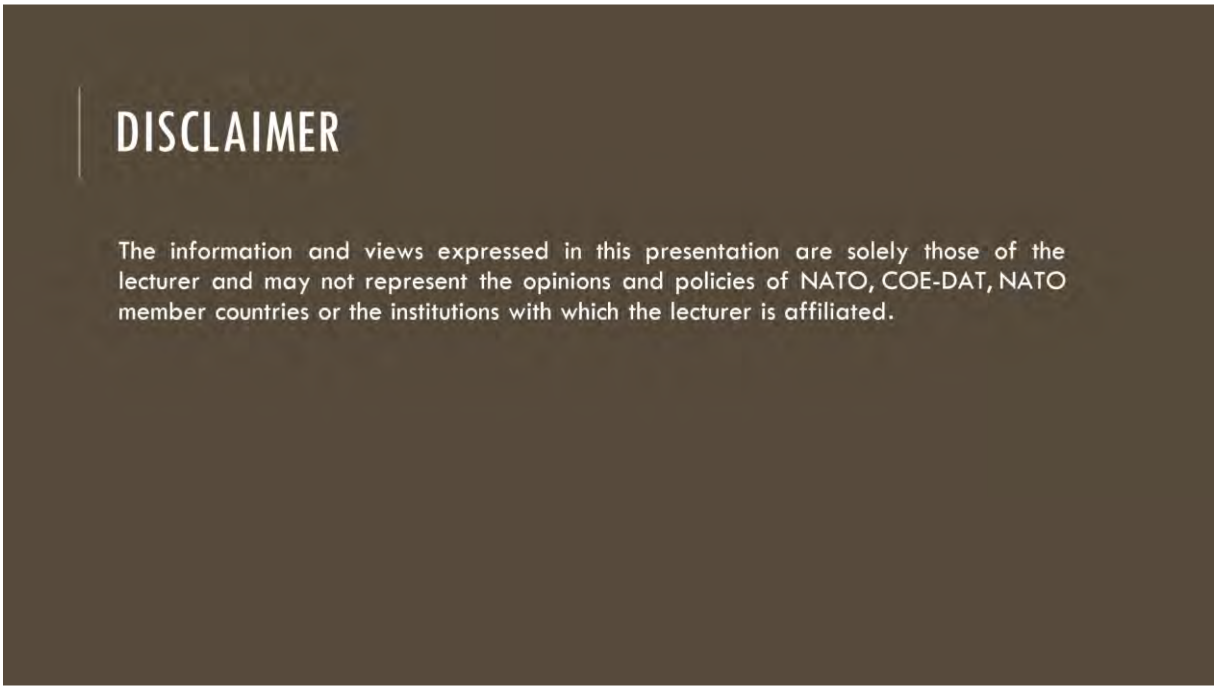
The workshop will also follow the same broad topic of how SOF can help inform a crisis response to CT, and the roles that CT may play in specific countries. Potential topics include crisis response in maritime security and SOF; Critical Infrastructure at CT; Crisis Response to Hybrid Threats; Non-urban CT; and how different NATO countries have developed crisis response cells or teams.

Presentation



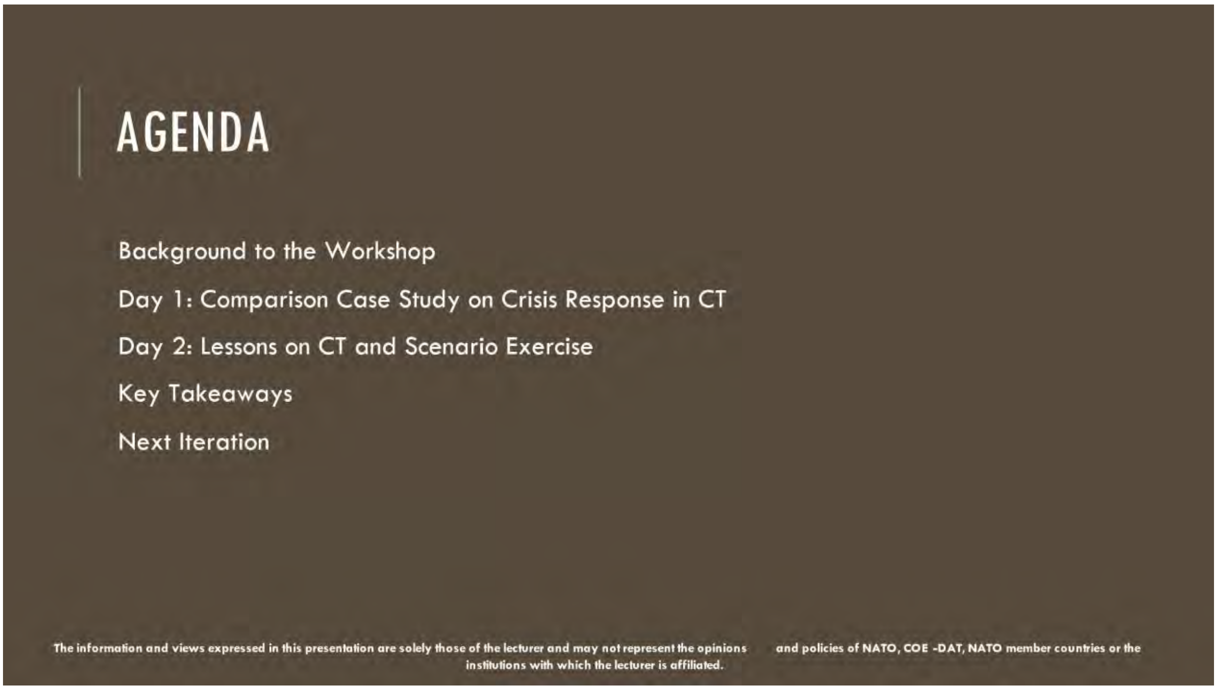
SOF ROLES IN
CRISIS/ CT
MANAGEMENT SEMINAR

Heather S. Gregg, PhD
U.S. Army War College
Terrorism Expert Conference
NATO COE-DAT, Ankara, Türkiye
18-19 October 2022



DISCLAIMER

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



AGENDA

Background to the Workshop

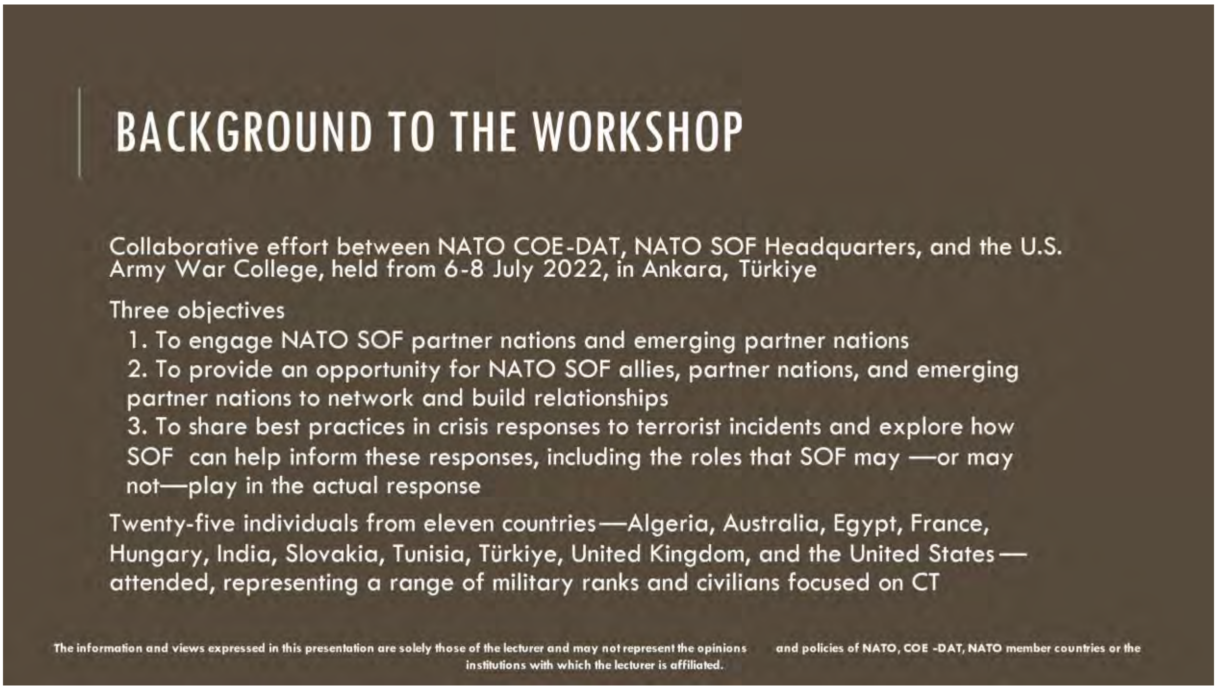
Day 1: Comparison Case Study on Crisis Response in CT

Day 2: Lessons on CT and Scenario Exercise

Key Takeaways

Next Iteration

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



BACKGROUND TO THE WORKSHOP

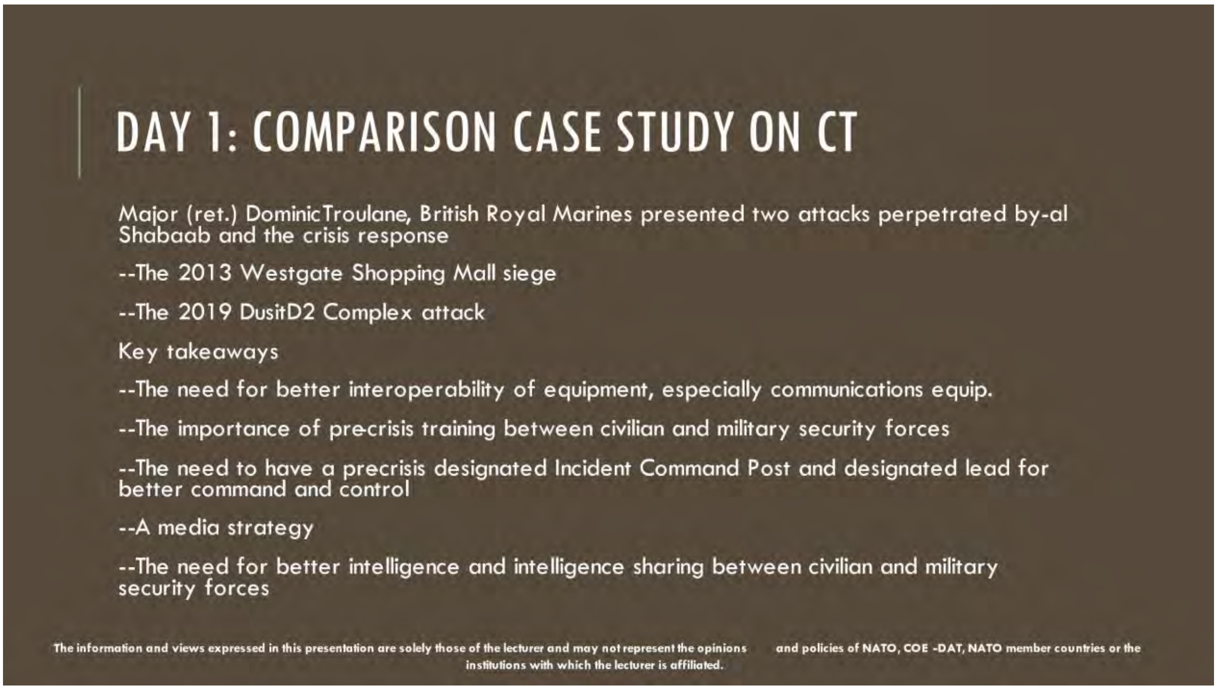
Collaborative effort between NATO COE-DAT, NATO SOF Headquarters, and the U.S. Army War College, held from 6-8 July 2022, in Ankara, Türkiye

Three objectives

1. To engage NATO SOF partner nations and emerging partner nations
2. To provide an opportunity for NATO SOF allies, partner nations, and emerging partner nations to network and build relationships
3. To share best practices in crisis responses to terrorist incidents and explore how SOF can help inform these responses, including the roles that SOF may —or may not—play in the actual response

Twenty-five individuals from eleven countries—Algeria, Australia, Egypt, France, Hungary, India, Slovakia, Tunisia, Türkiye, United Kingdom, and the United States—attended, representing a range of military ranks and civilians focused on CT

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



DAY 1: COMPARISON CASE STUDY ON CT

Major (ret.) DominicTroulane, British Royal Marines presented two attacks perpetrated by-al Shabaab and the crisis response

--The 2013 Westgate Shopping Mall siege

--The 2019 DusitD2 Complex attack

Key takeaways

--The need for better interoperability of equipment, especially communications equip.

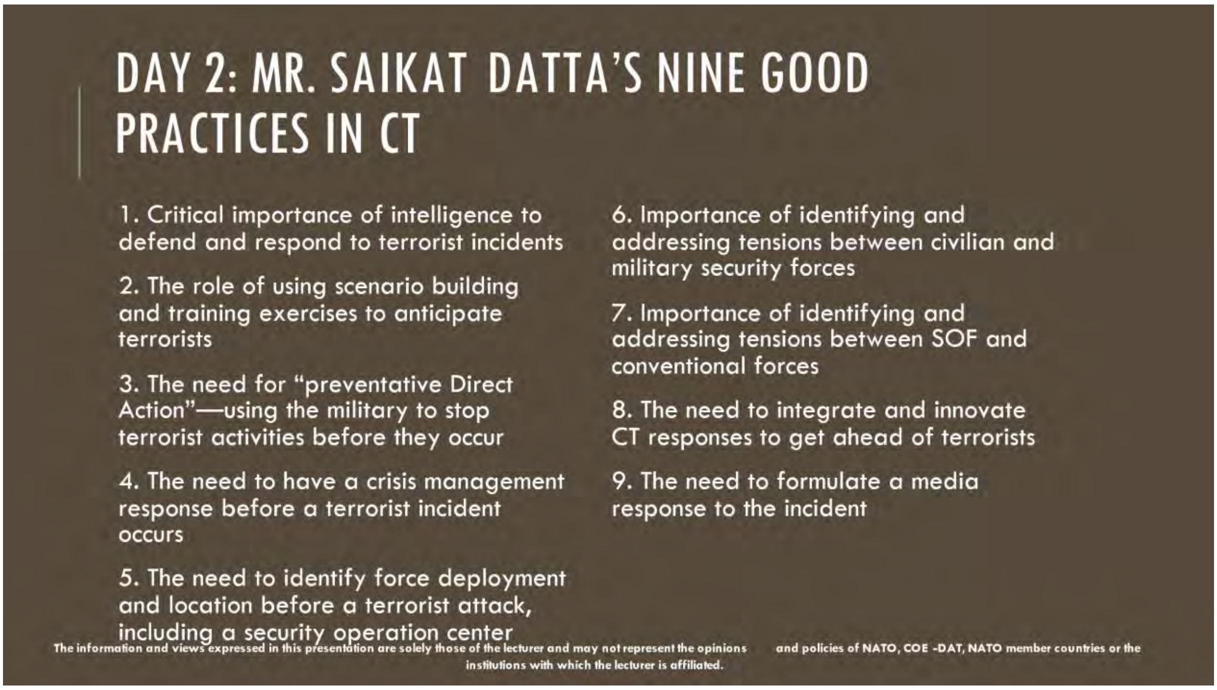
--The importance of pre-crisis training between civilian and military security forces

--The need to have a precrisis designated Incident Command Post and designated lead for better command and control

--A media strategy

--The need for better intelligence and intelligence sharing between civilian and military security forces

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



DAY 2: MR. SAIKAT DATTA'S NINE GOOD PRACTICES IN CT

1. Critical importance of intelligence to defend and respond to terrorist incidents

2. The role of using scenario building and training exercises to anticipate terrorists

3. The need for "preventative Direct Action"—using the military to stop terrorist activities before they occur

4. The need to have a crisis management response before a terrorist incident occurs

5. The need to identify force deployment and location before a terrorist attack, including a security operation center

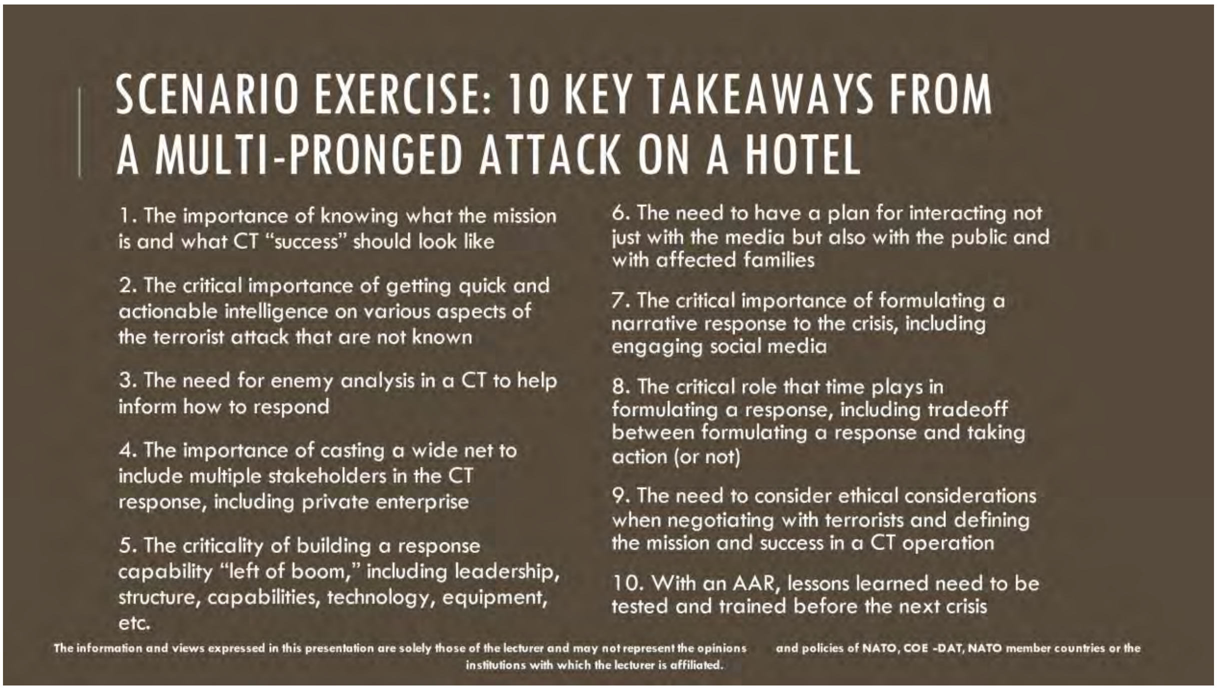
6. Importance of identifying and addressing tensions between civilian and military security forces

7. Importance of identifying and addressing tensions between SOF and conventional forces

8. The need to integrate and innovate CT responses to get ahead of terrorists

9. The need to formulate a media response to the incident

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



SCENARIO EXERCISE: 10 KEY TAKEAWAYS FROM A MULTI-PRONGED ATTACK ON A HOTEL

1. The importance of knowing what the mission is and what CT "success" should look like

2. The critical importance of getting quick and actionable intelligence on various aspects of the terrorist attack that are not known

3. The need for enemy analysis in a CT to help inform how to respond

4. The importance of casting a wide net to include multiple stakeholders in the CT response, including private enterprise

5. The criticality of building a response capability "left of boom," including leadership, structure, capabilities, technology, equipment, etc.

6. The need to have a plan for interacting not just with the media but also with the public and with affected families

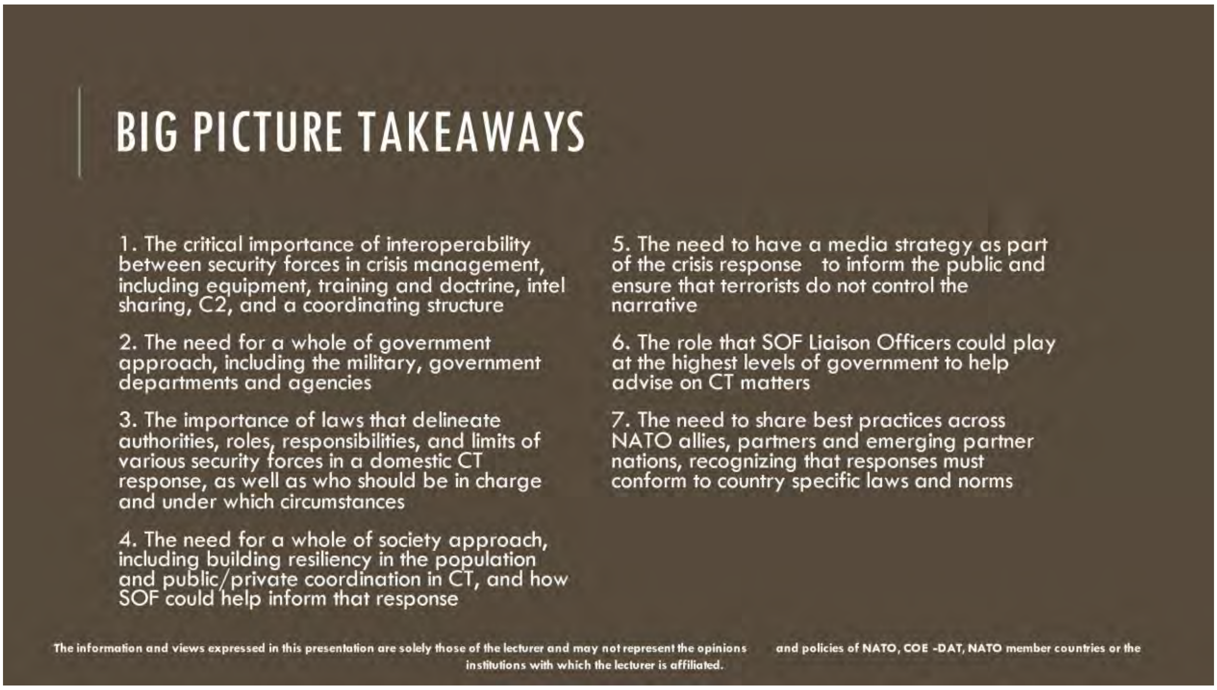
7. The critical importance of formulating a narrative response to the crisis, including engaging social media

8. The critical role that time plays in formulating a response, including tradeoff between formulating a response and taking action (or not)

9. The need to consider ethical considerations when negotiating with terrorists and defining the mission and success in a CT operation

10. With an AAR, lessons learned need to be tested and trained before the next crisis

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



BIG PICTURE TAKEAWAYS

1. The critical importance of interoperability between security forces in crisis management, including equipment, training and doctrine, intel sharing, C2, and a coordinating structure

2. The need for a whole of government approach, including the military, government departments and agencies

3. The importance of laws that delineate authorities, roles, responsibilities, and limits of various security forces in a domestic CT response, as well as who should be in charge and under which circumstances

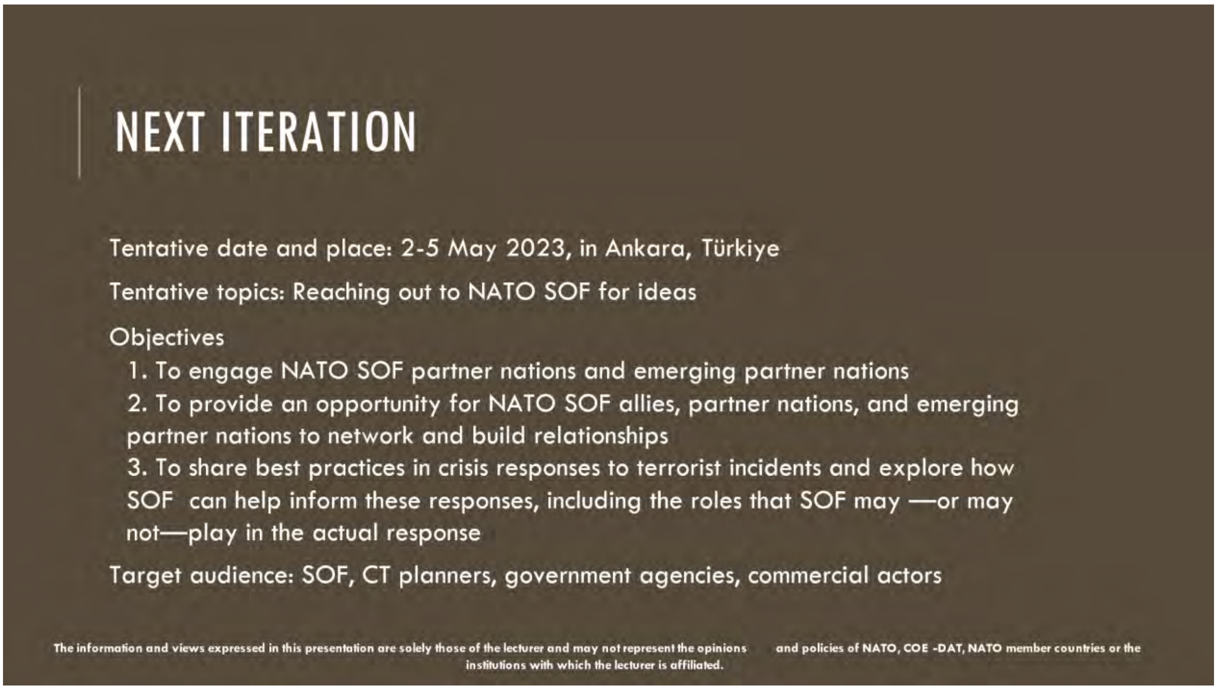
4. The need for a whole of society approach, including building resiliency in the population and public/private coordination in CT, and how SOF could help inform that response

5. The need to have a media strategy as part of the crisis response to inform the public and ensure that terrorists do not control the narrative

6. The role that SOF Liaison Officers could play at the highest levels of government to help advise on CT matters

7. The need to share best practices across NATO allies, partners and emerging partner nations, recognizing that responses must conform to country specific laws and norms

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



NEXT ITERATION

Tentative date and place: 2-5 May 2023, in Ankara, Türkiye

Tentative topics: Reaching out to NATO SOF for ideas

Objectives

1. To engage NATO SOF partner nations and emerging partner nations
2. To provide an opportunity for NATO SOF allies, partner nations, and emerging partner nations to network and build relationships
3. To share best practices in crisis responses to terrorist incidents and explore how SOF can help inform these responses, including the roles that SOF may —or may not—play in the actual response

Target audience: SOF, CT planners, government agencies, commercial actors

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

QUESTIONS

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Emerging Threats in Terrorism and Counter-terrorism

Prof. Dr. Haldun YALÇINKAYA

The incidents in the 21st century confirmed that international security is no longer challenged only by traditional means and threats. Especially the pace of technological developments, in this sense, triggered concerns about the possibility that these advanced technological tools could proliferate in the hands of terrorist groups. Considering the fact that these are easily adaptable and learning organizations, conducting research on *Emerging Threats in Terrorism: From a Multidisciplinary Approach* was born out of necessity.

The question to be answered in detail in this project is "*What are the emerging threats in the future from European and Asian perspectives in terms of terrorism?*". To have a comprehensive approach to emerging threats, this project utilized the Delphi Technique. This technique, in essence, allows the researcher to benefit from the experts' competency for future forecasting. In line with the goals of the project, the research team specified 30 experts from different fields to take part in the two rounds of the Delphi Technique surveys. The areas of expertise of the participants are as follow: Biosecurity and Health Security, Changing World Order, Critical Infrastructure, Cyber Security, Economical Security and Development, Emerging Technologies, Energy Security, Environmental Security, Hybrid Warfare, Intelligence, Maritime Security, Migration, National Security, Nuclear Threats (CBRN), Social Media, Terrorism, Radicalization, Terrorist Financing.

In the first round, the experts were expected to provide answers to open-ended questions depending on their expertise about the main security challenges, emerging threats, comparison between traditional and emerging threats in terms of the severity of the challenge, the possible trends in terrorism within 10 years period, and the vulnerabilities and strengths of states for countering emerging terrorist threats.

Depending on the answers of the first round, the research team prepared a multiple-choice questionnaire for the second round and shared it with the experts who participated in the first round. The majority of the experts (63,3%) stated that ***Geopolitical Threats*** are likely to pose the greatest threats in terms of Emerging Threats. Geopolitical Threats are followed by Economic Threats, Environmental Threats, Societal Threats, and Technological Threats, respectively.

From regional perspectives, experts expressed that the threats which are going to occupy **Africa's** agenda are related to food security, lack of governmental experience, population growth, and terrorism. **Asia**, on the other hand, will be occupied by great power politics, climate change, population growth and change in demography, inter-state political disputes, sub-nationalism, terrorism, and economic grievances. For the concerns of the European continent, frequently raised issue was ***Russian aggression***. Other issues that Europe is going to be dealing with are climate change, intensifying far-right and far-left movements, cyber security, and political instability in the Balkans. As the last region in terms of the scope of the research, the Middle East is seemed to be threatened by ethnic-religious clashes, radicalization, religiously motivated terrorism, civil wars climate change, and energy demand. 40% of the experts stressed that among these four regions, **Europe** will be more vulnerable to emerging threats.

The experts listed twelve different emerging terrorist threats that we should approach by understanding their diversification and their relationship with evolving nature of the environment as follows:

Cyber threats directed at critical infrastructure systems	Economic instability
The growing rate of radicalization due to dissatisfying life conditions	Marginalized and segregated migrant groups
Online radicalization and use of social media as a means of violence	Use of social media as a means of violence
The proliferation of emerging technologies to malicious groups	Nuclear security and nuclear terrorism
Far-right/ far-left/ anti-globalization violence	Agricultural policies for the future of food security
Armed ethnic sub-nationalism	Biotechnology and genetic modification and manipulation

Despite technological innovations that ease various things in human life, the abuse of developed technologies has been paving the way for new challenges. Some of the experts found these threats to be more challenging than ever whereas some shared the idea that they were not different at all. In opposition to this approach, several experts believe that the basics of threat have not changed such as the political motivation and the search for the means to give harm.

The possible vulnerabilities for states in detecting and responding to these threats could be categorized as

- The lack of inter-agency cooperation and the lack of a common view of the existence and imminence of the threat, Bureaucratic inefficiency and lack of agility to emerging threats, and Lack of flexibility and adaptability to changing environments.
- Societal polarization, distrust of government, Hypocrisy and double standards of security forces and policymakers in handling terrorist threats, Inequality among the citizens, and Access to information networks.
- Failing to follow the norms and rules set by themselves and not being able to cooperate against common threats but expect the others to follow them by creating dependencies and transactional relations.
- The inability to grasp and handle specifics of Emerging Destructive Technologies
- Lone wolf attacks, non-international terrorist attacks.

However, there are also well-established agencies, capabilities, and elements of states that make them pursue their strengths including enforcement capacities, legitimate authority, sufficient resources, manpower and expertise, experience, large-scale surveillance capabilities, and information technology.

To frame the emerging threats depending on our experts, we identified four different clusters that show the trends and foresights in the answers:

- Developing Technology-Related Threats,
- Innovative New Threats Against Conventional Sectors,
- Accumulation of Classical Terrorist Threats,
- Innovative New Threats against Non-Conventional Sector

Presentation

CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

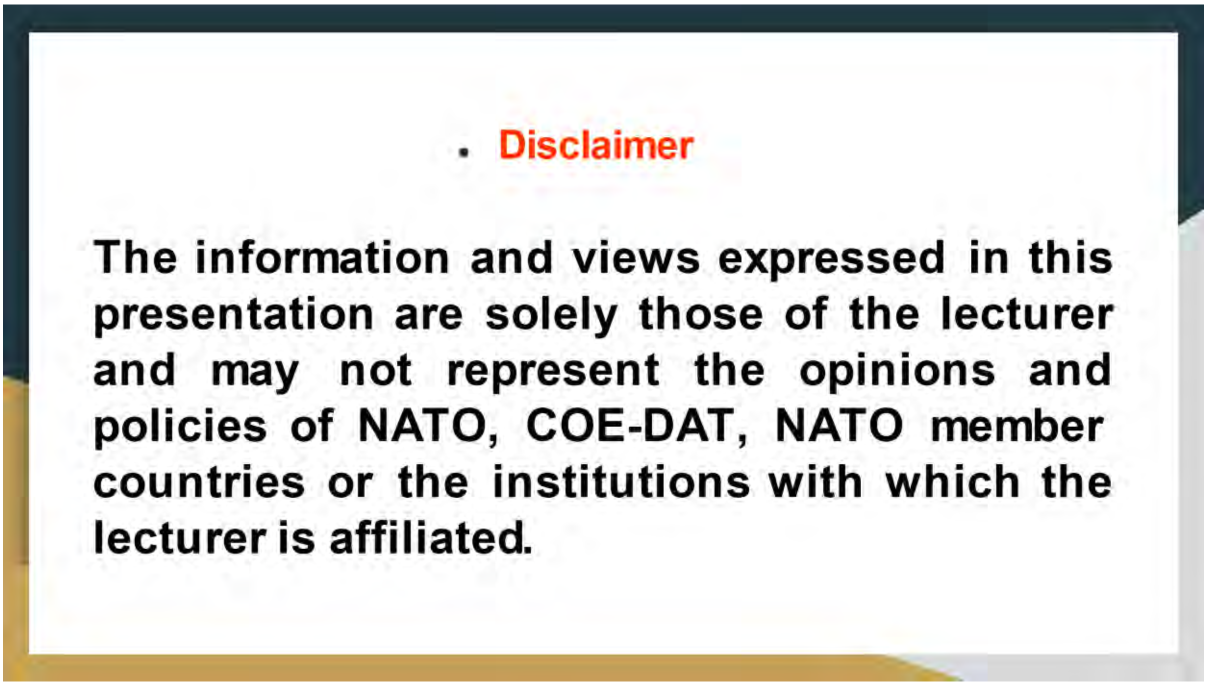
Researc Projec
Prelimina
Result

Emerging Threats in Terrorism:
With a Multidisciplinary Approach

Terroris
Expert Conferen
2022

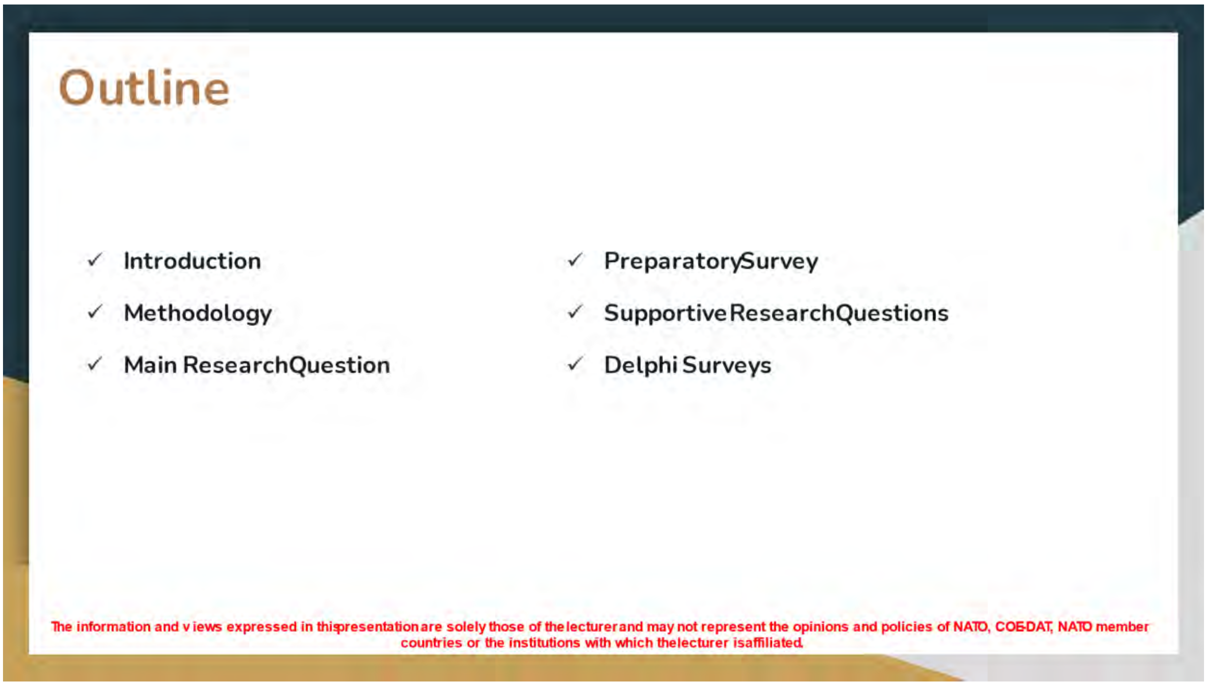
Octobe 18-19, 202

Prof. Haldun YALÇINKAYA & Elif Merve DUMANKAYA



- Disclaimer

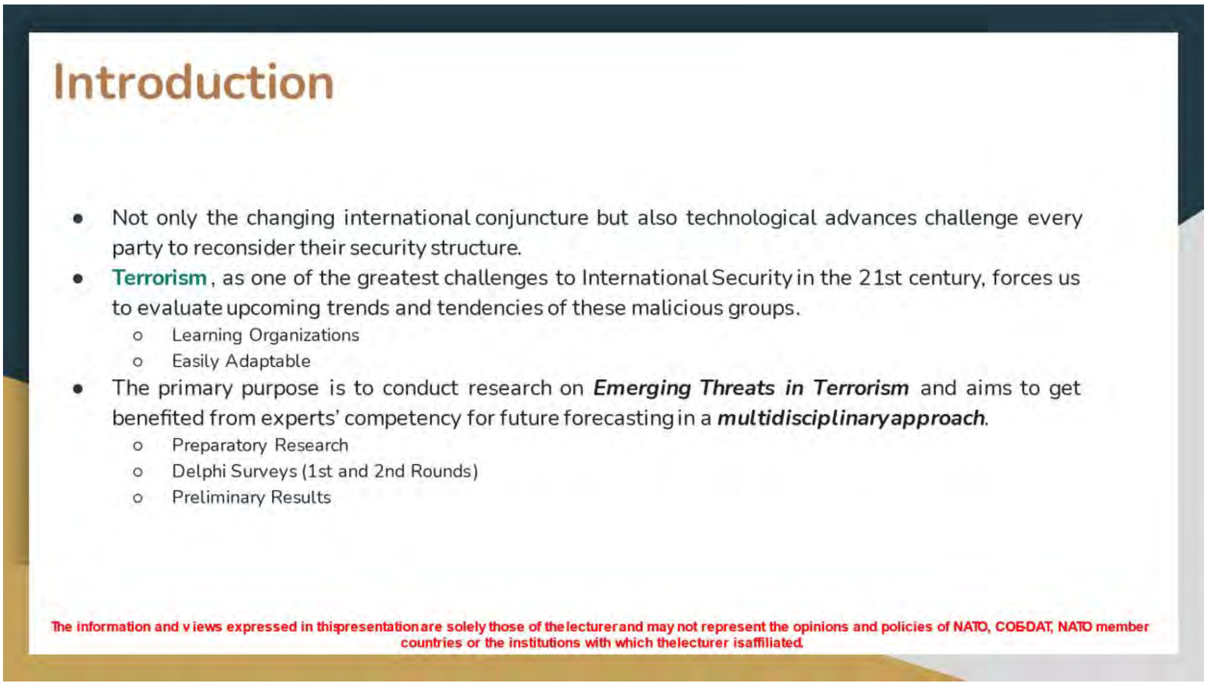
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Outline

- ✓ Introduction
- ✓ Methodology
- ✓ Main ResearchQuestion
- ✓ PreparatorySurvey
- ✓ SupportiveResearchQuestions
- ✓ Delphi Surveys

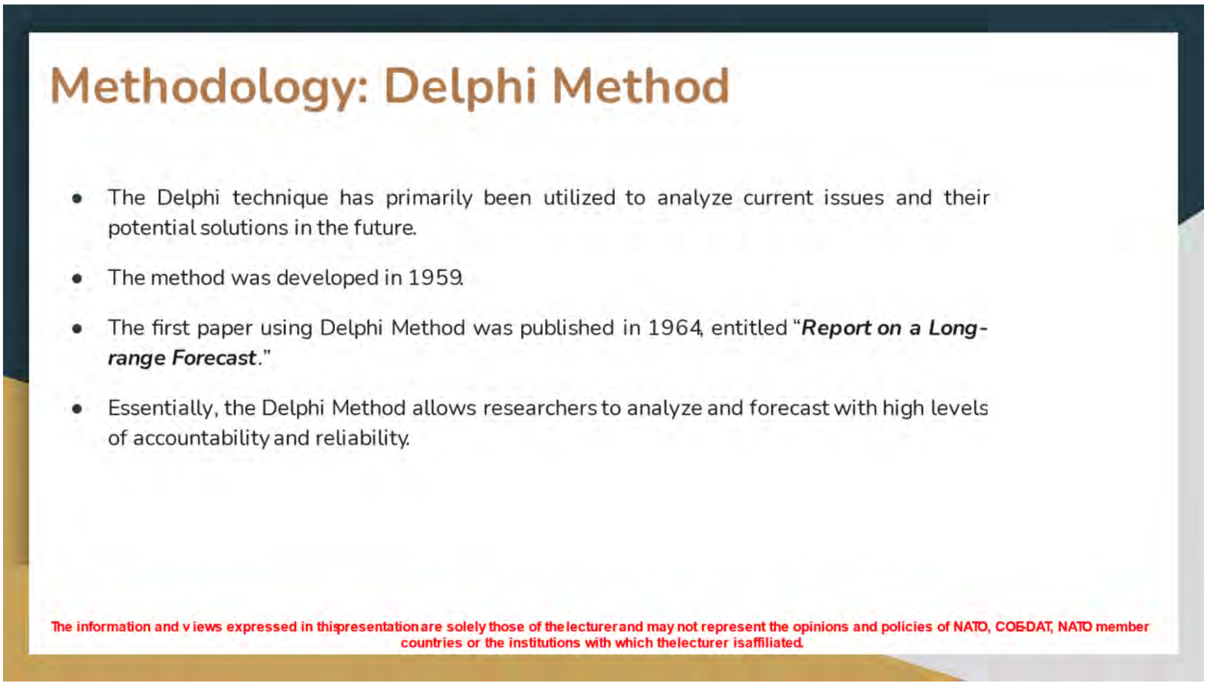
The information and v iews expressed in thispresentationare solely those of the lecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Introduction

- Not only the changing international conjuncture but also technological advances challenge every party to reconsider their security structure.
- Terrorism , as one of the greatest challenges to International Security in the 21st century, forces us to evaluate upcoming trends and tendencies of these malicious groups.
  - Learning Organizations
  - Easily Adaptable
- The primary purpose is to conduct research on ***Emerging Threats in Terrorism*** and aims to get benefited from experts' competency for future forecasting in a ***multidisciplinaryapproach***.
  - Preparatory Research
  - Delphi Surveys (1st and 2nd Rounds)
  - Preliminary Results

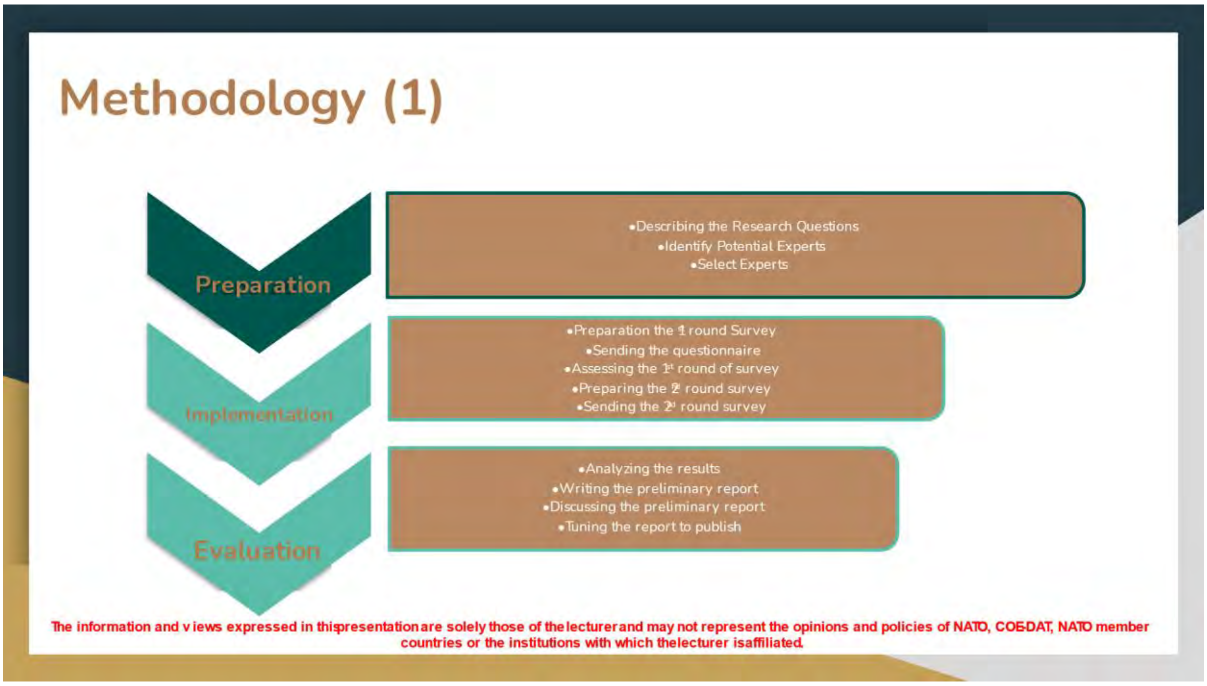
The information and v iews expressed in thispresentationare solely those of the lecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Methodology: Delphi Method

- The Delphi technique has primarily been utilized to analyze current issues and their potential solutions in the future.
- The method was developed in 1959.
- The first paper using Delphi Method was published in 1964, entitled "***Report on a Long-range Forecast***."
- Essentially, the Delphi Method allows researchers to analyze and forecast with high levels of accountability and reliability.

The information and v iews expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



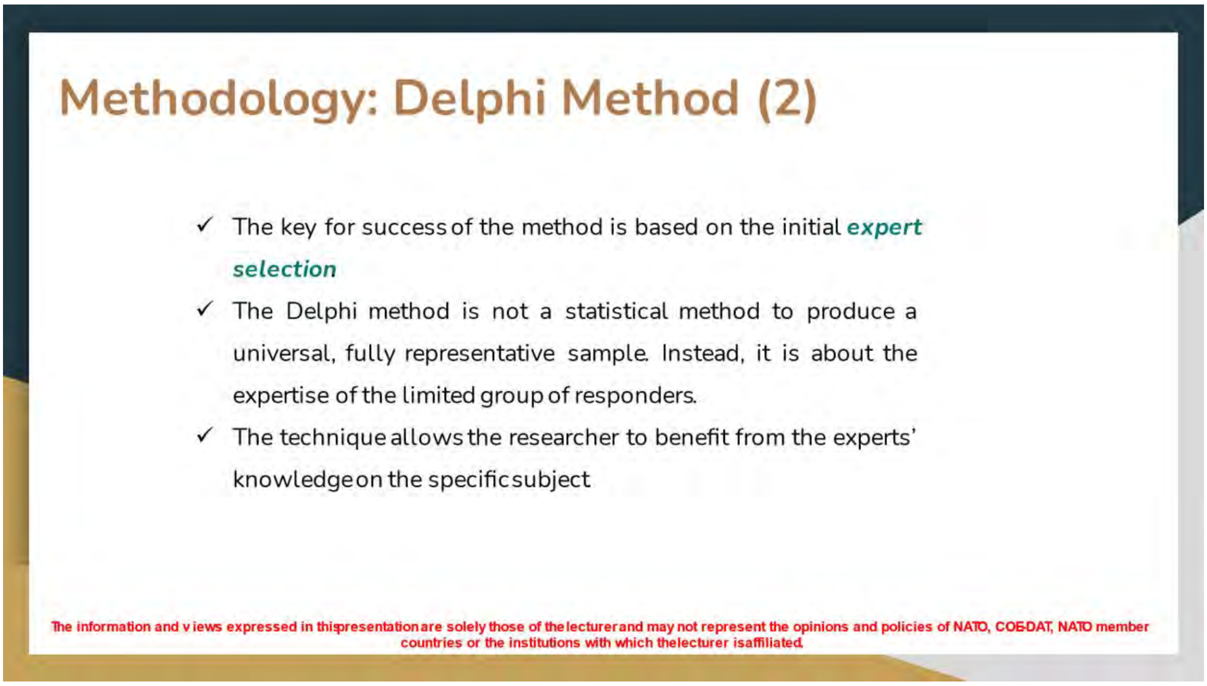
Methodology (1)

- •Describing the Research Questions
- •Identify Potential Experts
- •Select Experts

- •Preparation the 1st round Survey
- •Sending the questionnaire
- •Assessing the 1st round of survey
- •Preparing the 2nd round survey
- •Sending the 2nd round survey

- •Analyzing the results
- •Writing the preliminary report
- •Discussing the preliminary report
- •Tuning the report to publish

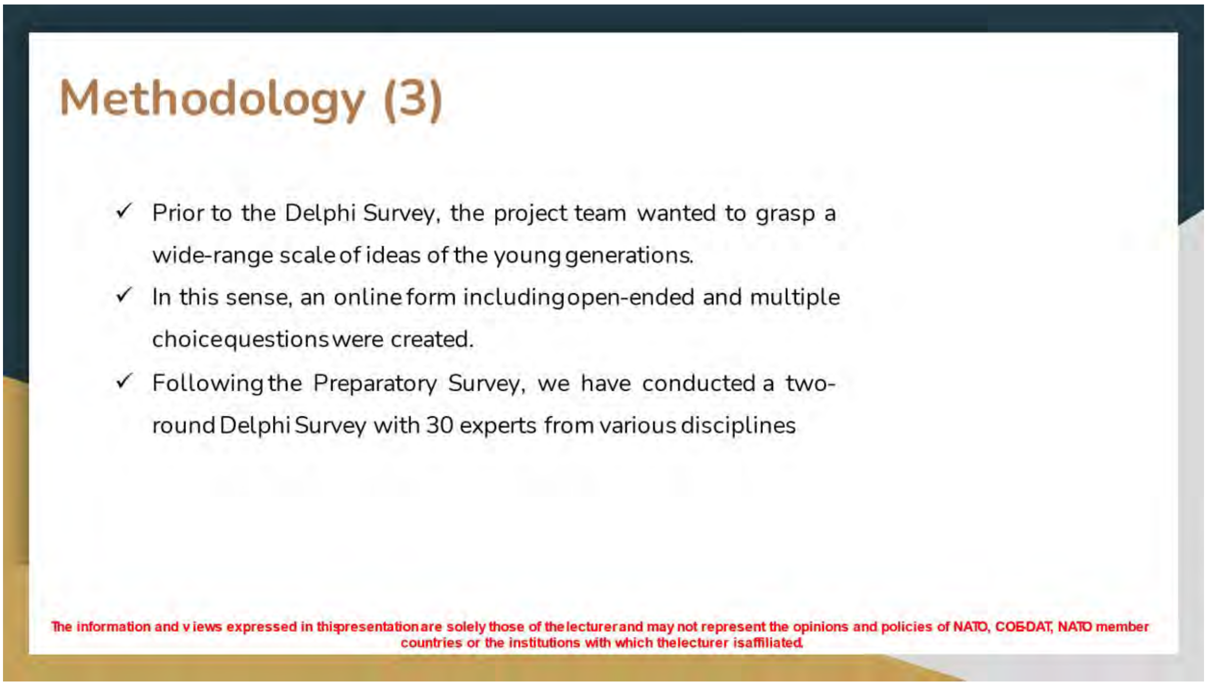
The information and v iews expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Methodology: Delphi Method (2)

- ✓ The key for success of the method is based on the initial ***expert selection***
- ✓ The Delphi method is not a statistical method to produce a universal, fully representative sample. Instead, it is about the expertise of the limited group of responders.
- ✓ The technique allows the researcher to benefit from the experts' knowledge on the specific subject

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Methodology (3)

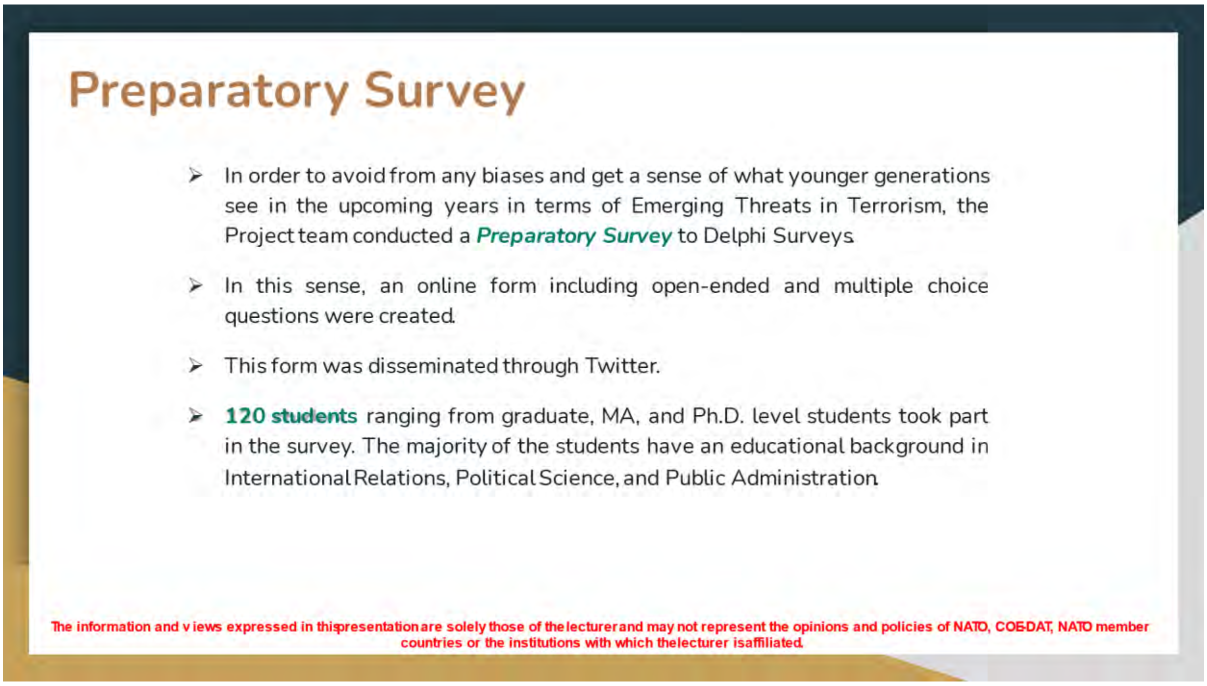
- ✓ Prior to the Delphi Survey, the project team wanted to grasp a wide-range scale of ideas of the young generations.
- ✓ In this sense, an online form including open-ended and multiple choice questions were created.
- ✓ Following the Preparatory Survey, we have conducted a two-round Delphi Survey with 30 experts from various disciplines

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Main Research Question

«What are the emerging threats in the future from European and Asian perspectives in terms of terrorism? »

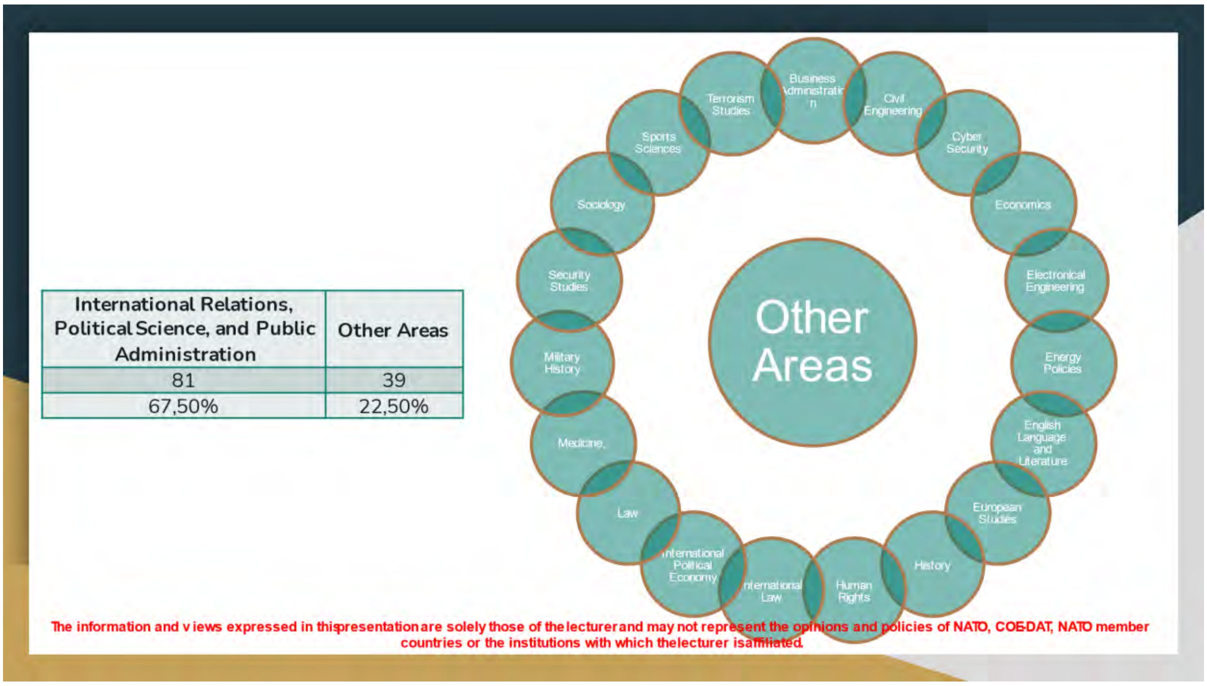
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Preparatory Survey

- In order to avoid from any biases and get a sense of what younger generations see in the upcoming years in terms of Emerging Threats in Terrorism, the Project team conducted a ***Preparatory Survey*** to Delphi Surveys.
- In this sense, an online form including open-ended and multiple choice questions were created.
- This form was disseminated through Twitter.
- **120 students** ranging from graduate, MA, and Ph.D. level students took part in the survey. The majority of the students have an educational background in International Relations, Political Science, and Public Administration.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

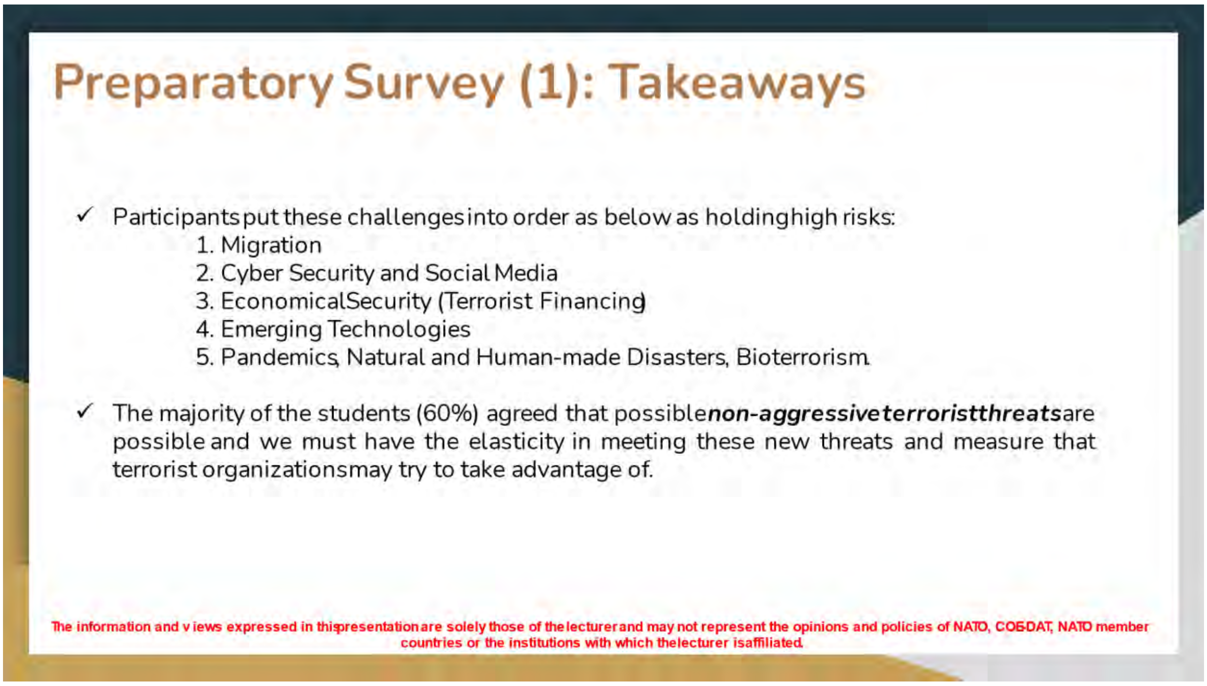


International Relations, Political Science, and Public Administration	Other Areas
81	39
67,50%	22,50%

Other Areas

Business Administration
Civil Engineering
Cyber Security
Economics
Electronical Engineering
Energy Policies
English Language and Literature
European Studies
History
Human Rights
nternational Law
nternational Political Economy
Law
Medicine,
Military History
Security Studies
Sociology
Sports Sciences
Terrorism Studies

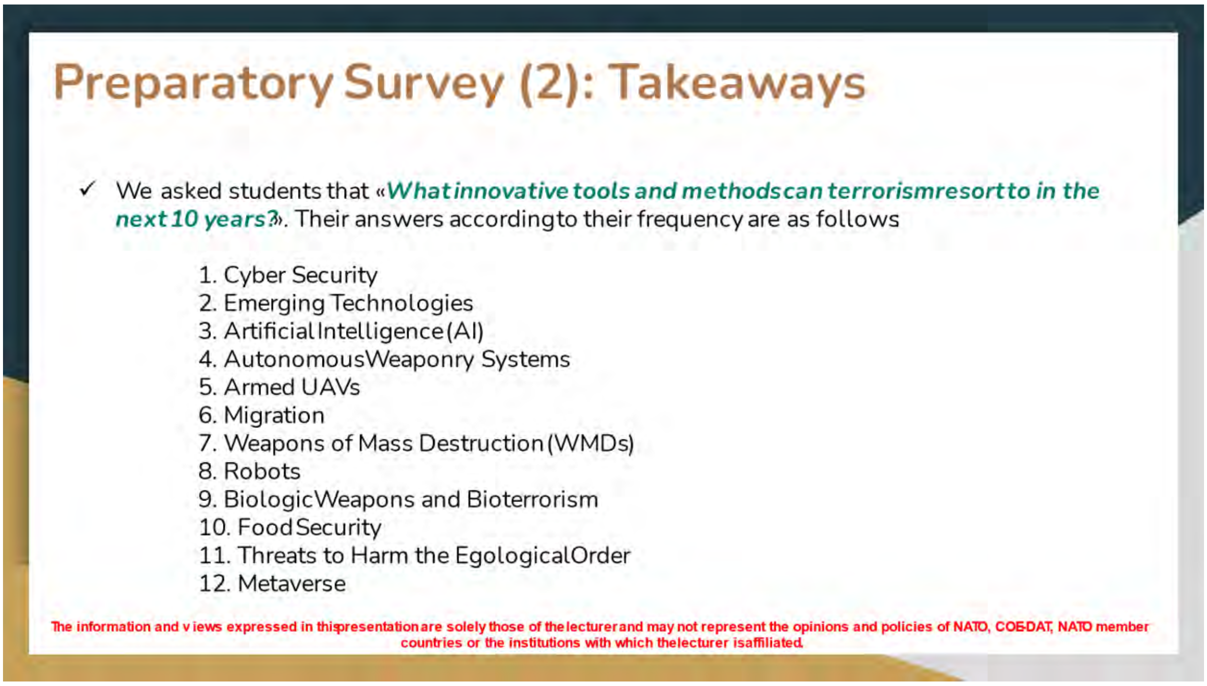
The information and v iews expressed in thispresentationare solely those of the lecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Preparatory Survey (1): Takeaways

- ✓ Participants put these challenges into order as below as holding high risks:
  1. Migration
  2. Cyber Security and Social Media
  3. Economical Security (Terrorist Financing)
  4. Emerging Technologies
  5. Pandemics, Natural and Human-made Disasters, Bioterrorism.
- ✓ The majority of the students (60%) agreed that possible ***non-aggressive terrorist threats*** are possible and we must have the elasticity in meeting these new threats and measure that terrorist organizations may try to take advantage of.

The information and v iews expressed in thispresentationare solely those of the lecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.

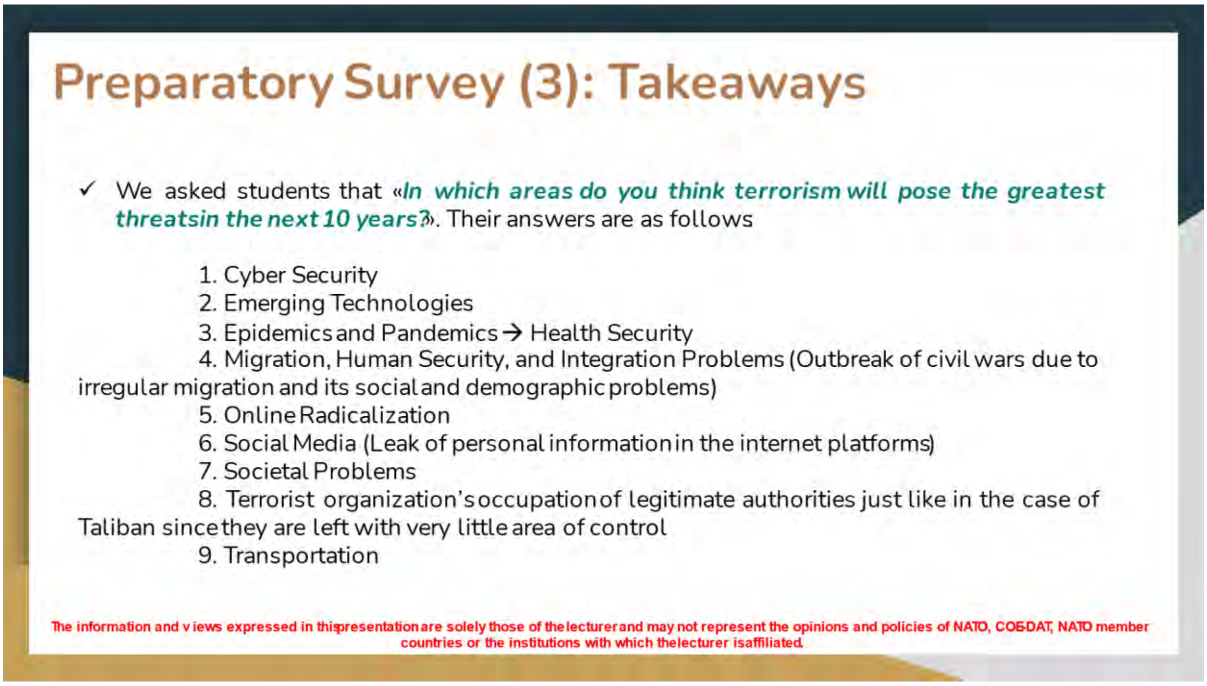


Preparatory Survey (2): Takeaways

✓ We asked students that «*What innovative tools and methods can terrorism resort to in the next 10 years?*». Their answers according to their frequency are as follows

1. Cyber Security
2. Emerging Technologies
3. Artificial Intelligence (AI)
4. Autonomous Weaponry Systems
5. Armed UAVs
6. Migration
7. Weapons of Mass Destruction (WMDs)
8. Robots
9. Biologic Weapons and Bioterrorism
10. Food Security
11. Threats to Harm the Egological Order
12. Metaverse

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

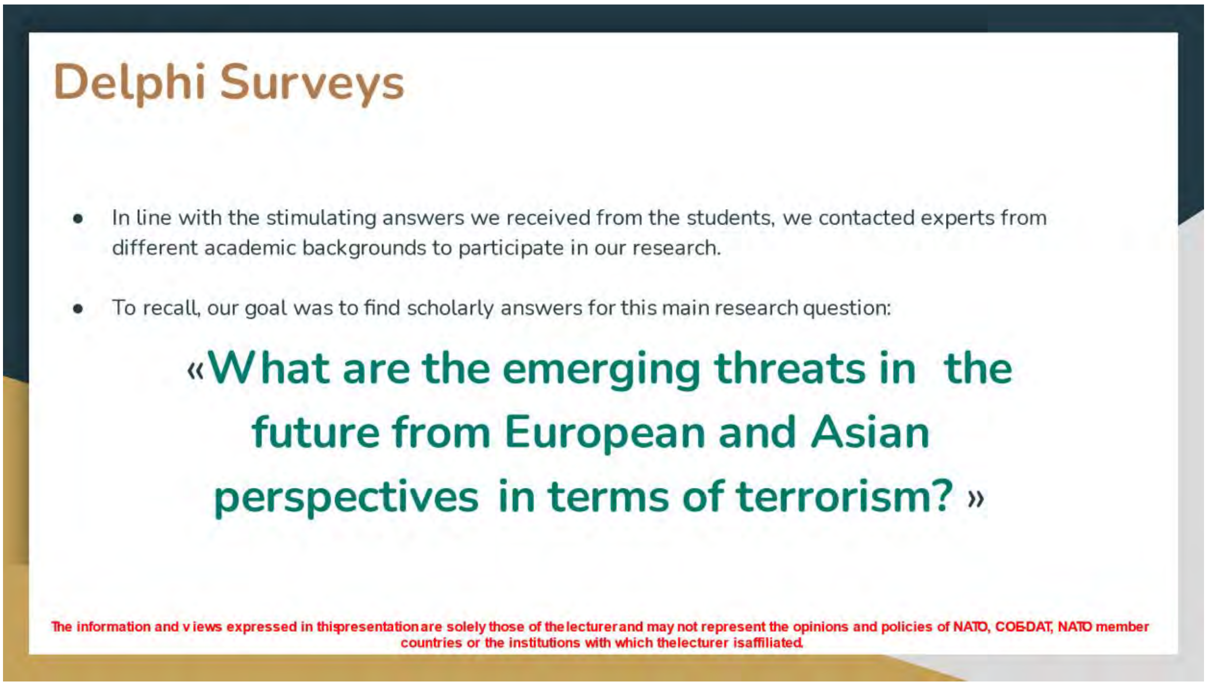


Preparatory Survey (3): Takeaways

✓ We asked students that «*In which areas do you think terrorism will pose the greatest threats in the next 10 years?*». Their answers are as follows

1. Cyber Security
2. Emerging Technologies
3. Epidemics and Pandemics → Health Security
4. Migration, Human Security, and Integration Problems (Outbreak of civil wars due to irregular migration and its social and demographic problems)
5. Online Radicalization
6. Social Media (Leak of personal information in the internet platforms)
7. Societal Problems
8. Terrorist organization's occupation of legitimate authorities just like in the case of Taliban since they are left with very little area of control
9. Transportation

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

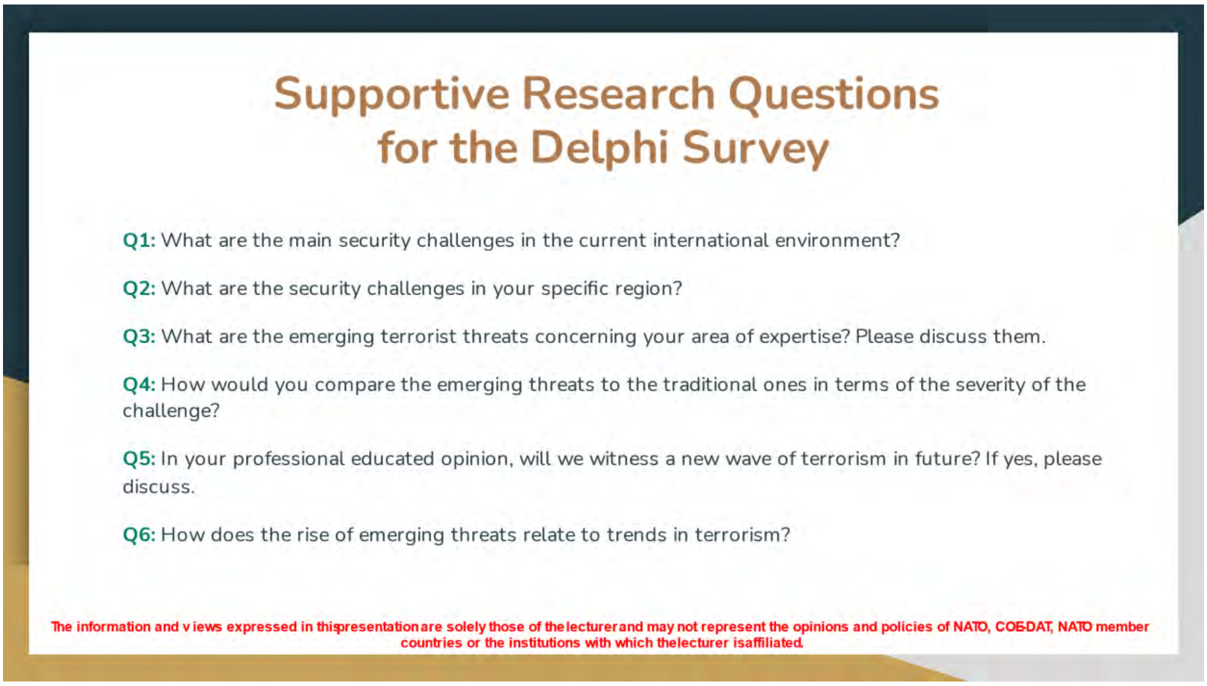


Delphi Surveys

- In line with the stimulating answers we received from the students, we contacted experts from different academic backgrounds to participate in our research.
- To recall, our goal was to find scholarly answers for this main research question:

«What are the emerging threats in the future from European and Asian perspectives in terms of terrorism? »

The information and v iews expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Supportive Research Questions for the Delphi Survey

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

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

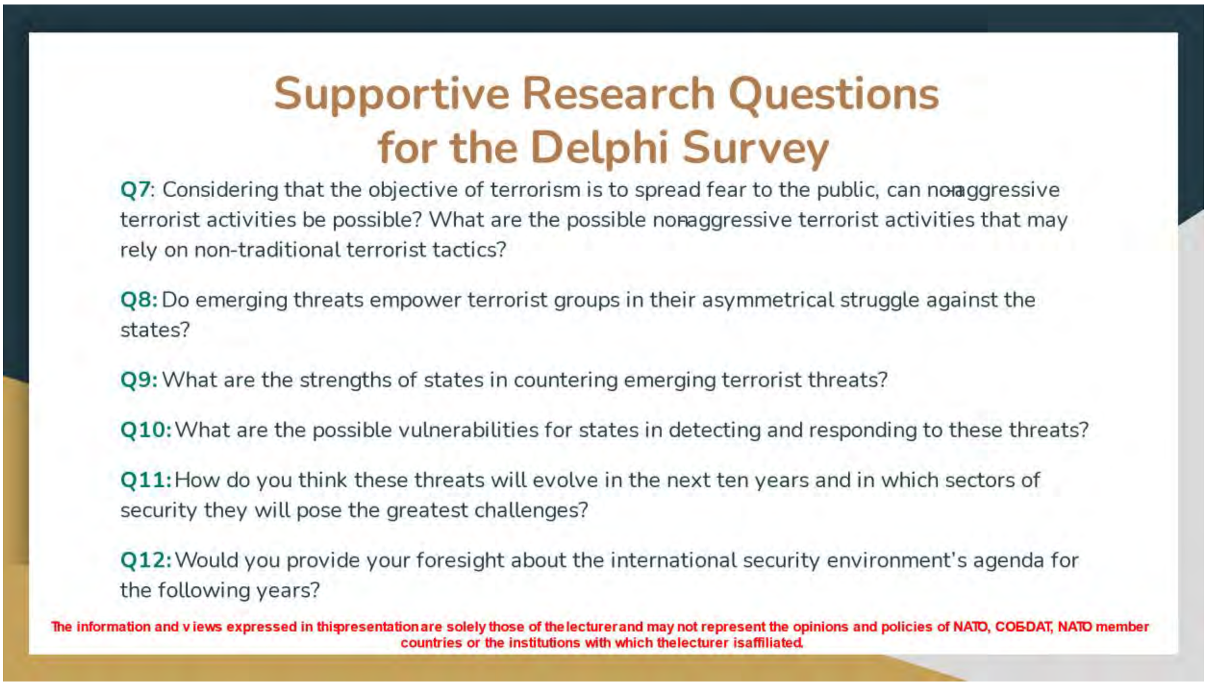
Q3: What are the emerging terrorist threats concerning your area of expertise? Please discuss them.

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

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

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

The information and v iews expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Supportive Research Questions for the Delphi Survey

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

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

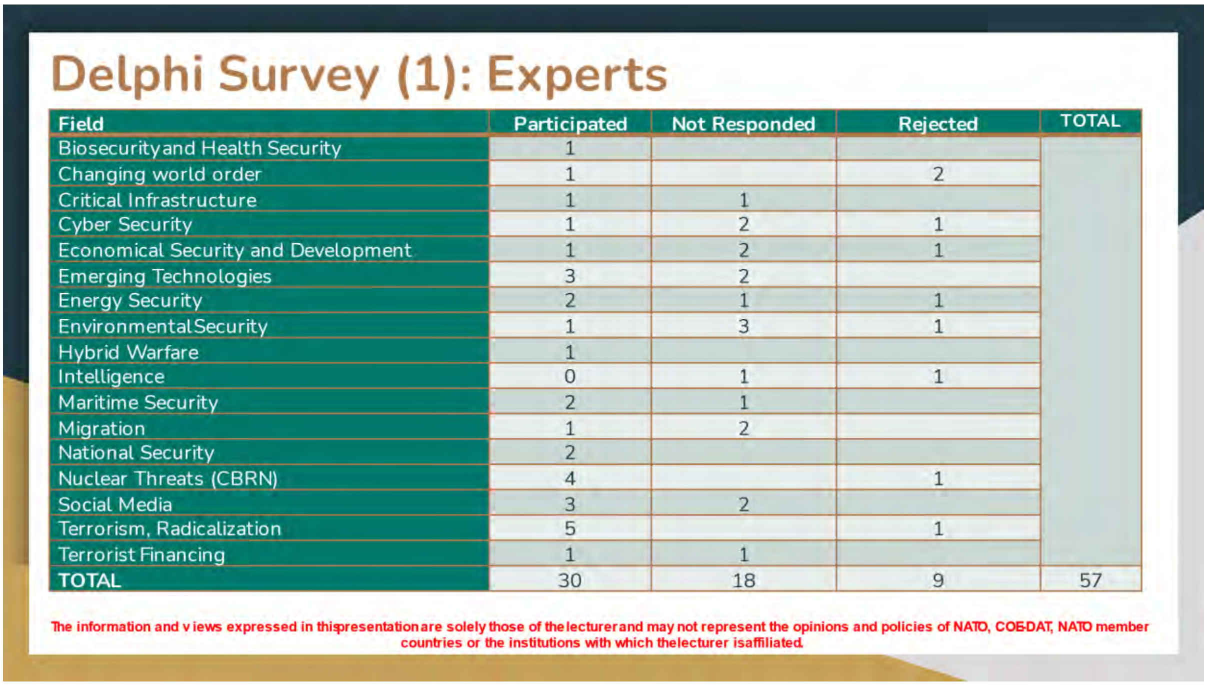
Q9: What are the strengths of states in countering emerging terrorist threats?

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

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

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

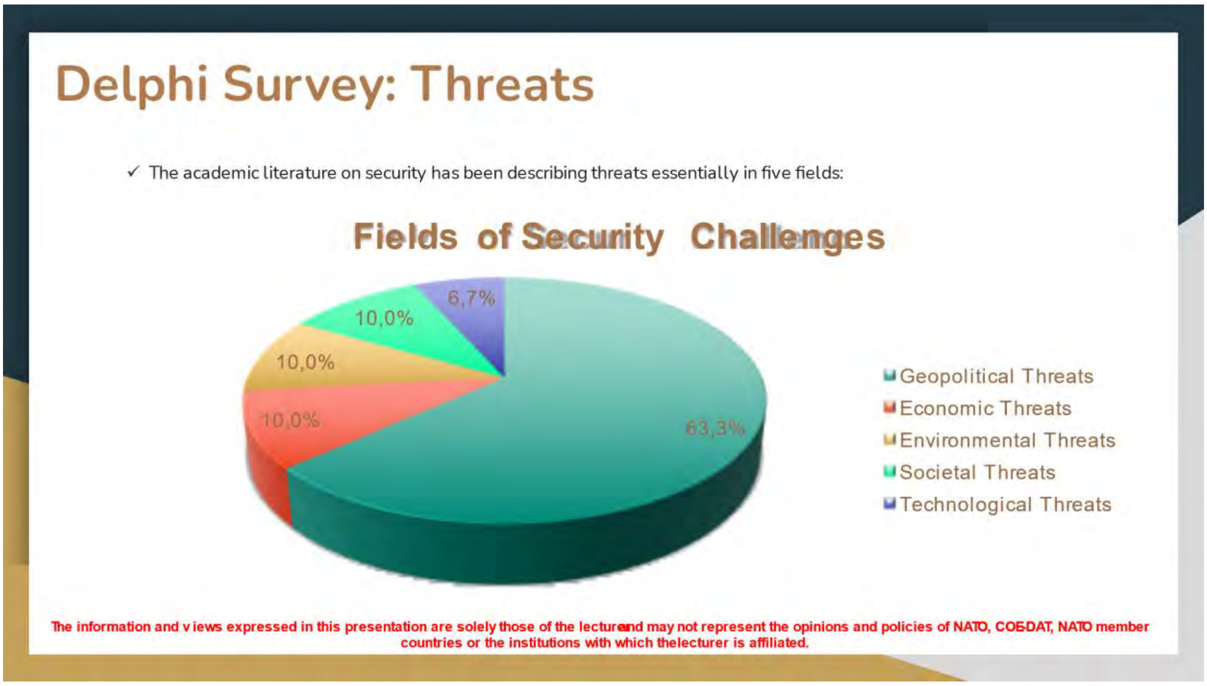
The information and v iews expressed in thispresentationare solely those of the lecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Delphi Survey (1): Experts

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

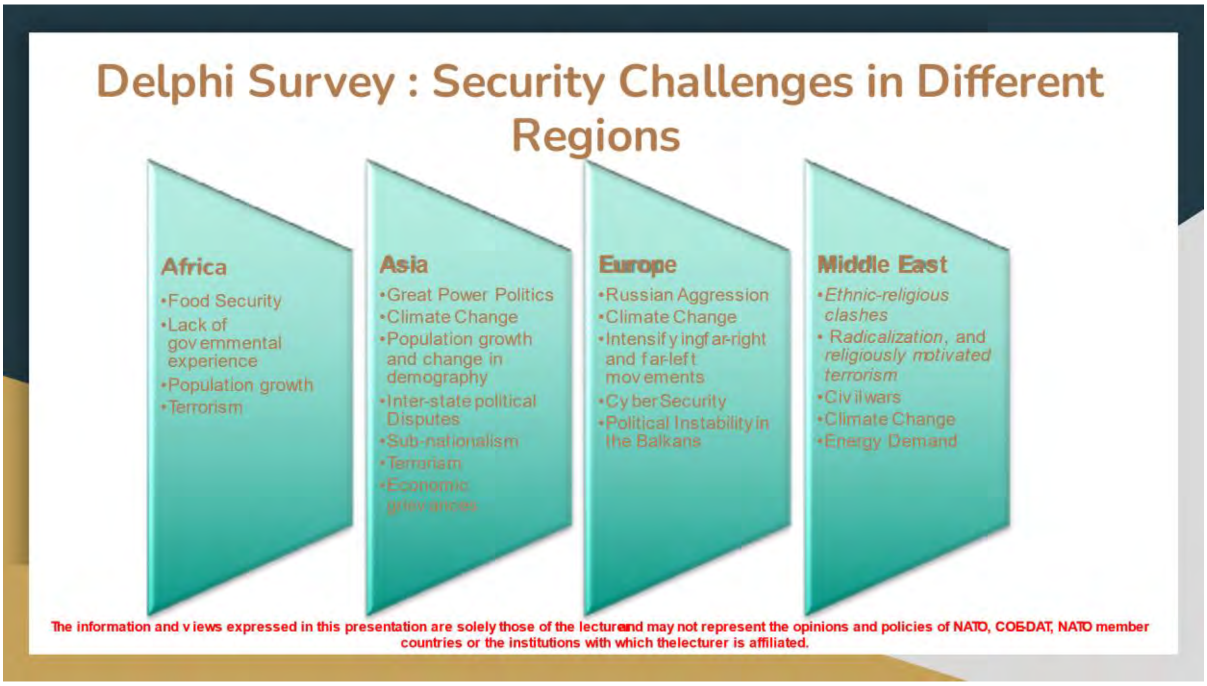
The information and v iews expressed in thispresentationare solely those of the lecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Delphi Survey: Threats

✓ The academic literature on security has been describing threats essentially in five fields:

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Delphi Survey : Security Challenges in Different Regions

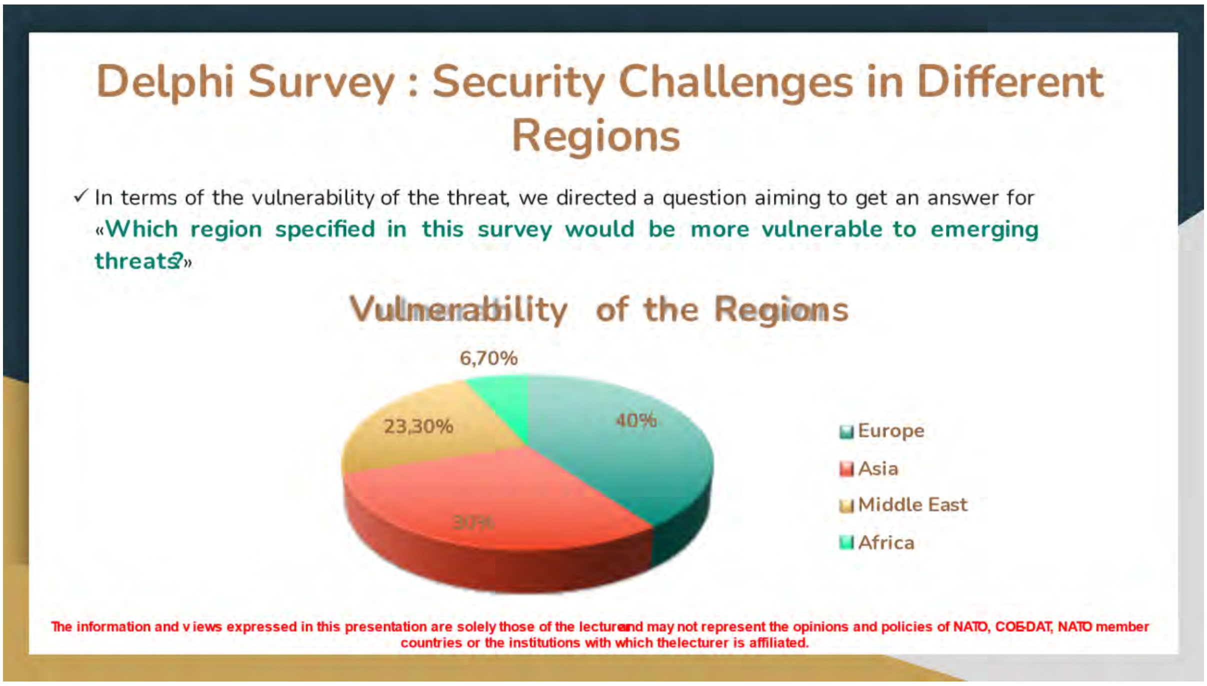
Africa
- Food Security
- Lack of governmental experience
- Population growth
- Terrorism

Asia
- Great Power Politics
- Climate Change
- Population growth and change in demography
- Inter-state political Disputes
- Sub-nationalism
- Terrorism
- Economic grievances

Europe
- Russian Aggression
- Climate Change
- Intensifying far-right and far-left movements
- Cyber Security
- Political Instability in the Balkans

Middle East
- *Ethnic-religious clashes*
- *Radicalization*, and *religiously motivated terrorism*
- Civil wars
- Climate Change
- Energy Demand

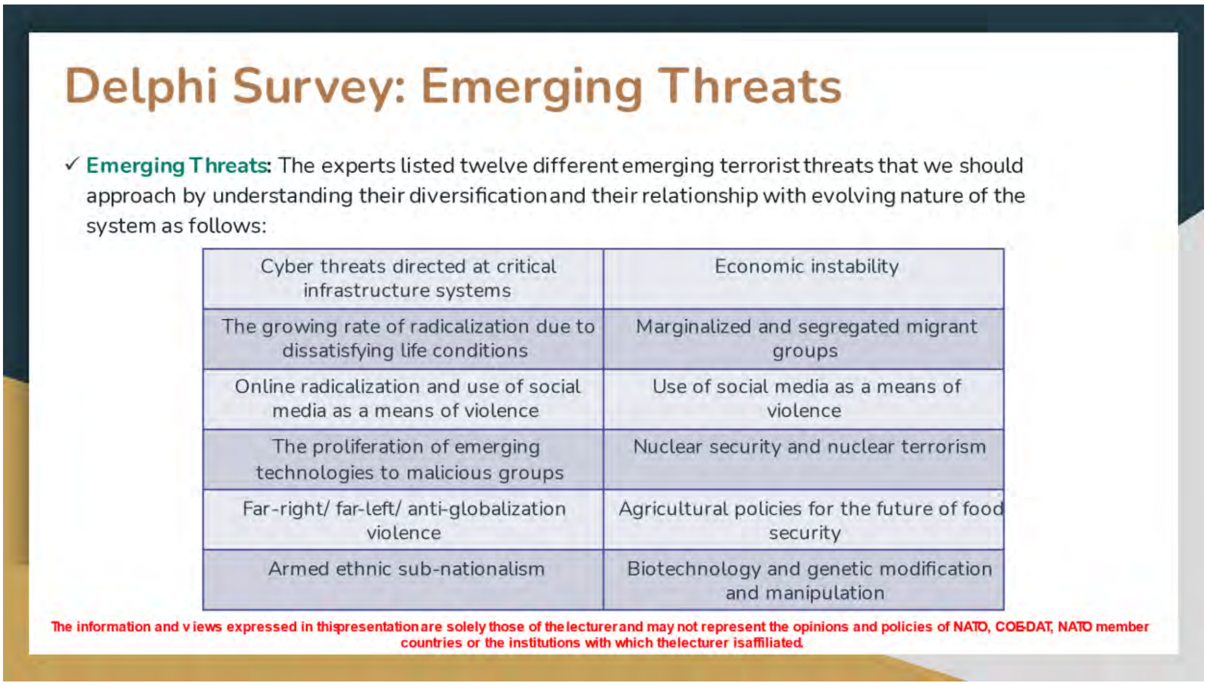
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Delphi Survey : Security Challenges in Different Regions

✓ In terms of the vulnerability of the threat, we directed a question aiming to get an answer for «**Which region specified in this survey would be more vulnerable to emerging threats?**»

The information and views expressed in this presentation are solely those of the lectureand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer is affiliated.

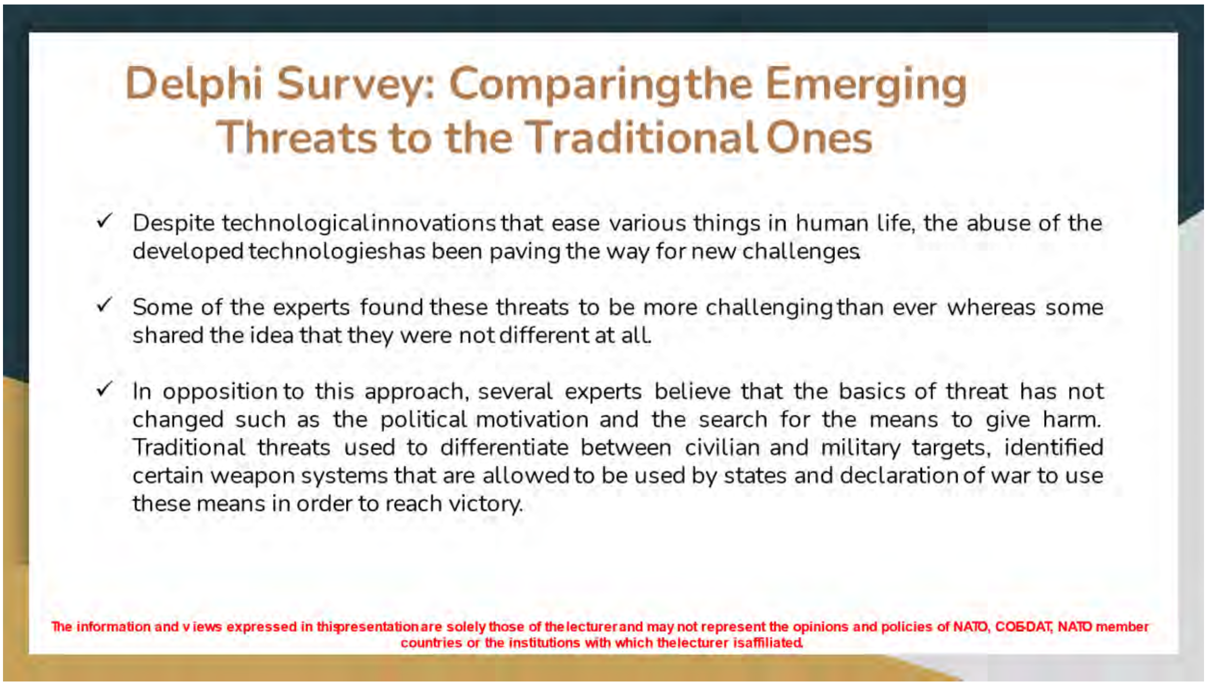


Delphi Survey: Emerging Threats

✓ **Emerging Threats:** The experts listed twelve different emerging terrorist threats that we should approach by understanding their diversification and their relationship with evolving nature of the system as follows:

Cyber threats directed at critical infrastructure systems	Economic instability
The growing rate of radicalization due to dissatisfying life conditions	Marginalized and segregated migrant groups
Online radicalization and use of social media as a means of violence	Use of social media as a means of violence
The proliferation of emerging technologies to malicious groups	Nuclear security and nuclear terrorism
Far-right/ far-left/ anti-globalization violence	Agricultural policies for the future of food security
Armed ethnic sub-nationalism	Biotechnology and genetic modification and manipulation

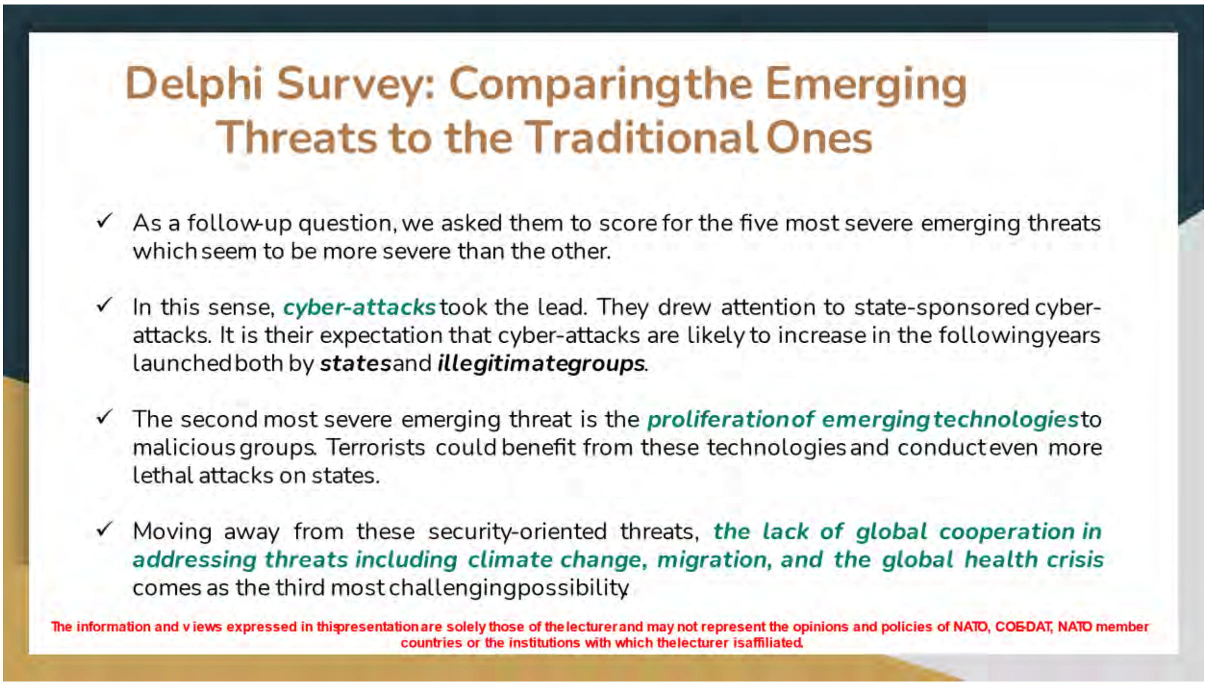
The information and views expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Delphi Survey: Comparingthe Emerging Threats to the Traditional Ones

- ✓ Despite technologicalinnovations that ease various things in human life, the abuse of the developed technologieshas been paving the way for new challenges.
- ✓ Some of the experts found these threats to be more challengingthan ever whereas some shared the idea that they were not different at all.
- ✓ In opposition to this approach, several experts believe that the basics of threat has not changed such as the political motivation and the search for the means to give harm. Traditional threats used to differentiate between civilian and military targets, identified certain weapon systems that are allowed to be used by states and declaration of war to use these means in order to reach victory.

The information and views expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Delphi Survey: Comparingthe Emerging Threats to the Traditional Ones

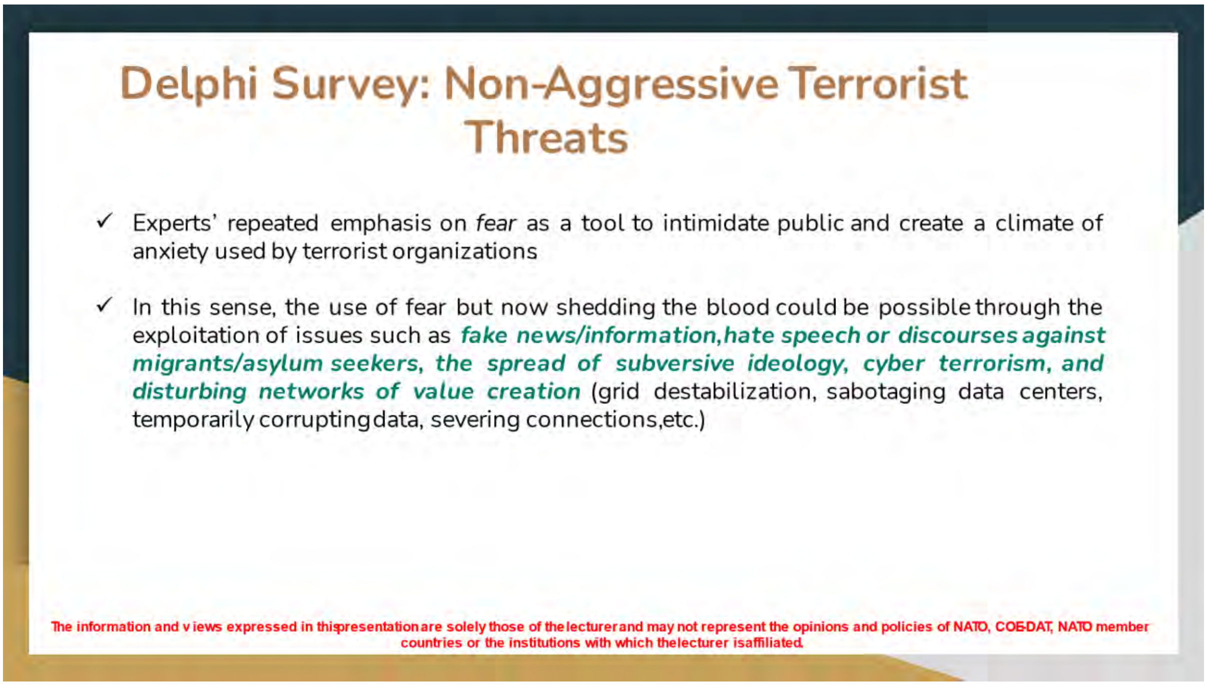
- ✓ As a follow-up question, we asked them to score for the five most severe emerging threats which seem to be more severe than the other.
- ✓ In this sense, ***cyber-attacks*** took the lead. They drew attention to state-sponsored cyber-attacks. It is their expectation that cyber-attacks are likely to increase in the followingyears launched both by ***states*** and ***illegitimategroups***.
- ✓ The second most severe emerging threat is the ***proliferationof emerging technologies*** to malicious groups. Terrorists could benefit from these technologies and conduct even more lethal attacks on states.
- ✓ Moving away from these security-oriented threats, ***the lack of global cooperation in addressing threats including climate change, migration, and the global health crisis*** comes as the third most challengingpossibility.

The information and views expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.

Delphi Survey: Comparing the Emerging Threats to the Traditional Ones

- ✓ These are followed by the challenges posed by ***infectious diseases to health and livestock*** The risk is that biotechnology can be used to accelerate such threats. Furthermore, we can categorize infectious diseases in this sense.
- ✓ Turning back to threats that challenge national security structures, the experts drew attention to the spread of ***far-right, far-left, and anti-globalization extremist movements***
- ✓ As the last scenario, experts reminded ***nuclear terrorism*** However, some of the experts made a differentiation and stated that nuclear challenges can be either from terrorist groups or states, stressing that state-nuclear terrorism can be much more severe than traditional nuclear terrorism because a state like Russia has more military means at its disposal than non-state actors.

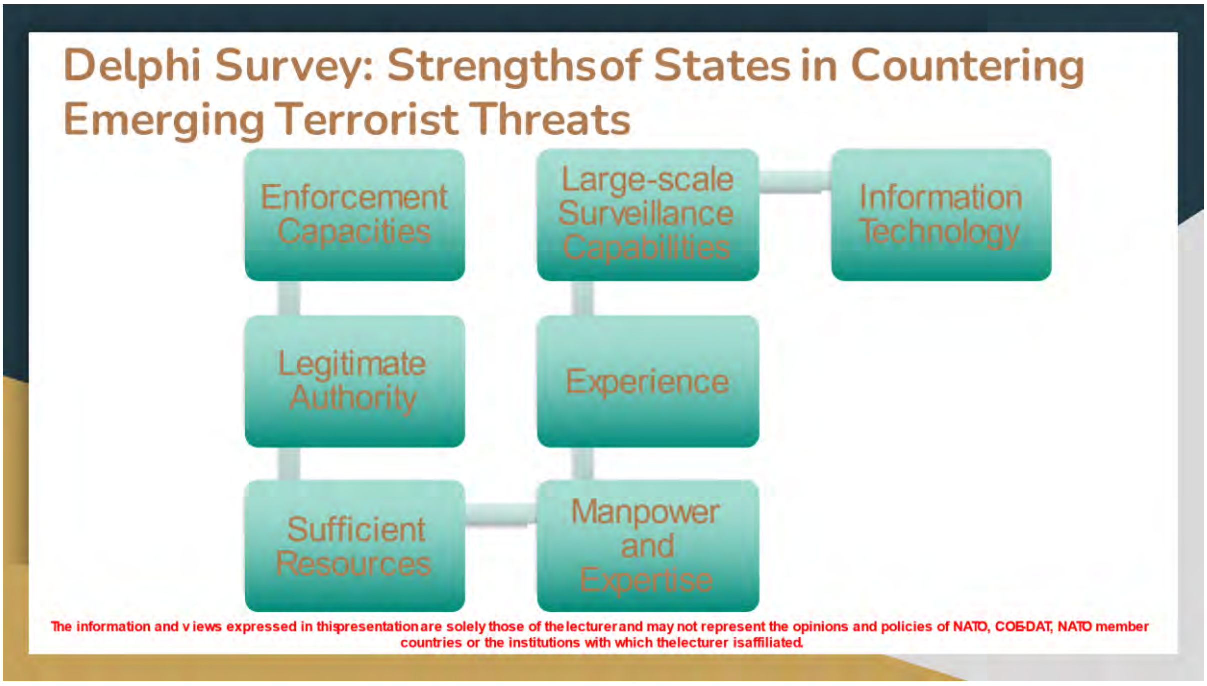
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Delphi Survey: Non-Aggressive Terrorist Threats

- ✓ Experts' repeated emphasis on *fear* as a tool to intimidate public and create a climate of anxiety used by terrorist organizations
- ✓ In this sense, the use of fear but now shedding the blood could be possible through the exploitation of issues such as ***fake news/information, hate speech or discourses against migrants/asylum seekers, the spread of subversive ideology, cyber terrorism, and disturbing networks of value creation*** (grid destabilization, sabotaging data centers, temporarily corrupting data, severing connections, etc.)

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Delphi Survey: Strengthsof States in Countering Emerging Terrorist Threats

Enforcement Capacities

Legitimate Authority

Sufficient Resources

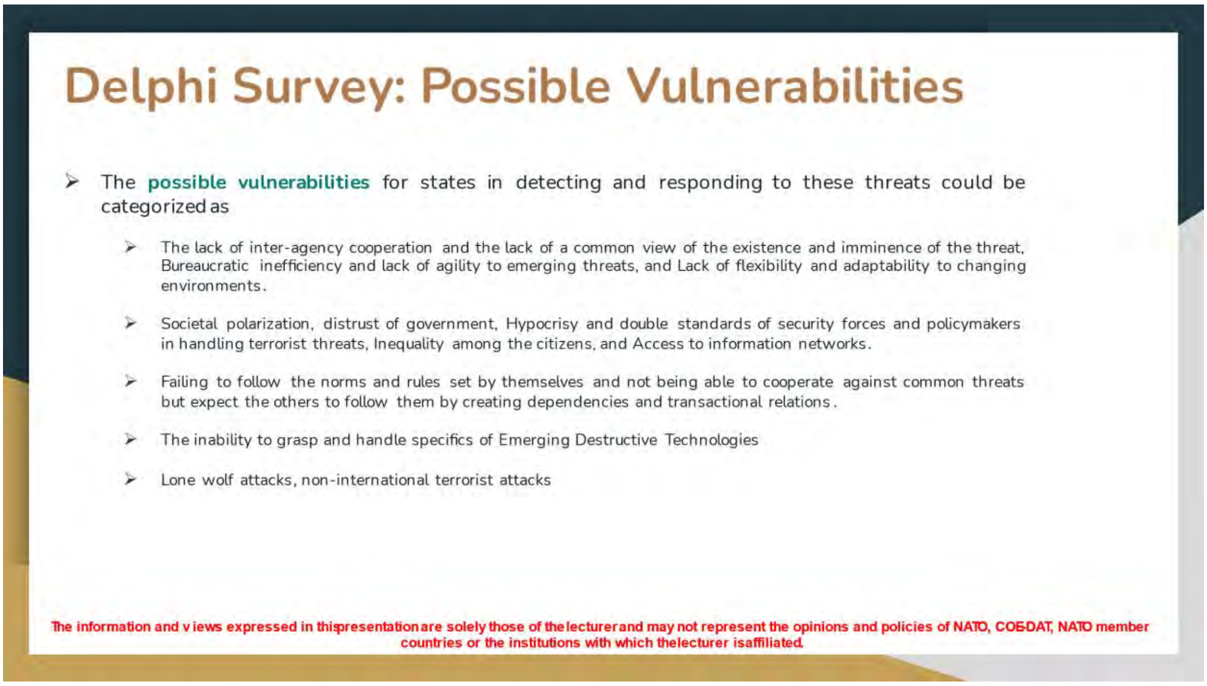
Manpower and Expertise

Experience

Large-scale Surveillance Capabilities

Information Technology

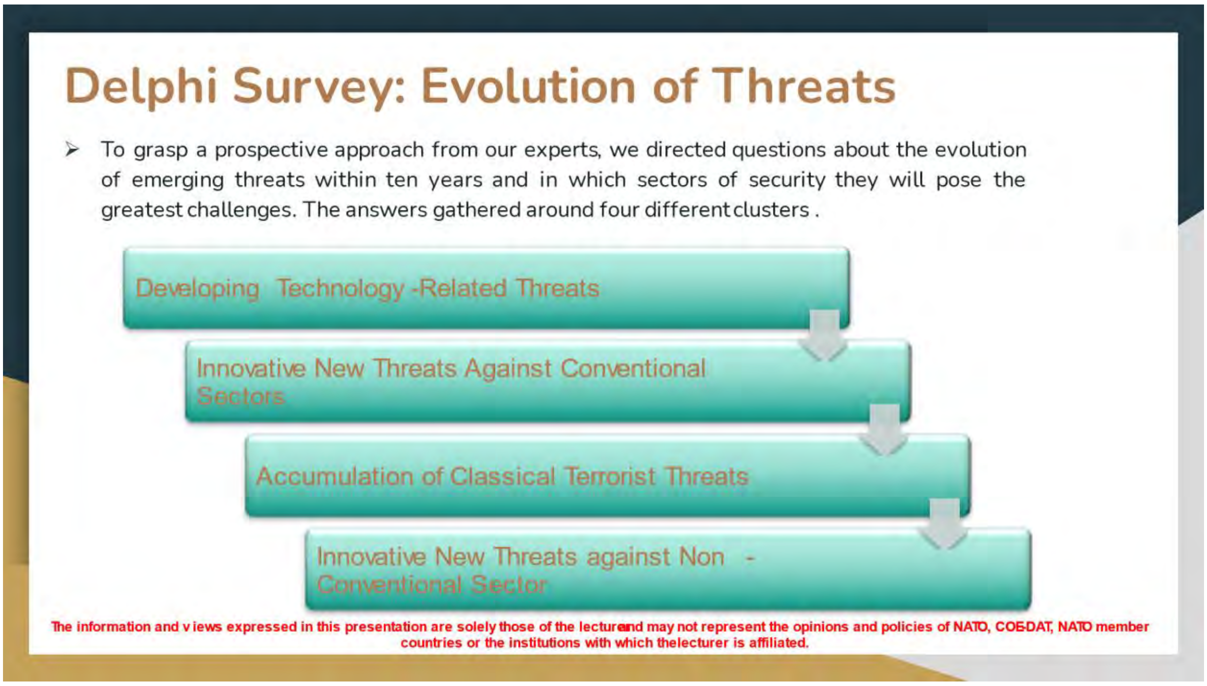
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Delphi Survey: Possible Vulnerabilities

- The **possible vulnerabilities** for states in detecting and responding to these threats could be categorized as
  - The lack of inter-agency cooperation and the lack of a common view of the existence and imminence of the threat, Bureaucratic inefficiency and lack of agility to emerging threats, and Lack of flexibility and adaptability to changing environments.
  - Societal polarization, distrust of government, Hypocrisy and double standards of security forces and policymakers in handling terrorist threats, Inequality among the citizens, and Access to information networks.
  - Failing to follow the norms and rules set by themselves and not being able to cooperate against common threats but expect the others to follow them by creating dependencies and transactional relations.
  - The inability to grasp and handle specifics of Emerging Destructive Technologies
  - Lone wolf attacks, non-international terrorist attacks

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Delphi Survey: Evolution of Threats

- To grasp a prospective approach from our experts, we directed questions about the evolution of emerging threats within ten years and in which sectors of security they will pose the greatest challenges. The answers gathered around four different clusters .

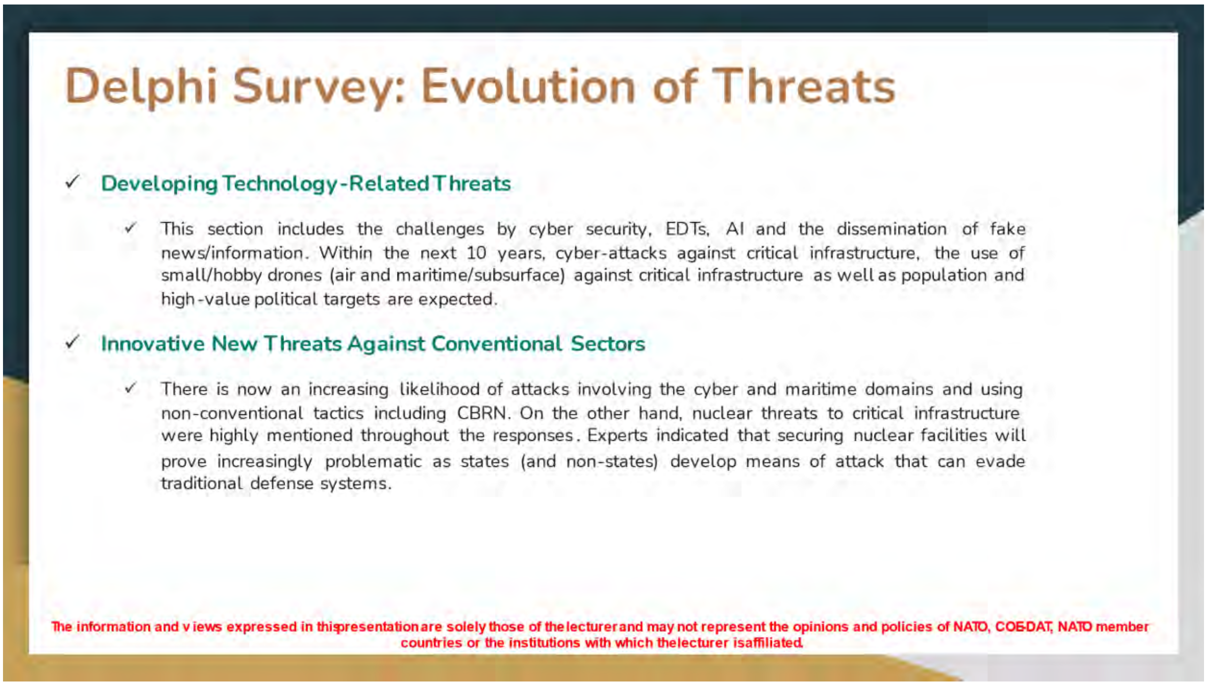
Developing Technology -Related Threats

Innovative New Threats Against Conventional Sectors

Accumulation of Classical Terrorist Threats

Innovative New Threats against Non - Conventional Sector

The information and views expressed in this presentation are solely those of the lecturand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer is affiliated.



Delphi Survey: Evolution of Threats

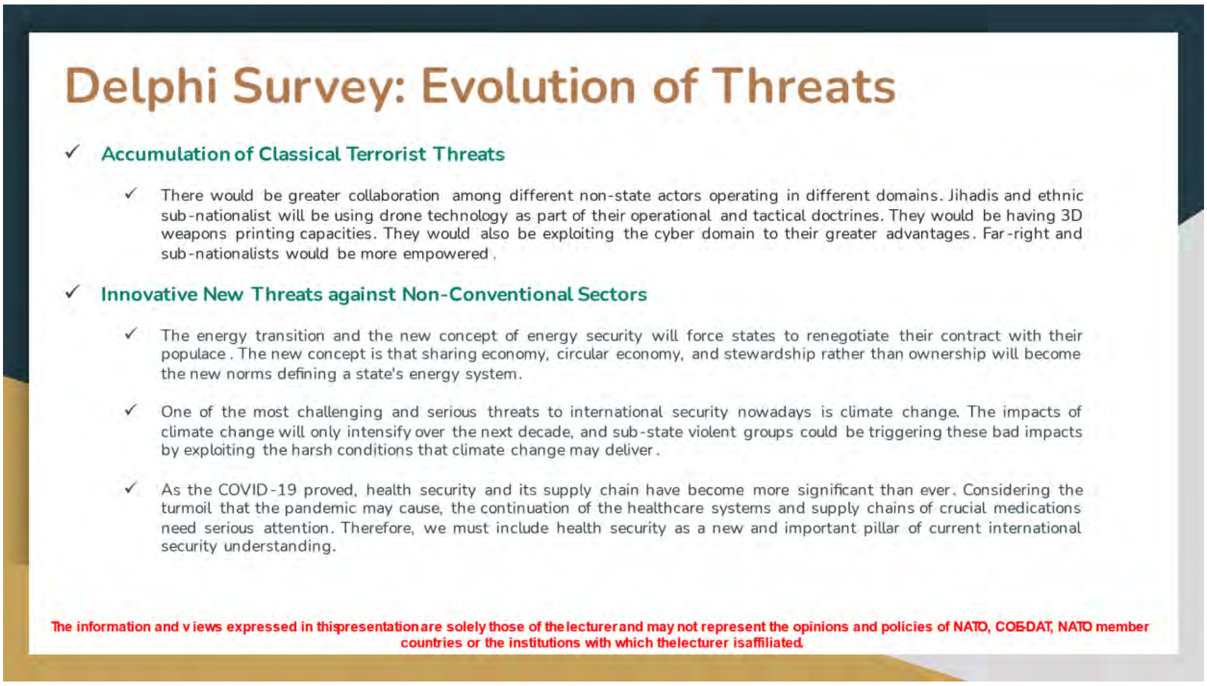
✓ **Developing Technology-Related Threats**

✓ This section includes the challenges by cyber security, EDTs, AI and the dissemination of fake news/information. Within the next 10 years, cyber-attacks against critical infrastructure, the use of small/hobby drones (air and maritime/subsurface) against critical infrastructure as well as population and high-value political targets are expected.

✓ **Innovative New Threats Against Conventional Sectors**

✓ There is now an increasing likelihood of attacks involving the cyber and maritime domains and using non-conventional tactics including CBRN. On the other hand, nuclear threats to critical infrastructure were highly mentioned throughout the responses. Experts indicated that securing nuclear facilities will prove increasingly problematic as states (and non-states) develop means of attack that can evade traditional defense systems.

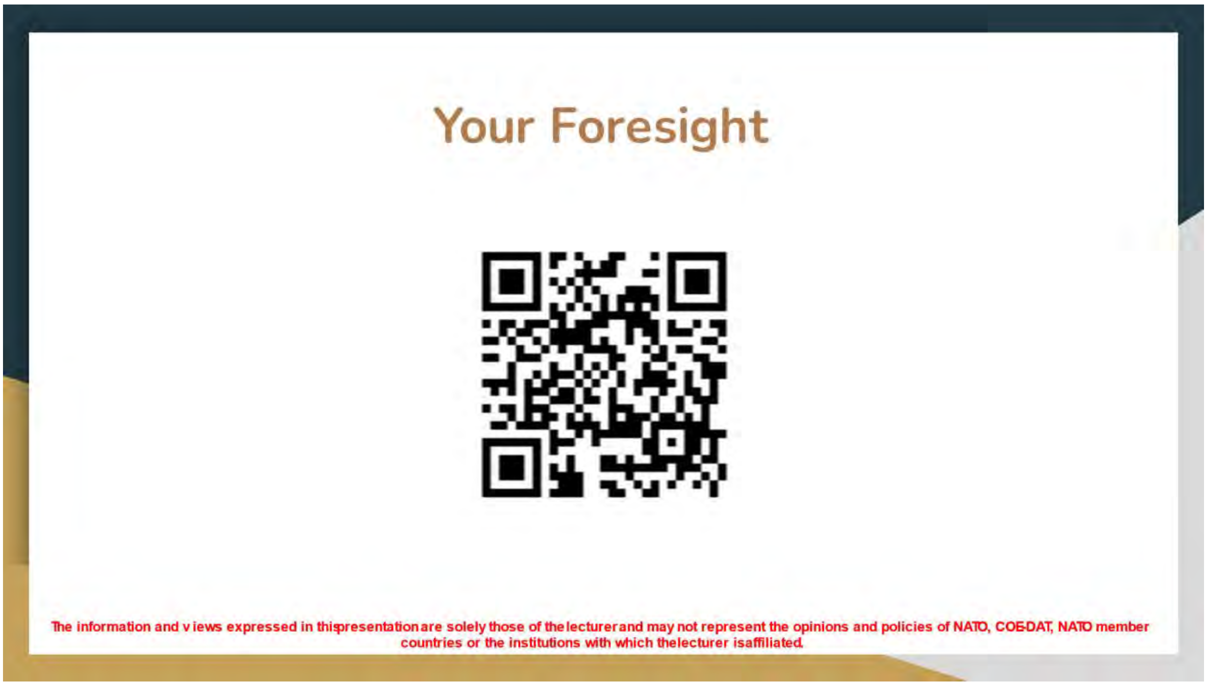
The information and views expressed in thispresentationare solely those of thelecturerand may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which thelecturer isaffiliated.



Delphi Survey: Evolution of Threats

- ✓ Accumulation of Classical Terrorist Threats
  - ✓ There would be greater collaboration among different non-state actors operating in different domains. Jihadis and ethnic sub-nationalist will be using drone technology as part of their operational and tactical doctrines. They would be having 3D weapons printing capacities. They would also be exploiting the cyber domain to their greater advantages. Far-right and sub-nationalists would be more empowered.
- ✓ Innovative New Threats against Non-Conventional Sectors
  - ✓ The energy transition and the new concept of energy security will force states to renegotiate their contract with their populace. The new concept is that sharing economy, circular economy, and stewardship rather than ownership will become the new norms defining a state's energy system.
  - ✓ One of the most challenging and serious threats to international security nowadays is climate change. The impacts of climate change will only intensify over the next decade, and sub-state violent groups could be triggering these bad impacts by exploiting the harsh conditions that climate change may deliver.
  - ✓ As the COVID-19 proved, health security and its supply chain have become more significant than ever. Considering the turmoil that the pandemic may cause, the continuation of the healthcare systems and supply chains of crucial medications need serious attention. Therefore, we must include health security as a new and important pillar of current international security understanding.

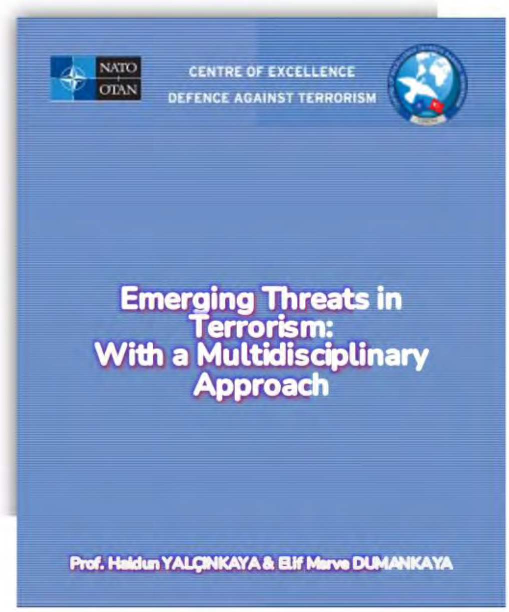
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Your Foresight

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Research Project Preliminary Results



NATO OTAN

CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

Emerging Threats in Terrorism: With a Multidisciplinary Approach

Prof. Haldun YALÇINKAYA & Elif Merve DUMANKAYA

Terrorism Experts Conference 2022

October 18-19, 2022

Critical Infrastructure Security and Resilience (CISR) / Advanced CISR Protection from Terrorist Attacks

Mr. Ronald BEARSE

Mr. Ronald Bearse, who has been a long-time academic advisor and lecturer at COEDAT provided an overview of COEDAT's new Basic and Advanced Courses on Critical Infrastructure Security and Resilience Against Terrorists Attacks (CISRATA) Courses. He began his presentation by defining critical infrastructure (CI) and Critical Infrastructure Security and Resilience (CISR) and providing a little background as to how COEDAT came to produce it first course on Critical Infrastructure Protection in 2012.

He then described the goals and objectives for each of the new courses that were developed earlier this year—the new basic course was taught in Bosnia-Herzegovina in early October of 2022 and will be delivered on line by COE in early November.

Mr. Bearse stated that the purpose of the Basic CISRATA Course is to provide students at the 0-2 to 0-6 or civilian equivalent levels a basic understanding of what CISR is, why it is important, the basic elements of what he calls the 'Modern CISR Model' and how NATO and Partner Nations can build and maintain effective national CISR capabilities and foster a culture of resilience.

A representative list of Basic Course objectives include: realizing how CISR supports national and economic security and prosperity; understanding the roles and responsibility of CISR stakeholders; the importance of building partnership between the military, civil government and the private sector owners and operators of critical infrastructure; understanding the importance of government and industry being able to share actionable information and intelligence; and discussing concepts, methods, and tools for improving many components comprising CISR.

The purpose of the Advanced CISRATA Course for 0-6 to 0-9 and civilian equivalents is served strategic thinkers, senior managers, and practitioners responsible for developing and implementing CISR plans, policies, and procedures (and related activities) including how CISR should be integrated within a nation's national security planning framework.

Many of the objectives for the Basic Course are the same as those of the Badic Course but are presented and discussed at the strategic level versus the operational and tactical levels Among the key objectives for the Advanced Course which are different include: discussing participant-defined issues, concerns, and challenges relating to CISR activities , or lack thereof, in their home countries; understanding now national CISR policy ties to the fundamental building blocks and key drivers of of CISR planning; and learning how specific security and resilience measures are being employed in different critical infrastructure sectors, as well as what research and development activities are underway to solve urgent needs.

The Advanced Course also discusses the many CISR governance 'levers' which participants are able to influence, able to control more directly, or unable to impact. Therefore, we talk about 'levers' such as regulation, policy, fines, taxes, incentives, investment, ownership, divestiture, shaming, and publicity. And we ask these senior participants what they play to do with the information and insights gained from this course when they return to their countries. For example: will they share more information; will the change, influence or write new policies; will they develop new strategies; or will the build and implement a road map for establishing a viable CISR capability in their country, if none exists.

Mr. Bearse then reviewed listed some of the presentations and discussion points which are covered in both course, such as:

- Introduction to CISR

- NATO Policy on CISR

- Current and Emerging Threats to CI

- What you need to know about cybersecurity

- Risk Management

- Information/Intelligence sharing

- Crisis Management and Incidence Response

- Building and Sustaining Public Private Partnership

- Current and emerging CISR issues, concerns and challenges

- Good and best practices for improving security and resilience of NATO and Partner Nations against terrorist attacks

- Security of the critical “Life-line” infrastructure sectors

He concluded his presentation by listing the many works teams involved in CISR planning and operations from identifying CI and assessing its risk to defining clear stakeholder roles and responsibilities. Other examples of work streams included: mapping CI dependencies and interdependencies, determining CI vulnerabilities, using applicable risk assessment and analysis methods and tools and adopting a sound Risk Management, and others.

He concluded his presentation on the two new courses by stating COEDAT can now provide these courses in-house, on-line or tailed for specific requesting nations as a **Mobile Education Training** (MET) mission. He had just completed a CISR MET in Bosnia-Herzegovina that was very well received. And asked the audience to share the fact that these two courses are available and that a nation can ask for a team of experts to deliver either of this course in country to reach a much larger audience.

Mr. Bearse concluded his presentation with a key lesson he has learn after being involved in the important national security domain since the 1980s. He stated that the work stream identified in his presentation define much of ‘WHAT’ needs to be done to build and sustain viable CISR capabilities; but the extent to a nation effectively develops and implements the ‘WHAT’ is a function of how well those responsible for leading and managing CISR activities foster the **collaboration, cooperation, coordination, communication, and concentration** required to:

1. Harmonize all the work streams to reduce known risks to CI;

2. Produce economies of scale and optimize resources; and

3. Establish a culture of security and resilience to help build and sustain a viable, risk-based, national CIRS posture.

Presentation

Overview of COEDAT’s New Basic and Advanced *Critical Infrastructure Security and Resilience Against Terrorist Attacks (CISRATA)* Courses

Ronald S. Bearse
President, Ronald S. Bearse Global Associates, Inc.
Adjunct Professor, Massachusetts Maritime Academy

NATO COEDAT TERRORISM EXPERTS CONFERENCE
18 - 19 OCT 2022

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

AGENDA

- Key Definitions
- Background
- Basic Course Purpose/Objectives
- Advanced Course Purpose/Objectives
- Course Presentation Discussion Topics
- Key CISR Work Streams

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

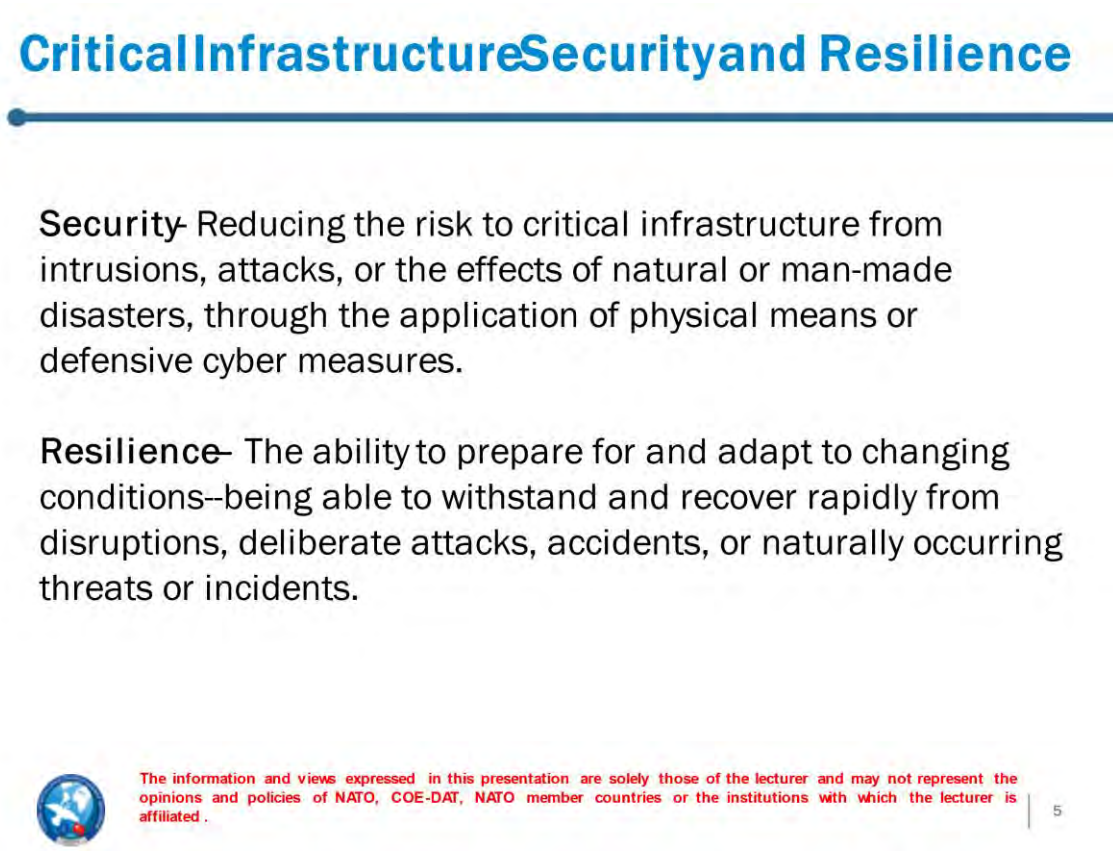
Disclaimer

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

CriticalInfrastructure (CI)

No universal definition…but most countries that have a National CIP/CISR Policy basically define CI as:

… those *physical and cyber systems and assets that are so vital to the country that their incapacity or destruction would have a debilitating impact on its physical or economic security or public health or safety…*



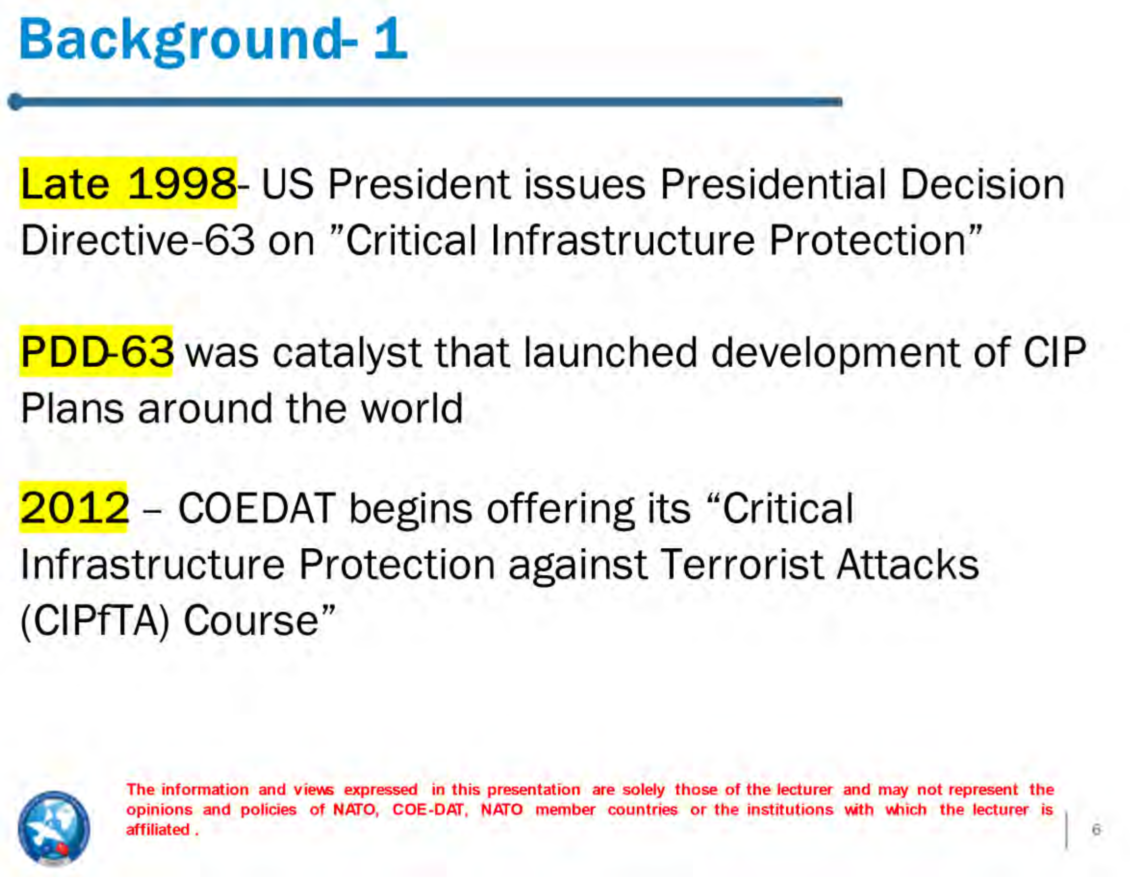
CriticalInfrastructureSecurityand Resilience

Security- Reducing the risk to critical infrastructure from intrusions, attacks, or the effects of natural or man-made disasters, through the application of physical means or defensive cyber measures.

Resilience– The ability to prepare for and adapt to changing conditions--being able to withstand and recover rapidly from disruptions, deliberate attacks, accidents, or naturally occurring threats or incidents.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

5



Background- 1

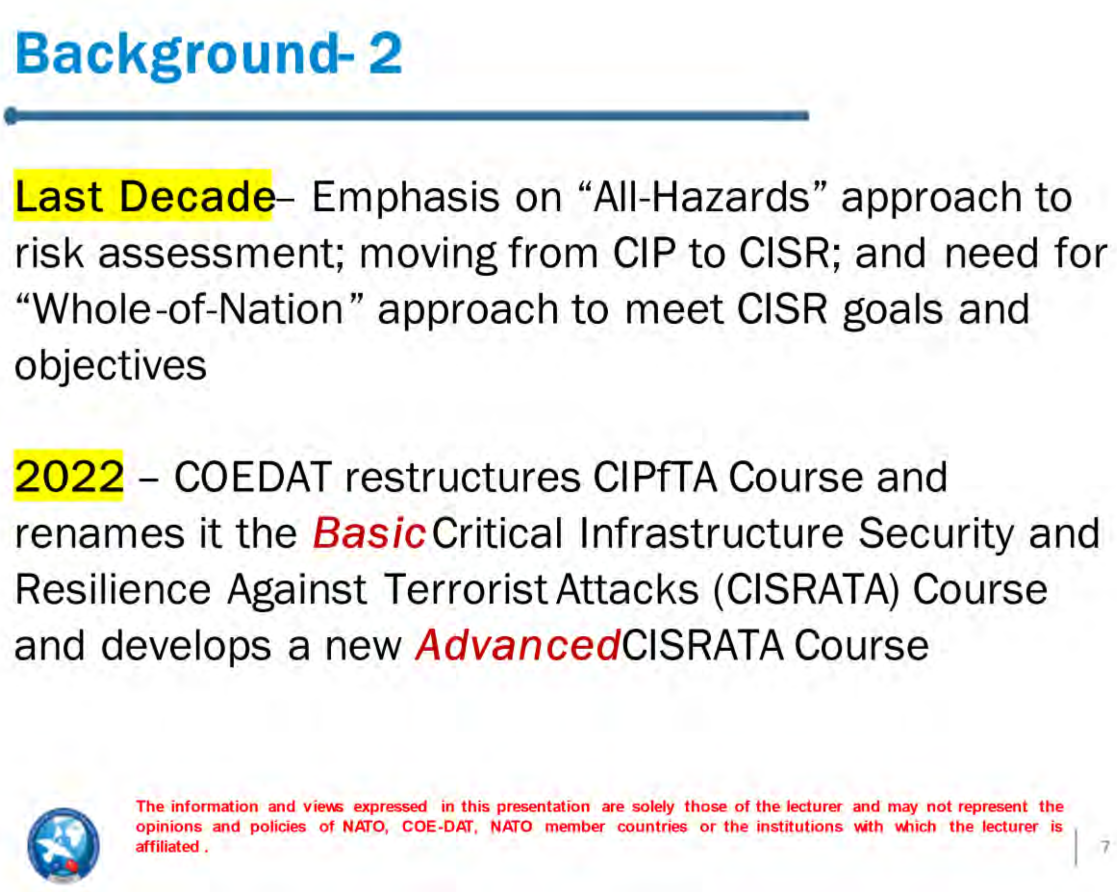
Late 1998- US President issues Presidential Decision Directive-63 on ”Critical Infrastructure Protection”

PDD-63 was catalyst that launched development of CIP Plans around the world

2012 – COEDAT begins offering its “Critical Infrastructure Protection against Terrorist Attacks (CIPfTA) Course”

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

6

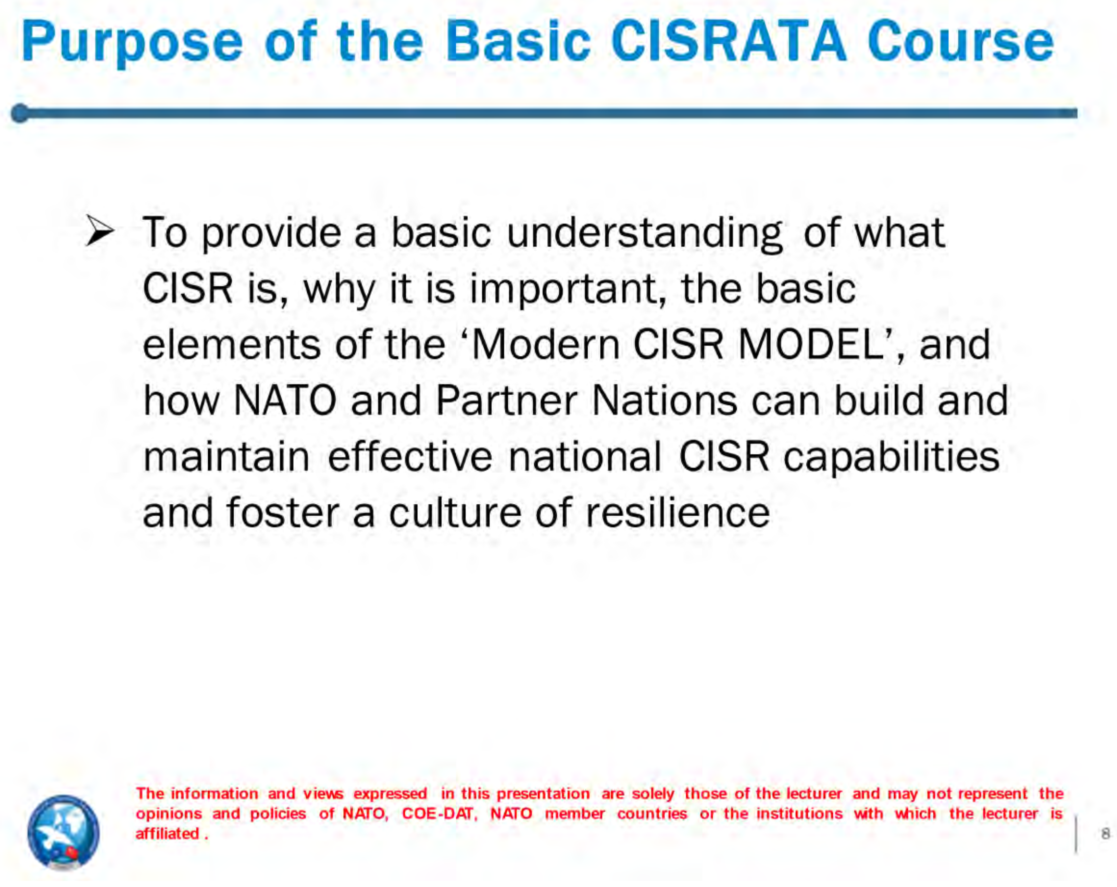


Background- 2

Last Decade– Emphasis on “All-Hazards” approach to risk assessment; moving from CIP to CISR; and need for “Whole-of-Nation” approach to meet CISR goals and objectives

2022 – COEDAT restructures CIPfTA Course and renames it the *Basic* Critical Infrastructure Security and Resilience Against Terrorist Attacks (CISRATA) Course and develops a new *Advanced* CISRATA Course

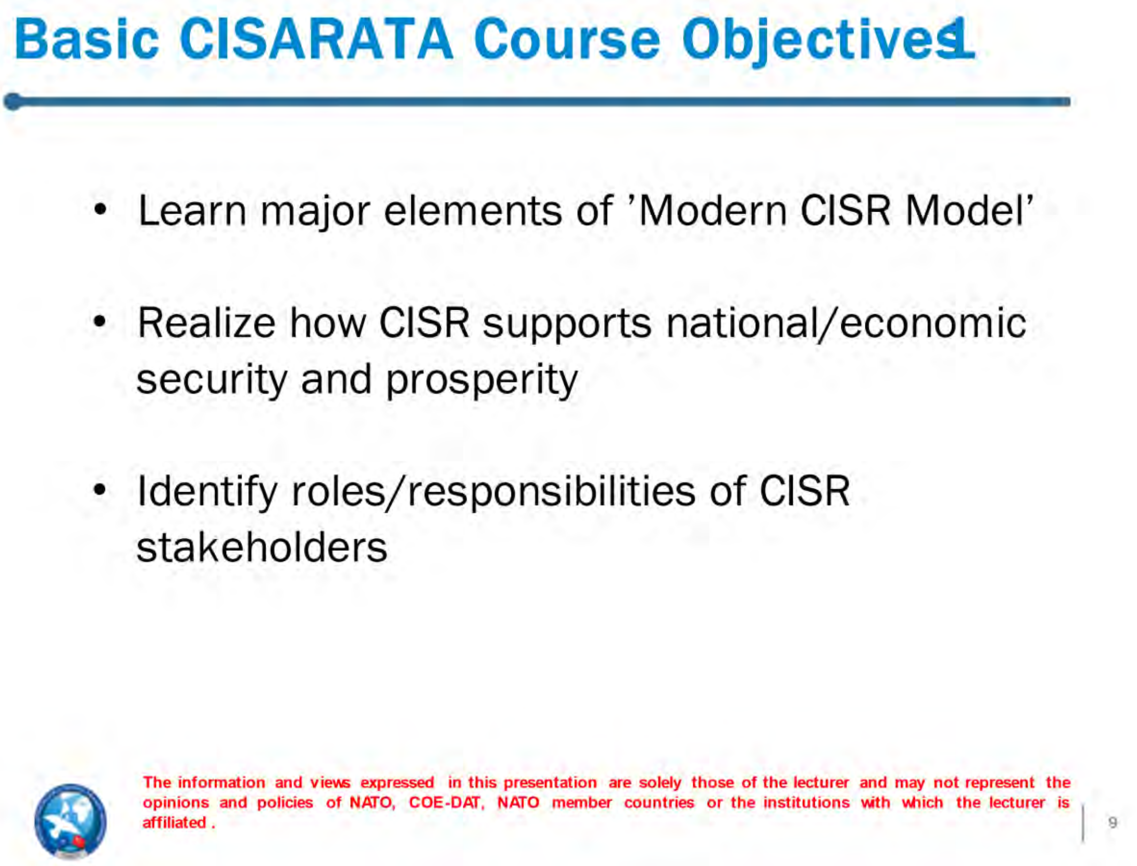
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .



Purpose of the Basic CISRATA Course

➢ To provide a basic understanding of what CISR is, why it is important, the basic elements of the ‘Modern CISR MODEL’, and how NATO and Partner Nations can build and maintain effective national CISR capabilities and foster a culture of resilience

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

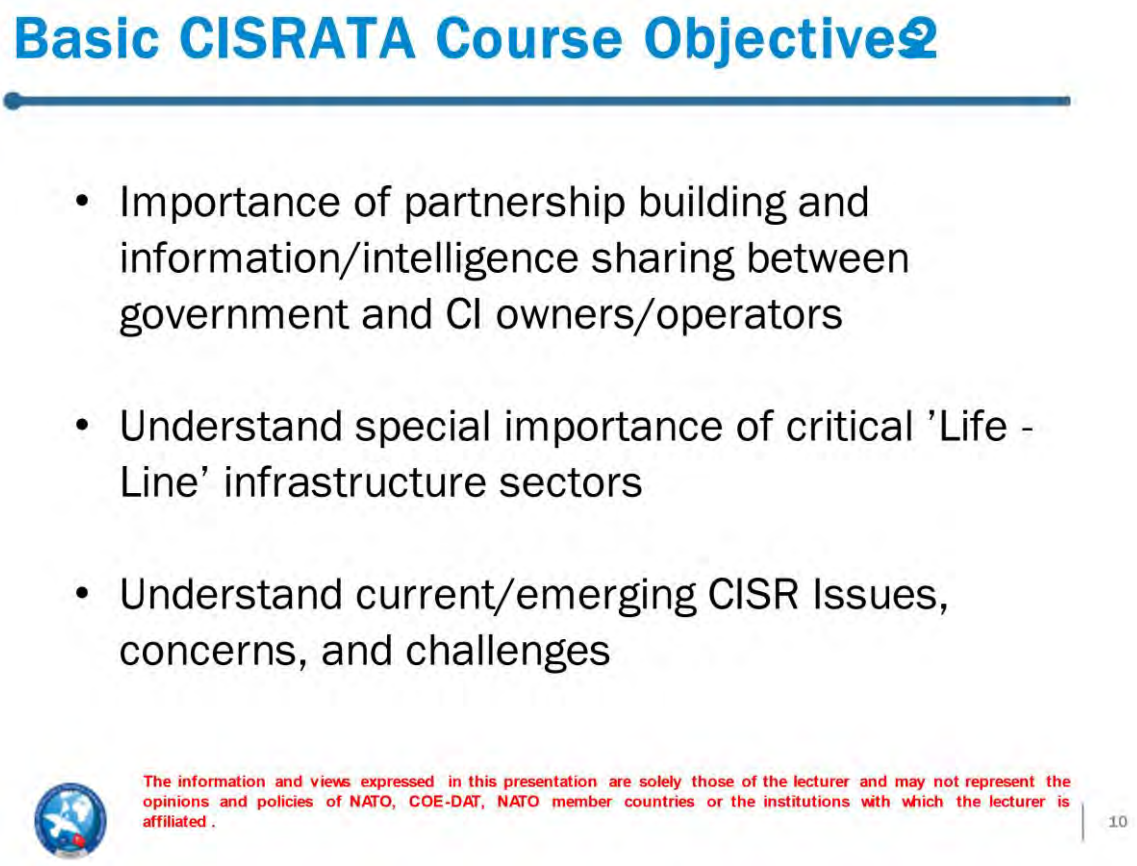


Basic CISARATA Course Objectives1

- Learn major elements of ’Modern CISR Model’
- Realize how CISR supports national/economic security and prosperity
- Identify roles/responsibilities of CISR stakeholders

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

9

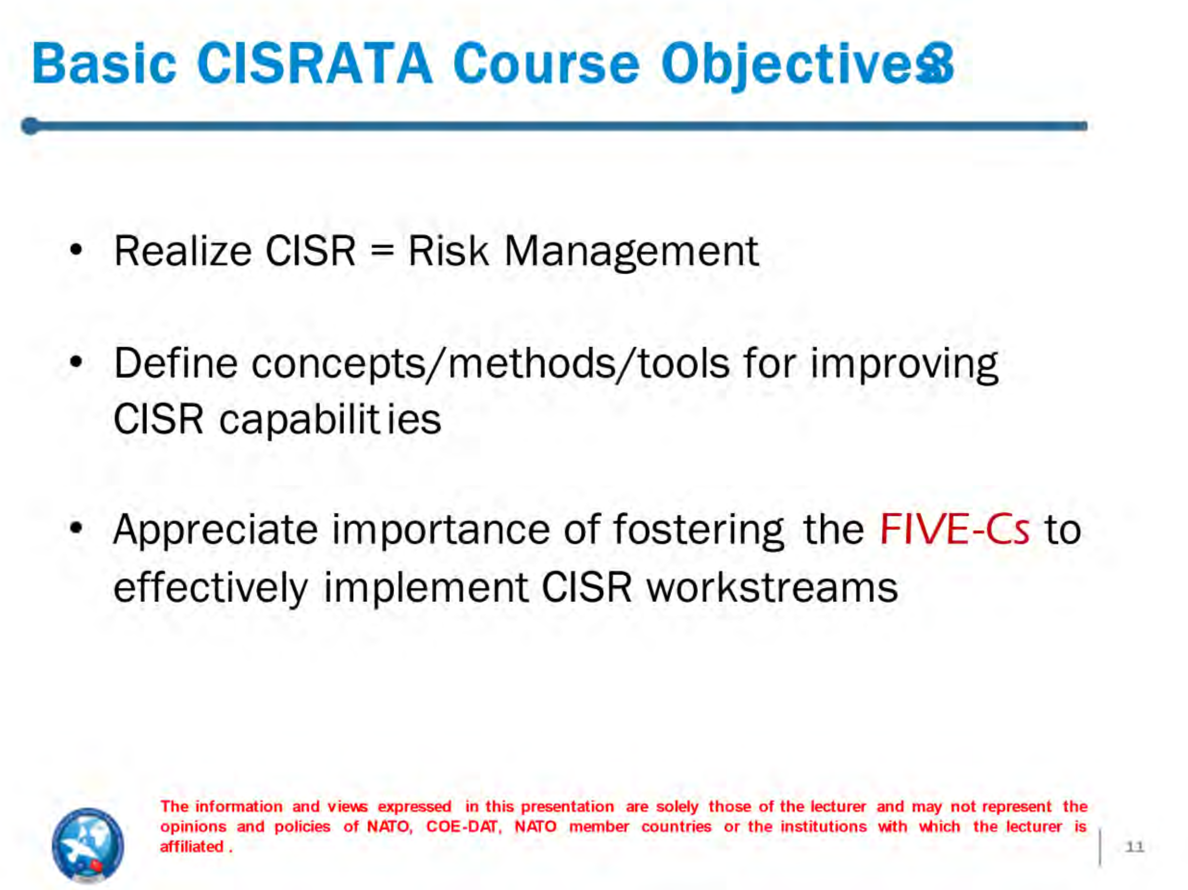


Basic CISRATA Course Objectives2

- Importance of partnership building and information/intelligence sharing between government and CI owners/operators
- Understand special importance of critical ’Life - Line’ infrastructure sectors
- Understand current/emerging CISR Issues, concerns, and challenges

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

10

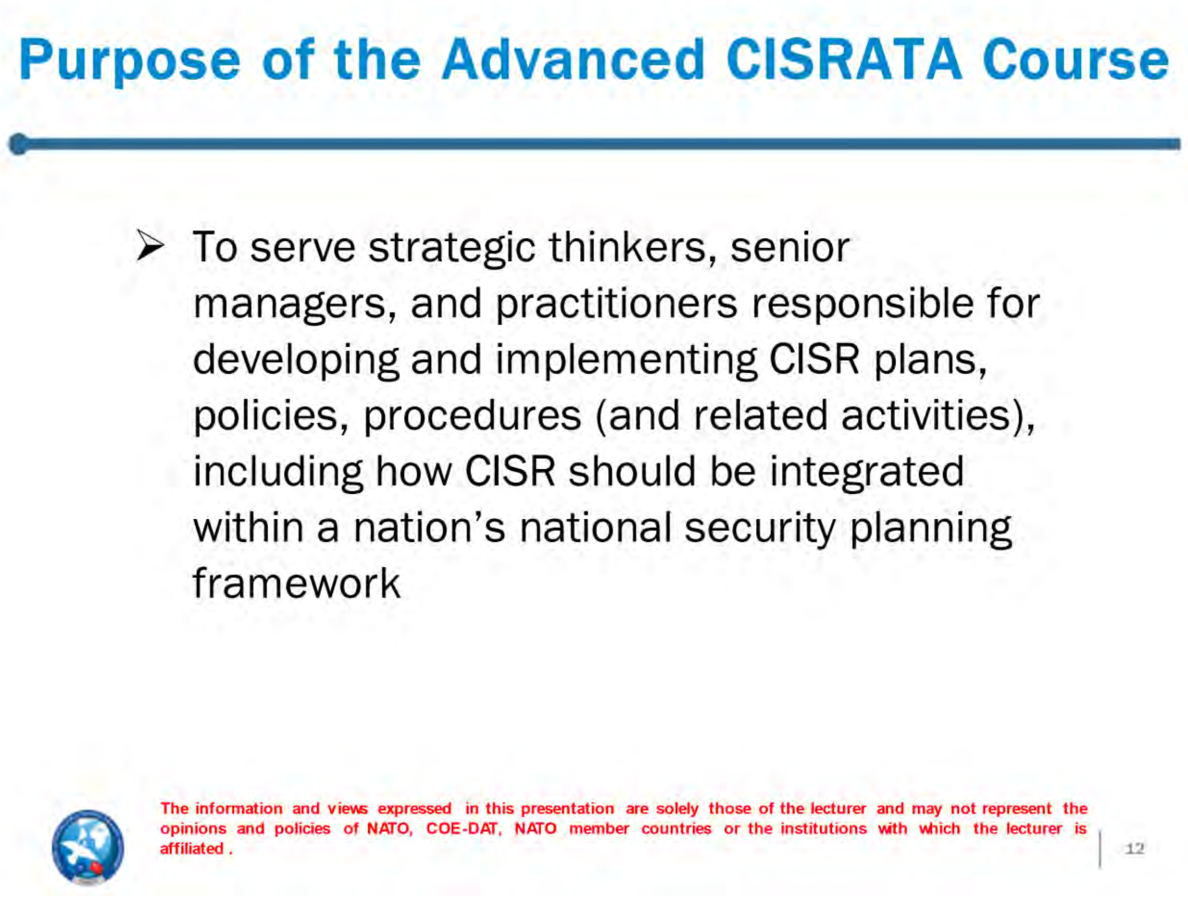


Basic CISRATA Course Objectives3

- Realize CISR = Risk Management
- Define concepts/methods/tools for improving CISR capabilit ies
- Appreciate importance of fostering the FIVE-Cs to effectively implement CISR workstreams

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

11

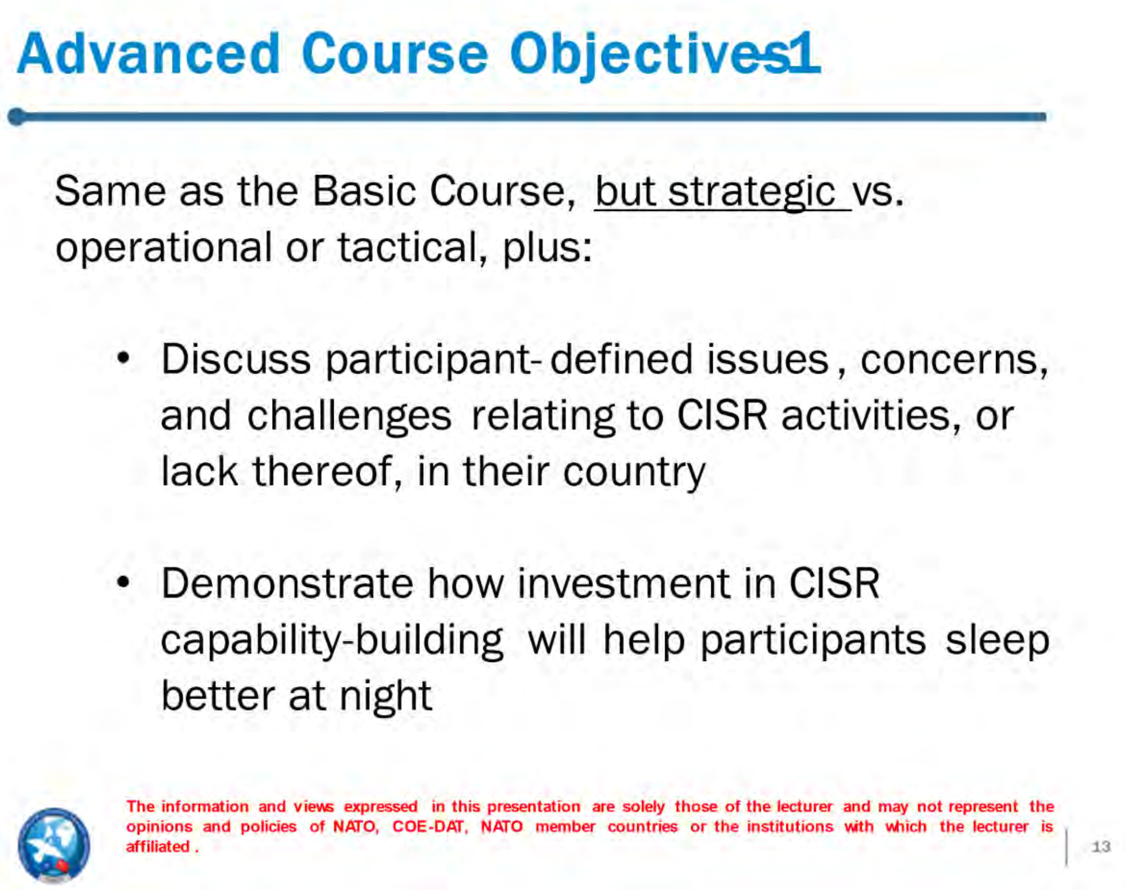


Purpose of the Advanced CISRATA Course

➢ To serve strategic thinkers, senior managers, and practitioners responsible for developing and implementing CISR plans, policies, procedures (and related activities), including how CISR should be integrated within a nation’s national security planning framework

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

12



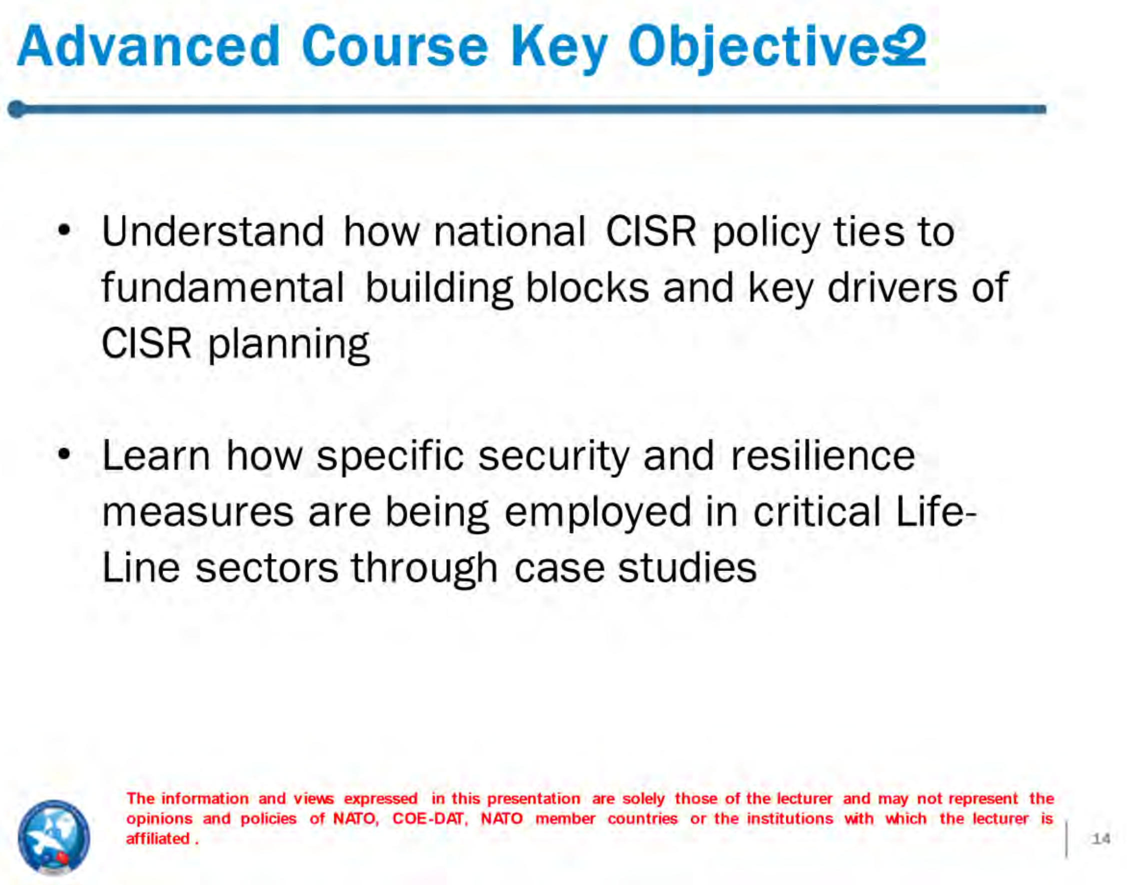
Advanced Course Objectives1

Same as the Basic Course, but strategic vs. operational or tactical, plus:

- Discuss participant-defined issues, concerns, and challenges relating to CISR activities, or lack thereof, in their country
- Demonstrate how investment in CISR capability-building will help participants sleep better at night

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

13

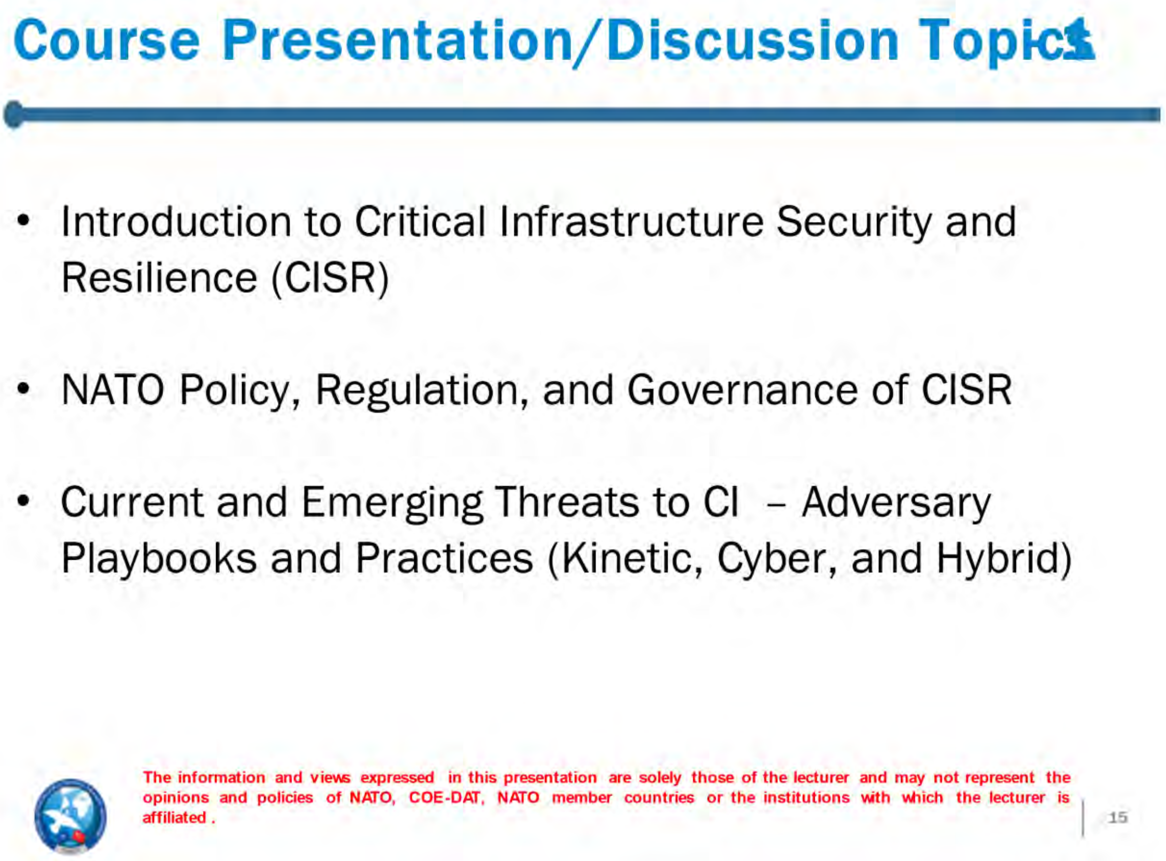


Advanced Course Key Objectives2

- Understand how national CISR policy ties to fundamental building blocks and key drivers of CISR planning
- Learn how specific security and resilience measures are being employed in critical Life-Line sectors through case studies

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

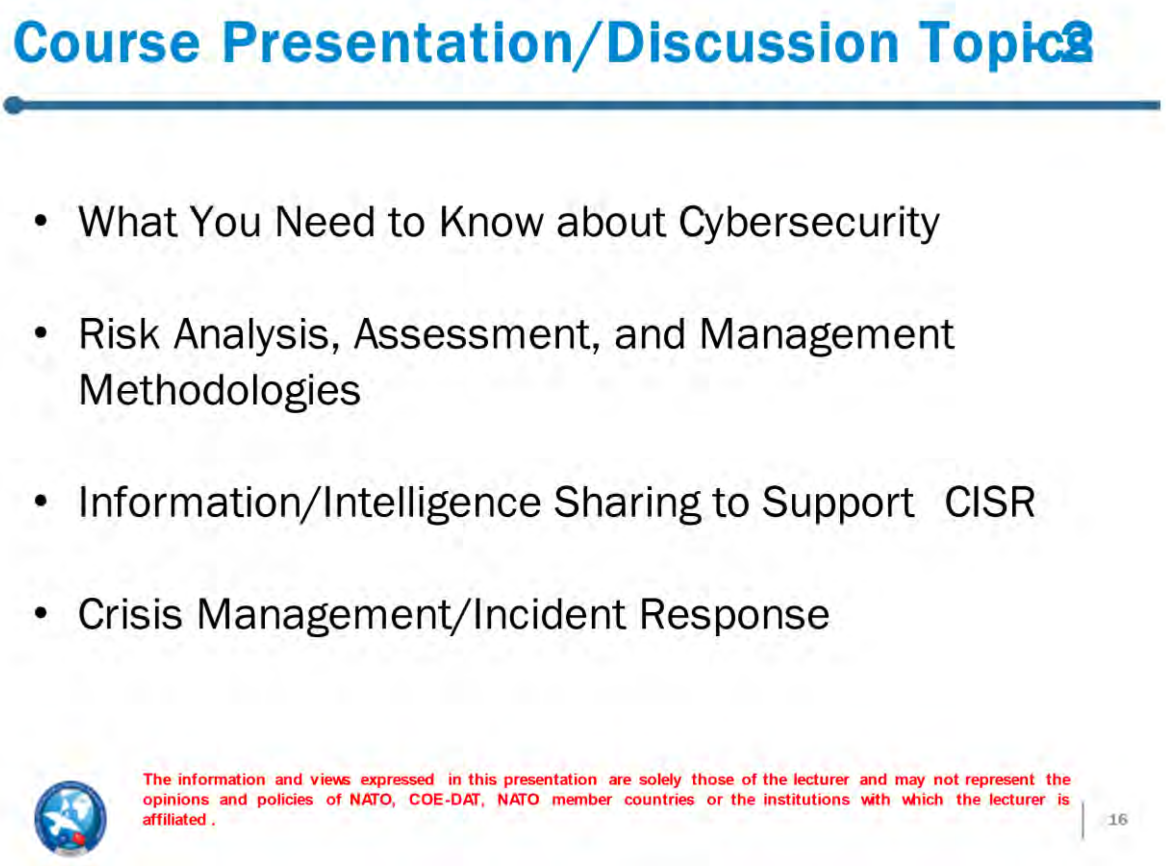
14



Course Presentation/Discussion Topics 1

- Introduction to Critical Infrastructure Security and Resilience (CISR)
- NATO Policy, Regulation, and Governance of CISR
- Current and Emerging Threats to CI – Adversary Playbooks and Practices (Kinetic, Cyber, and Hybrid)

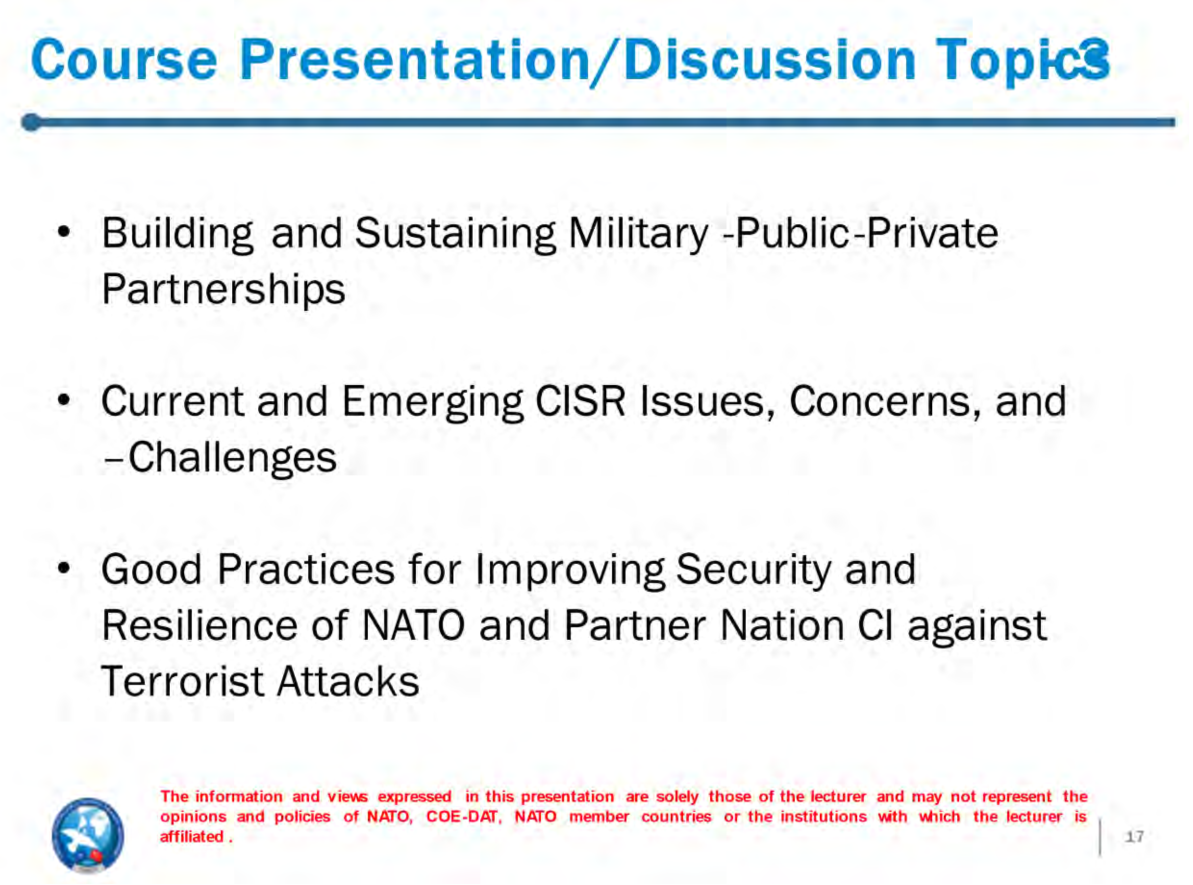
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .



Course Presentation/Discussion Topics 2

- What You Need to Know about Cybersecurity
- Risk Analysis, Assessment, and Management Methodologies
- Information/Intelligence Sharing to Support CISR
- Crisis Management/Incident Response

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

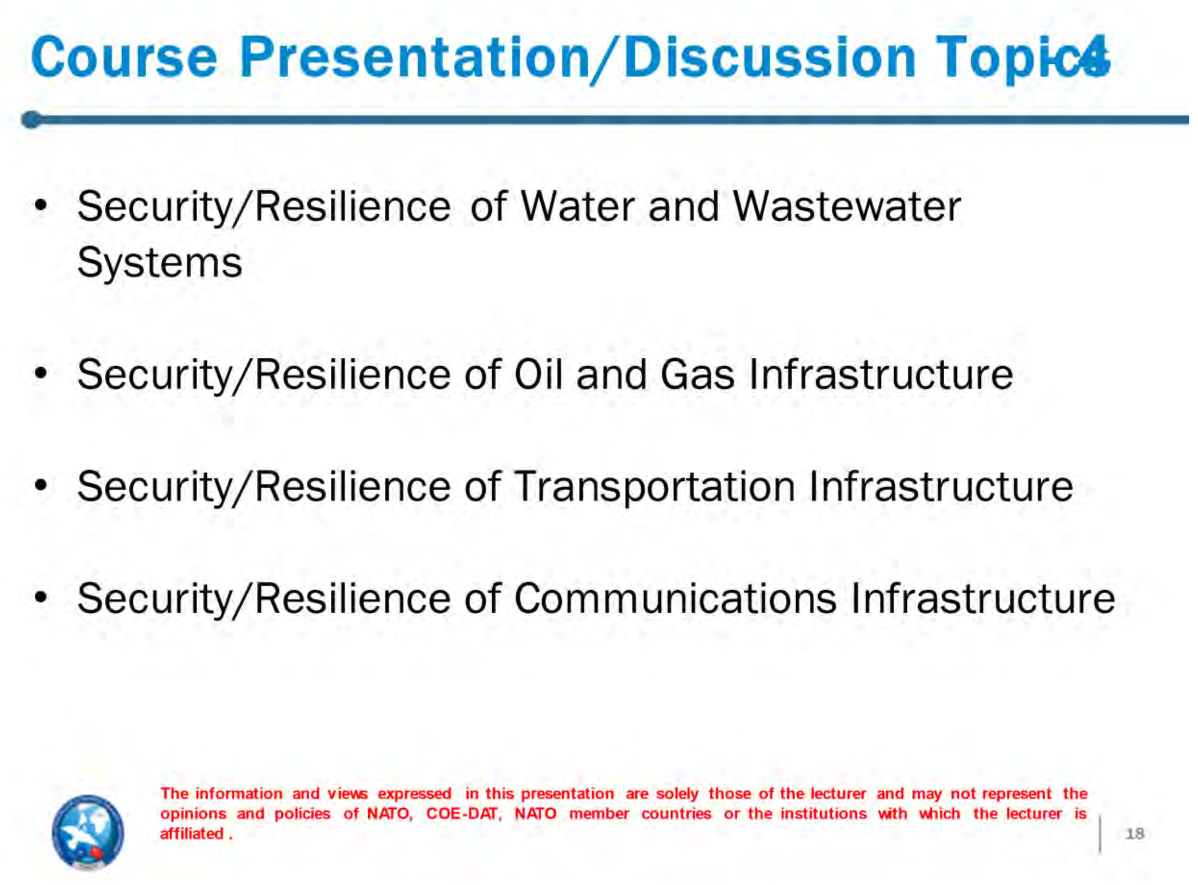


Course Presentation/Discussion Topic3

- Building and Sustaining Military -Public-Private Partnerships
- Current and Emerging CISR Issues, Concerns, and –Challenges
- Good Practices for Improving Security and Resilience of NATO and Partner Nation CI against Terrorist Attacks

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

17

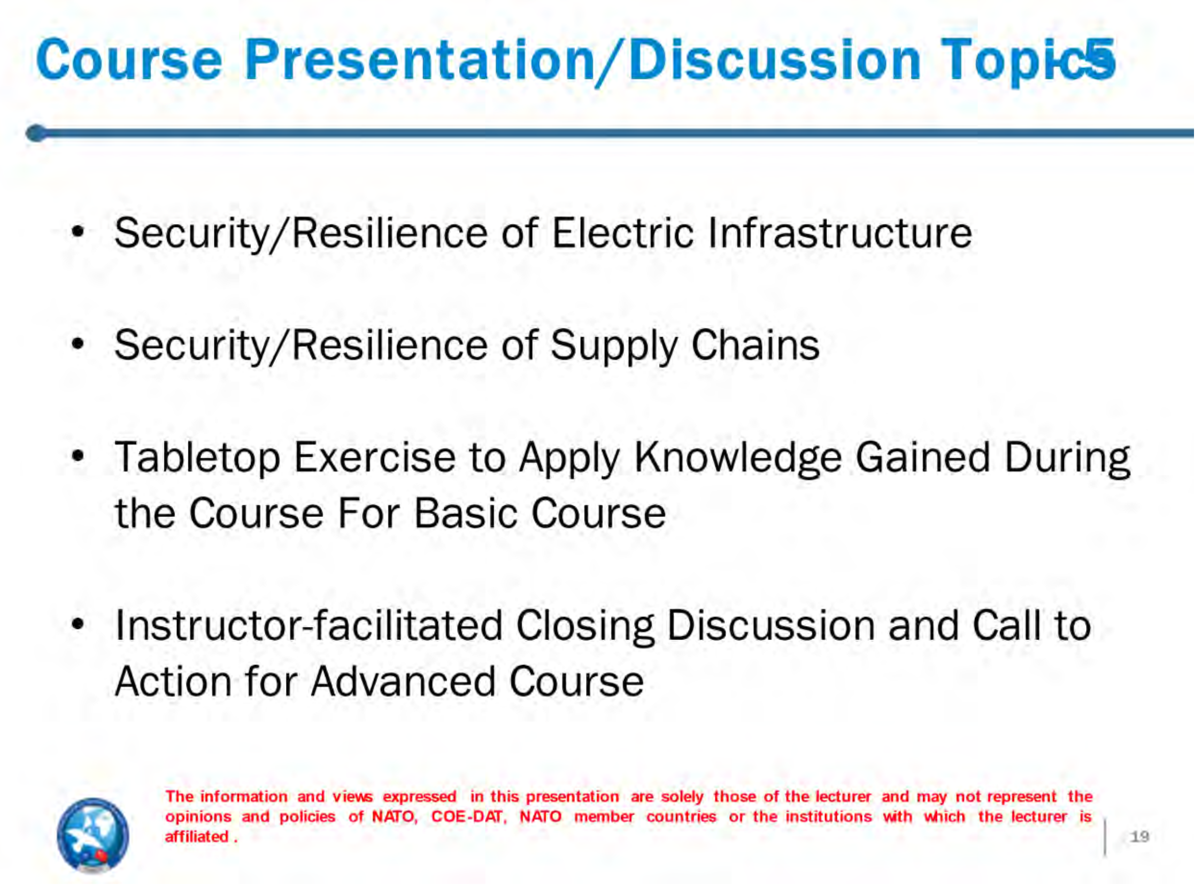


Course Presentation/Discussion Topic4

- Security/Resilience of Water and Wastewater Systems
- Security/Resilience of Oil and Gas Infrastructure
- Security/Resilience of Transportation Infrastructure
- Security/Resilience of Communications Infrastructure

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

18

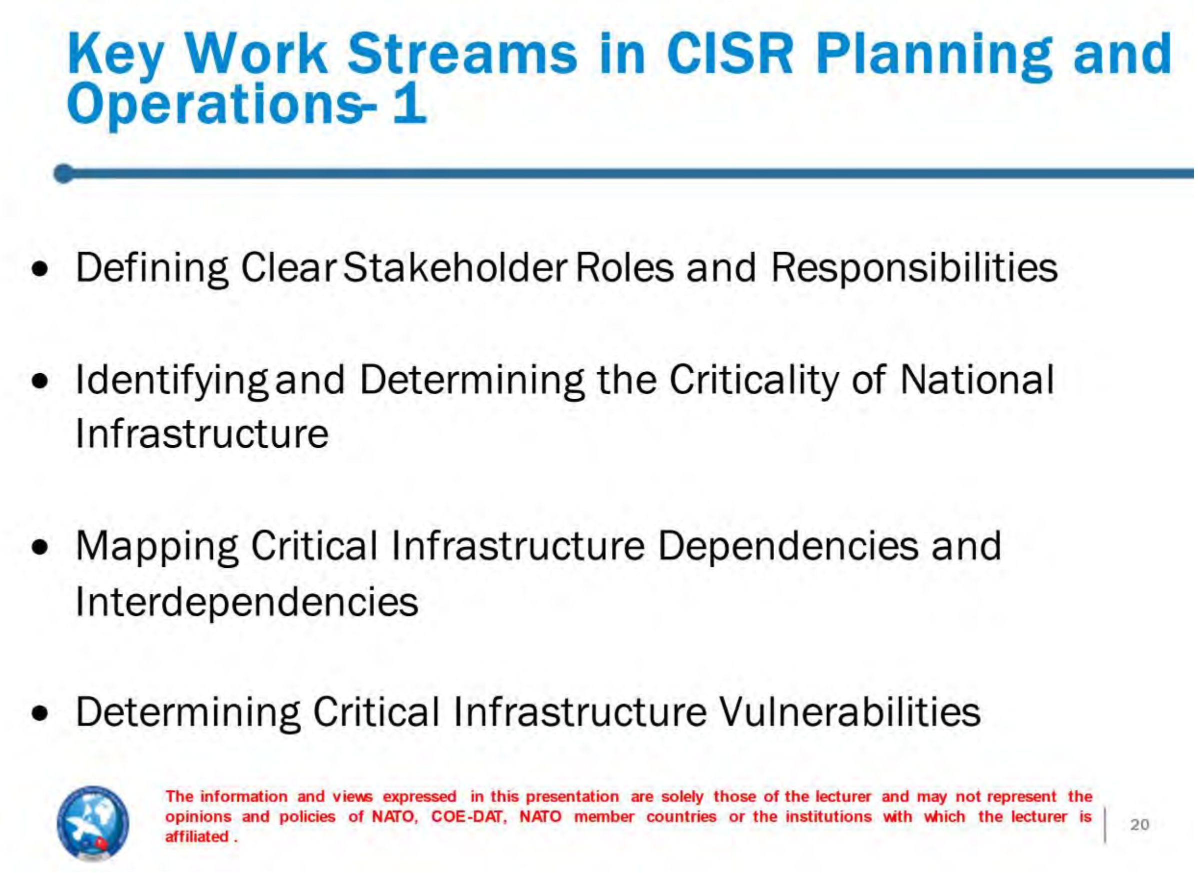


Course Presentation/Discussion Topics5

- Security/Resilience of Electric Infrastructure
- Security/Resilience of Supply Chains
- Tabletop Exercise to Apply Knowledge Gained During the Course For Basic Course
- Instructor-facilitated Closing Discussion and Call to Action for Advanced Course

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

19

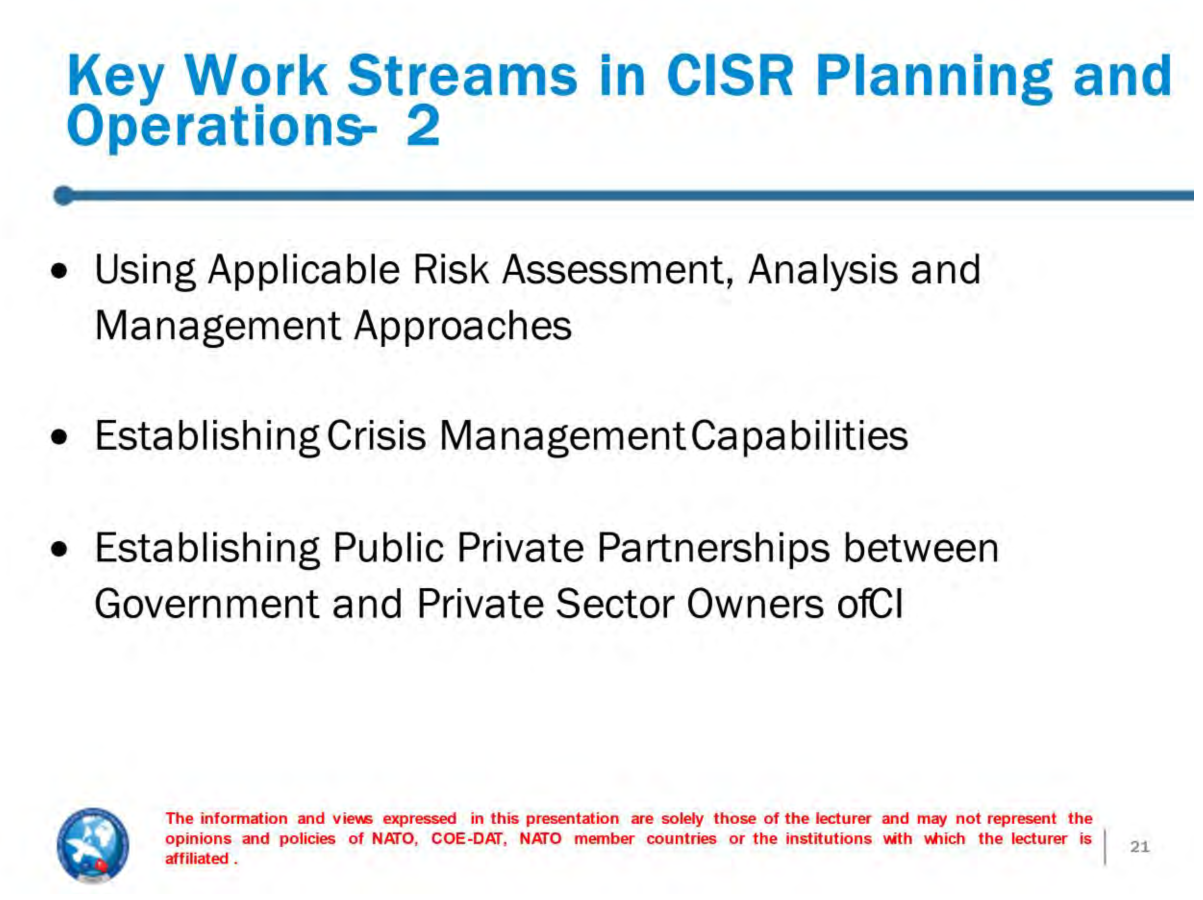


Key Work Streams in CISR Planning and Operations- 1

- Defining Clear Stakeholder Roles and Responsibilities
- Identifying and Determining the Criticality of National Infrastructure
- Mapping Critical Infrastructure Dependencies and Interdependencies
- Determining Critical Infrastructure Vulnerabilities

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

20

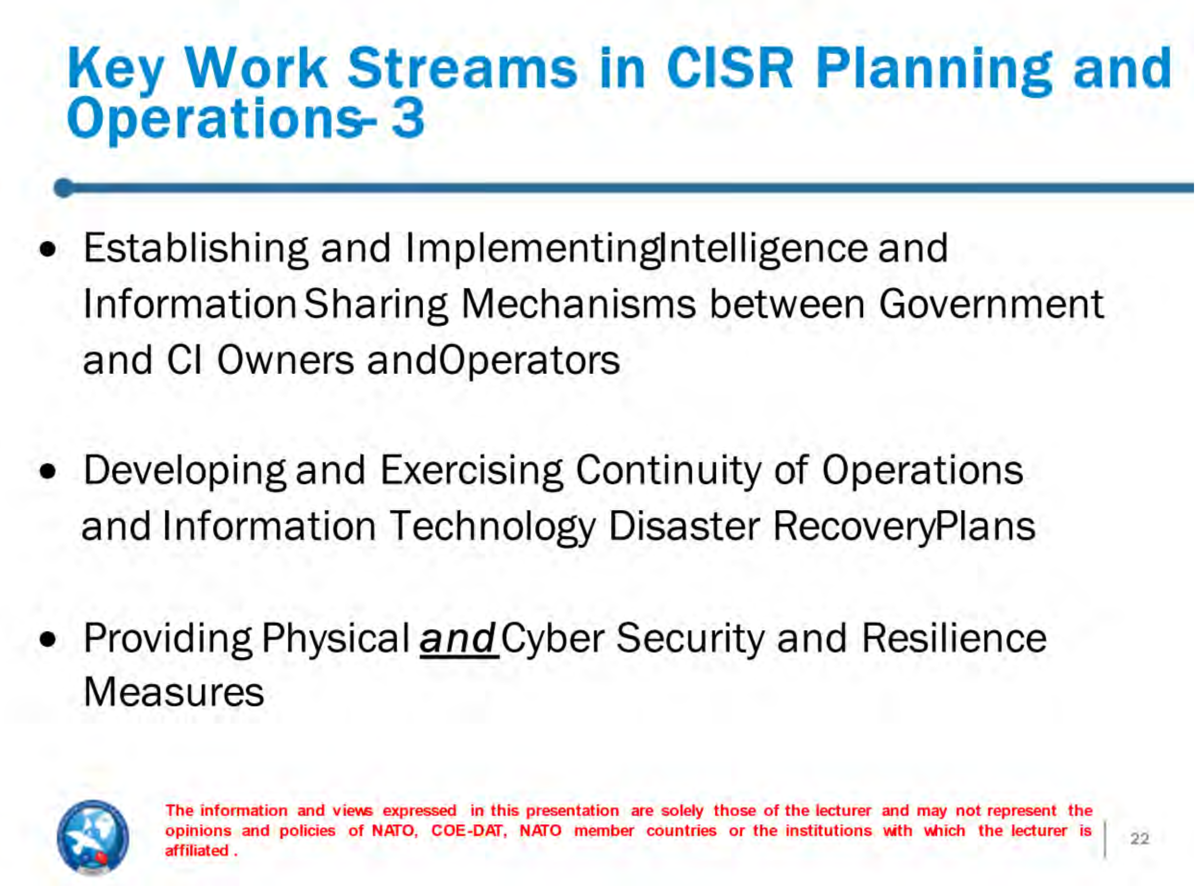


Key Work Streams in CISR Planning and Operations- 2

- Using Applicable Risk Assessment, Analysis and Management Approaches
- Establishing Crisis Management Capabilities
- Establishing Public Private Partnerships between Government and Private Sector Owners ofCI

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

21



Key Work Streams in CISR Planning and Operations- 3

- Establishing and ImplementingIntelligence and Information Sharing Mechanisms between Government and CI Owners andOperators
- Developing and Exercising Continuity of Operations and Information Technology Disaster RecoveryPlans
- Providing Physical *and* Cyber Security and Resilience Measures

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

22

Key Work Streams in CISR Planning and Operations- 4

- Ensuring the Integrity, Security, and Continuity of Critical Infrastructure SupplyChains
- Expanding opportunities to develop and deliver CISR education and training to accomplish work streams
- Implementing a robust Test, Training, andExercise Program

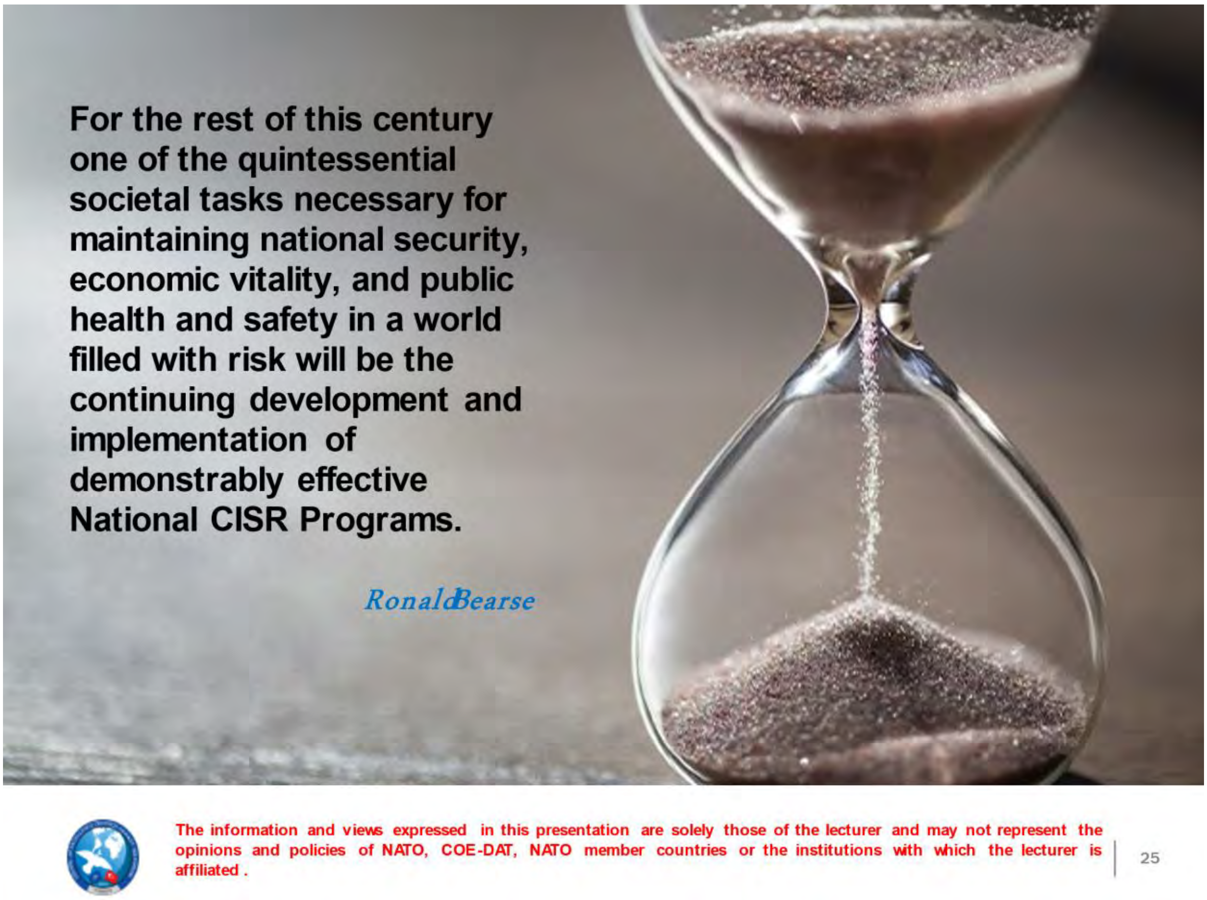
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

Key “Lesson-to-be-Learned” this Century

While the last three slides define much of “***what***” needs to be done, the extent to which a nation effectively develops and implements the “***what***” is a function of “***how***” people responsible for leading and managing CISR activities foster the collaboration, cooperation, coordination, communication, ar concentrationrequired to:

1. Harmonize all work streams and implementeffective measures to reduce risk to CI
2. Produce economies of scale and optimize resources
3. Establish a culture of security and resilience, and build and sustain a viable, risk based, national CISR posture

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

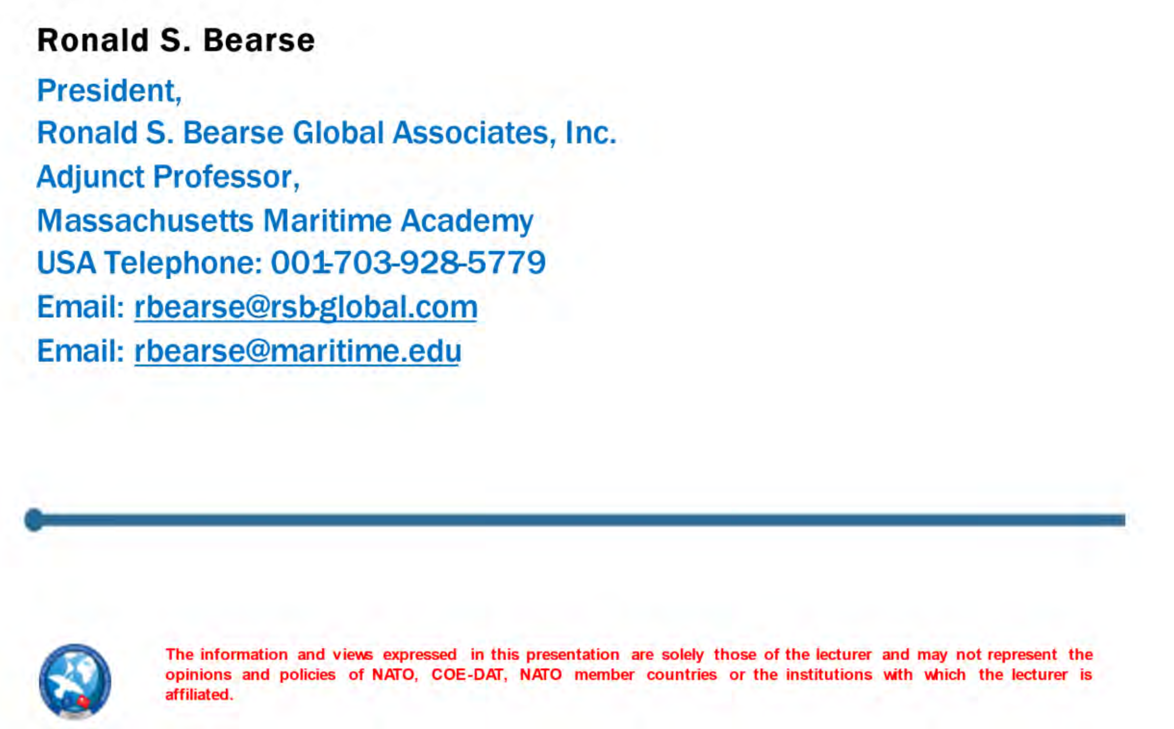


For the rest of this century one of the quintessential societal tasks necessary for maintaining national security, economic vitality, and public health and safety in a world filled with risk will be the continuing development and implementation of demonstrably effective National CISR Programs.

RonaldBearse

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated .

25



Ronald S. Bearse

President,
Ronald S. Bearse Global Associates, Inc.
Adjunct Professor,
Massachusetts Maritime Academy
USA Telephone: 001-703-928-5779
Email: rbearse@rsb-global.com
Email: rbearse@maritime.edu

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

DAY II

SESSION 1: Questions and Answers

Questions to Asst. Prof. Omi HODWITZ

1. *What would you predict for participation in arrest rates for women in the Middle East?*

I am a data scientist; therefore, I am always a bit hesitant to make predictions without the data. But I do appreciate the question. Thank you for asking it. The data does not publicly exist right now. And that was something that we wanted to examine in our research. I am also the director of the Terrorist Recidivism Study, which is a major data project that collects data on terrorist prosecutions and follows them upon release to see reoffending and recidivism rates. So, we are adding the Middle East, selecting countries in the Middle East. Thanks to that project, we can better understand what the criminal justice practices in this area are when it comes to extremism and what the long-term consequences are. In fact, that is my roundabout way of saying I cannot. I am reticent to reflect on what the data will tell us, but we are in the process of collecting it so that I can provide a well-informed evidence-based response to that question.

Questions to Prof. Dr. Haldun YALÇINKAYA

1. *I have to make my own disclaimer that I am fully aware of the fact that you said about the not being about fortune telling. But my questions about actually about the future. So, it's about the transformation of the threat. Actually, on my list I have 4 milestones in the near past starting from the collapse of USSR which we had no more conventional and nuclear threats and then switching to 9/11 to asymmetric terrorist threats and 2014. Now we have the annexation of Crimea, and then on the agenda we have started talking about learning about the hybrid threats. Finally, starting from February 22, now we have again on the agenda conventional and nuclear threats. So, my simple question to you is, do you think that when you put on the scale the conventional and the military threats will outrank the terrorist and asymmetric threats in the future?*

Especially, you begin talking about four breaks in the recent history. Breakthroughs in the changing International Security environment. I was about to answer your question with our research which is only limited to terrorism. You timely changed the direction and ask the question proper. I point out scaling and comparing the terrorist threat and the international security threat. Originally, I am not a scholar who study terrorism, but war. I thought during my education and studies the foundation of International Security after Second World War was based on nonterritorial gain. Since we are about to open Pandora's box for the territorial gains, I would not compare windows of states to the values of terrorist organizations. Unfortunately, the previous one was much capable of creating violence as we see from the history. I mean, the fear from state violence is not comparable with the terrorist fears.

Questions to Mr. Ronald BEARSE

1. *You know, many CI are interconnected, as you know, by definition. Does NATO, should NATO define some specific CI to be defended in the alliance?*

   NATO does define critical infrastructure. They get actually three types of critical infrastructure that they define. It is basically key to the operational missions. What we need to do is to support these missions across the NATO country. NATO does have very specific military kind of connotation, definitions of critical infrastructure that take a military focus.

2. You have spoken about the whole of nation approach in terms of risk assessments and that's critical and important to integrate all the different parts. I am wondering if you see a need for a regional risk assessment in some cases. Given the nature of terrorism being cross-border, is there any value in a regional exercise to mimic a whole of nation approach?

   The good news is that the nations that have these plans and policies in place that have been working on them for 20 or 30 years. A lot of lessons learned. We can help the countries that do not have such plans and policies. If you only know particular element, so don't have a national policy, you don't have a plan. Therefore, those are things that we also teach in the courses and there are a lot of technologies, a lot of methods that you know the Western nations had to learn the hard way. Going back to your whole of nation approach, we use that term a lot in the United States. You are going to hear it because the world is getting smaller and everybody plays a role. You cannot always depend on government. You have to be self-sufficient, whole of nation. We need to develop a culture of resilience. You asked about risk assessments in the United States and in other parts of Europe. I believe no, we do regional assessments. We do regional risk assessments. We have done them in every region in the United States. And those are very important because we were even in some cases moving beyond, looking at critical infrastructure. But I am telling you about the United States. But we are looking at functions that have to be protected. Now, what's the function? What are the functional nodes that are really critical? When the United States first identified its critical infrastructure tens of thousands of things because everybody thought what they had was critical. That is not the way it works. And we were almost trying to move beyond that. Now we got a pretty good idea of what our critical infrastructure is, our very critical infrastructure of the loss or destruction of which or incapacity is going to hurt us a lot. And going back to the whole of nation support, there are things that everybody can do to help. They can play a role. And we have a lot of stakeholders and we need to share with people of America exactly what we are doing, and people need to be aware. More people need to be involved in this at all levels. They can all help. They all play a role. It's really that simple. And governments should be telling people that they are doing and building these plans and why it's important. That way they will get the political support to move and maybe change some resources in the right direction.

General Comment from the Audience

I have some comments from Special Forces point of view, if I may. First of all, I would like to say we had discussions during partnerships of all in counter-terrorism and crisis management workshop. And as we all know the crucial role of the special operation forces has increased especially after 9/11 in terms of counter-terrorism. I would like to highlight here another important role of special operation forces related to indirect response to terrorism. We are now witnessing unconventional implication of special operation forces during a conventional war, ongoing Ukraine-Russia Conflict. Ukrainian SOF are contributing nations comprehensive defense such as resistance movements, supporting to social resilience and also resilience of critical infrastructure in terms of unconventional warfare. Besides SOF's impacts and response to these implications, unconventional implications are rising again in hybrid environment. Secondly, I would like to convey my thoughts about the previous workshop. I have another question for the academia who study special operations and regular warfare. I think we need a more constructive and more idealistic approach to be formed for the international SOF community especially, with international community in order to contribute to our understanding of different aspects of irregular warfare, special operations, counterterrorism and especially terrorism as the tool of hybrid warfare. This would also help us to understand human domain because the technological developments are not enough without understanding human domain. And SOF are strategic assets and the critical assets which play important role being employed in human domain, while countering terrorist traits and hybrid threats.

DAY II

SESSION 2 – Countering the Financing of Terrorism

Assessing Opportunity and Innovation in Terrorist Financing in a Post Covid Environment

Dr. Sheelagh BRADY

Innovation within crime and terrorism activity is nothing new, albeit it is receiving increasing levels of academic and research interest. This trend has been less focused towards innovation as it relates to terrorist financing however, especially regarding the opportunities and drivers that influence such innovation. This gap is surprising, given that terrorist financing is often postulated as a requisite of terrorist activity. Despite this gap in literature, some is available. For example, Keating and Danner found "***that much of the development in terrorist financing methods is opportunistic with innovation born out of necessity and in reaction to external forces beyond a group's control, rather than being planned, proactive, or strategic***"[5]. This presentation echoes this thesis, that innovation in terrorist financing is the result of necessity and opportunity.

Theoretical Framework

The rationale behind seeking to maximize or exploit existing financial methods lies at the kernel of rational choice theory[6], given that the theory presupposes individuals are reasoned actors who decide about their role in certain actions primarily in the context of costs and benefits, i.e., a person's own self-interest influence the choices they make, weighing up what they believe serves them the best. In this context, this article views terrorists as rational actors, similar to entrepreneurs, comparing both groups to illustrate how they use similar means of innovation to secure finance for their nascent ideas.

[5] Tom Keating and Kerstin Danner (2021). Assessing Innovation in Terrorist Financing, Studies in Conflict & Terrorism, 44:6, 455-472, p. 466.

[6] Cornish and Clarke 2008.

Entrepreneurs and Terrorist Groups

Comparing entrepreneurs with terrorists may appear tangential at best but the environment in which they operate is very similar, especially in the context of innovation, financing, and as importantly, persuasion. While we are often side tracked by outliers, the unicorns (META, TWITTER, GOOGLE) or well-known terrorist groups (Al Qaeda, Basque Euskadi Ta Askatasuna (ETA), Irish Republican Army (IRA), etc), some interesting similarities exist between the two. Both groups need to persuade potential supporters that their idea or cause is worth supporting, often under conditions of risk and extreme uncertainty, helping them to build an ecosystem or community of followers or shared attitudes.

Financing Innovations

Like start-ups, terrorists have to be innovative in creating opportunities to secure funding. Outside of the traditional banking systems, available options for start-ups often include, equity finance, crowdfunding, own resources, those from family or friends, or government grants and incentives. Terrorist groups often use similar means, especially evident if we change the term equity funding to donor funding. These types of funding often come at a cost – autonomy over how such funds are spent. Investment or donations often requires a trade-off to some oversight into management decisions.

Despite the range of activities terrorists use, it is still difficult to assess how innovative such terrorist groups are, in their acquisition of finances, given the lack of data. It is clear to see many of the examples discussed above would constitute innovation, if one accepts the application of existing mechanisms used in one area applied to the area of terrorist financing. This might be called **innovation by appropriation**, which differs slightly from innovation in the technical sense of developing something that is truly unique. Thus, it appears that terrorist groups have not attempted to be uniquely creative in the financial sources they seek, or the methods used to acquire funds, rather have adopted or appropriated mechanisms from other sectors and applied them to use in terrorist financing. This is likely to be the result of the limitations of the grey or black financial systems in which they often operate, and the need to engage with larger value finances within the licit financial sector.

COVID-19 Opportunity

COVID-19 has and will continue to create opportunity for terrorist financing[7], further exacerbated by a convergence of multiple factors, such as the war in Ukraine, possible global recession and increased technological change. The impact of the pandemic on wider society has provided an environment suitable for exploitation; responses such as restricted movement, social distancing measures, supply chain issues, reduced travel, etc. As the impacts of the pandemic continue to evolve, the opportunities presented with develop with them, which some terrorist groups will try to capitalize on. Societal impacts, such as rising unemployment, rising inflation, the risk of recession, financial distress, the bankruptcy of companies, the increased circulation of cash in economies, and the potential for increased need of stimulus programs may individually, and collectively, represent vulnerabilities that terrorist groups may try to capitalize on and exploit. This might result in diversification by some groups to exploit new and emerging opportunities. Opportunities are likely to present differently in different geographical areas, which may result in different circumvention techniques displayed, or for the real opportunistic innovators, they may use the collective advantage of multiple different approaches to capitalize on the evolving situation.

Learning for NATO and related partners;

- One size does not fit all approach.
- Need for greater digital transformation for FATFs.
- Realign their focus on outputs over outcomes.
- Increasing cooperation & engagement with stakeholders outside law enforcement.
- Horizon Scanning – of wider context to identify sources & opportunity for funds acquisition.
- Avoid promising the merits and potential of Artificial Intelligence & Machine Learning.
- Differentiate between methods, means and opportunity.

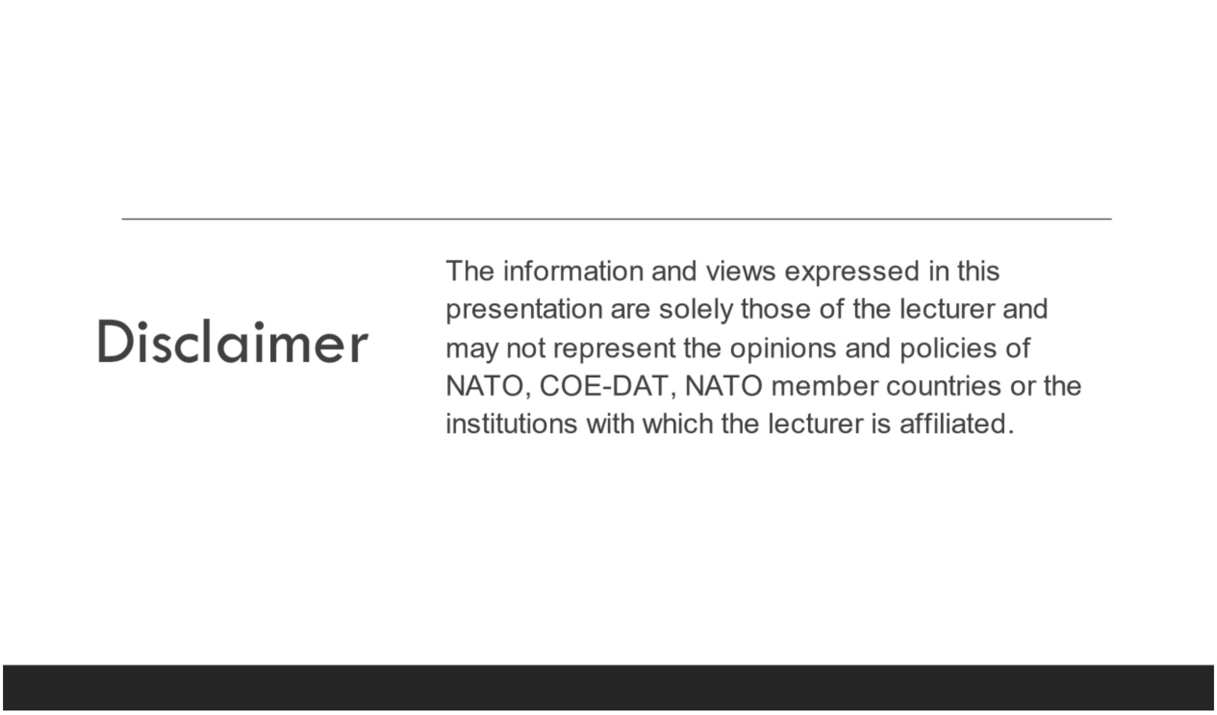
[7] https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/grc-740074

Presentation

Assessing opportunity and innovation in terrorist financing, in a post covid environment.

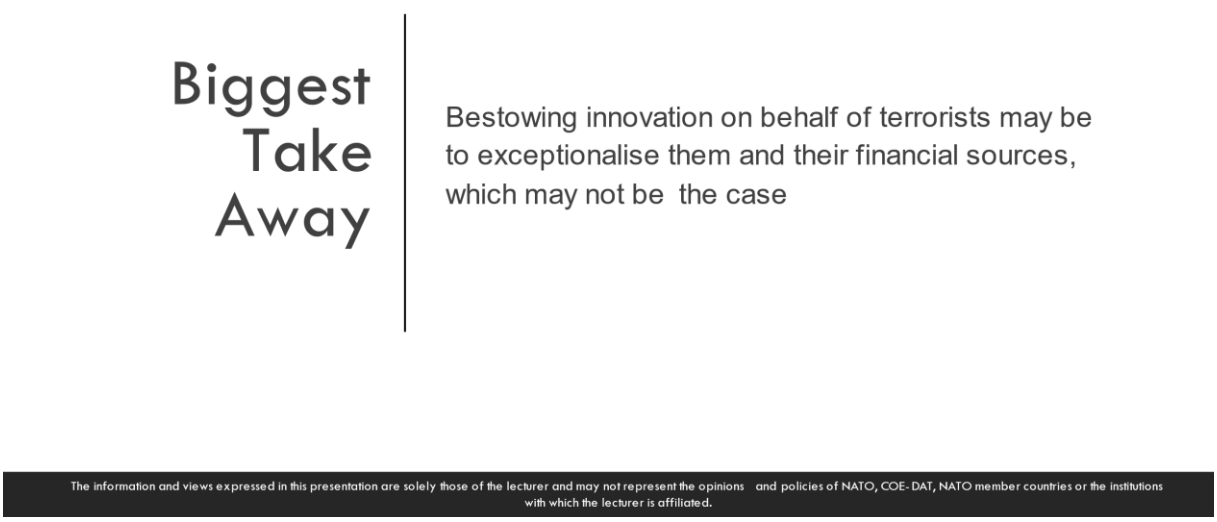
DR SHEELAGH BRADY

DUBLIN CITY UNIVERSITY



Disclaimer

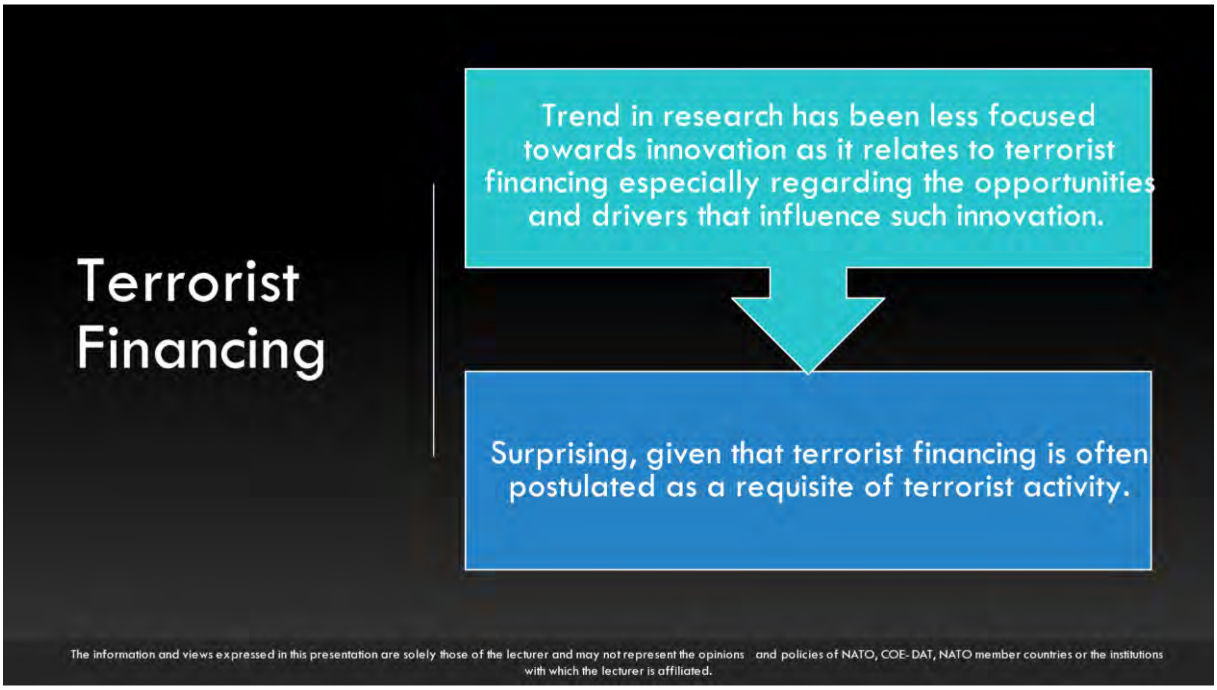
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Biggest Take Away

Bestowing innovation on behalf of terrorists may be to exceptionalise them and their financial sources, which may not be the case

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

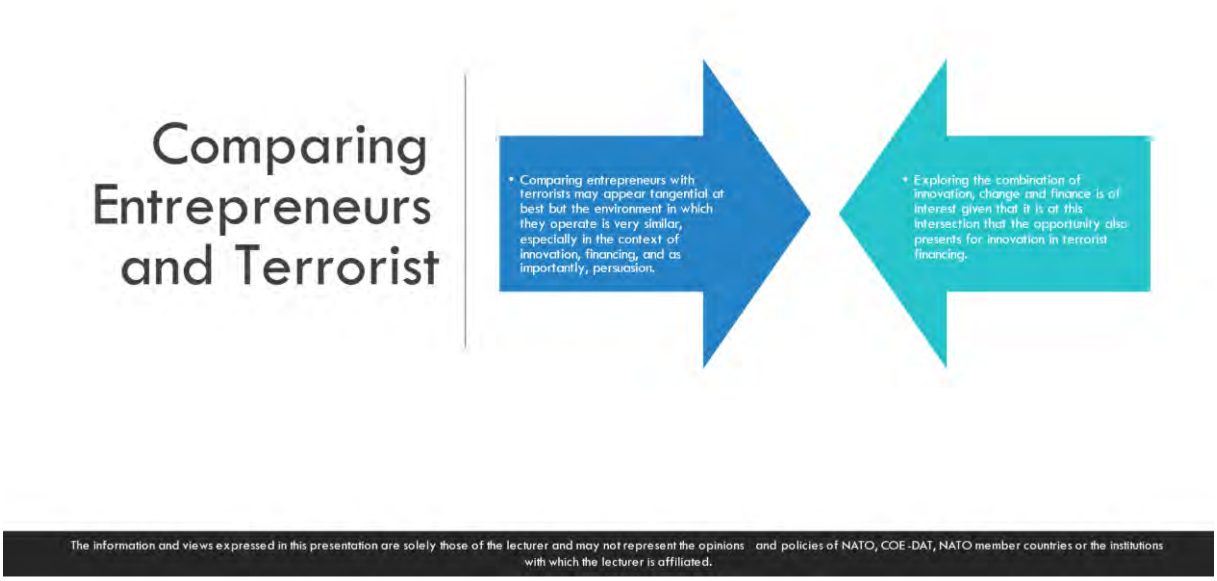


Terrorist Financing

Trend in research has been less focused towards innovation as it relates to terrorist financing especially regarding the opportunities and drivers that influence such innovation.

Surprising, given that terrorist financing is often postulated as a requisite of terrorist activity.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

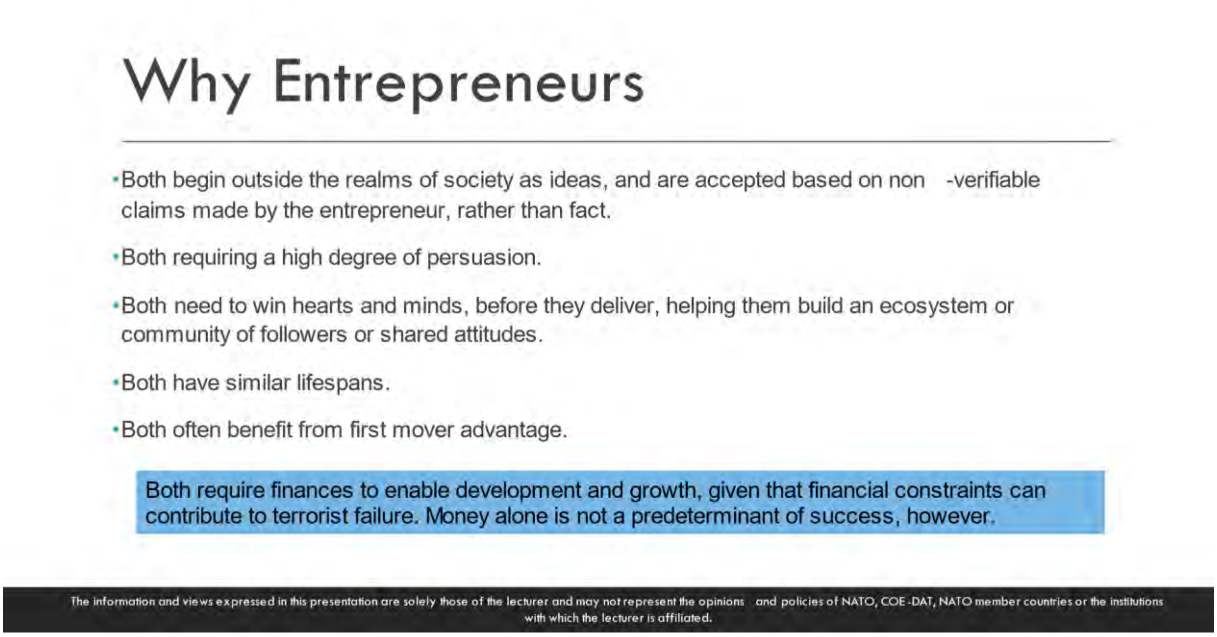


Comparing Entrepreneurs and Terrorist

- Comparing entrepreneurs with terrorists may appear tangential at best but the environment in which they operate is very similar, especially in the context of innovation, financing, and as importantly, persuasion.

- Exploring the combination of innovation, change and finance is of interest given that it is at this intersection that the opportunity also presents for innovation in terrorist financing.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

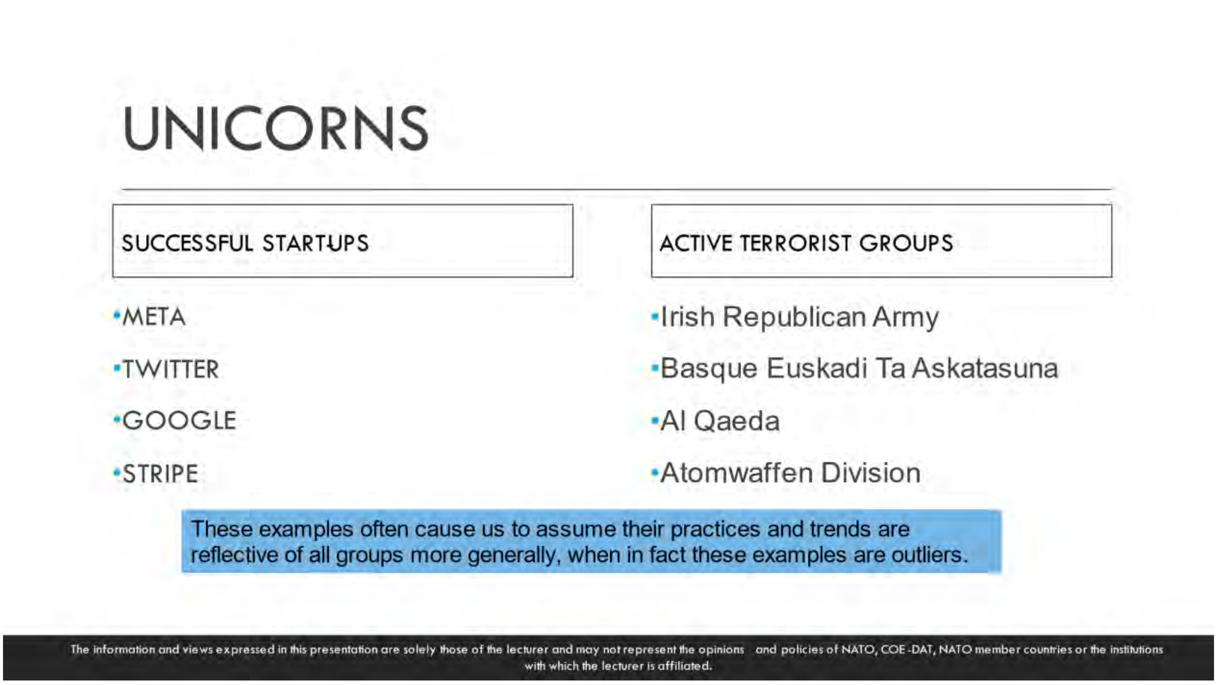


Why Entrepreneurs

- Both begin outside the realms of society as ideas, and are accepted based on non -verifiable claims made by the entrepreneur, rather than fact.
- Both requiring a high degree of persuasion.
- Both need to win hearts and minds, before they deliver, helping them build an ecosystem or community of followers or shared attitudes.
- Both have similar lifespans.
- Both often benefit from first mover advantage.

Both require finances to enable development and growth, given that financial constraints can contribute to terrorist failure. Money alone is not a predeterminant of success, however.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

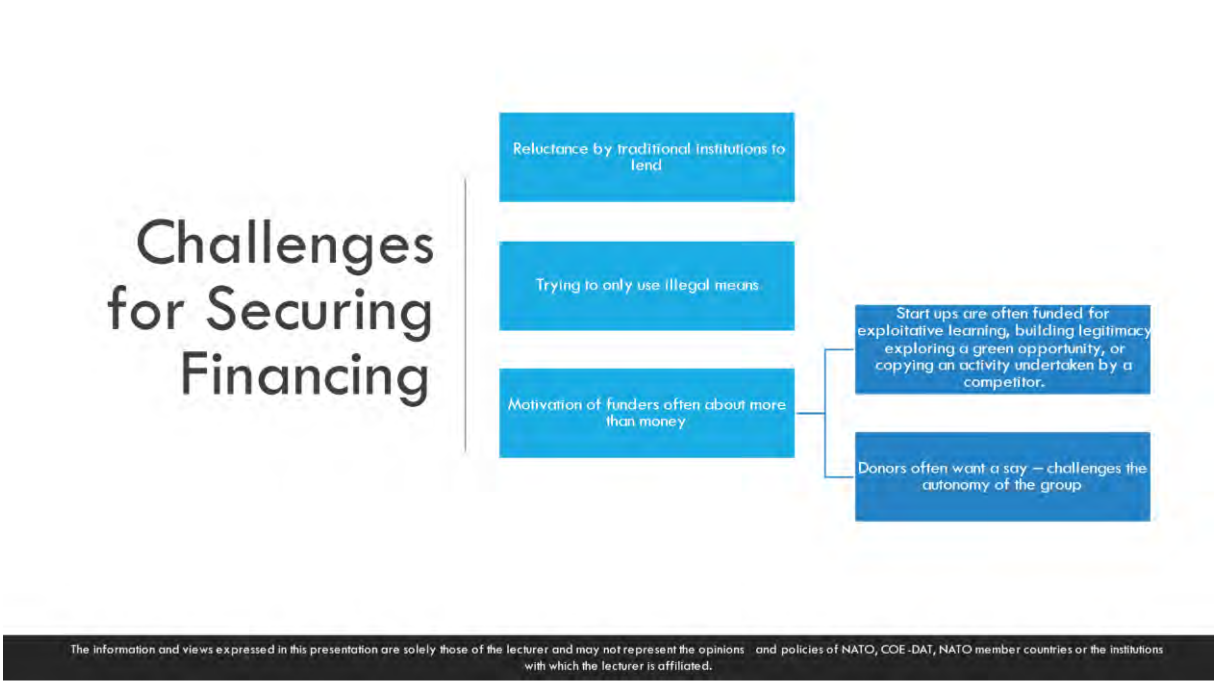


UNICORNS

SUCCESSFUL STARTUPS	ACTIVE TERRORIST GROUPS
META	Irish Republican Army
TWITTER	Basque Euskadi Ta Askatasuna
GOOGLE	Al Qaeda
STRIPE	Atomwaffen Division

These examples often cause us to assume their practices and trends are reflective of all groups more generally, when in fact these examples are outliers.

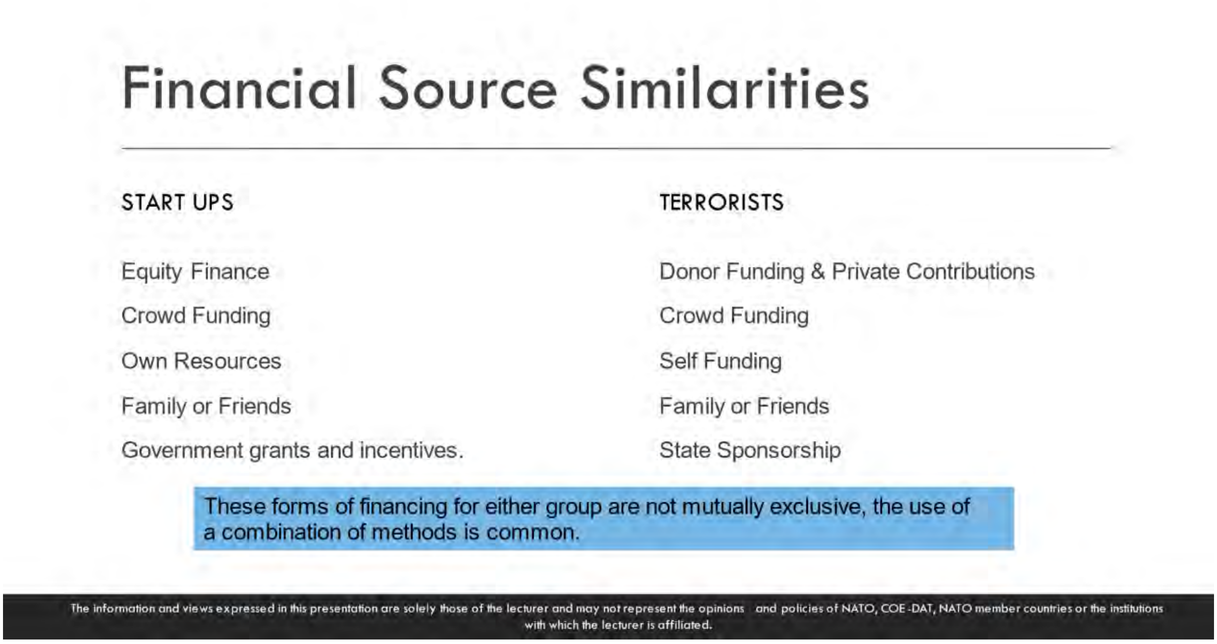
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Challenges for Securing Financing

- Reluctance by traditional institutions to lend
- Trying to only use illegal means
- Motivation of funders often about more than money
  - Start ups are often funded for exploitative learning, building legitimacy exploring a green opportunity, or copying an activity undertaken by a competitor.
  - Donors often want a say – challenges the autonomy of the group

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.

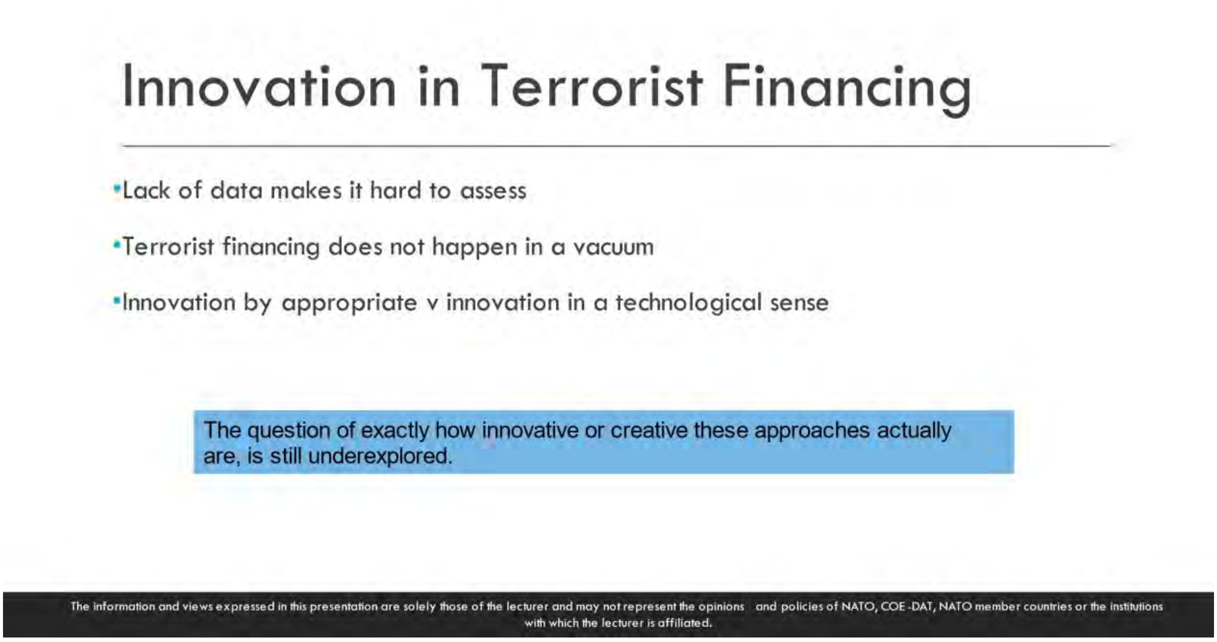


Financial Source Similarities

START UPS	TERRORISTS
Equity Finance	Donor Funding & Private Contributions
Crowd Funding	Crowd Funding
Own Resources	Self Funding
Family or Friends	Family or Friends
Government grants and incentives.	State Sponsorship

These forms of financing for either group are not mutually exclusive, the use of a combination of methods is common.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

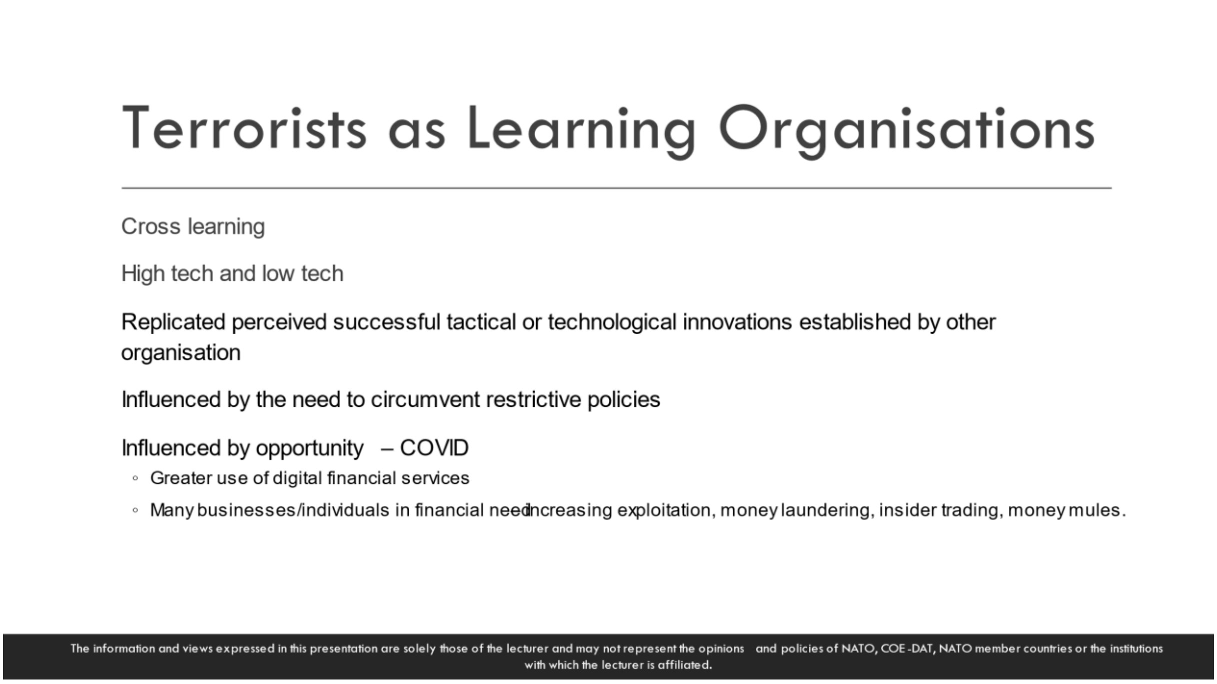


Innovation in Terrorist Financing

- Lack of data makes it hard to assess
- Terrorist financing does not happen in a vacuum
- Innovation by appropriate v innovation in a technological sense

The question of exactly how innovative or creative these approaches actually are, is still underexplored.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Terrorists as Learning Organisations

Cross learning

High tech and low tech

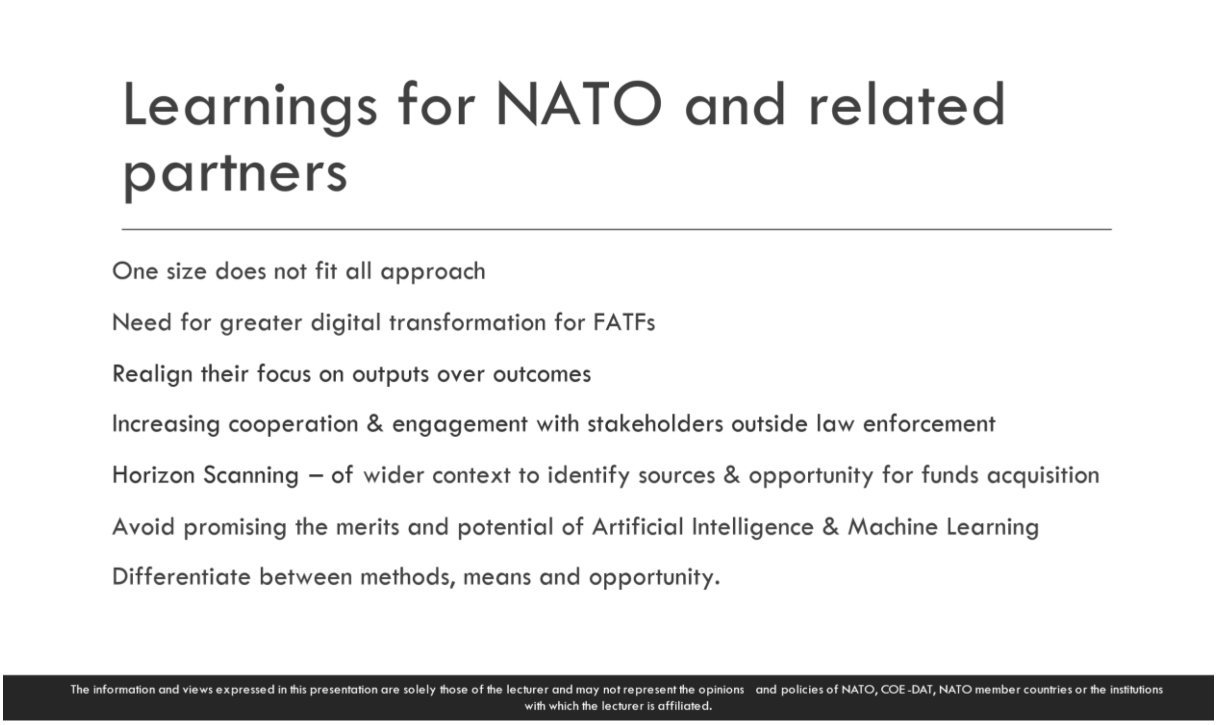
Replicated perceived successful tactical or technological innovations established by other organisation

Influenced by the need to circumvent restrictive policies

Influenced by opportunity – COVID

- Greater use of digital financial services
- Many businesses/individuals in financial needIncreasing exploitation, money laundering, insider trading, money mules.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Learnings for NATO and related partners

One size does not fit all approach

Need for greater digital transformation for FATFs

Realign their focus on outputs over outcomes

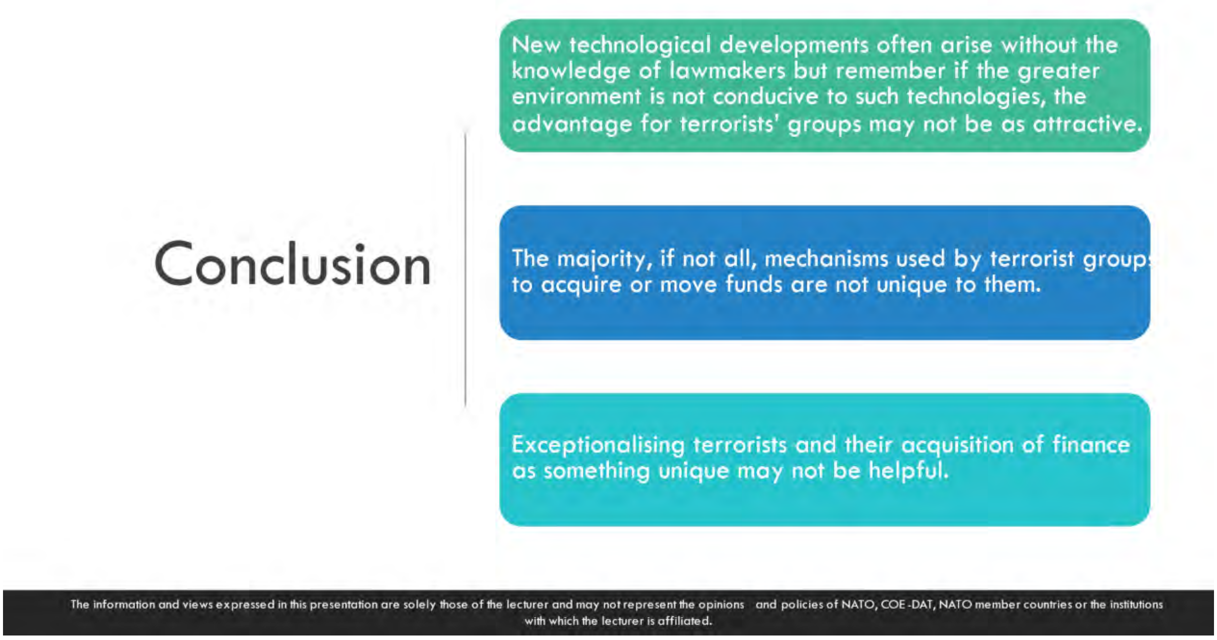
Increasing cooperation & engagement with stakeholders outside law enforcement

Horizon Scanning – of wider context to identify sources & opportunity for funds acquisition

Avoid promising the merits and potential of Artificial Intelligence & Machine Learning

Differentiate between methods, means and opportunity.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Conclusion

New technological developments often arise without the knowledge of lawmakers but remember if the greater environment is not conducive to such technologies, the advantage for terrorists' groups may not be as attractive.

The majority, if not all, mechanisms used by terrorist groups to acquire or move funds are not unique to them.

Exceptionalising terrorists and their acquisition of finance as something unique may not be helpful.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

The Uses of Cryptocurrency in Terrorism Financing and Money Laundering

Ms. Liat SHETRET

Elliptic shared perspectives and insights with regards to how cryptocurrencies can be misused for terrorism finance and money laundering purposes. Elliptic also shared examples of how those risks may be mitigated. The presentation begins with a brief timeline and overview of the evolution of cryptocurrencies including the dominant marketshare of bitcoin. The presentation continued discussing the 'State of Crypto Crime' and described opportunistic instances in which cryptocurrencies are used for ransomware, on darknet markets, in terrorism, thefts, scams and DeFi exploits. The presentation also included a case study example from the Twitter exploit in June 2020 and concludes by demonstrating the increase in regulation globally and the dramatic drop in illicit use of cryptocurrencies globally. For additional information please see www.elliptic.co.

Presentation

Confidential–Not for Sharing

Merhaba!

The Uses of Cryptocurrency in Terrorism Financing and Mone y Laundering

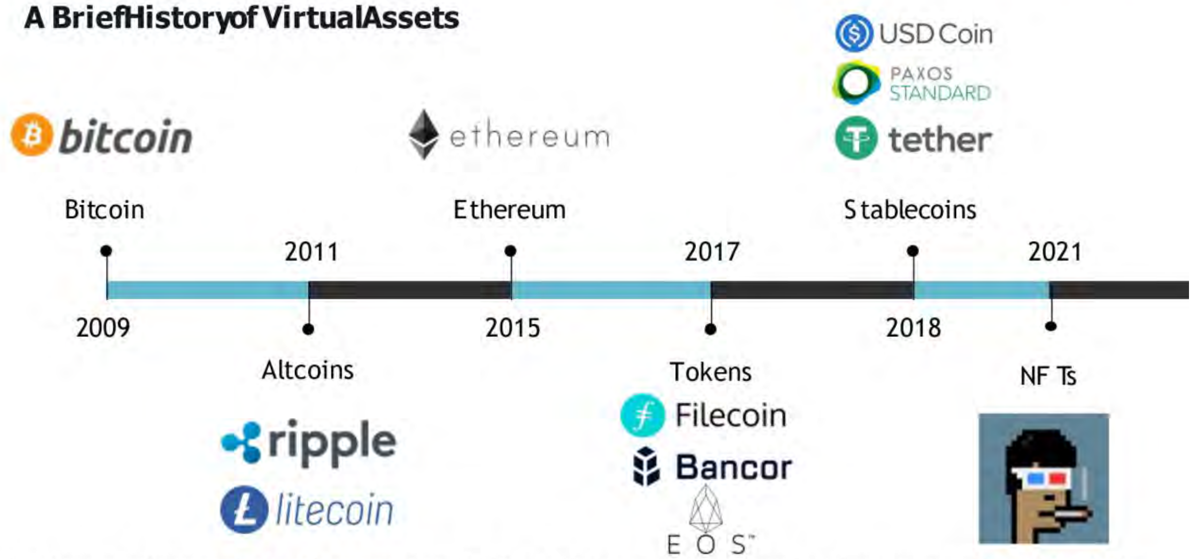
Liat Shetret| 18-19 October, 2022

ELLIPTIC

Disclaimer

The informationand viewsexpressedin this presentationare solely those of the lecturer and may not representthe opinions and policies of NATO, COE-DAT, NATOmembercountriesor theinstitutionswithwhichthelectureris affiliated

A BriefHistoryof VirtualAssets



Bitcoin 2009

2011 Altcoins

Ethereum 2015

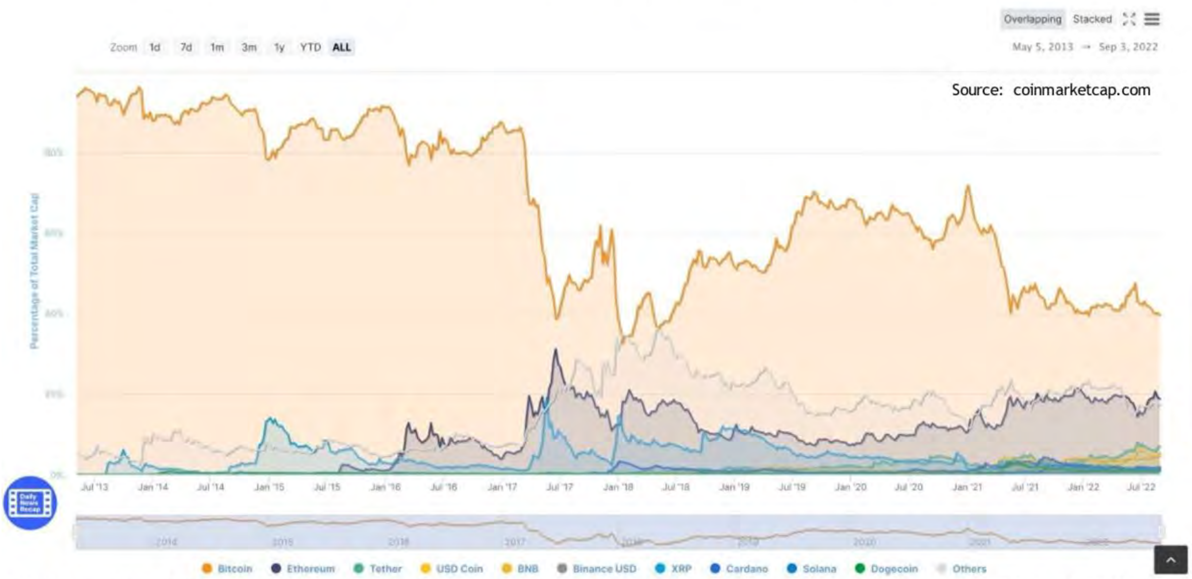
2017 Tokens

Stablecoins 2018

2021 NFTs

The information and viewsexpressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO membercountriesor theinstitutionswithwhichthelectureris affiliated.

Major Cryptoassets By Percentage of Total Market Capitalization (Bitcoin Dominance Chart)



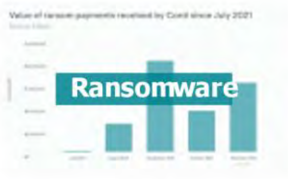
Source: coinmarketcap.com

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

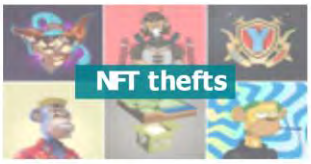
ELLIPTIC

TheState of Crypto Crime

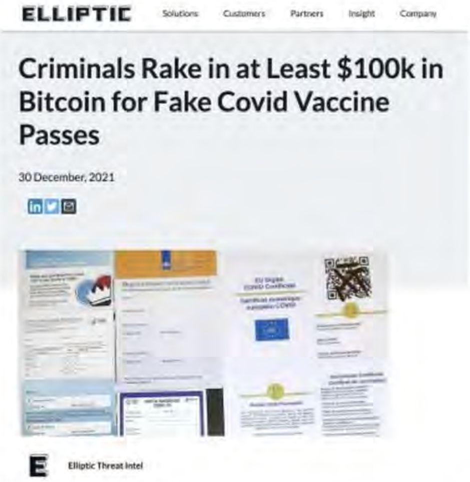
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



THE HAMAS BITCOIN FUNDRAISING CAMPAIGN
$108,000
total dona
Terrorism
$73,000
since 10th May
ELLIPTIC
FEB 2021
MAR 2021
APR 2021
MAY 2021

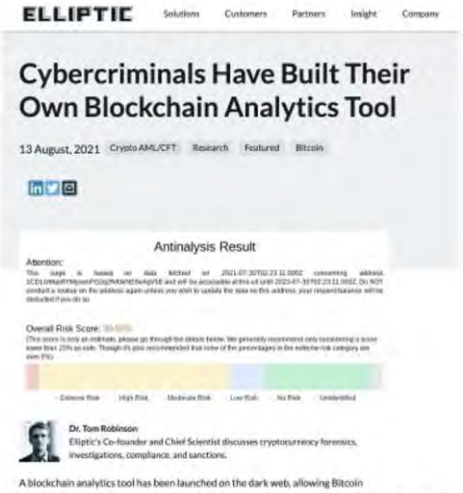


‘Temporary’ crimes



Criminals Rake in at Least $100k in Bitcoin for Fake Covid Vaccine Passes

30 December, 2021



Cybercriminals Have Built Their Own Blockchain Analytics Tool

13 August, 2021 Crypto AML/CFT Research Featured Bitcoin

Antinalysis Result

Attention:
This page is based on data fetched at 2021-07-30T02:23:11.000Z concerning address [illegible] and will be accessible at this url until 2023-07-30T02:23:11.000Z. Do NOT conduct a lookup on the address again unless you wish to update the data on this address, your request balance will be deducted if you do so.

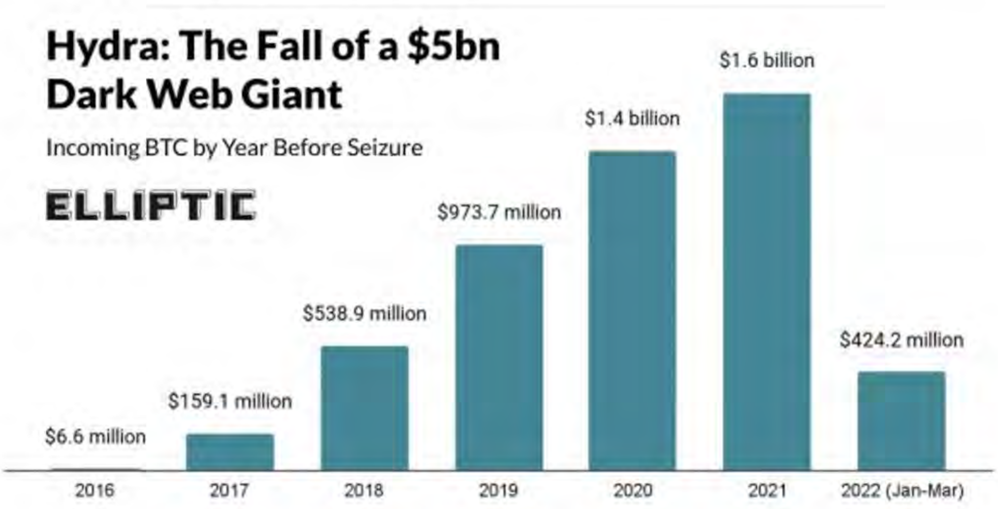
Overall Risk Score: [illegible]
(This score is only an estimate, please go through the details below. We generally recommend only considering a score lower than 25% as safe. Though it's also recommended that none of the percentages in the extreme-risk category are over 5%.)

Dr. Tom Robinson
Elliptic's Co-founder and Chief Scientist discusses cryptocurrency forensics, investigations, compliance, and sanctions.

A blockchain analytics tool has been launched on the dark web, allowing Bitcoin

The 6information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

ELLIPTIC



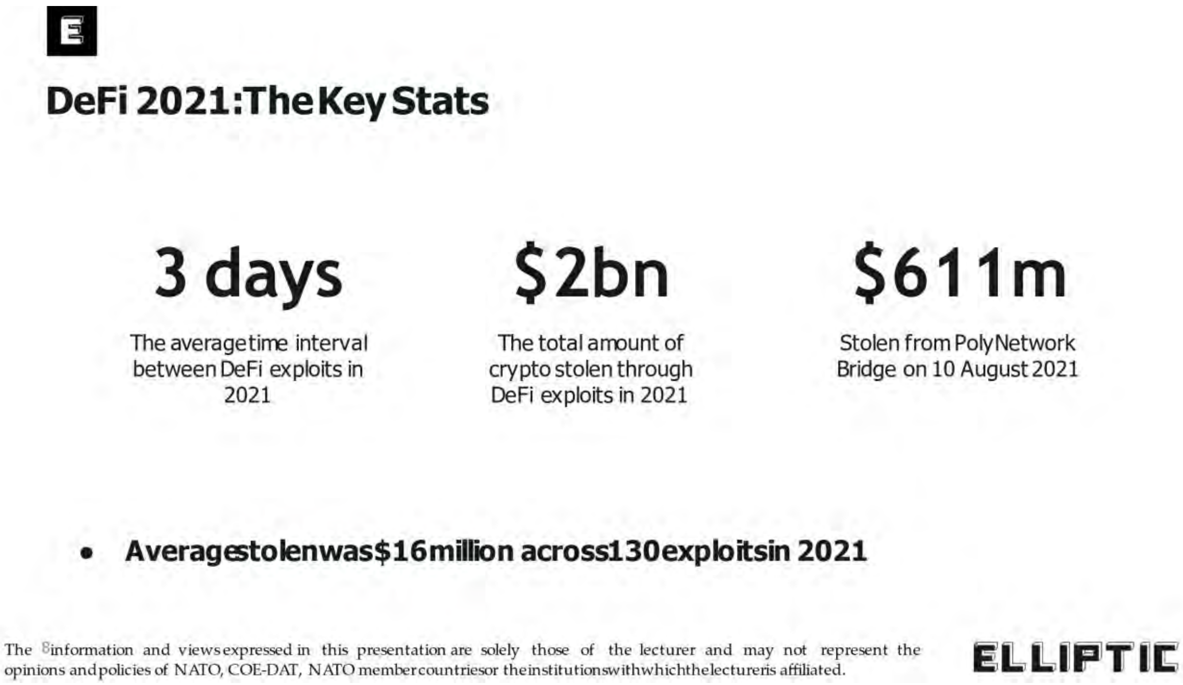
Hydra: The Fall of a $5bn Dark Web Giant

Incoming BTC by Year Before Seizure

ELLIPTIC

The 7information and viewsexpressed in this presentation are solely those of the lecturer and may not represent the opinions andpolicies of NATO, COE-DAT, NATO membercountriesor theinstitutionswithwhichthelectureris affiliated.

ELLIPTIC



DeFi 2021:TheKey Stats

3 days

The averagetime interval between DeFi exploits in 2021

$2bn

The total amount of crypto stolen through DeFi exploits in 2021

$611m

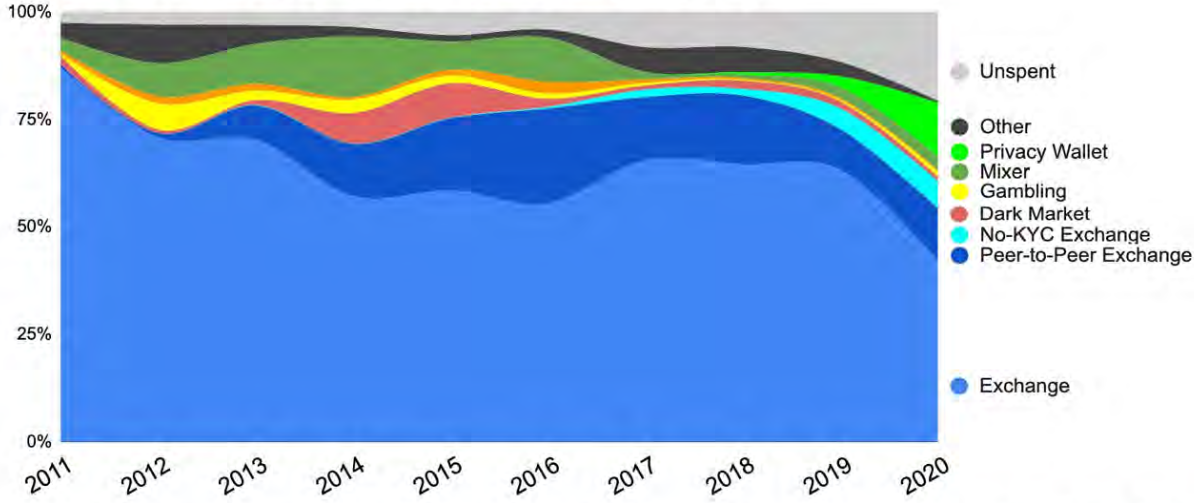
Stolen from PolyNetwork Bridge on 10 August 2021

- **Averagestolenwas$16million across130exploitsin 2021**

The 8information and viewsexpressed in this presentation are solely those of the lecturer and may not represent the opinions andpolicies of NATO, COE-DAT, NATO membercountriesor theinstitutionswithwhichthelectureris affiliated.

ELLIPTIC

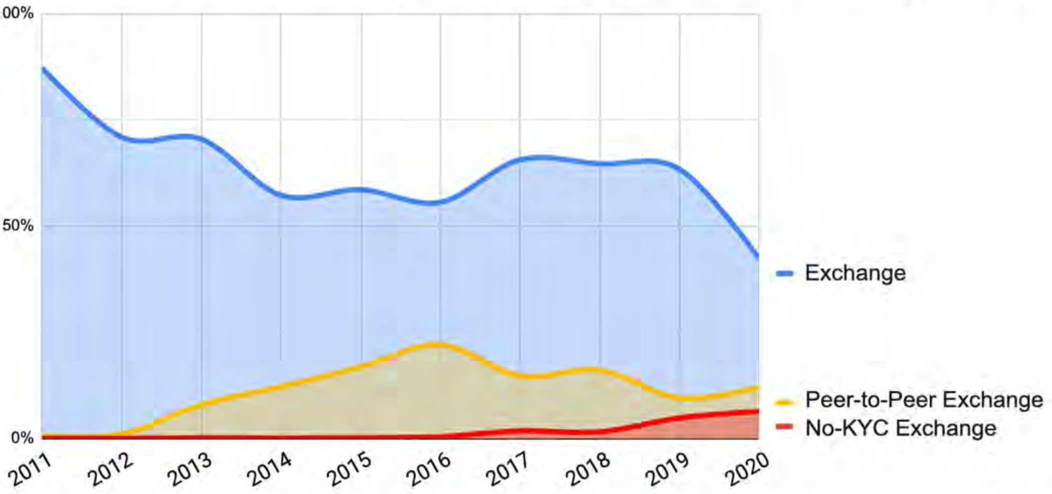
Destination of Criminal Proceeds in Bitcoin



The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

ELLIPTIC

Centralized/P2P Exchanges → Unregulated/Non-Compliant



The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

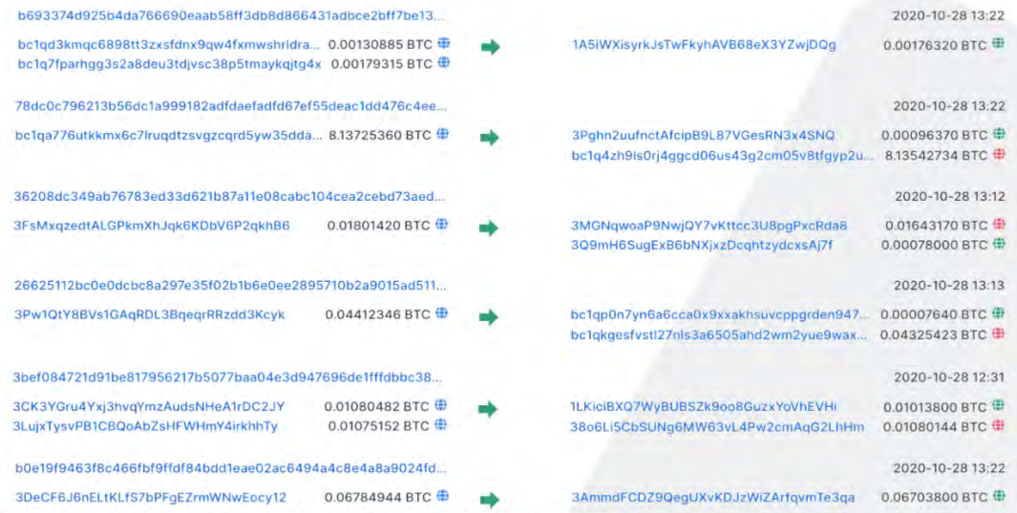
ELLIPTIC

Cryptocurrency on the Blockchain

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Confidential – Not for Sharing

Understanding and Tracing Cryptoassets

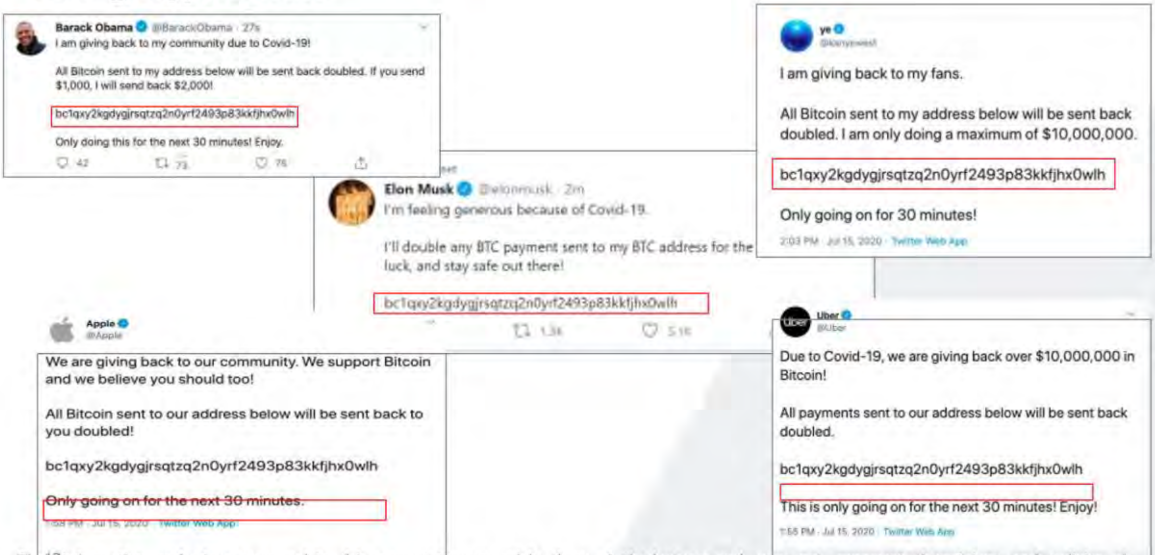


```
b693374d925b4da766690eaab58ff3db8d866431adbce2bff7be13...                                                       2020-10-28 13:22
bc1qd3kmqc6898tt3zxsfdnx9qw4fxmwshrldra... 0.00130885 BTC   ➡   1A5iWXisyrkJsTwFkyhAVB68eX3YZwjDQg            0.00176320 BTC
bc1q7fparhgg3s2a8deu3tdjvsc38p5tmaykqjtg4x 0.00179315 BTC

78dc0c796213b56dc1a999182adfdaefadfd67ef55deac1dd476c4ee...                                                       2020-10-28 13:22
bc1qa776utkkmx6c7lruqdtzsvgzcqrd5yw35dda... 8.13725360 BTC   ➡   3Pghn2uufnctAfcipB9L87VGesRN3x4SNQ            0.00096370 BTC
                                                                 bc1q4zh9ls0rj4ggcd06us43g2cm05v8tfgyp2u...     8.13542734 BTC

36208dc349ab76783ed33d621b87a11e08cabc104cea2cebd73aed...                                                         2020-10-28 13:12
3FsMxqzedtALGPkmXhJqk6KDbV6P2qkhB6         0.01801420 BTC   ➡   3MGNqwoaP9NwjQY7vKttcc3U8pgPxcRda8            0.01643170 BTC
                                                                 3Q9mH6SugExB6bNXjxzDcqhtzydcxsAj7f            0.00078000 BTC

26625112bc0e0dcbc8a297e35f02b1b6e0ee2895710b2a9015ad511...                                                        2020-10-28 13:13
3Pw1QtY8BVs1GAqRDL3BqeqrRRzdd3Kcyk         0.04412346 BTC   ➡   bc1qp0n7yn6a6cca0x9xxakhsuvcppgrden947...     0.00007640 BTC
                                                                 bc1qkgesfvstl27nls3a6505ahd2wm2yue9wax...     0.04325423 BTC

3bef084721d91be817956217b5077baa04e3d947696de1fffdbbc38...                                                        2020-10-28 12:31
3CK3YGru4Yxj3hvqYmzAudsNHeA1rDC2JY         0.01080482 BTC   ➡   1LKiciBXQ7WyBUBSZk9oo8GuzxYoVhEVHi            0.01013800 BTC
3LujxTysvPB1CBQoAbZsHFWHmY4irkhhTy         0.01075152 BTC        38o6Li5CbSUNg6MW63vL4Pw2cmAqG2LhHm            0.01080144 BTC

b0e19f9463f8c466fbf9ffdf84bdd1eae02ac6494a4c8e4a8a9024fd...                                                       2020-10-28 13:22
3DeCF6J6nELtKLfS7bPFgEZrmWNwEocy12         0.06784944 BTC   ➡   3AmmdFCDZ9QegUXvKDJzWiZArfqvmTe3qa            0.06703800 BTC
```

The 12 information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Confidential–Not for Sharing

Tracing Cryptoassets



Barack Obama @BarackObama · 27s

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send $1,000, I will send back $2,000!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only doing this for the next 30 minutes! Enjoy.

42 73 76

Elon Musk @elonmusk · 2m

I'm feeling generous because of Covid-19.

I'll double any BTC payment sent to my BTC address for the next hour. Good luck, and stay safe out there!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

1.3K 5.1K

ye @kanyewest

I am giving back to my fans.

All Bitcoin sent to my address below will be sent back doubled. I am only doing a maximum of $10,000,000.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only going on for 30 minutes!

2:03 PM · Jul 15, 2020 · Twitter Web App

Apple @Apple

We are giving back to our community. We support Bitcoin and we believe you should too!

All Bitcoin sent to our address below will be sent back to you doubled!

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

Only going on for the next 30 minutes.

1:58 PM · Jul 15, 2020 · Twitter Web App

Uber @Uber

Due to Covid-19, we are giving back over $10,000,000 in Bitcoin!

All payments sent to our address below will be sent back doubled.

bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

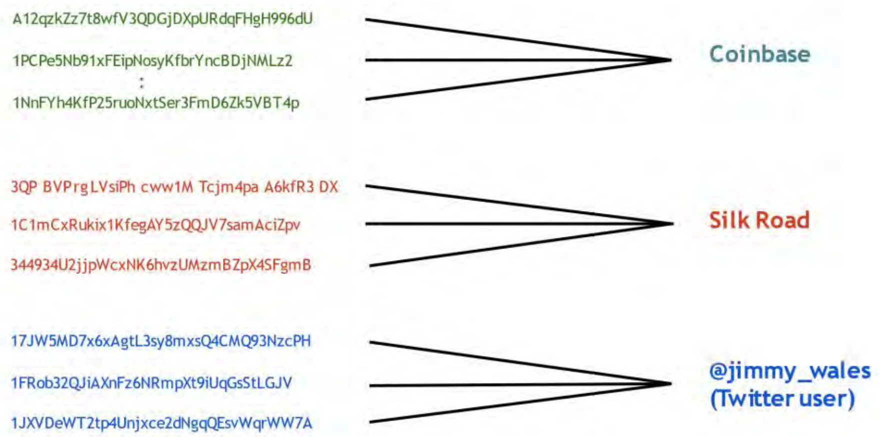
This is only going on for the next 30 minutes! Enjoy!

1:55 PM · Jul 15, 2020 · Twitter Web App

The 13 information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Confidential–Not for Sharing

Clustering Addresses



A12qzkZz7t8wfV3QDGjDXpURdqFHgH996dU

1PCPe5Nb91xFEipNosyKfbrYncBDjNMLz2

:

1NnFYh4KfP25ruoNxtSer3FmD6Zk5VBT4p

Coinbase

3QPBVPrgLVsiPhcww1MTcjm4paA6kfR3DX

1C1mCxRukix1KfegAY5zQQJV7samAciZpv

344934U2jjpWcxNK6hvzUMzmBZpX4SFgmB

Silk Road

17JW5MD7x6xAgtL3sy8mxsQ4CMQ93NzcPH

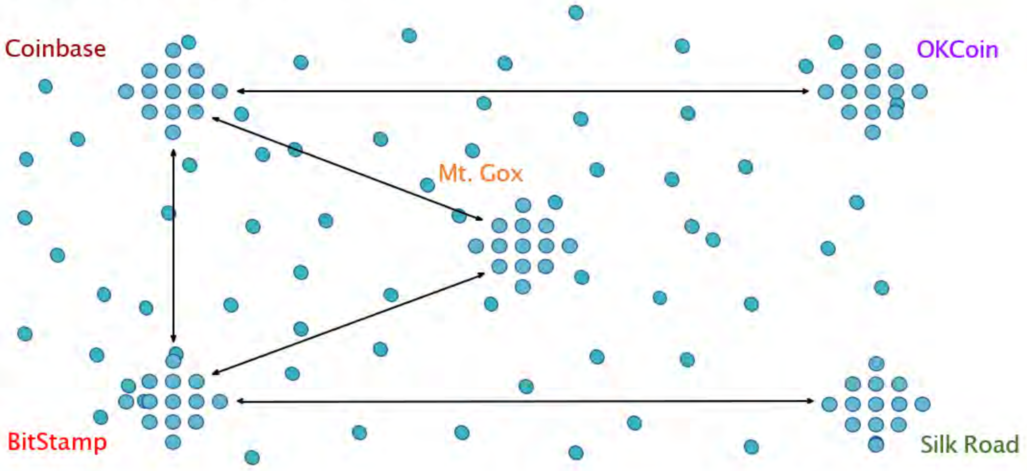
1FRob32QJiAXnFz6NRmpXt9iUqGsStLGJV

1JXVDeWT2tp4Unjxce2dNgqQEsvWqrWW7A

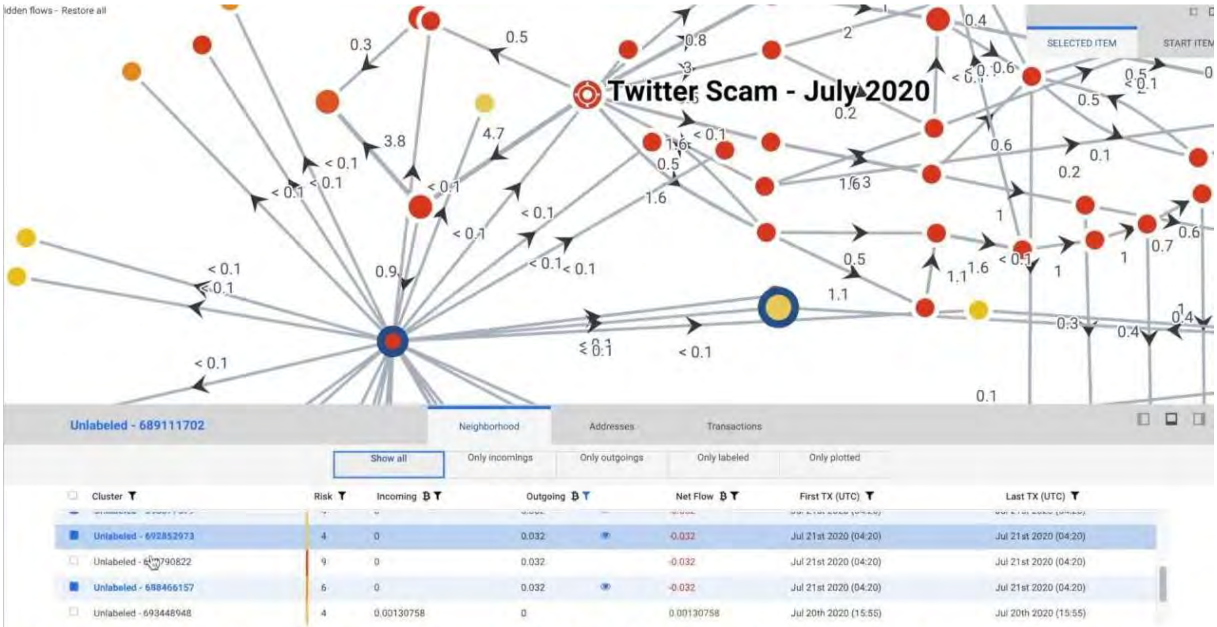
@jimmy_wales
(Twitter user)

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Understanding the Blockchain



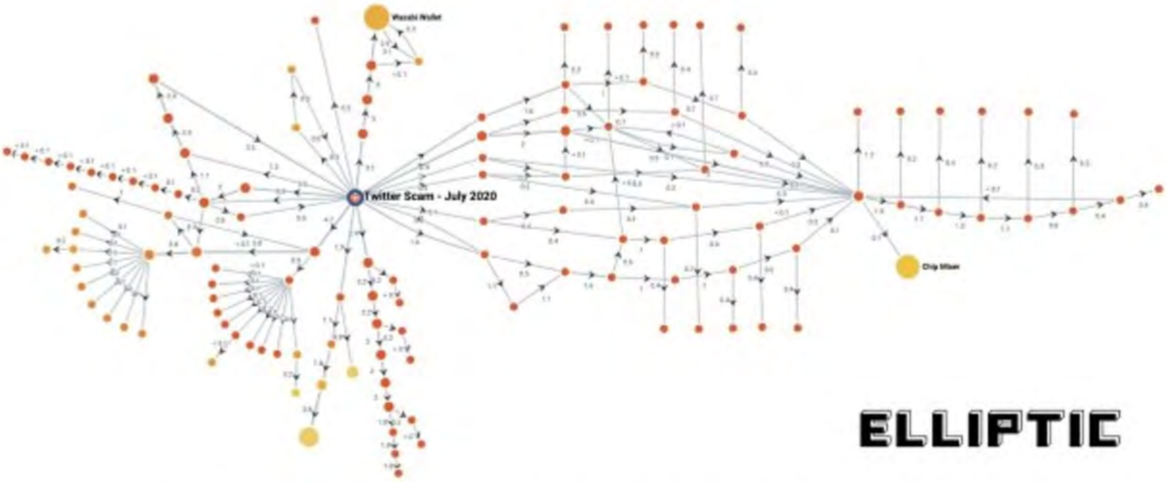
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Unlabeled - 689111702

Cluster	Risk	Incoming Ƀ	Outgoing Ƀ	Net Flow Ƀ	First TX (UTC)	Last TX (UTC)
■ Unlabeled - 692852973	4	0	0.032	-0.032	Jul 21st 2020 (04:20)	Jul 21st 2020 (04:20)
□ Unlabeled - 6[illegible]790822	9	0	0.032	-0.032	Jul 21st 2020 (04:20)	Jul 21st 2020 (04:20)
■ Unlabeled - 688466157	6	0	0.032	-0.032	Jul 21st 2020 (04:20)	Jul 21st 2020 (04:20)
□ Unlabeled - 693448948	4	0.00130758	0	0.00130758	Jul 20th 2020 (15:55)	Jul 20th 2020 (15:55)

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



ELLIPTIC

17 The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Tracing Cryptoassets

Twitter hack: US and UK teens arrested over breach of celebrity accounts

Three men charged in hack that saw accounts of Barack Obama, Joe Biden and Elon Musk compromised in bitcoin scam

BBC NEWS

Technology

Twitter hack: Exchange 'blocked 1,000 Bitcoin transactions'

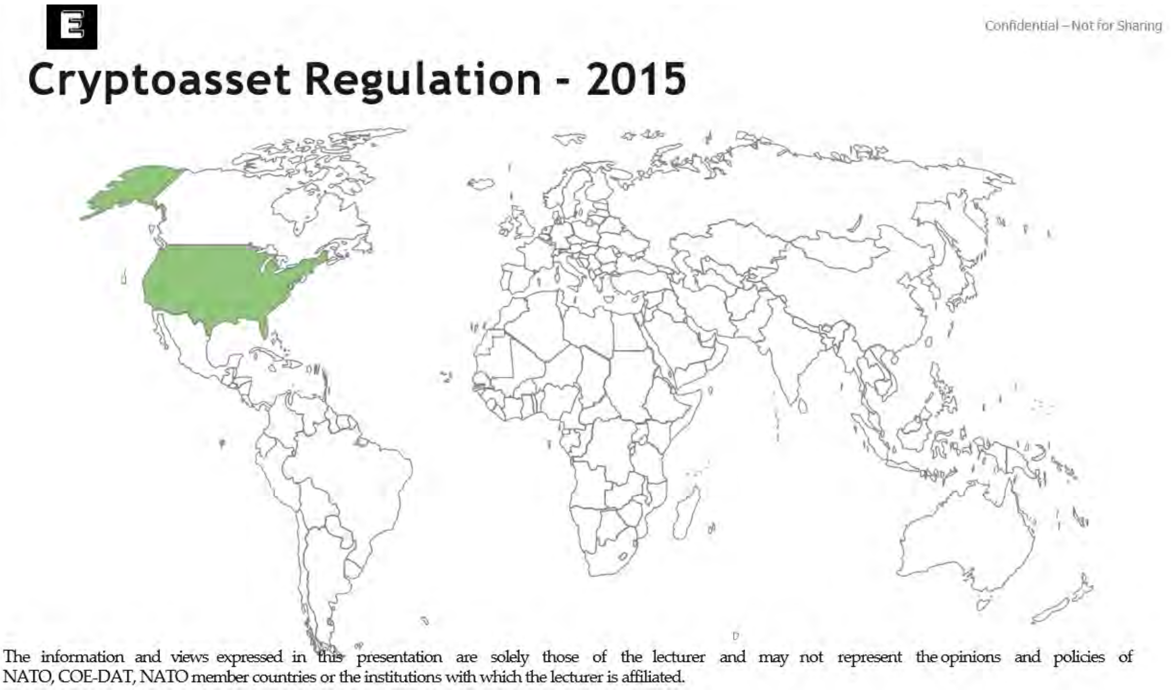
21 July 2020

Elon Musk, Kim Kardashian and Barack Obama are among victims of the hack

18 The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

How are we doing on regulation?

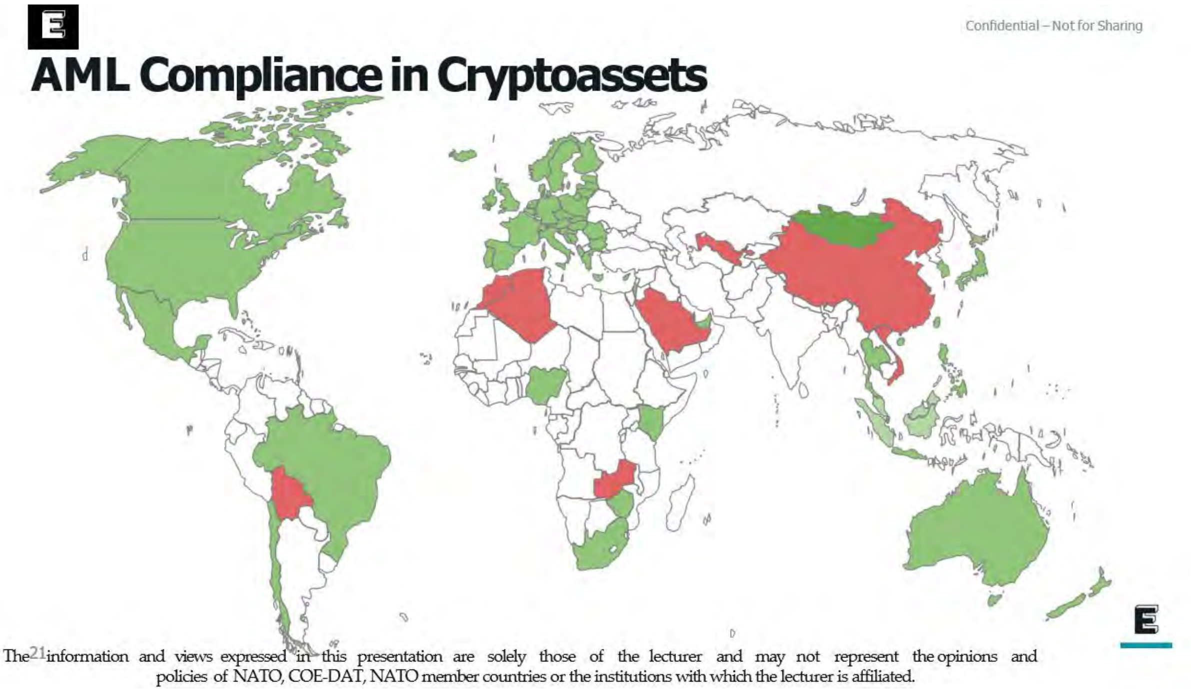
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Confidential – Not for Sharing

Cryptoasset Regulation - 2015

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

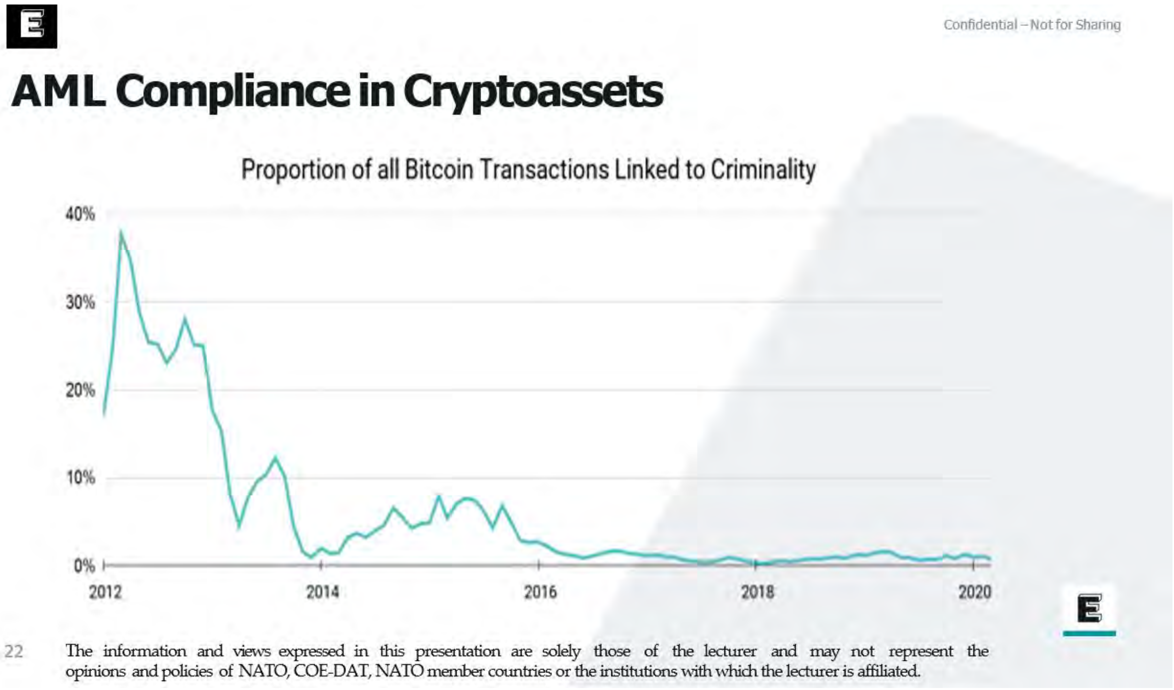


Confidential – Not for Sharing

AML Compliance in Cryptoassets

21

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Confidential – Not for Sharing

AML Compliance in Cryptoassets

Proportion of all Bitcoin Transactions Linked to Criminality

22

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

BlockchainAnalytics

- Used to satisfy requirementsto monitor customer transactionsand identify the source/destination of customer funds
- Allows regulatedbusinessesto:
    - Pre-screen customer transactionsto identify high risk or sanctioned wallets for KYC/CDD purposes
    - Follow customer transactionsthrough multiple "hops"(transfers through multiple wallets)to determineif they interact with illicit entities
    - Conduct extensive investigationsin support of suspiciousactivity report (SAR) filing
- Open-source blockchain explorer tools exist, but commercialsoftware contains much more reliable data,automation,and more sophisticated functionality suited for a regulatedenvironment

The information and views expressed in this presentation are solely those of the lecturer and may not represent theopinions and policies of NATO, COE-DAT, NATO membercountriesor theinstitutionswithwhichthelecturer is affiliated.

ELLIPTIC

Confidential–Not for Sharing

Tools of theTrade

Transactio Screening
Elliptic Navigator

- Identify financial crime risks in virtual asset transactions
- Drill downto source & destination of funds

Wallet Screening
Elliptic Lens

- De-anonymizecrypto wallets
- Identify walletsassociated with illicit, high risk, and sanctioned actors

BlockchainInvestigations
Elliptic Investigator

- Perform deep investigations
- Investigateboth transactions and addresses
- "Follow the money" with a graphical interface

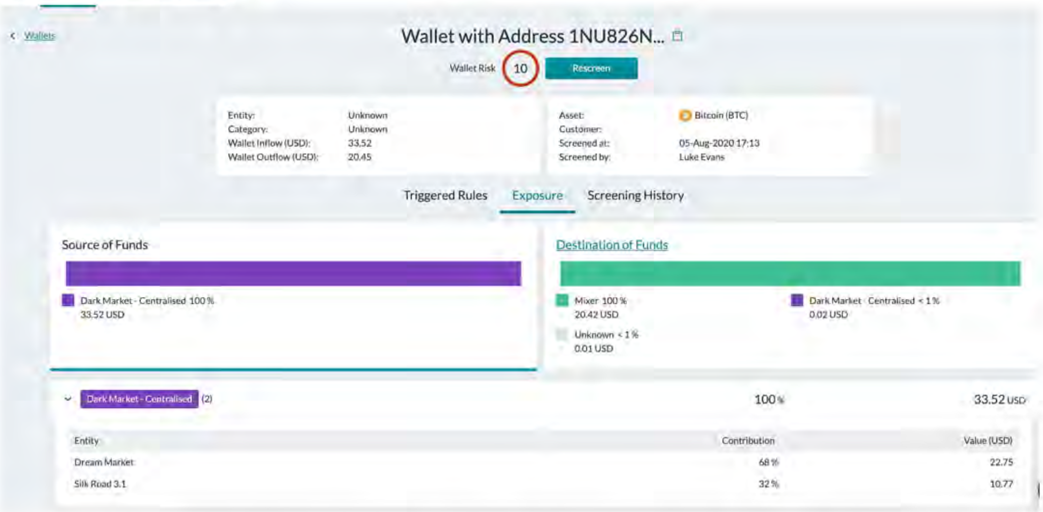
VASPRiskIndicators
Elliptic Discovery

- EvaluateVASPswith risk score for each entity
- Supplementwith rich profiles of VASPs,including historical transactional information

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO membercountriesor theinstitutionswithwhichthelectureris affiliated.

Confidential – Not for Sharing

End-to-End Visibility



< Wallets

Wallet with Address 1NU826N...

Wallet Risk 10 Rescreen

Entity:	Unknown
Category:	Unknown
Wallet Inflow (USD):	33.52
Wallet Outflow (USD):	20.45

Asset:	Bitcoin (BTC)
Customer:	
Screened at:	05-Aug-2020 17:13
Screened by:	Luke Evans

Triggered Rules | Exposure | Screening History

Source of Funds

- Dark Market - Centralised 100 %
33.52 USD

Destination of Funds

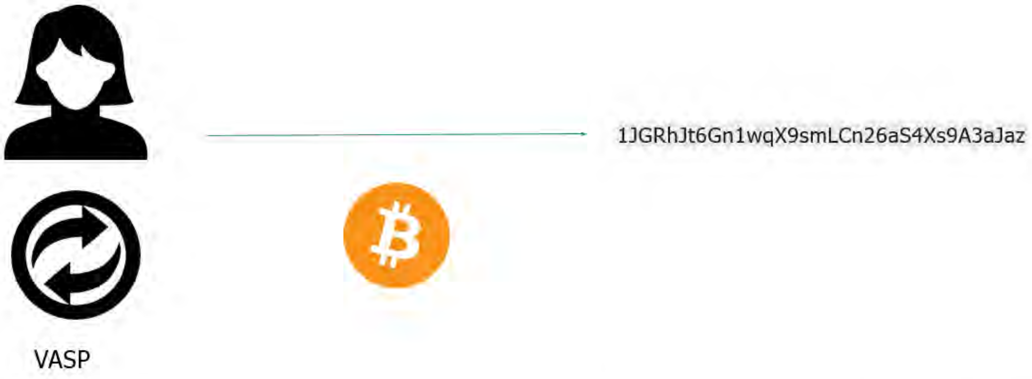
- Mixer 100 %
20.42 USD
- Dark Market · Centralised < 1 %
0.02 USD
- Unknown < 1 %
0.01 USD

Dark Market - Centralised (2) 100 % 33.52 USD

Entity	Contribution	Value (USD)
Dream Market	68 %	22.75
Silk Road 3.1	32 %	10.77

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

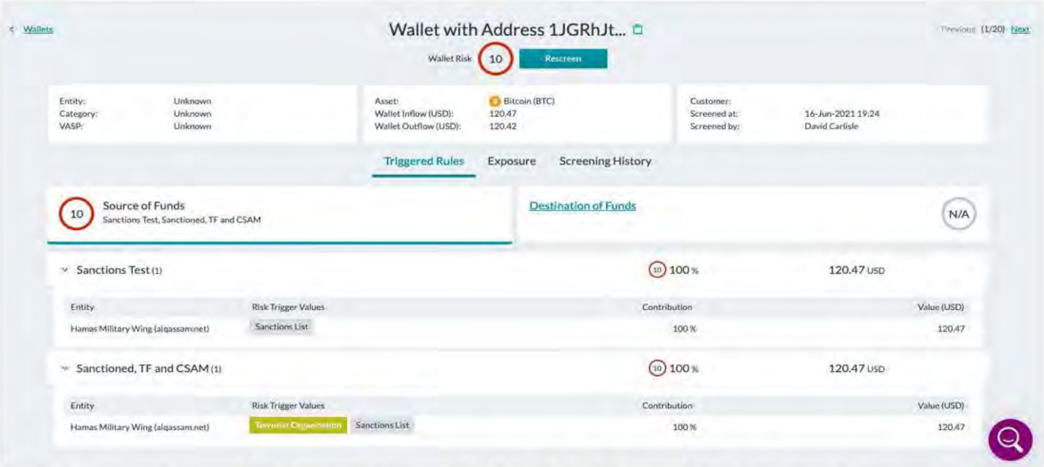
Blockchain Analytics: Pre-transaction screening



The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

ELLIPTIC

Blockchain Analytics: Pre-transaction screening



< Wallets

Wallet with Address 1JGRhJt...

Previous (1/20) Next

Wallet Risk 10 Rescreen

Entity: Unknown
Category: Unknown
VASP: Unknown

Asset: Bitcoin (BTC)
Wallet Inflow (USD): 120.47
Wallet Outflow (USD): 120.42

Customer:
Screened at: 16-Jun-2021 19:24
Screened by: David Carlisle

Triggered Rules | Exposure | Screening History

10 Source of Funds
Sanctions Test, Sanctioned, TF and CSAM

Destination of Funds N/A

Sanctions Test (1) — 10 100 % — 120.47 USD

Entity	Risk Trigger Values	Contribution	Value (USD)
Hamas Military Wing (alqassam.net)	Sanctions List	100 %	120.47

Sanctioned, TF and CSAM (1) — 10 100 % — 120.47 USD

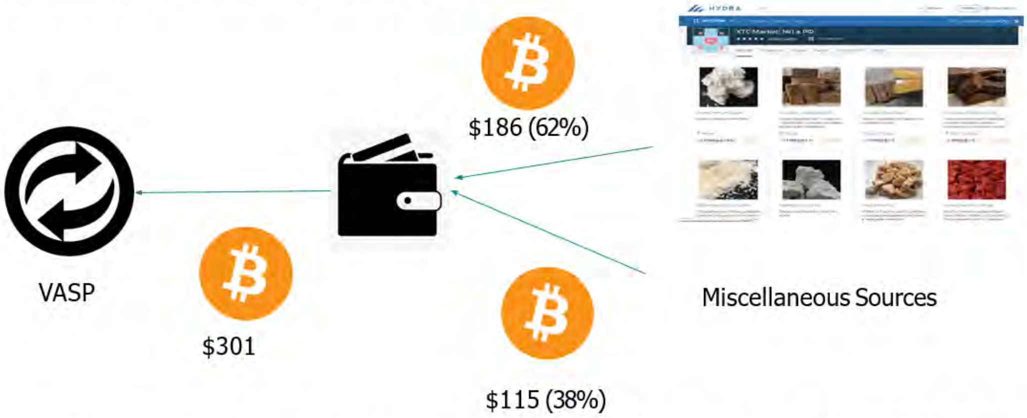
Entity	Risk Trigger Values	Contribution	Value (USD)
Hamas Military Wing (alqassam.net)	Terrorist Organisation Sanctions List	100 %	120.47

The 27 information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

ELLIPTIC

Blockchain Analytics: Assessing Transaction Exposure

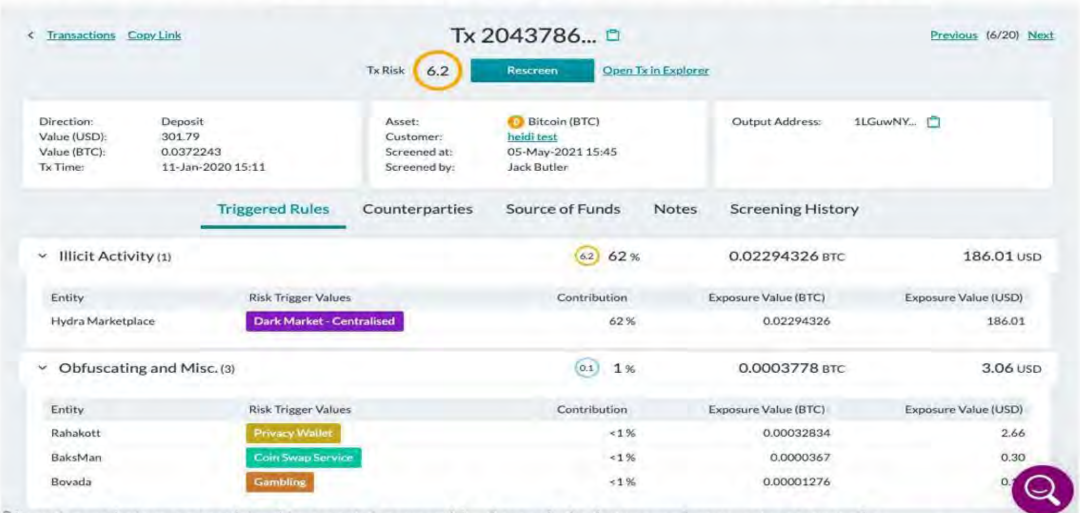
- In most cases, transactions that VASPs process will only have a partial exposure or tainting, so the VASP needs to decide how risky the transaction is



The 28 information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

ELLIPTIC

Blockchain Analytics: Assessing Transaction Exposure



< Transactions Copy Link

Tx 2043786...

Previous (6/20) Next

Tx Risk 6.2 Rescreen Open Tx in Explorer

Direction: Deposit
Value (USD): 301.79
Value (BTC): 0.0372243
Tx Time: 11-Jan-2020 15:11

Asset: Bitcoin (BTC)
Customer: heidi test
Screened at: 05-May-2021 15:45
Screened by: Jack Butler

Output Address: 1LGuwNY...

Triggered Rules | Counterparties | Source of Funds | Notes | Screening History

Illicit Activity (1) 6.2 62 % 0.02294326 BTC 186.01 USD

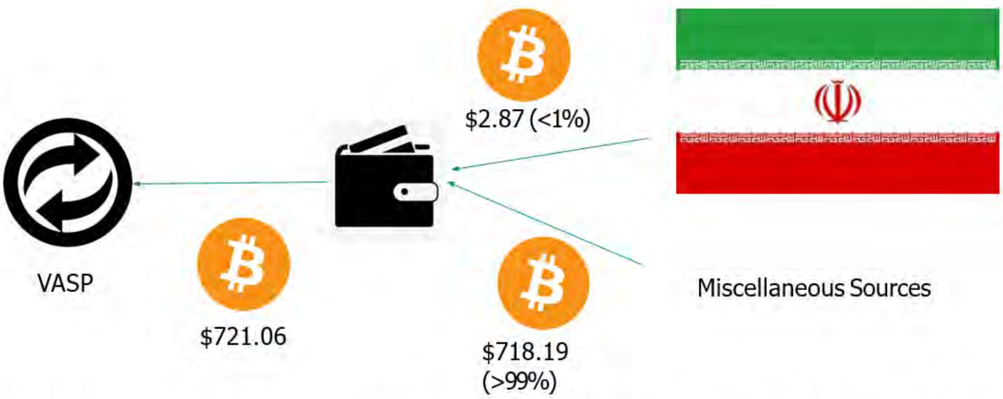
Entity	Risk Trigger Values	Contribution	Exposure Value (BTC)	Exposure Value (USD)
Hydra Marketplace	Dark Market - Centralised	62 %	0.02294326	186.01

Obfuscating and Misc. (3) 0.1 1 % 0.0003778 BTC 3.06 USD

Entity	Risk Trigger Values	Contribution	Exposure Value (BTC)	Exposure Value (USD)
Rahakott	Privacy Wallet	<1 %	0.00032834	2.66
BaksMan	Coin Swap Service	<1 %	0.0000367	0.30
Bovada	Gambling	<1 %	0.00001276	0.

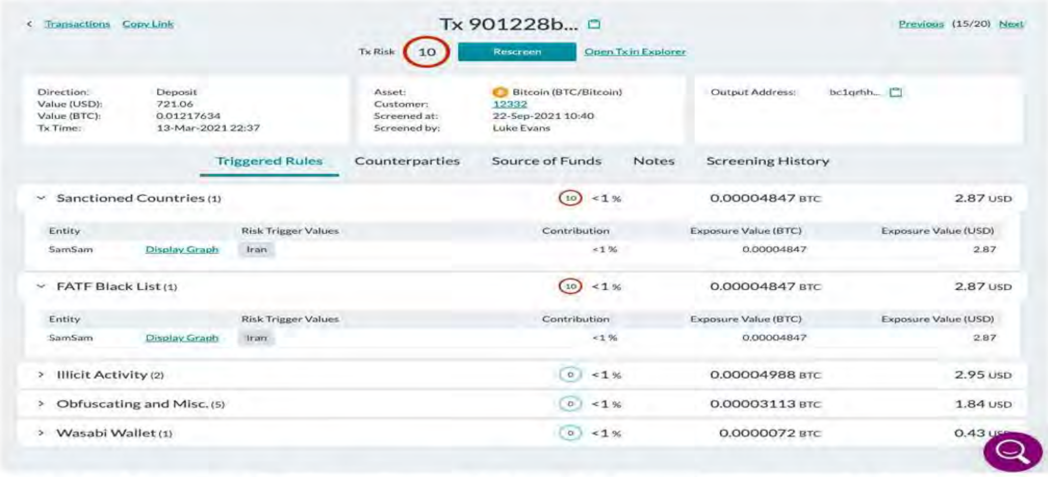
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Blockchain Analytics: Assessing Transaction Exposure



The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Blockchain Analytics: Assessing Transaction Exposure



< Transactions Copy Link

Tx 901228b...

Previous (15/20) Next

Tx Risk 10 Rescreen Open Tx in Explorer

Direction:	Deposit	Asset:	Bitcoin (BTC/Bitcoin)	Output Address:	bc1qrhh...
Value (USD):	721.06	Customer:	12332		
Value (BTC):	0.01217634	Screened at:	22-Sep-2021 10:40		
Tx Time:	13-Mar-2021 22:37	Screened by:	Luke Evans		

Triggered Rules | Counterparties | Source of Funds | Notes | Screening History

Sanctioned Countries (1)	10	<1 %	0.00004847 BTC	2.87 USD

Entity		Risk Trigger Values	Contribution	Exposure Value (BTC)	Exposure Value (USD)
SamSam	Display Graph	Iran	<1 %	0.00004847	2.87

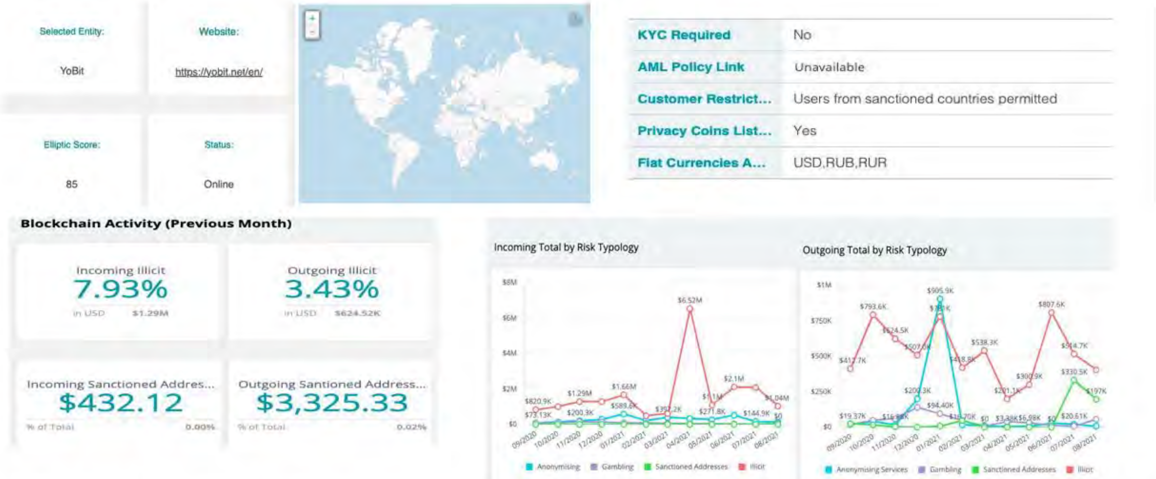
FATF Black List (1)	10	<1 %	0.00004847 BTC	2.87 USD

Entity		Risk Trigger Values	Contribution	Exposure Value (BTC)	Exposure Value (USD)
SamSam	Display Graph	Iran	<1 %	0.00004847	2.87

Illicit Activity (2)	0	<1 %	0.00004988 BTC	2.95 USD
Obfuscating and Misc. (5)	0	<1 %	0.00003113 BTC	1.84 USD
Wasabi Wallet (1)	0	<1 %	0.0000072 BTC	0.43 USD

The 3in1formation and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Licensing and Registration Assessments



Selected Entity:	Website:
YoBit	https://yobit.net/en/
Elliptic Score:	Status:
85	Online

KYC Required	No
AML Policy Link	Unavailable
Customer Restrict...	Users from sanctioned countries permitted
Privacy Coins List...	Yes
Fiat Currencies A...	USD,RUB,RUR

Blockchain Activity (Previous Month)

Incoming Illicit 7.93% in USD $1.29M	Outgoing Illicit 3.43% in USD $624.52K
Incoming Sanctioned Addres... $432.12 % of Total 0.00%	Outgoing Santioned Address... $3,325.33 % of Total 0.02%

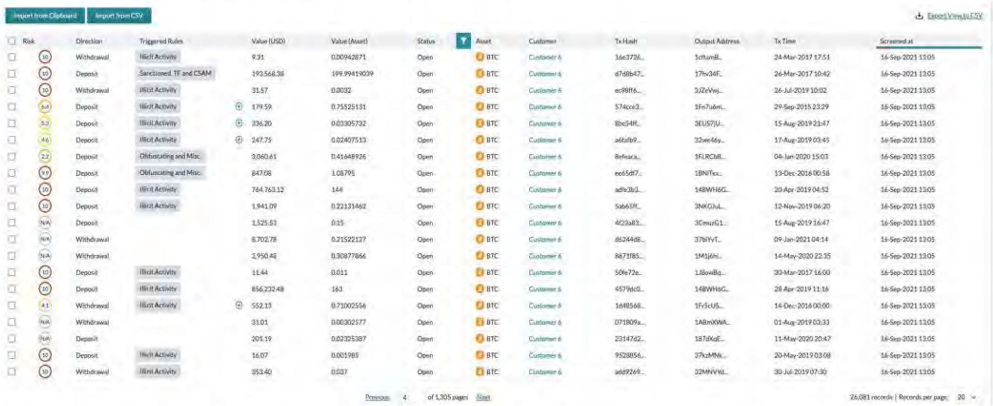
Incoming Total by Risk Typology

Outgoing Total by Risk Typology

The 3in2formation and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Ongoing Supervision

- Supervisors use blockchain analytics solutions to review the adequacy of VASPs' AML/CFT controls after they have been authorized



□	Risk	Direction	Triggered Rules		Value (USD)	Value (Asset)	Status	Asset	Customer	Tx Hash	Output Address	Tx Time	Screened at
□	10	Withdrawal	Illicit Activity		9.31	0.00942871	Open	BTC	Customer 6	16e3726...	1cftamB...	24-Mar-2017 17:51	16-Sep-2021 13:05
□	10	Deposit	Sanctioned, TF and CSAM		193,568.36	199.99419039	Open	BTC	Customer 6	d7d8b47...	17hv34F...	26-Mar-2017 10:42	16-Sep-2021 13:05
□	10	Withdrawal	Illicit Activity		31.57	0.0032	Open	BTC	Customer 6	ec98ff6...	3JZeVwj...	26-Jul-2019 10:02	16-Sep-2021 13:05
□	6.8	Deposit	Illicit Activity	⊕	179.59	0.75525131	Open	BTC	Customer 6	574cce3...	1Fn7u6m...	29-Sep-2015 23:29	16-Sep-2021 13:05
□	5.2	Deposit	Illicit Activity	⊕	336.20	0.03305732	Open	BTC	Customer 6	8bc54ff...	3EUS7jU...	15-Aug-2019 21:47	16-Sep-2021 13:05
□	4.6	Deposit	Illicit Activity	⊕	247.75	0.02407513	Open	BTC	Customer 6	a6fafb9...	32we46y...	17-Aug-2019 03:45	16-Sep-2021 13:05
□	2.2	Deposit	Obfuscating and Misc.		3,060.61	0.41648926	Open	BTC	Customer 6	8efeaca...	1FLRCbB...	04-Jan-2020 15:03	16-Sep-2021 13:05
□	9.9	Deposit	Obfuscating and Misc.		847.08	1.08795	Open	BTC	Customer 6	ee65df7...	1BNiTkx...	13-Dec-2016 00:58	16-Sep-2021 13:05
□	10	Deposit	Illicit Activity		764,763.12	144	Open	BTC	Customer 6	adfe3b3...	14BWH6G...	20-Apr-2019 04:52	16-Sep-2021 13:05
□	10	Deposit	Illicit Activity		1,941.09	0.22131462	Open	BTC	Customer 6	5ab65ff...	3NKGJuL...	12-Nov-2019 06:20	16-Sep-2021 13:05
□	N/A	Deposit			1,525.53	0.15	Open	BTC	Customer 6	4f23a83...	3CmuzG1...	15-Aug-2019 16:47	16-Sep-2021 13:05
□	N/A	Withdrawal			8,702.78	0.21522127	Open	BTC	Customer 6	d6244d8...	37biYvT...	09-Jan-2021 04:14	16-Sep-2021 13:05
□	N/A	Withdrawal			2,950.48	0.30877866	Open	BTC	Customer 6	8671f85...	1M1j6Hi...	14-May-2020 22:35	16-Sep-2021 13:05
□	10	Deposit	Illicit Activity		11.44	0.011	Open	BTC	Customer 6	50fe72e...	1J8owBq...	30-Mar-2017 16:00	16-Sep-2021 13:05
□	10	Deposit	Illicit Activity		856,232.48	163	Open	BTC	Customer 6	4579dc0...	14BWH6G...	28-Apr-2019 11:16	16-Sep-2021 13:05
□	4.1	Withdrawal	Illicit Activity	⊕	552.13	0.71002556	Open	BTC	Customer 6	1d48568...	1Fr5cUS...	14-Dec-2016 00:00	16-Sep-2021 13:05
□	N/A	Withdrawal			31.01	0.00302577	Open	BTC	Customer 6	071809a...	1ABmXWA...	01-Aug-2019 03:33	16-Sep-2021 13:05
□	N/A	Deposit			201.19	0.02325387	Open	BTC	Customer 6	23147d2...	187dKqE...	11-May-2020 20:47	16-Sep-2021 13:05
□	10	Deposit	Illicit Activity		16.07	0.001985	Open	BTC	Customer 6	9528856...	37kzMNk...	20-May-2019 03:08	16-Sep-2021 13:05
□	10	Withdrawal	Illicit Activity		353.40	0.037	Open	BTC	Customer 6	add9269...	32MNVYd...	30-Jul-2019 07:30	16-Sep-2021 13:05

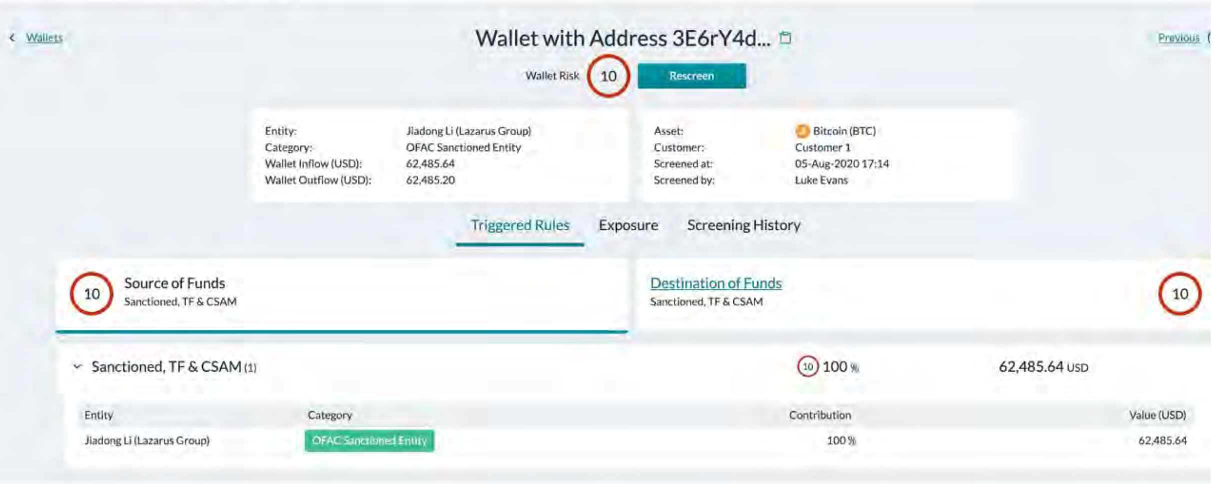
Previous 4 of 1,305 pages Next

26,081 records | Records per page: 20

The 3in3formation and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Confidential – Not for Sharing

Sanctions



Wallet with Address 3E6rY4d...

Wallet Risk 10

Entity:	Jiadong Li (Lazarus Group)
Category:	OFAC Sanctioned Entity
Wallet Inflow (USD):	62,485.64
Wallet Outflow (USD):	62,485.20
Asset:	Bitcoin (BTC)
Customer:	Customer 1
Screened at:	05-Aug-2020 17:14
Screened by:	Luke Evans

10 Source of Funds
Sanctioned, TF & CSAM

Destination of Funds
Sanctioned, TF & CSAM 10

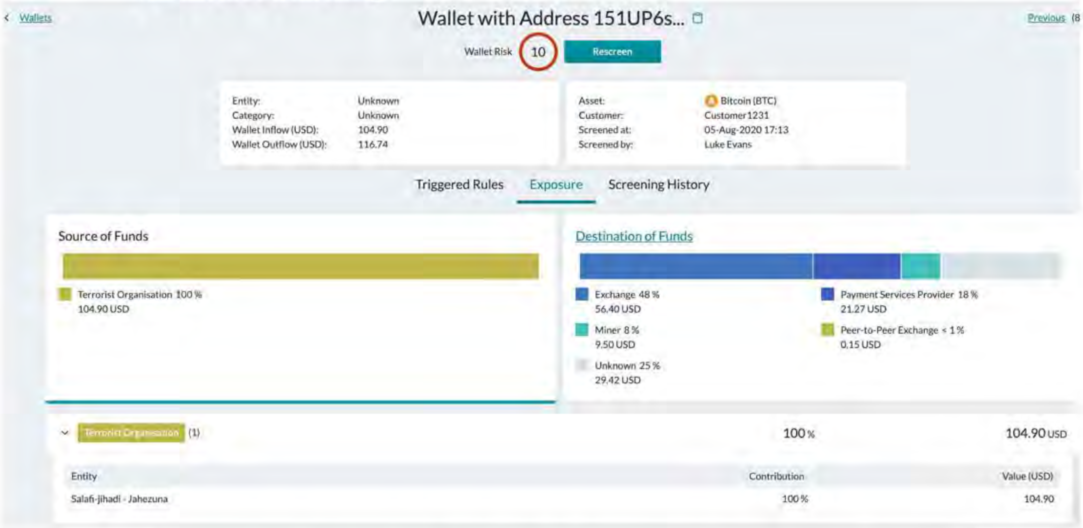
Sanctioned, TF & CSAM (1) 10 100 % 62,485.64 USD

Entity	Category	Contribution	Value (USD)
Jiadong Li (Lazarus Group)	OFAC Sanctioned Entity	100 %	62,485.64

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Confidential – Not for Sharing

Terrorist Financing



Wallet with Address 151UP6s...

Wallet Risk 10

Entity: Unknown
Category: Unknown
Wallet Inflow (USD): 104.90
Wallet Outflow (USD): 116.74

Asset: Bitcoin (BTC)
Customer: Customer1231
Screened at: 05-Aug-2020 17:13
Screened by: Luke Evans

Source of Funds

🟨 Terrorist Organisation 100 %
104.90 USD

Destination of Funds

🟦 Exchange 48 %
56.40 USD

🟦 Payment Services Provider 18 %
21.27 USD

🟩 Miner 8 %
9.50 USD

🟩 Peer-to-Peer Exchange < 1 %
0.15 USD

⬜ Unknown 25 %
29.42 USD

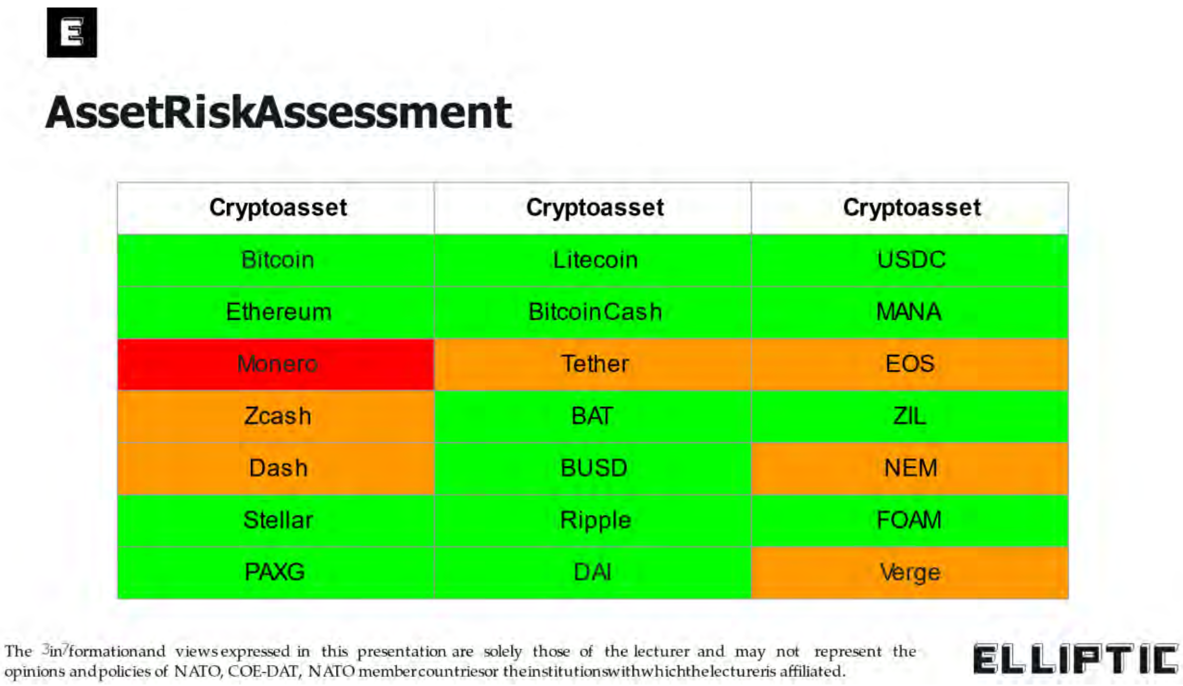
Terrorist Organisation (1) 100 % 104.90 USD

Entity	Contribution	Value (USD)
Salafi-jihadi - Jahezuna	100 %	104.90

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

RiskAssessment

Risk Category	Risk Factors
Customer	• Purpose of cryptoasset trading • Level of sophistication and requirements (e.g. accredited investor vs. retail consumers) • Compliance and risk management standards of customer or counterparty
Geographical	• Location of customer or counterparty • Regulated status of customer or counterparty in country of domicile/registration • Does the jurisdiction adhere to the FATF standards on virtual assets?
Product	• Types of cryptoasset • Purpose of use of the cryptoasset • Transparency and traceability of cryptoasset • Regulatory status of cryptoasset (e.g. payment vs. security token)
Transactional	• Source and destination of funds by level of illicit exposure • Macro-level analysis of funds flows over time • Triggering of specific transaction monitoring risk rules • Suspicious activity reports (SARs)

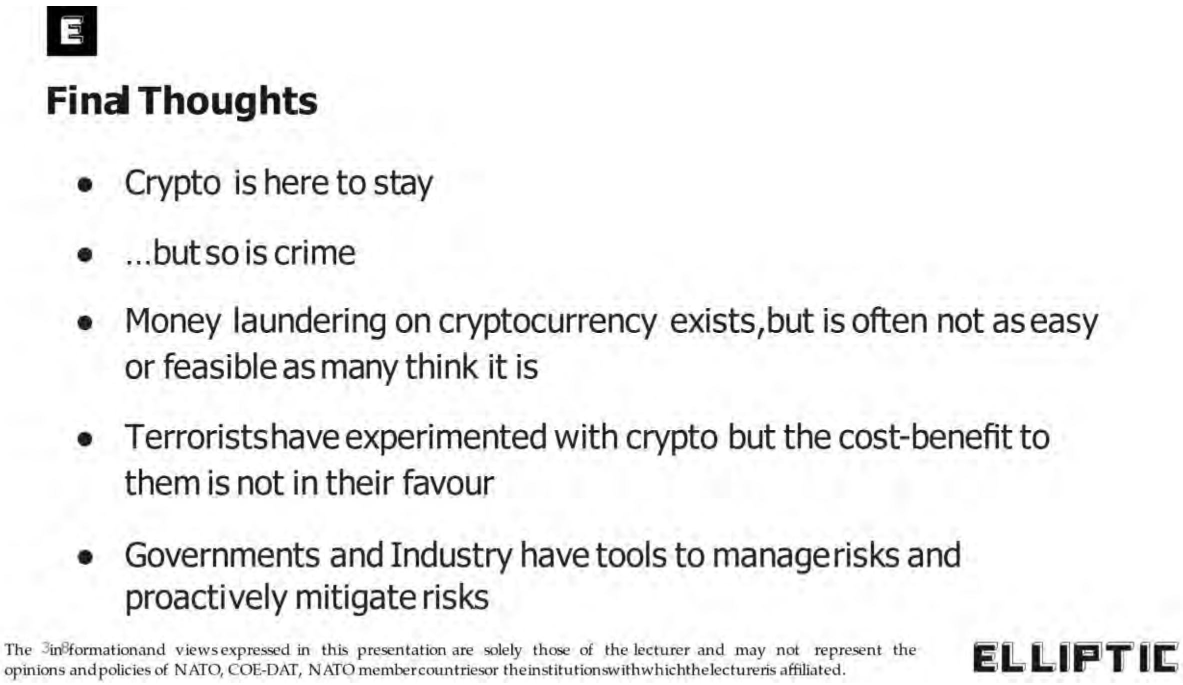


AssetRiskAssessment

Cryptoasset	Cryptoasset	Cryptoasset
🟩 Bitcoin	🟩 Litecoin	🟩 USDC
🟩 Ethereum	🟩 BitcoinCash	🟩 MANA
🟥 Monero	🟧 Tether	🟧 EOS
🟧 Zcash	🟩 BAT	🟩 ZIL
🟧 Dash	🟩 BUSD	🟧 NEM
🟩 Stellar	🟩 Ripple	🟩 FOAM
🟩 PAXG	🟩 DAI	🟧 Verge

The 3in7formationand views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

ELLIPTIC



Final Thoughts

- Crypto is here to stay
- ...but so is crime
- Money laundering on cryptocurrency exists,but is often not as easy or feasible as many think it is
- Terroristshave experimented with crypto but the cost-benefit to them is not in their favour
- Governments and Industry have tools to managerisks and proactively mitigate risks

The 3in8formationand views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

ELLIPTIC

Confidential–Not for Sharing

Pleaseget in touch!

Liat.Shetret@Elliptic.co

CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM

ThankYou! 🙏

ELLIPTIC

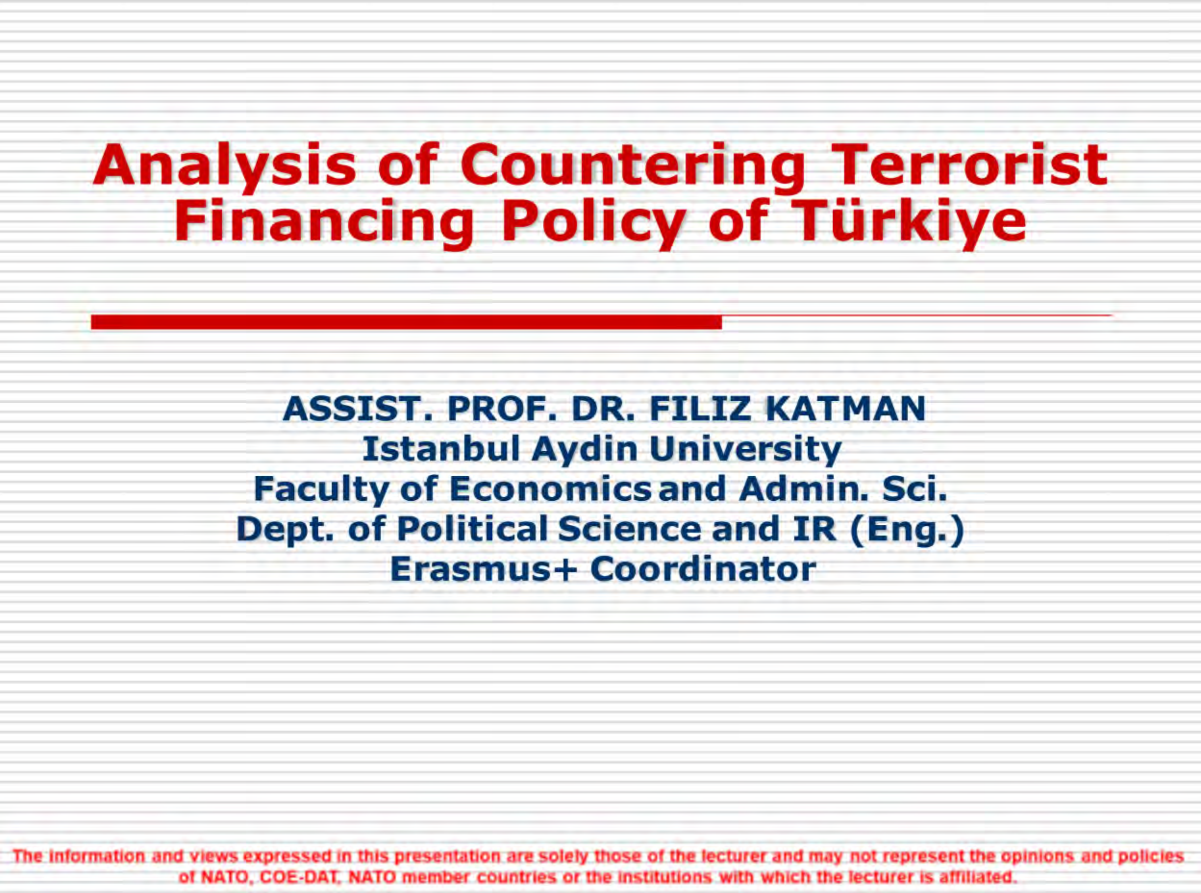
The information and views expressed in this presentation are solely those of the lecturer and may not represent theopinions and policies of NATO, COE-DAT, NATO membercountriesor theinstitutionswithwhichthelectureris affiliated.

Analysis of Countering Terrorism Financing Policy of Türkiye

Dr. Filiz KATMAN

Terrorism, as being one of the main challenging phenomena to security, consists several aspects including the financial one as one of the major aspect in the 21st century. Like counterterrorism policies, international cooperation is vital in countering terrorism financing as well. Thus, a monitoring mechanism is necessary to oversee the progress in countering terrorism financing in individual national countering terrorism policies. Türkiye, being one of the countries challenged by terrorism, has been implementing comprehensive countering terrorism policies including countering terrorism financing. In this study, countering terrorism financing policy of Türkiye, one of the main areas of countering terrorism that requires international cooperation due to the characteristics of terrorism, is analyzed in a comprehensive way including challenges and strengths. Both conventional and contemporary aspects of terrorism financing and countering policies are analyzed with respect to international monitoring mechanisms. The geostrategic position of Türkiye in its neighborhood and long history of countering terrorism experience requires a comprehensive analysis including cyber and digital arena as well.

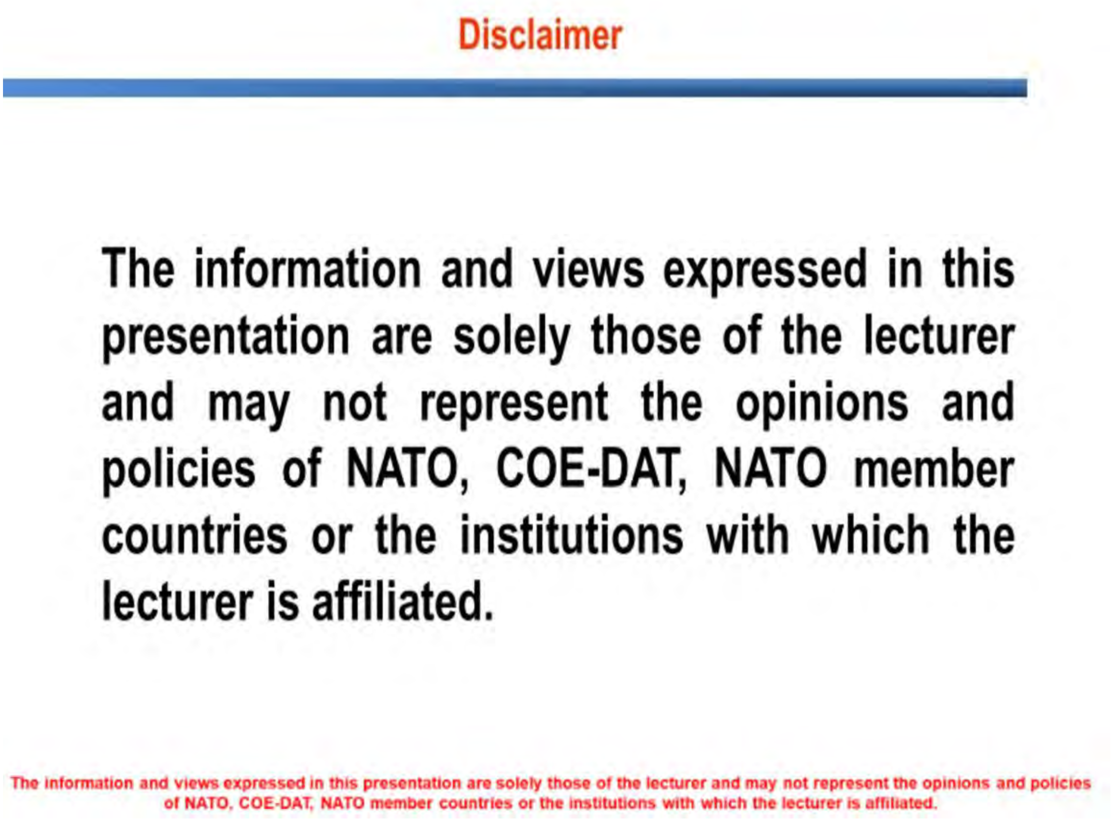
Presentation



Analysis of Countering Terrorist Financing Policy of Türkiye

ASSIST. PROF. DR. FILIZ KATMAN
Istanbul Aydin University
Faculty of Economics and Admin. Sci.
Dept. of Political Science and IR (Eng.)
Erasmus+ Coordinator

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Disclaimer

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

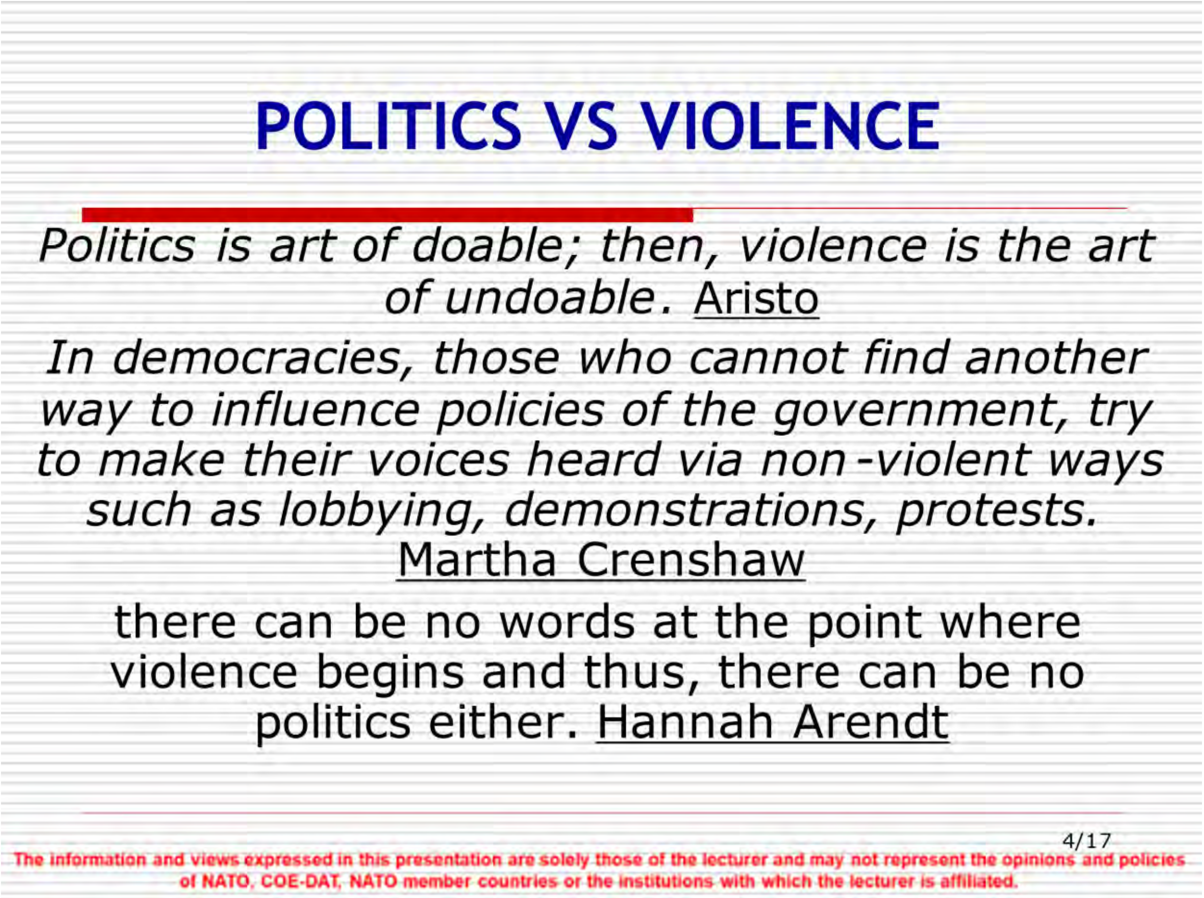
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Agenda

- Politics vs Violence
- Terrorism
- Financing Terrorism
- Characteristics
- Contemporary Challenges
- Global Standards
- Turkish Legal Framework
- Assessment of Turkish Counter-Terrorism Financing Policy
- Conclusion

3

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



POLITICS VS VIOLENCE

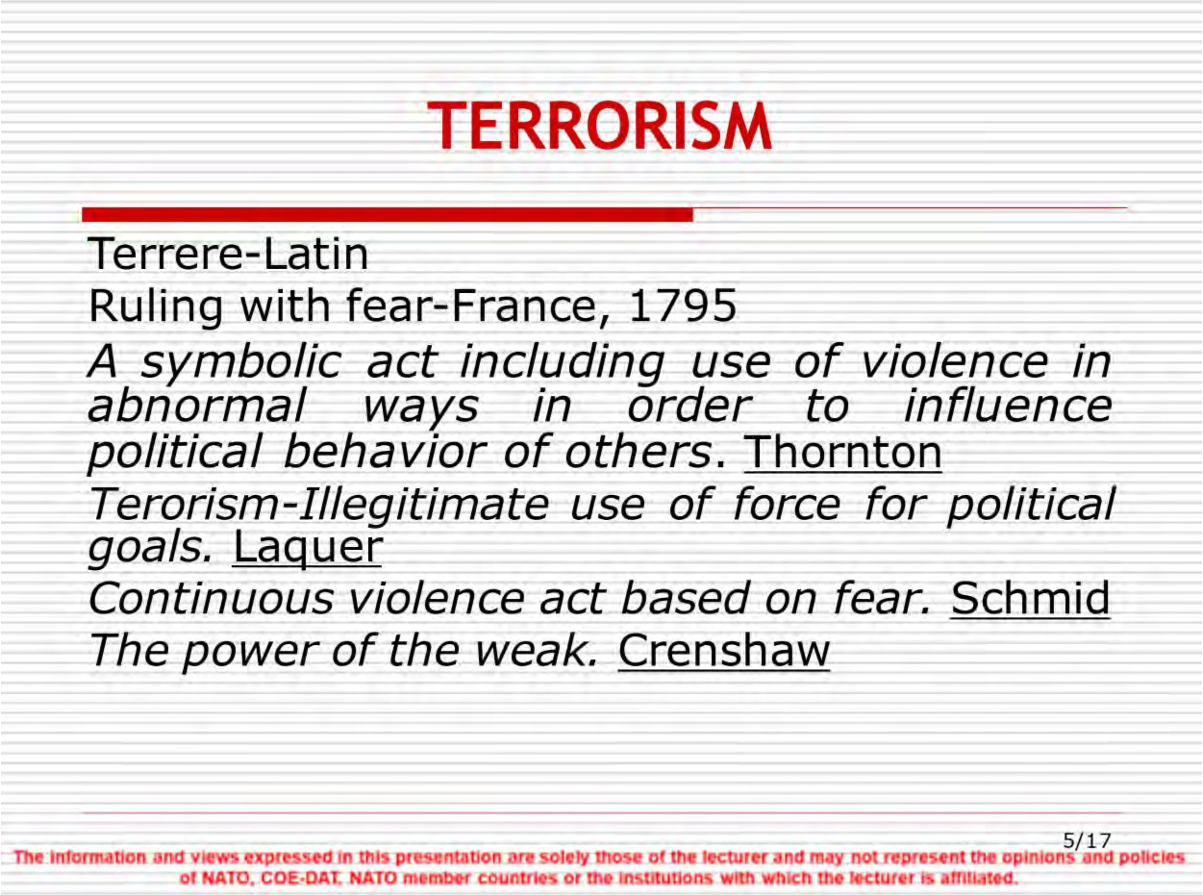
Politics is art of doable; then, violence is the art of undoable. Aristo

In democracies, those who cannot find another way to influence policies of the government, try to make their voices heard via non-violent ways such as lobbying, demonstrations, protests. Martha Crenshaw

there can be no words at the point where violence begins and thus, there can be no politics either. Hannah Arendt

4/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



TERRORISM

Terrere-Latin

Ruling with fear-France, 1795

A symbolic act including use of violence in abnormal ways in order to influence political behavior of others. Thornton

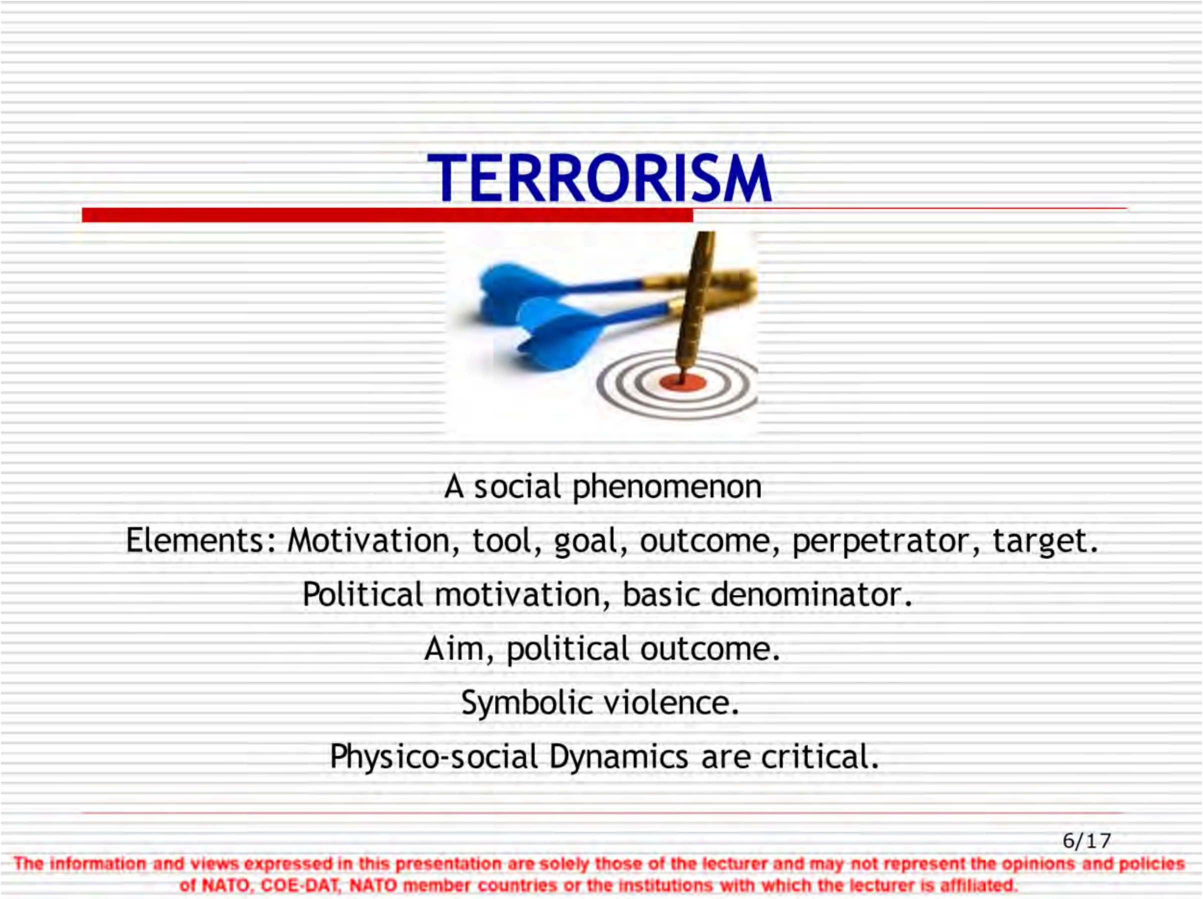
Terorism-Illegitimate use of force for political goals. Laquer

Continuous violence act based on fear. Schmid

The power of the weak. Crenshaw

5/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



TERRORISM

A social phenomenon

Elements: Motivation, tool, goal, outcome, perpetrator, target.

Political motivation, basic denominator.

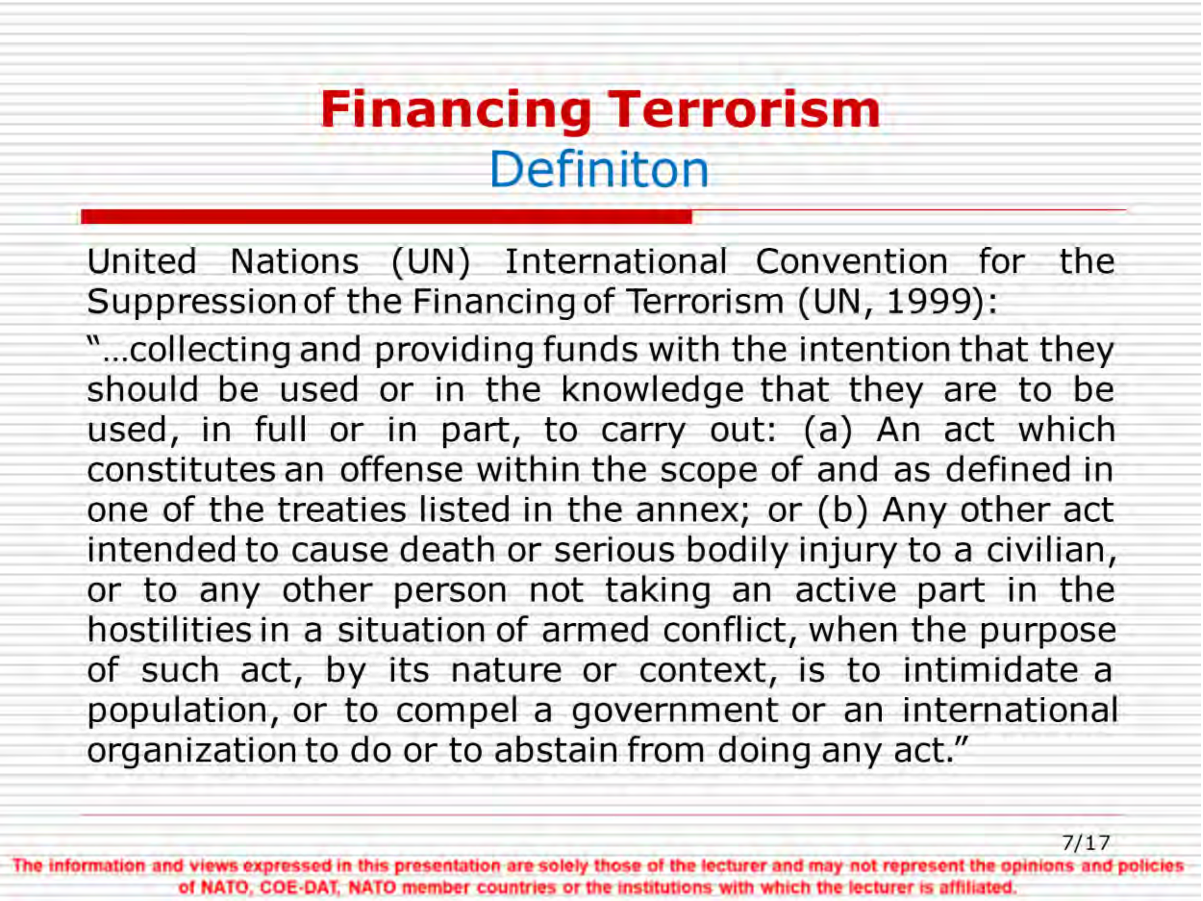
Aim, political outcome.

Symbolic violence.

Physico-social Dynamics are critical.

6/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



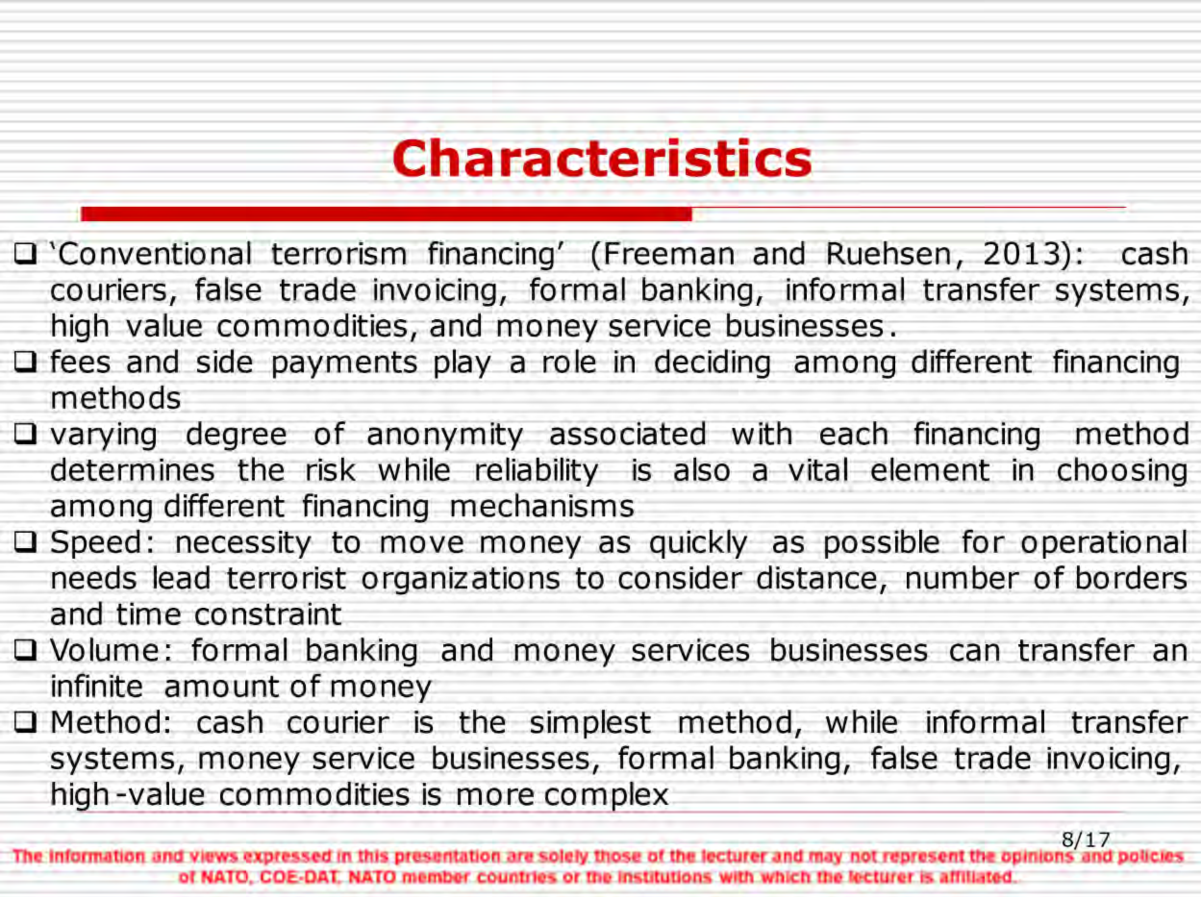
Financing Terrorism
Definiton

United Nations (UN) International Convention for the Suppression of the Financing of Terrorism (UN, 1999):

"…collecting and providing funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, to carry out: (a) An act which constitutes an offense within the scope of and as defined in one of the treaties listed in the annex; or (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."

7/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

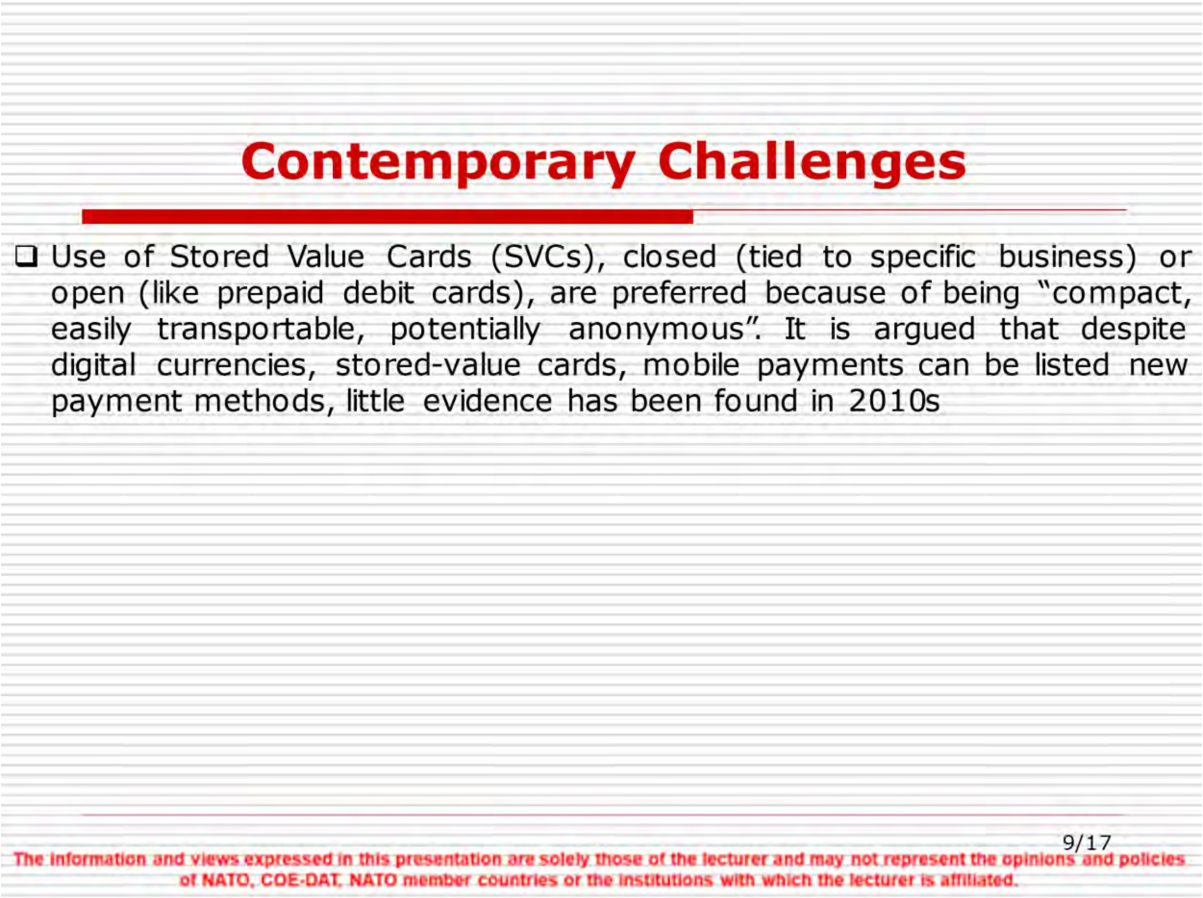


Characteristics

- ❑ 'Conventional terrorism financing' (Freeman and Ruehsen, 2013): cash couriers, false trade invoicing, formal banking, informal transfer systems, high value commodities, and money service businesses.
- ❑ fees and side payments play a role in deciding among different financing methods
- ❑ varying degree of anonymity associated with each financing method determines the risk while reliability is also a vital element in choosing among different financing mechanisms
- ❑ Speed: necessity to move money as quickly as possible for operational needs lead terrorist organizations to consider distance, number of borders and time constraint
- ❑ Volume: formal banking and money services businesses can transfer an infinite amount of money
- ❑ Method: cash courier is the simplest method, while informal transfer systems, money service businesses, formal banking, false trade invoicing, high-value commodities is more complex

8/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

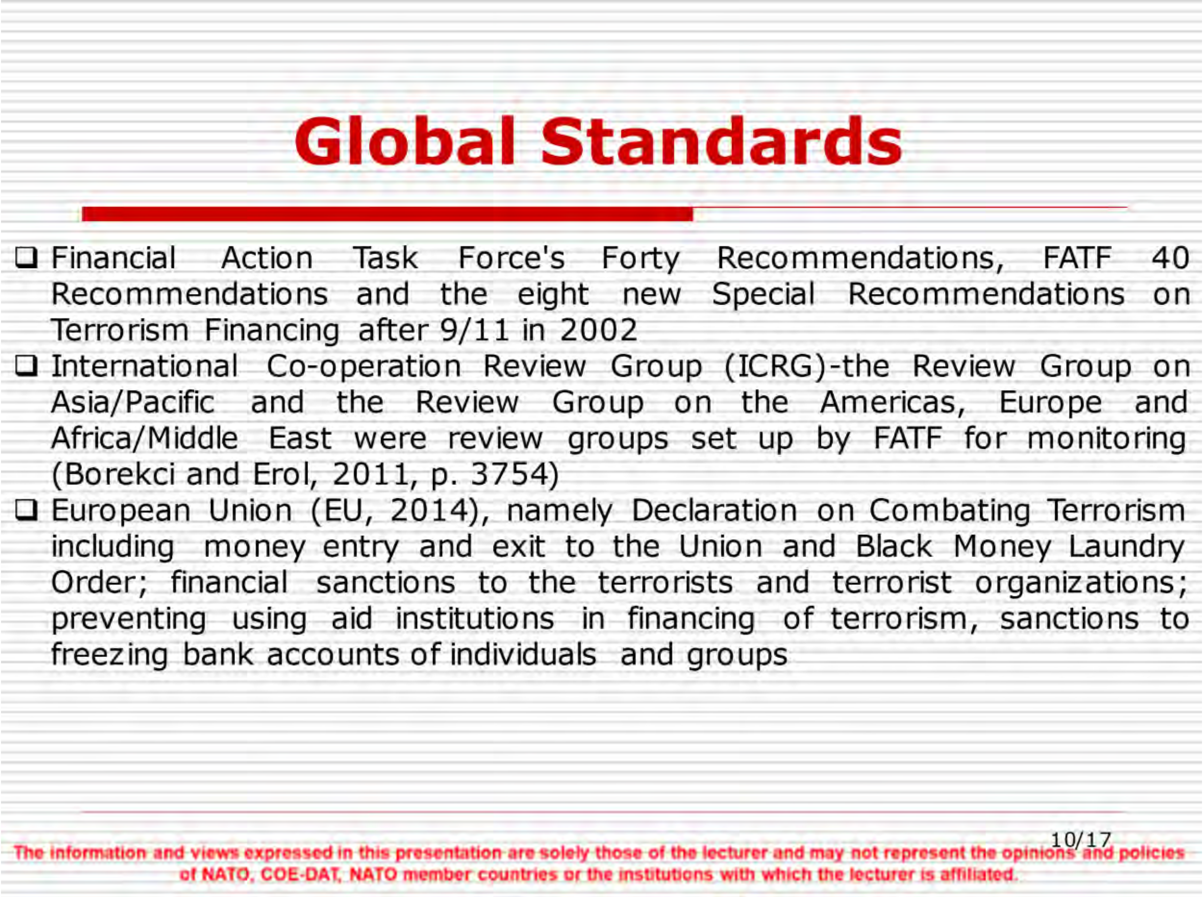


Contemporary Challenges

- ❑ Use of Stored Value Cards (SVCs), closed (tied to specific business) or open (like prepaid debit cards), are preferred because of being "compact, easily transportable, potentially anonymous". It is argued that despite digital currencies, stored-value cards, mobile payments can be listed new payment methods, little evidence has been found in 2010s

9/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

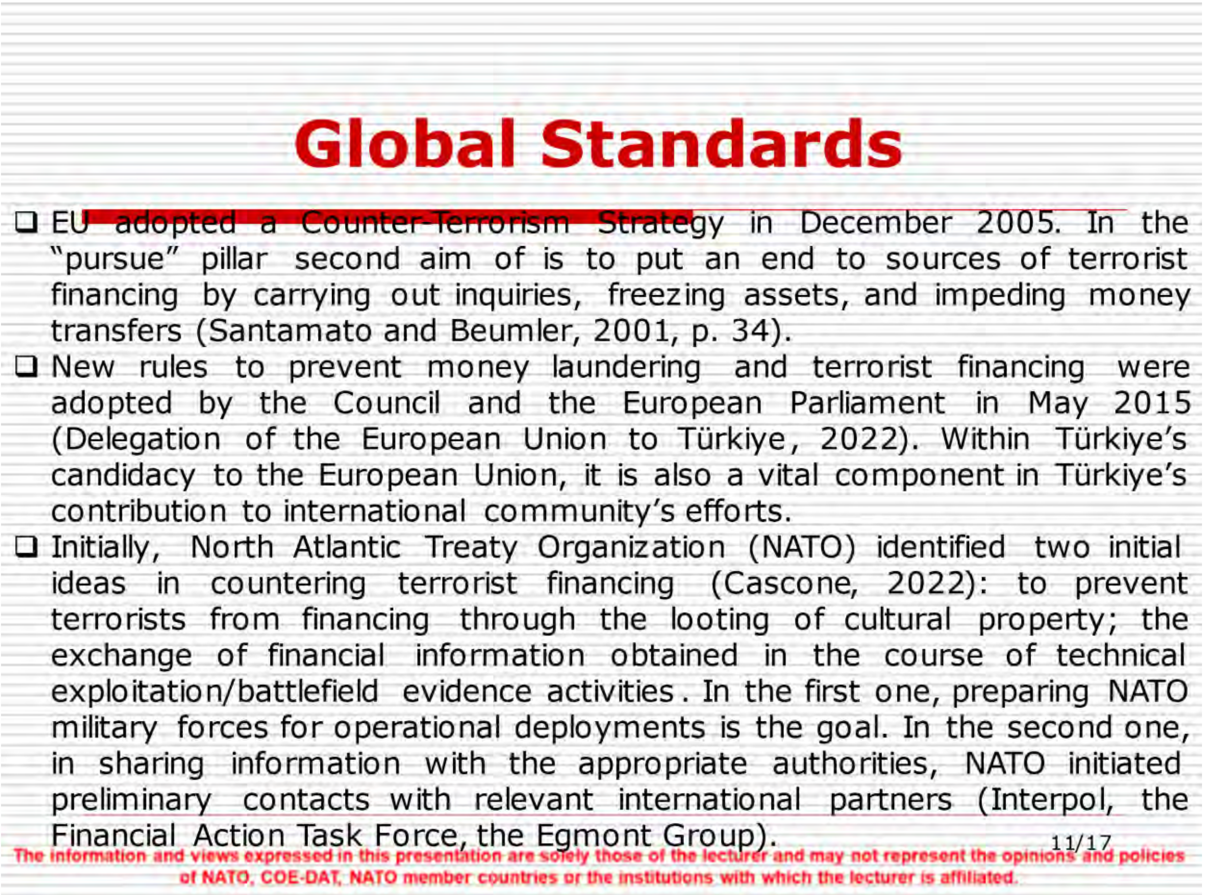


Global Standards

- ❑ Financial Action Task Force's Forty Recommendations, FATF 40 Recommendations and the eight new Special Recommendations on Terrorism Financing after 9/11 in 2002
- ❑ International Co-operation Review Group (ICRG)-the Review Group on Asia/Pacific and the Review Group on the Americas, Europe and Africa/Middle East were review groups set up by FATF for monitoring (Borekci and Erol, 2011, p. 3754)
- ❑ European Union (EU, 2014), namely Declaration on Combating Terrorism including money entry and exit to the Union and Black Money Laundry Order; financial sanctions to the terrorists and terrorist organizations; preventing using aid institutions in financing of terrorism, sanctions to freezing bank accounts of individuals and groups

10/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

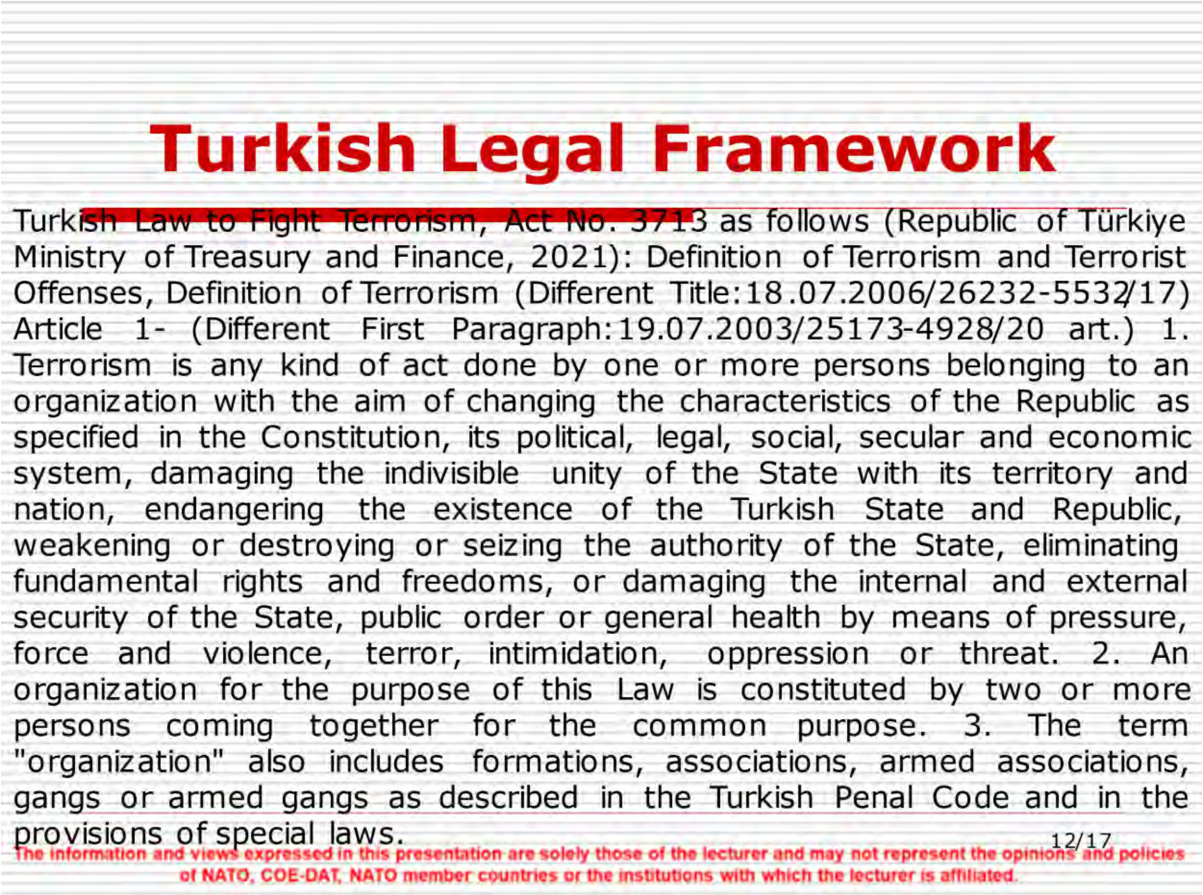


Global Standards

- ❑ EU adopted a Counter-Terrorism Strategy in December 2005. In the "pursue" pillar second aim of is to put an end to sources of terrorist financing by carrying out inquiries, freezing assets, and impeding money transfers (Santamato and Beumler, 2001, p. 34).
- ❑ New rules to prevent money laundering and terrorist financing were adopted by the Council and the European Parliament in May 2015 (Delegation of the European Union to Türkiye, 2022). Within Türkiye's candidacy to the European Union, it is also a vital component in Türkiye's contribution to international community's efforts.
- ❑ Initially, North Atlantic Treaty Organization (NATO) identified two initial ideas in countering terrorist financing (Cascone, 2022): to prevent terrorists from financing through the looting of cultural property; the exchange of financial information obtained in the course of technical exploitation/battlefield evidence activities. In the first one, preparing NATO military forces for operational deployments is the goal. In the second one, in sharing information with the appropriate authorities, NATO initiated preliminary contacts with relevant international partners (Interpol, the Financial Action Task Force, the Egmont Group).

11/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

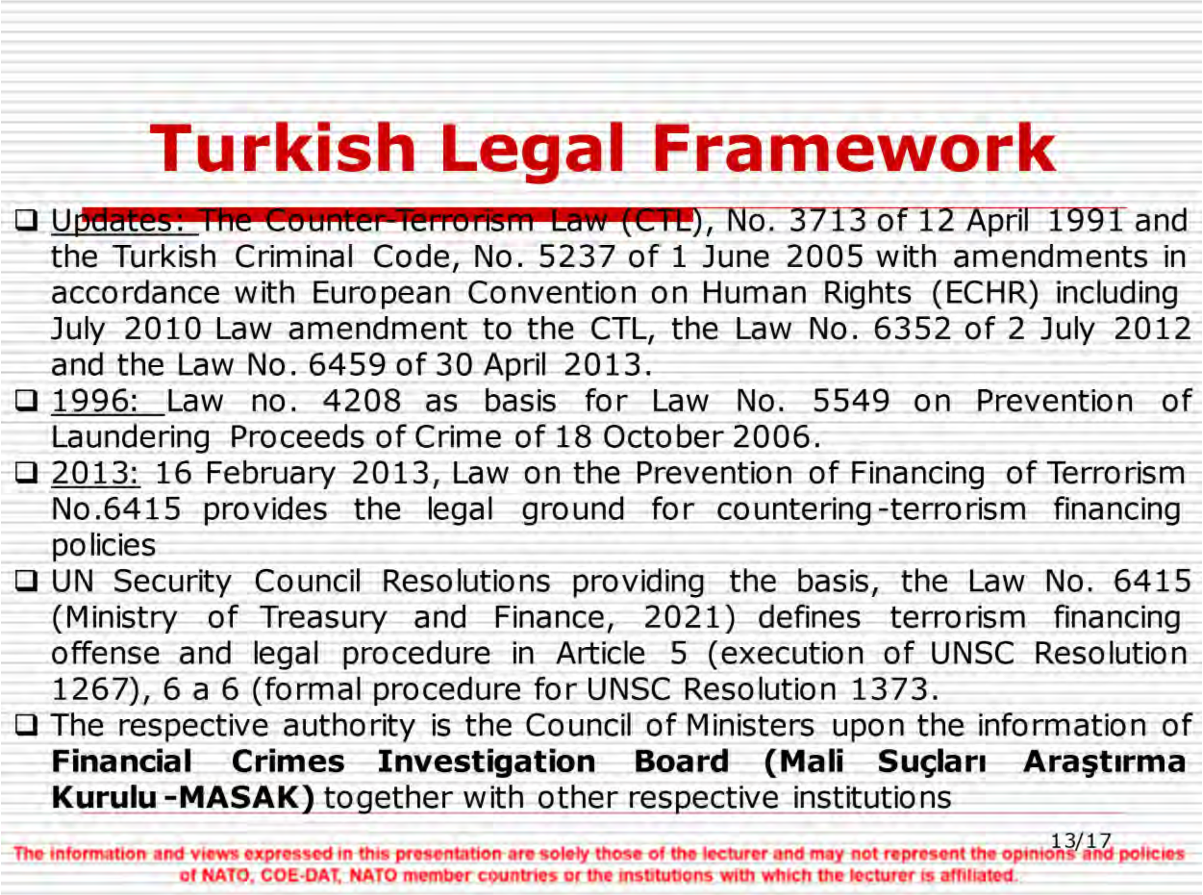


Turkish Legal Framework

Turkish Law to Fight Terrorism, Act No. 3713 as follows (Republic of Türkiye Ministry of Treasury and Finance, 2021): Definition of Terrorism and Terrorist Offenses, Definition of Terrorism (Different Title:18.07.2006/26232-5532/17) Article 1- (Different First Paragraph:19.07.2003/25173-4928/20 art.) 1. Terrorism is any kind of act done by one or more persons belonging to an organization with the aim of changing the characteristics of the Republic as specified in the Constitution, its political, legal, social, secular and economic system, damaging the indivisible unity of the State with its territory and nation, endangering the existence of the Turkish State and Republic, weakening or destroying or seizing the authority of the State, eliminating fundamental rights and freedoms, or damaging the internal and external security of the State, public order or general health by means of pressure, force and violence, terror, intimidation, oppression or threat. 2. An organization for the purpose of this Law is constituted by two or more persons coming together for the common purpose. 3. The term "organization" also includes formations, associations, armed associations, gangs or armed gangs as described in the Turkish Penal Code and in the provisions of special laws.

12/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

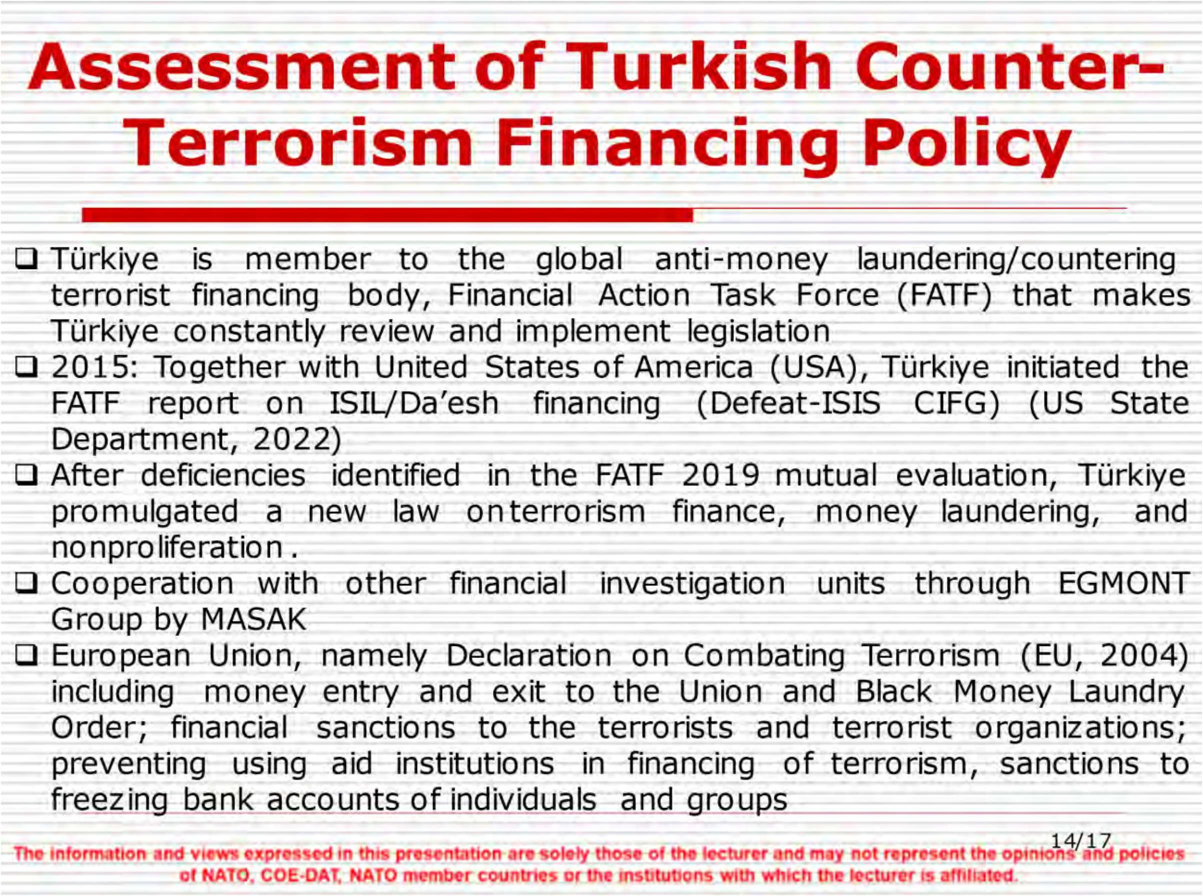


Turkish Legal Framework

- ❑ Updates: The Counter-Terrorism Law (CTL), No. 3713 of 12 April 1991 and the Turkish Criminal Code, No. 5237 of 1 June 2005 with amendments in accordance with European Convention on Human Rights (ECHR) including July 2010 Law amendment to the CTL, the Law No. 6352 of 2 July 2012 and the Law No. 6459 of 30 April 2013.
- ❑ 1996: Law no. 4208 as basis for Law No. 5549 on Prevention of Laundering Proceeds of Crime of 18 October 2006.
- ❑ 2013: 16 February 2013, Law on the Prevention of Financing of Terrorism No.6415 provides the legal ground for countering-terrorism financing policies
- ❑ UN Security Council Resolutions providing the basis, the Law No. 6415 (Ministry of Treasury and Finance, 2021) defines terrorism financing offense and legal procedure in Article 5 (execution of UNSC Resolution 1267), 6 a 6 (formal procedure for UNSC Resolution 1373.
- ❑ The respective authority is the Council of Ministers upon the information of **Financial Crimes Investigation Board (Mali Suçları Araştırma Kurulu -MASAK)** together with other respective institutions

13/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

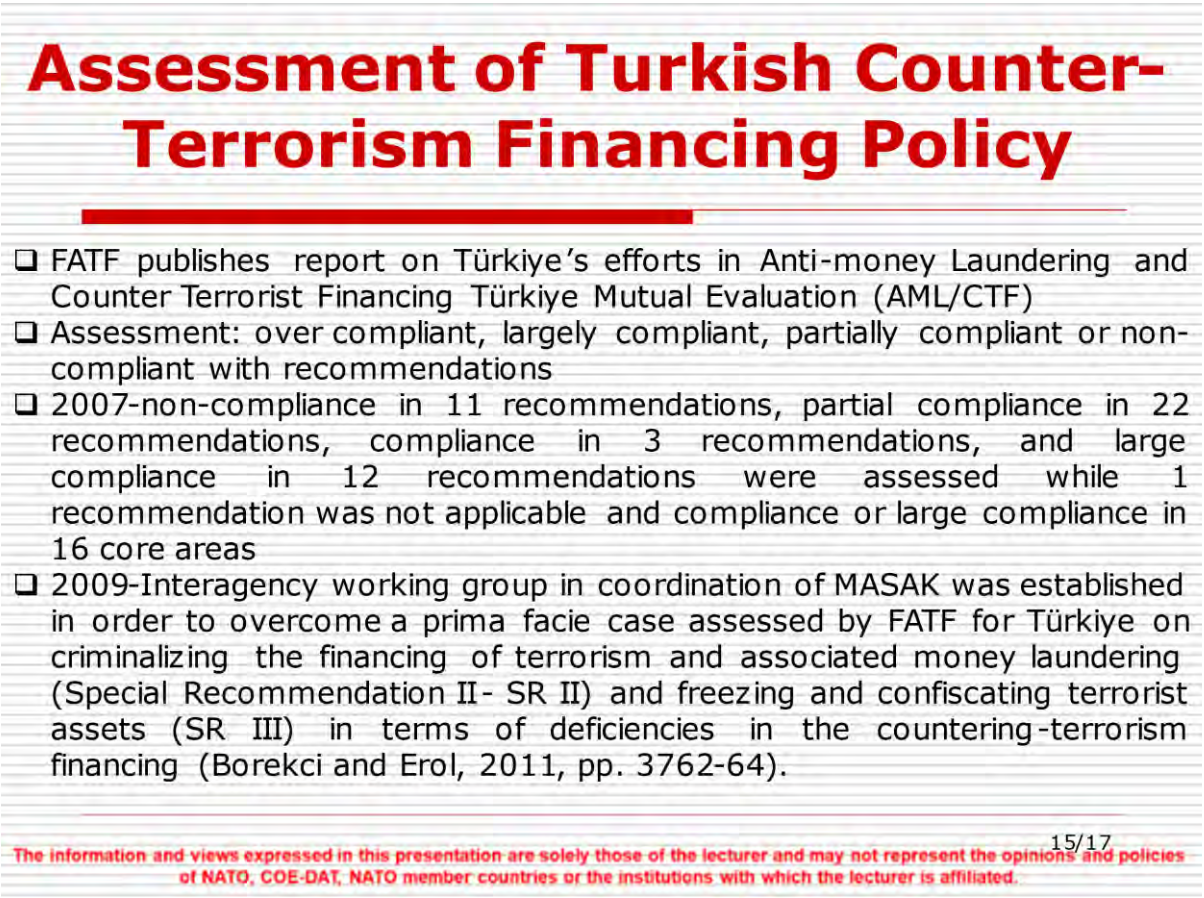


Assessment of Turkish Counter-Terrorism Financing Policy

- ❑ Türkiye is member to the global anti-money laundering/countering terrorist financing body, Financial Action Task Force (FATF) that makes Türkiye constantly review and implement legislation
- ❑ 2015: Together with United States of America (USA), Türkiye initiated the FATF report on ISIL/Da'esh financing (Defeat-ISIS CIFG) (US State Department, 2022)
- ❑ After deficiencies identified in the FATF 2019 mutual evaluation, Türkiye promulgated a new law on terrorism finance, money laundering, and nonproliferation .
- ❑ Cooperation with other financial investigation units through EGMONT Group by MASAK
- ❑ European Union, namely Declaration on Combating Terrorism (EU, 2004) including money entry and exit to the Union and Black Money Laundry Order; financial sanctions to the terrorists and terrorist organizations; preventing using aid institutions in financing of terrorism, sanctions to freezing bank accounts of individuals and groups

14/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Assessment of Turkish Counter-Terrorism Financing Policy

❑ FATF publishes report on Türkiye's efforts in Anti-money Laundering and Counter Terrorist Financing Türkiye Mutual Evaluation (AML/CTF)

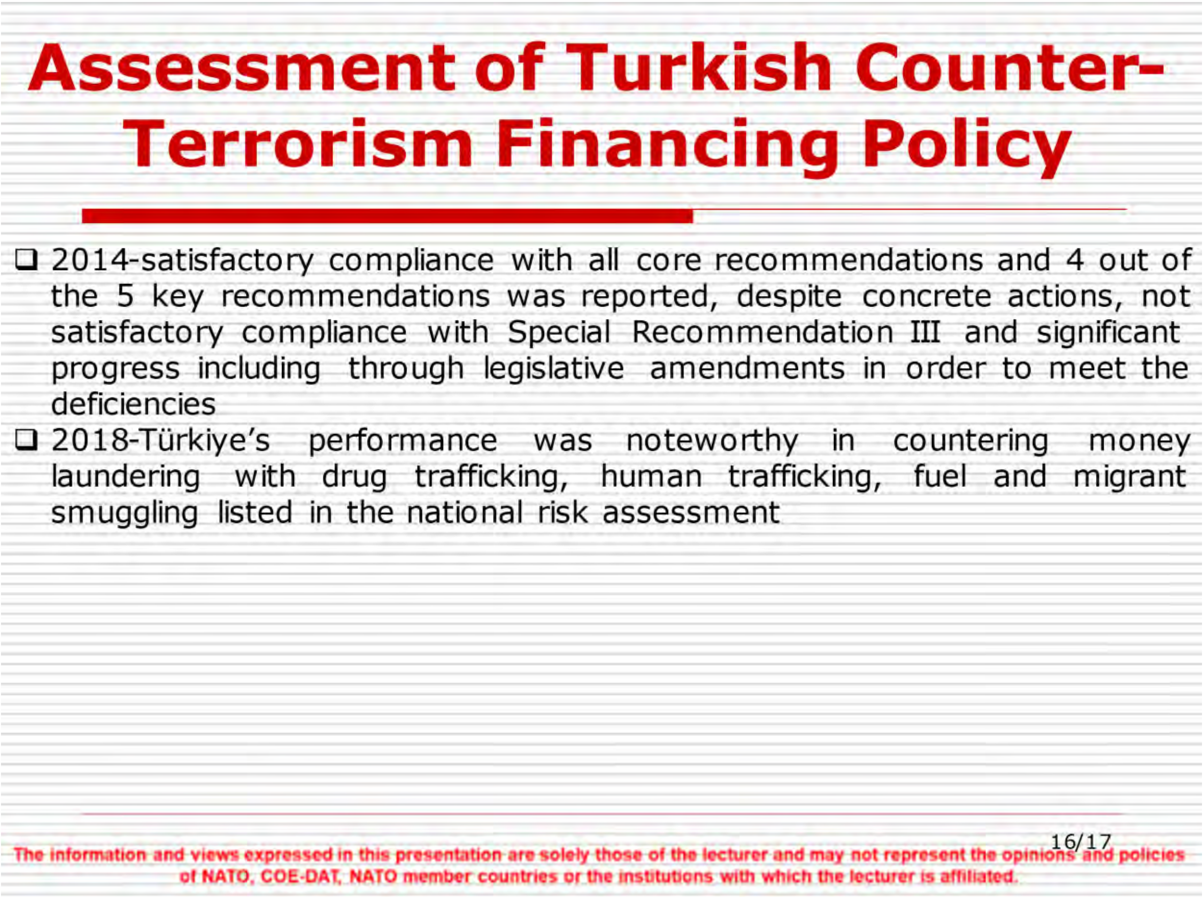
❑ Assessment: over compliant, largely compliant, partially compliant or non-compliant with recommendations

❑ 2007-non-compliance in 11 recommendations, partial compliance in 22 recommendations, compliance in 3 recommendations, and large compliance in 12 recommendations were assessed while 1 recommendation was not applicable and compliance or large compliance in 16 core areas

❑ 2009-Interagency working group in coordination of MASAK was established in order to overcome a prima facie case assessed by FATF for Türkiye on criminalizing the financing of terrorism and associated money laundering (Special Recommendation II- SR II) and freezing and confiscating terrorist assets (SR III) in terms of deficiencies in the countering-terrorism financing (Borekci and Erol, 2011, pp. 3762-64).

15/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



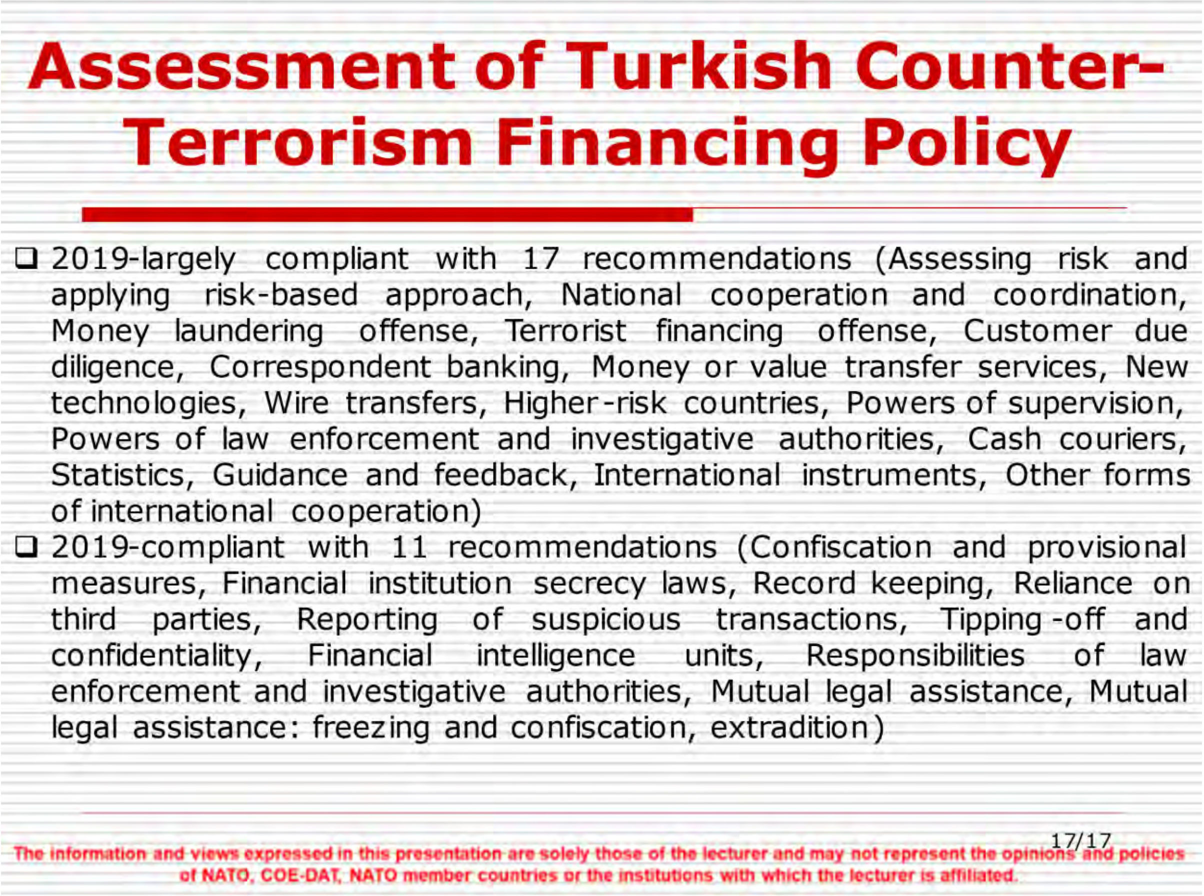
Assessment of Turkish Counter-Terrorism Financing Policy

❑ 2014-satisfactory compliance with all core recommendations and 4 out of the 5 key recommendations was reported, despite concrete actions, not satisfactory compliance with Special Recommendation III and significant progress including through legislative amendments in order to meet the deficiencies

❑ 2018-Türkiye's performance was noteworthy in countering money laundering with drug trafficking, human trafficking, fuel and migrant smuggling listed in the national risk assessment

16/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

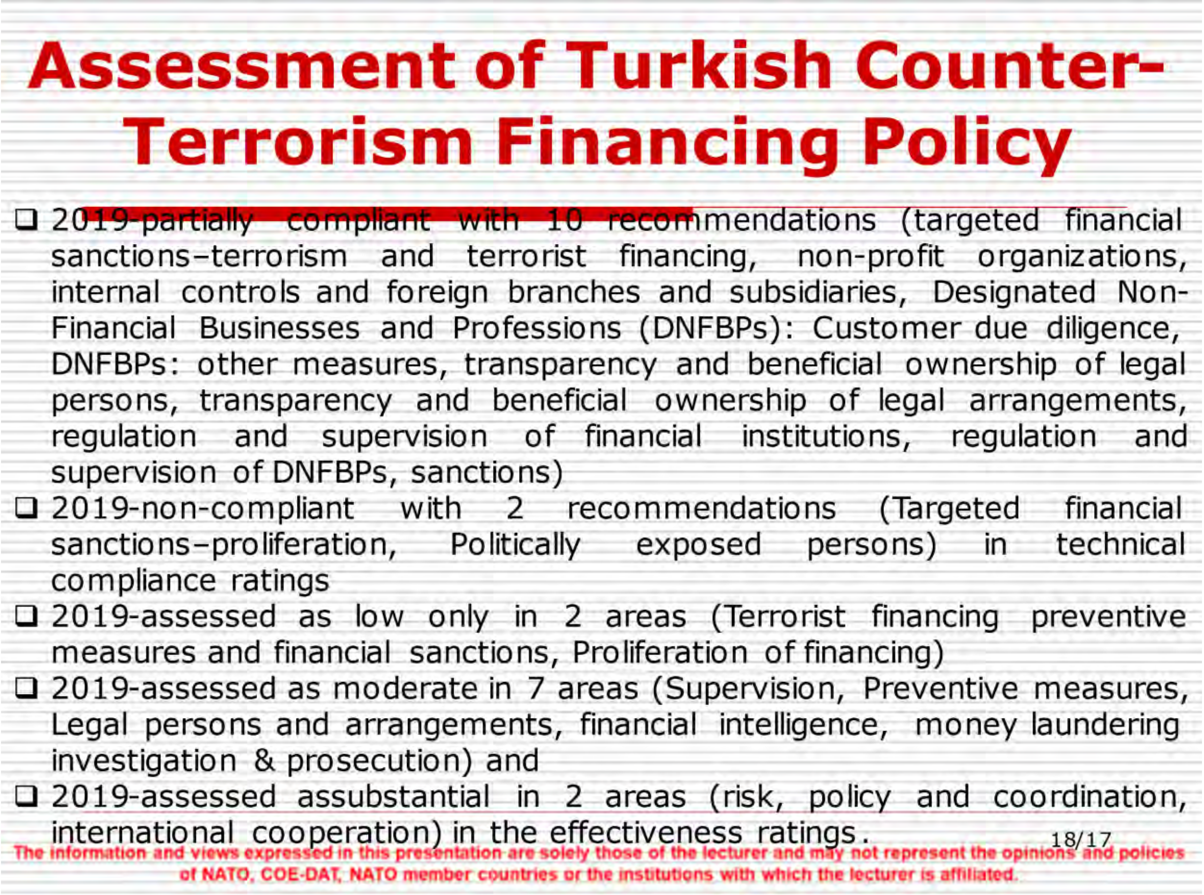


Assessment of Turkish Counter-Terrorism Financing Policy

- ❑ 2019-largely compliant with 17 recommendations (Assessing risk and applying risk-based approach, National cooperation and coordination, Money laundering offense, Terrorist financing offense, Customer due diligence, Correspondent banking, Money or value transfer services, New technologies, Wire transfers, Higher-risk countries, Powers of supervision, Powers of law enforcement and investigative authorities, Cash couriers, Statistics, Guidance and feedback, International instruments, Other forms of international cooperation)
- ❑ 2019-compliant with 11 recommendations (Confiscation and provisional measures, Financial institution secrecy laws, Record keeping, Reliance on third parties, Reporting of suspicious transactions, Tipping-off and confidentiality, Financial intelligence units, Responsibilities of law enforcement and investigative authorities, Mutual legal assistance, Mutual legal assistance: freezing and confiscation, extradition)

17/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

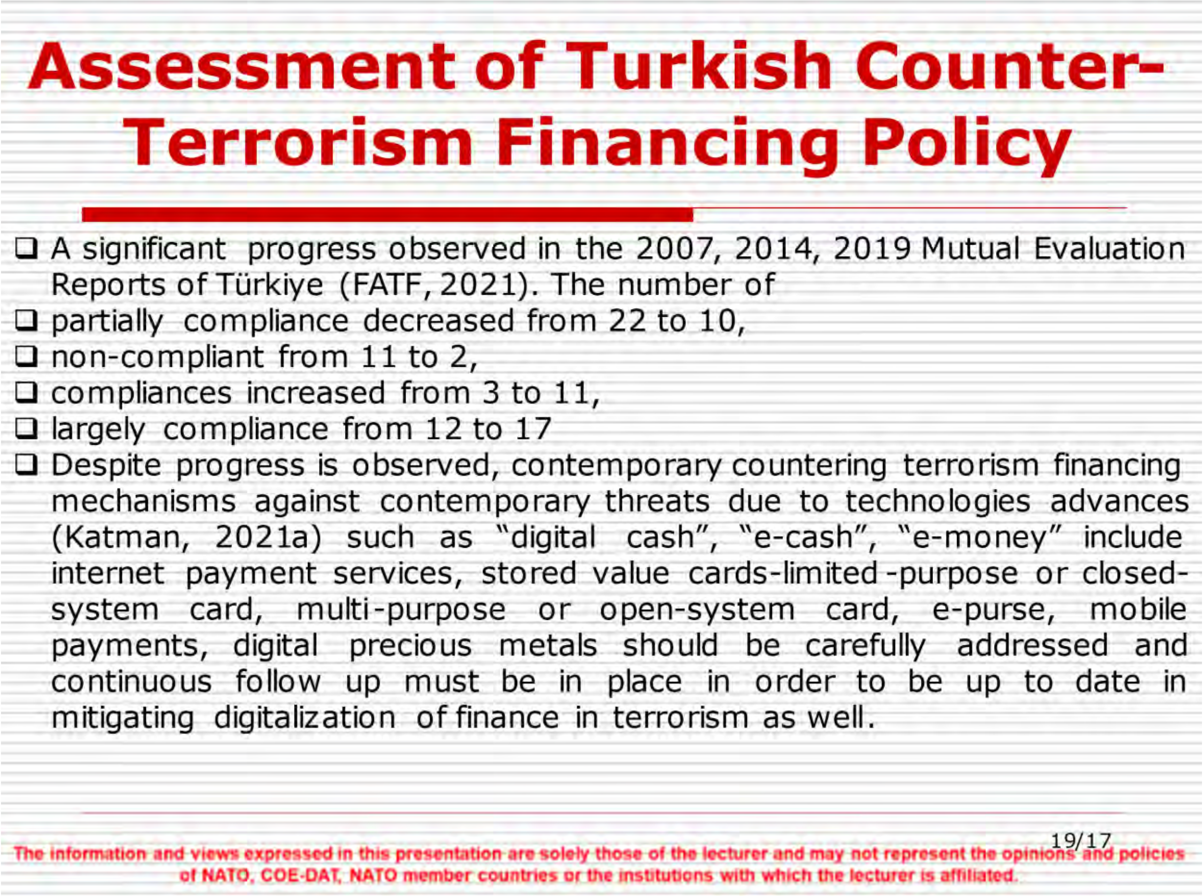


Assessment of Turkish Counter-Terrorism Financing Policy

- ❑ 2019-partially compliant with 10 recommendations (targeted financial sanctions–terrorism and terrorist financing, non-profit organizations, internal controls and foreign branches and subsidiaries, Designated Non-Financial Businesses and Professions (DNFBPs): Customer due diligence, DNFBPs: other measures, transparency and beneficial ownership of legal persons, transparency and beneficial ownership of legal arrangements, regulation and supervision of financial institutions, regulation and supervision of DNFBPs, sanctions)
- ❑ 2019-non-compliant with 2 recommendations (Targeted financial sanctions–proliferation, Politically exposed persons) in technical compliance ratings
- ❑ 2019-assessed as low only in 2 areas (Terrorist financing preventive measures and financial sanctions, Proliferation of financing)
- ❑ 2019-assessed as moderate in 7 areas (Supervision, Preventive measures, Legal persons and arrangements, financial intelligence, money laundering investigation & prosecution) and
- ❑ 2019-assessed assubstantial in 2 areas (risk, policy and coordination, international cooperation) in the effectiveness ratings.

18/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

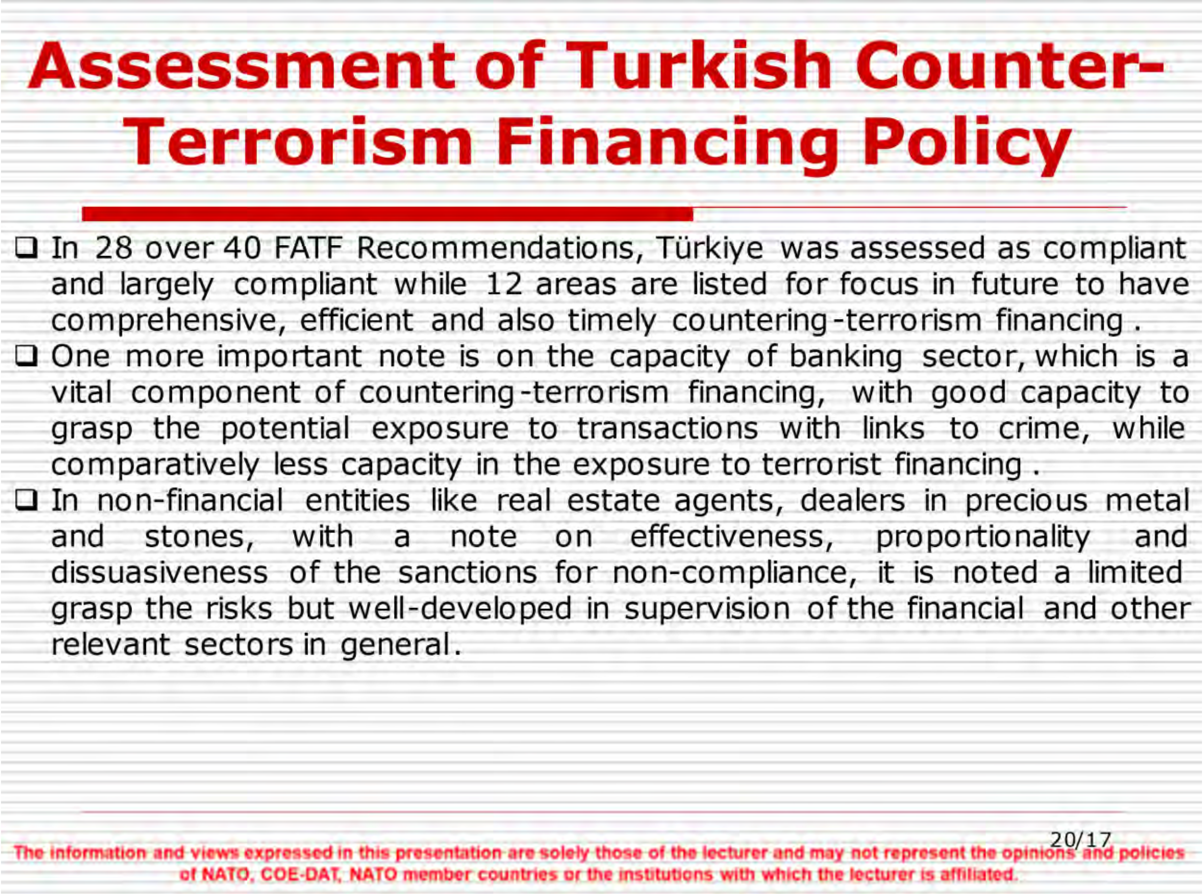


Assessment of Turkish Counter-Terrorism Financing Policy

- ❑ A significant progress observed in the 2007, 2014, 2019 Mutual Evaluation Reports of Türkiye (FATF, 2021). The number of
- ❑ partially compliance decreased from 22 to 10,
- ❑ non-compliant from 11 to 2,
- ❑ compliances increased from 3 to 11,
- ❑ largely compliance from 12 to 17
- ❑ Despite progress is observed, contemporary countering terrorism financing mechanisms against contemporary threats due to technologies advances (Katman, 2021a) such as "digital cash", "e-cash", "e-money" include internet payment services, stored value cards-limited-purpose or closed-system card, multi-purpose or open-system card, e-purse, mobile payments, digital precious metals should be carefully addressed and continuous follow up must be in place in order to be up to date in mitigating digitalization of finance in terrorism as well.

19/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

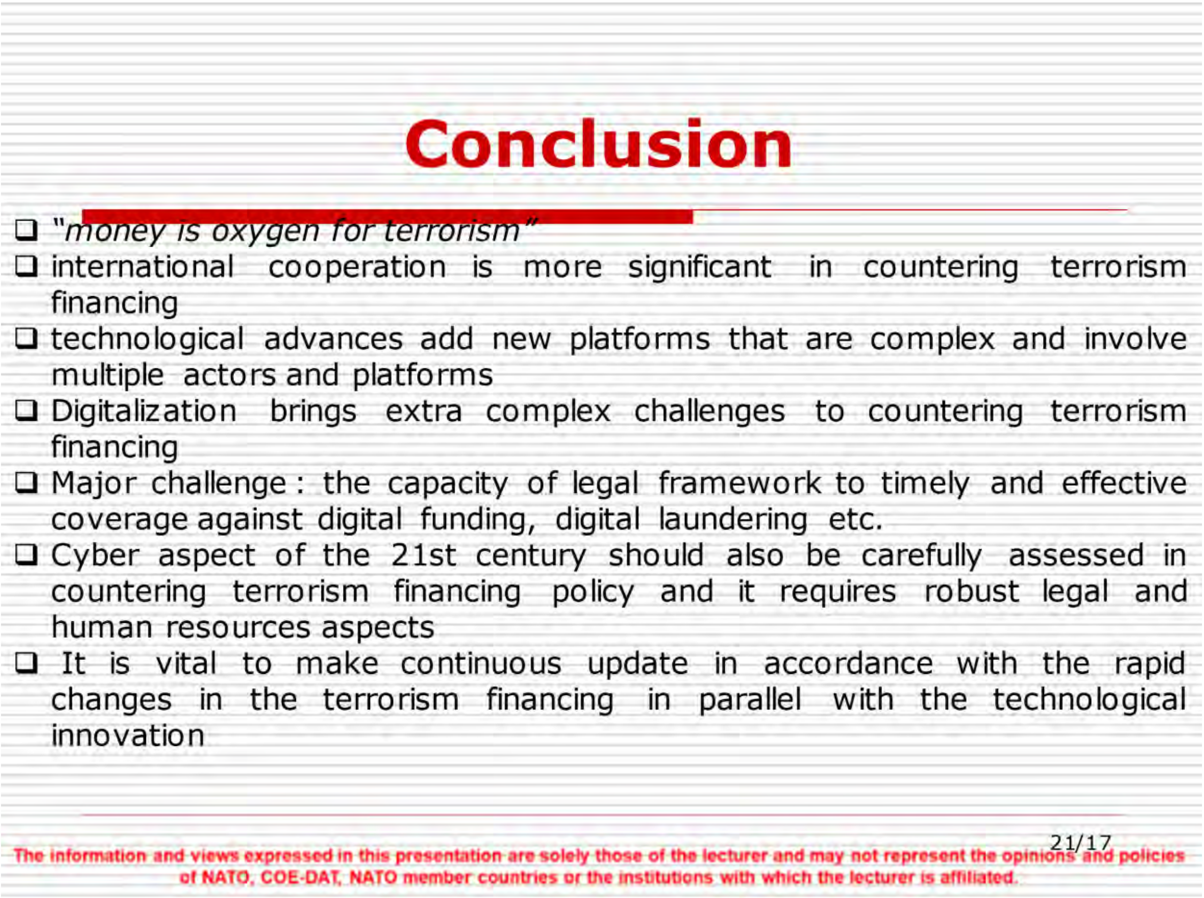


Assessment of Turkish Counter-Terrorism Financing Policy

- ❑ In 28 over 40 FATF Recommendations, Türkiye was assessed as compliant and largely compliant while 12 areas are listed for focus in future to have comprehensive, efficient and also timely countering-terrorism financing .
- ❑ One more important note is on the capacity of banking sector, which is a vital component of countering-terrorism financing, with good capacity to grasp the potential exposure to transactions with links to crime, while comparatively less capacity in the exposure to terrorist financing .
- ❑ In non-financial entities like real estate agents, dealers in precious metal and stones, with a note on effectiveness, proportionality and dissuasiveness of the sanctions for non-compliance, it is noted a limited grasp the risks but well-developed in supervision of the financial and other relevant sectors in general.

20/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

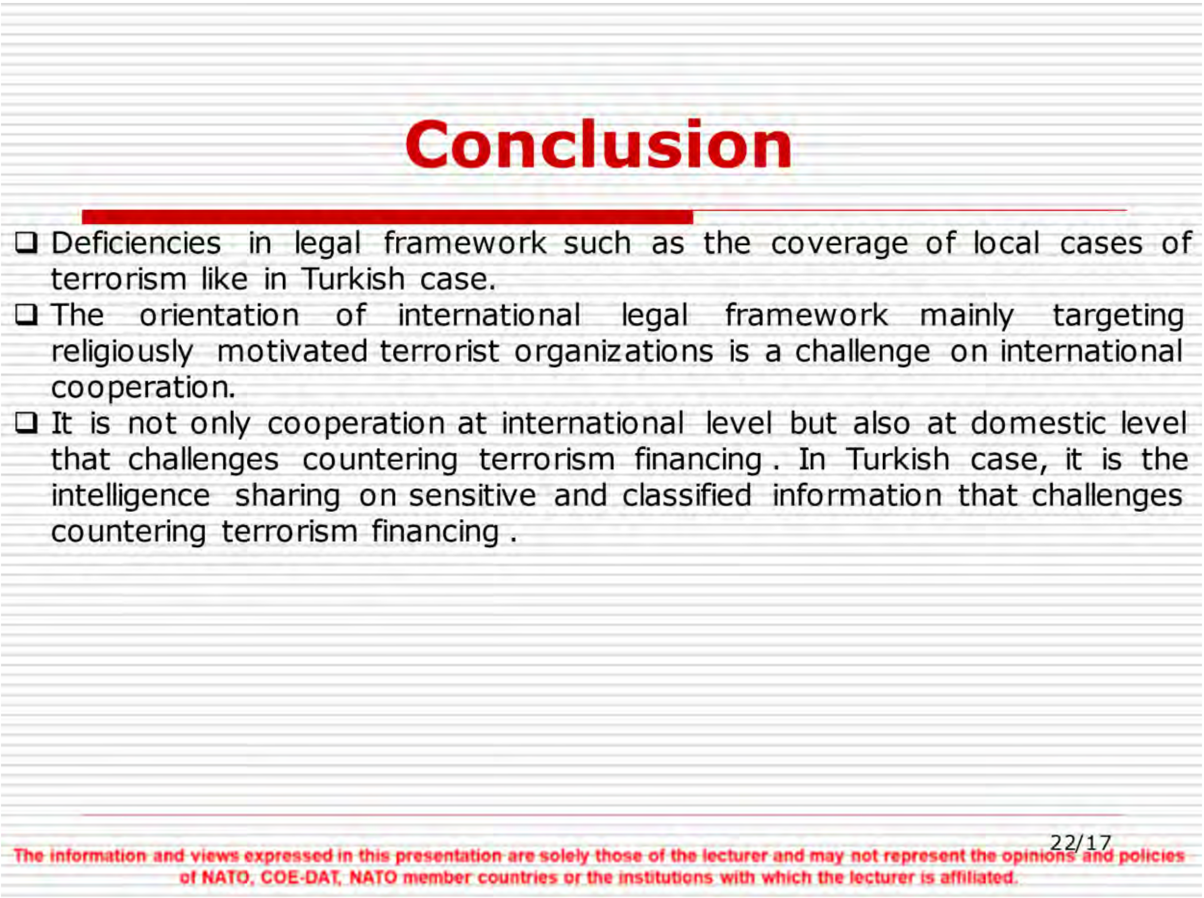


Conclusion

- ❑ *"money is oxygen for terrorism"*
- ❑ international cooperation is more significant in countering terrorism financing
- ❑ technological advances add new platforms that are complex and involve multiple actors and platforms
- ❑ Digitalization brings extra complex challenges to countering terrorism financing
- ❑ Major challenge : the capacity of legal framework to timely and effective coverage against digital funding, digital laundering etc.
- ❑ Cyber aspect of the 21st century should also be carefully assessed in countering terrorism financing policy and it requires robust legal and human resources aspects
- ❑ It is vital to make continuous update in accordance with the rapid changes in the terrorism financing in parallel with the technological innovation

21/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Conclusion

- ❑ Deficiencies in legal framework such as the coverage of local cases of terrorism like in Turkish case.
- ❑ The orientation of international legal framework mainly targeting religiously motivated terrorist organizations is a challenge on international cooperation.
- ❑ It is not only cooperation at international level but also at domestic level that challenges countering terrorism financing . In Turkish case, it is the intelligence sharing on sensitive and classified information that challenges countering terrorism financing .

22/17

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

QUESTIONS?

THANK YOU

filizkatman@aydin.edu.tr

23/14

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

Implementation of International Restrictive Measures - An Effective Tool in Prevention of Financing of Terrorism

Mr. Ivica SIMONOVSKI

Cutting off financing channels for terrorists and depriving them of funds and property is one the most effective ways to undermine terrorist activities. For instance, the author provides a number of powerful tools to counter terrorist financing. Effective implementation of such tools can stop flows of funds into the hands of terrorists, and significantly contribute to broader counter terrorism efforts. A combined and intelligent application of these tools could also provide **valuable financial data** on terrorists and their facilitators that would help to reveal previously unknown links between them and identify new targets for investigations.

Effective freezing regimes are critical to combating the financing of terrorism and, as a preventive tool, accomplish much more than freezing terrorist-related funds or other assets present at any particular time. Effective freezing regimes also combat terrorism by:

a) **Deterring** non-designated persons or entities who might otherwise be willing to finance terrorist activity.

b) **Exposing** terrorist financing “money trails” that may generate leads to previously unknown terrorist cells and financiers.

c) **Dismantling** terrorist financing networks by encouraging designated persons or entities to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups.

d) **Terminating** terrorist cash flows by shutting down the pipelines used to move terrorist related funds or other assets.

e) **Forcing** terrorists to use more costly and higher risk means of financing their activities, which makes them more susceptible to detection and disruption.

f) **Fostering** international co-operation and compliance with obligations under the UNSC Resolutions.

The main focus of the presentation was the importance of the implementation of targeted financial measures against targeted individuals and entities in order to prevent the financing of further terrorist activities. It also provides a general overview of the international and national instruments and mechanisms in place to impose targeted financial sanctions against individual terrorists and terrorist organizations. There are different measures that can be taken as part of these programs, with asset freezing being just one category of these measures. **Freezing measures** represent a temporary limitation to the right to property, but they are not the same as its expropriation. According to United Nations Security Council Resolution 1267, the term freeze means "*the prohibition of the transfer, conversion, disposal or movement of funds or other assets*". The persons subject to such measures are determined by the national authorities or by an international organization. Therefore, these measures are different from confiscation or confiscation measures imposed by the judicial authorities. Here the author makes a distinction between asset freezing and confiscation. Confiscation implies a penalty imposed by a court, while freezing assets is a preventive measure. Once the financial restrictive measures come into force, all financial and non-financial institutions, as well as the concerned state institutions, such as the Real Estate Cadastre Agency and the Central Securities Depository, are obliged to act on them. Failure to comply with the measure shall be considered an offense and subject to punishment by the state, otherwise, the state itself will be assessed as dysfunctional in the process of implementing restrictive financial measures, and international organizations may take concrete steps to sanction it.

Also, special focus was placed on the procedure for listing and delisting of individuals and entities on the national sanction lists introduced individually by the NATO member states that established a national legal mechanism. The presentation was prepared based on the research process, conducted through a desk analysis of primary and secondary literature, a comparative analysis of the legal framework of the NATO member states that have a legal mechanism for the introduction of autonomous sanctions, and special interviews with experts in the field.

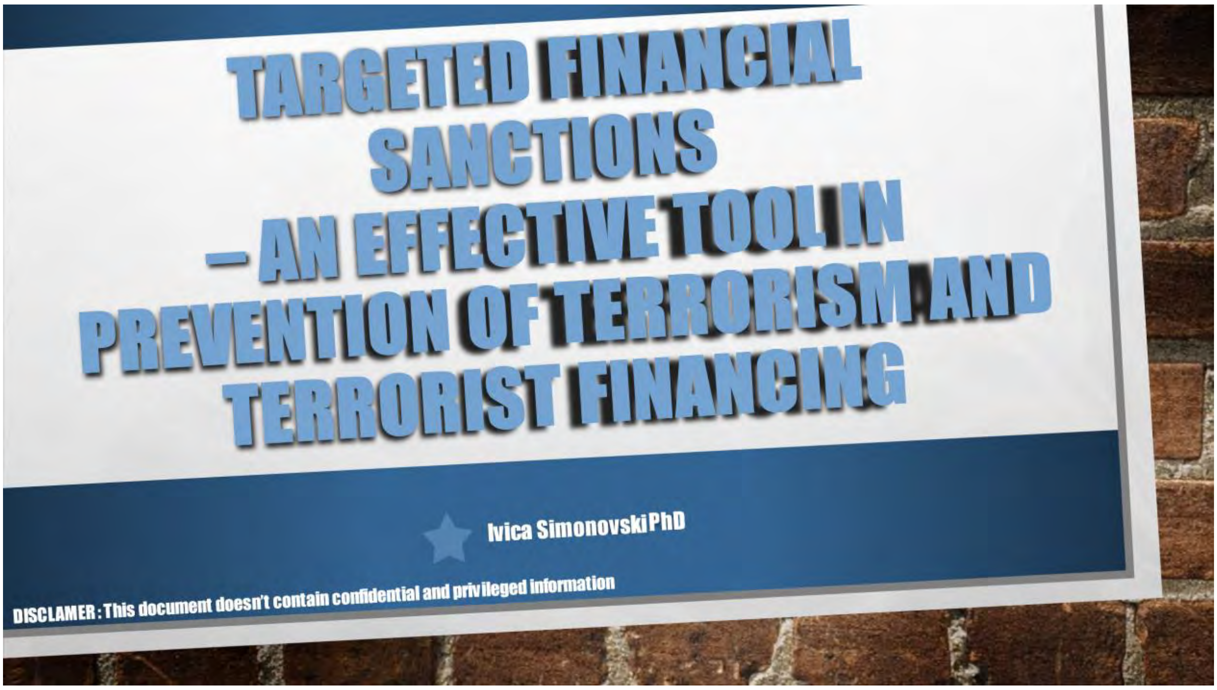
Also, a **vacuum** in relation to the implementation process occurs for those NATO countries that are members of the UN, and which also have the status of a candidate state for EU membership. In these countries, the Government or some other state administration body passes a decision on the introduction and application of sanctions introduced by the EU. It often happens that the decision to introduce and apply the sanctions adopted by the UN or the EU is made after a certain period (after a few days, weeks, or even after several months).

As the author presented, this practice represents an excellent opportunity for the property and assets of the persons for whom sanctions have been imposed to be relocated to a safe place for them. The same applies to the ban on entry/exit, the embargo of goods and services, the embargo of weapons, etc.

In order to overcome this legal vacuum, the author recommends that the NATO Alliance create a legal mechanism through which, at the political level, decisions will be made to introduce sanctions against persons and entities that pose a threat to security and international peace, including terrorists and terrorist organizations.

This, in turn, will result in the formation of an integrated list of entities (individuals, groups, legal entities and other organizations) which will be valid for NATO member countries. The list should be of a public nature and available to everyone in the Alliance, because both physical and legal persons as well as the bodies of state administrations have the obligation to implement the measures of restriction or sanctions and at the same time to take measures for their implementation.

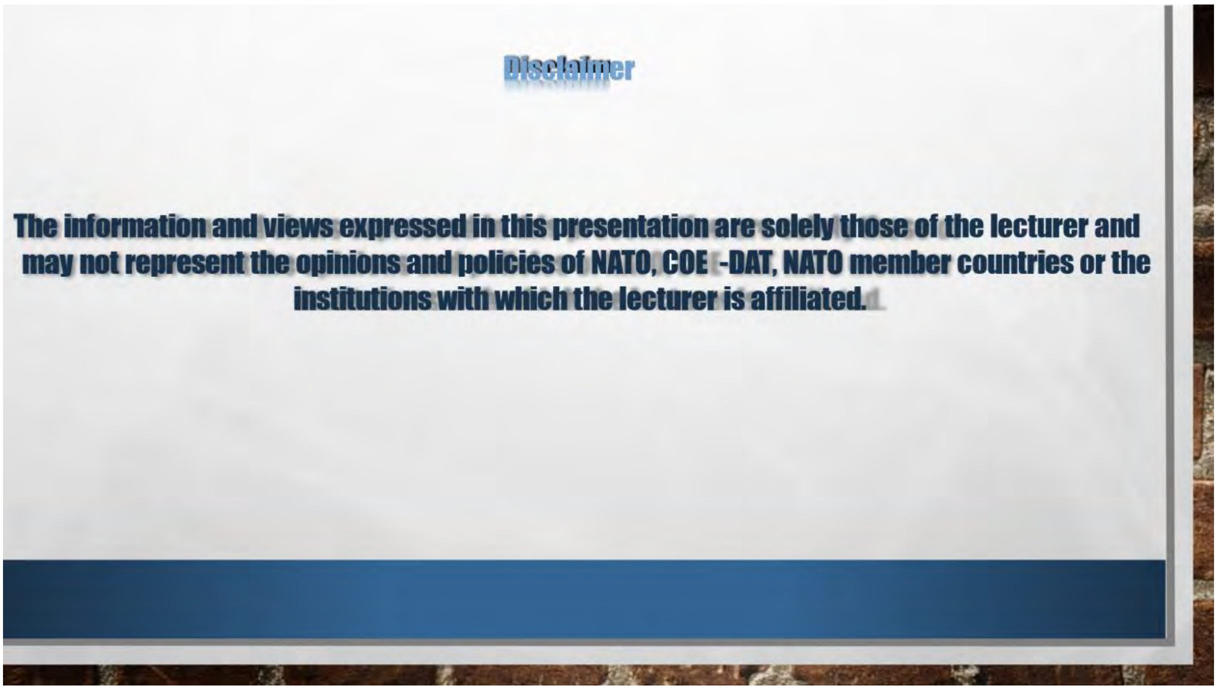
Presentation



TARGETED FINANCIAL SANCTIONS – AN EFFECTIVE TOOL IN PREVENTION OF TERRORISM AND TERRORIST FINANCING

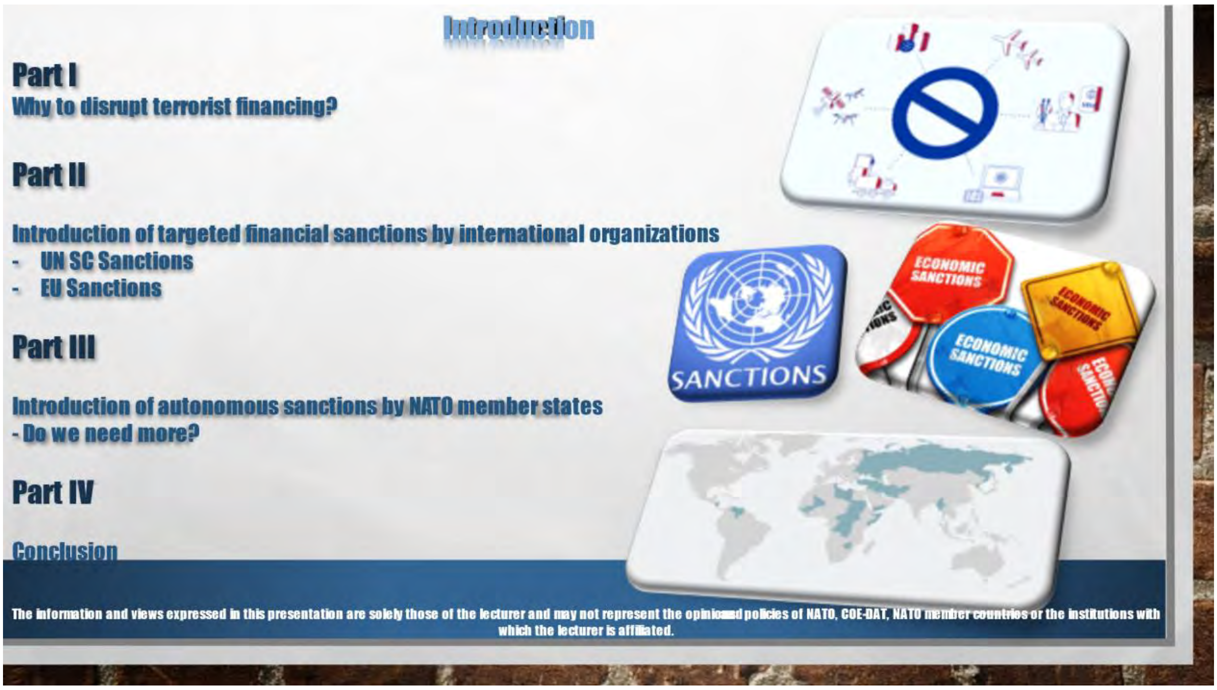
Ivica Simonovski PhD

DISCLAMER: This document doesn't contain confidential and privileged information



Disclaimer

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE -DAT, NATO member countries or the institutions with which the lecturer is affiliated.



Introduction

Part I

Why to disrupt terrorist financing?

Part II

Introduction of targeted financial sanctions by international organizations

- UN SC Sanctions
- EU Sanctions

Part III

Introduction of autonomous sanctions by NATO member states

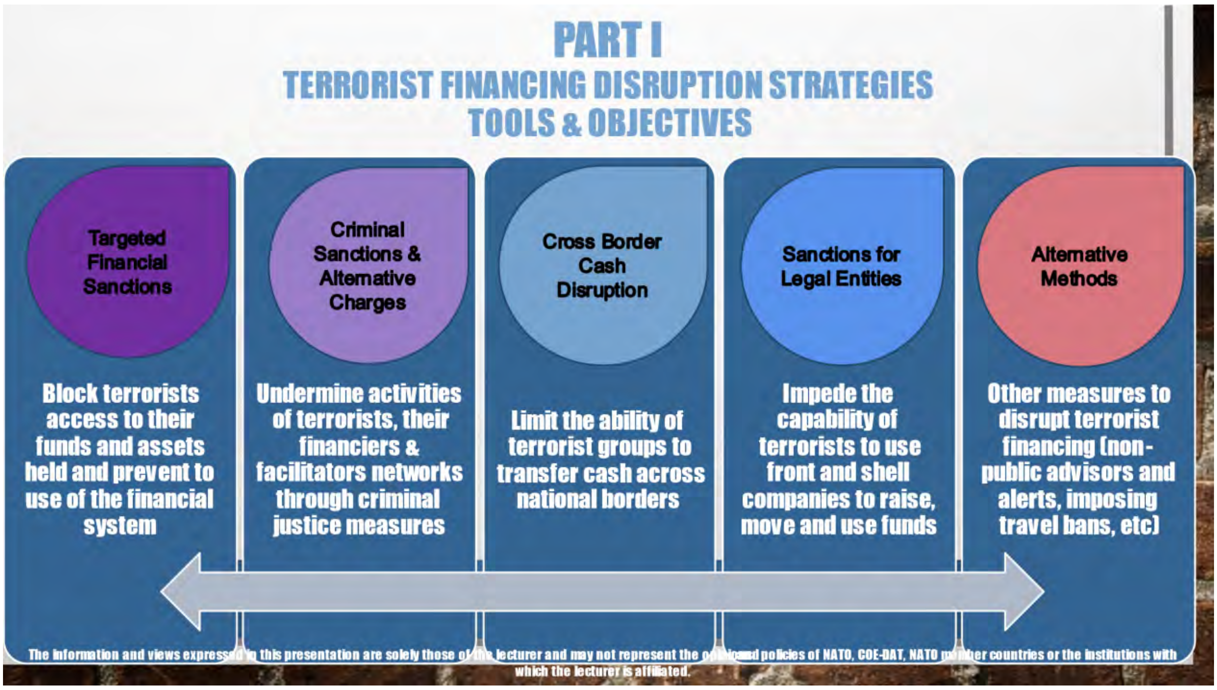
- Do we need more?

Part IV

Conclusion

SANCTIONS
ECONOMIC SANCTIONS
ECONOMIC SANCTIONS
ECONOMIC SANCTIONS

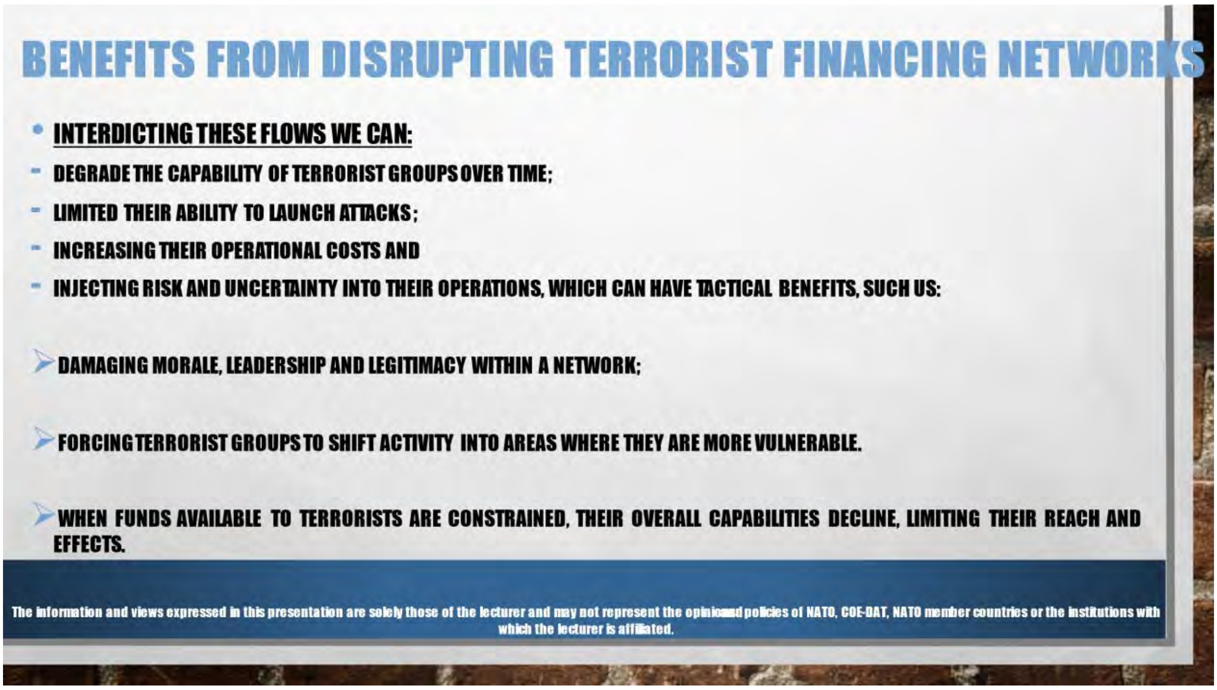
The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinioand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



PART I
TERRORIST FINANCING DISRUPTION STRATEGIES TOOLS & OBJECTIVES

Targeted Financial Sanctions	Criminal Sanctions & Alternative Charges	Cross Border Cash Disruption	Sanctions for Legal Entities	Alternative Methods
Block terrorists access to their funds and assets held and prevent to use of the financial system	Undermine activities of terrorists, their financiers & facilitators networks through criminal justice measures	Limit the ability of terrorist groups to transfer cash across national borders	Impede the capability of terrorists to use front and shell companies to raise, move and use funds	Other measures to disrupt terrorist financing (non-public advisors and alerts, imposing travel bans, etc)

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinions and policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



BENEFITS FROM DISRUPTING TERRORIST FINANCING NETWORKS

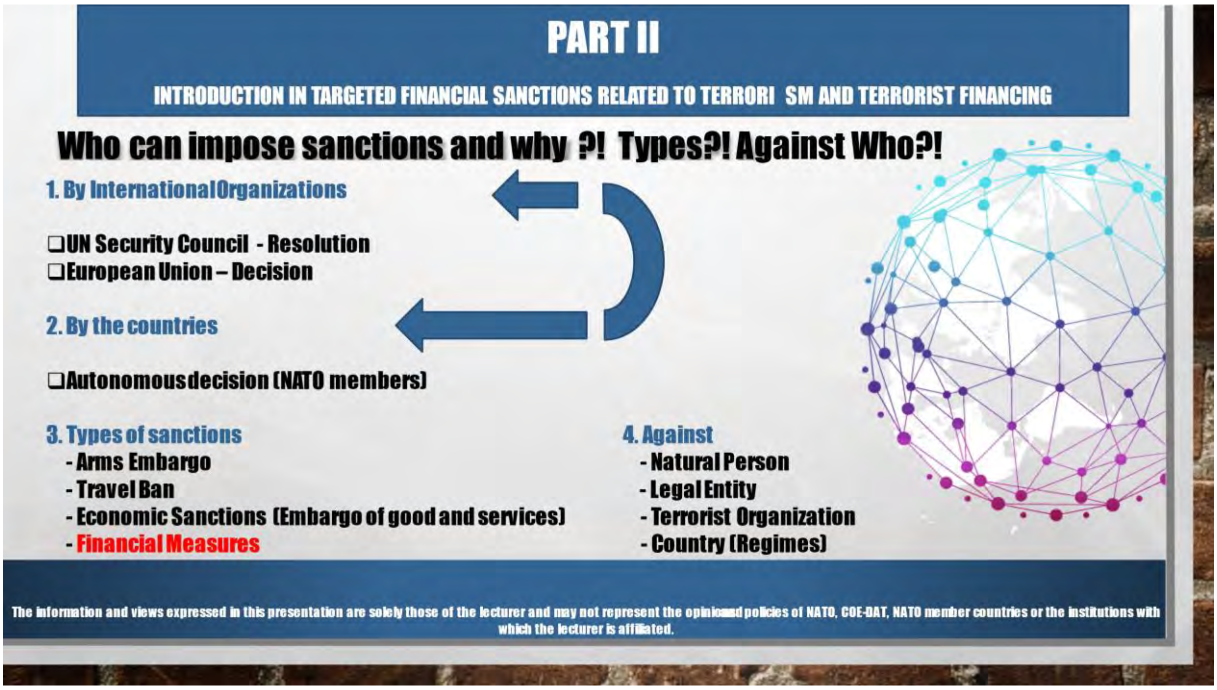
- **INTERDICTING THESE FLOWS WE CAN:**
- DEGRADE THE CAPABILITY OF TERRORIST GROUPS OVER TIME;
- LIMITED THEIR ABILITY TO LAUNCH ATTACKS;
- INCREASING THEIR OPERATIONAL COSTS AND
- INJECTING RISK AND UNCERTAINTY INTO THEIR OPERATIONS, WHICH CAN HAVE TACTICAL BENEFITS, SUCH US:

➢ DAMAGING MORALE, LEADERSHIP AND LEGITIMACY WITHIN A NETWORK;

➢ FORCING TERRORIST GROUPS TO SHIFT ACTIVITY INTO AREAS WHERE THEY ARE MORE VULNERABLE.

➢ WHEN FUNDS AVAILABLE TO TERRORISTS ARE CONSTRAINED, THEIR OVERALL CAPABILITIES DECLINE, LIMITING THEIR REACH AND EFFECTS.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinioand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



PART II

INTRODUCTION IN TARGETED FINANCIAL SANCTIONS RELATED TO TERRORI SM AND TERRORIST FINANCING

Who can impose sanctions and why ?! Types?! Against Who?!

1. By InternationalOrganizations

❑UN Security Council - Resolution
❑European Union – Decision

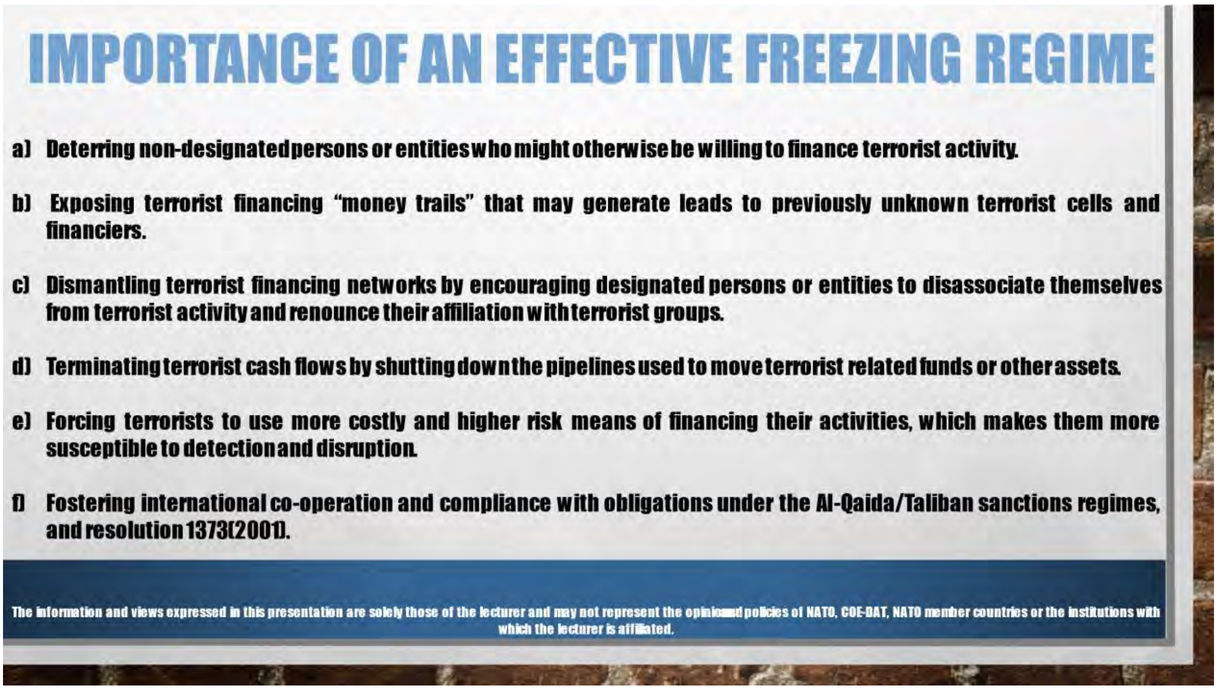
2. By the countries

❑Autonomousdecision (NATO members)

3. Types of sanctions
- Arms Embargo
- Travel Ban
- Economic Sanctions (Embargo of good and services)
- **Financial Measures**

4. Against
- Natural Person
- Legal Entity
- Terrorist Organization
- Country (Regimes)

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinionand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



IMPORTANCE OF AN EFFECTIVE FREEZING REGIME

a) Deterring non-designatedpersons or entitieswho might otherwise be willing to finance terrorist activity.

b) Exposing terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers.

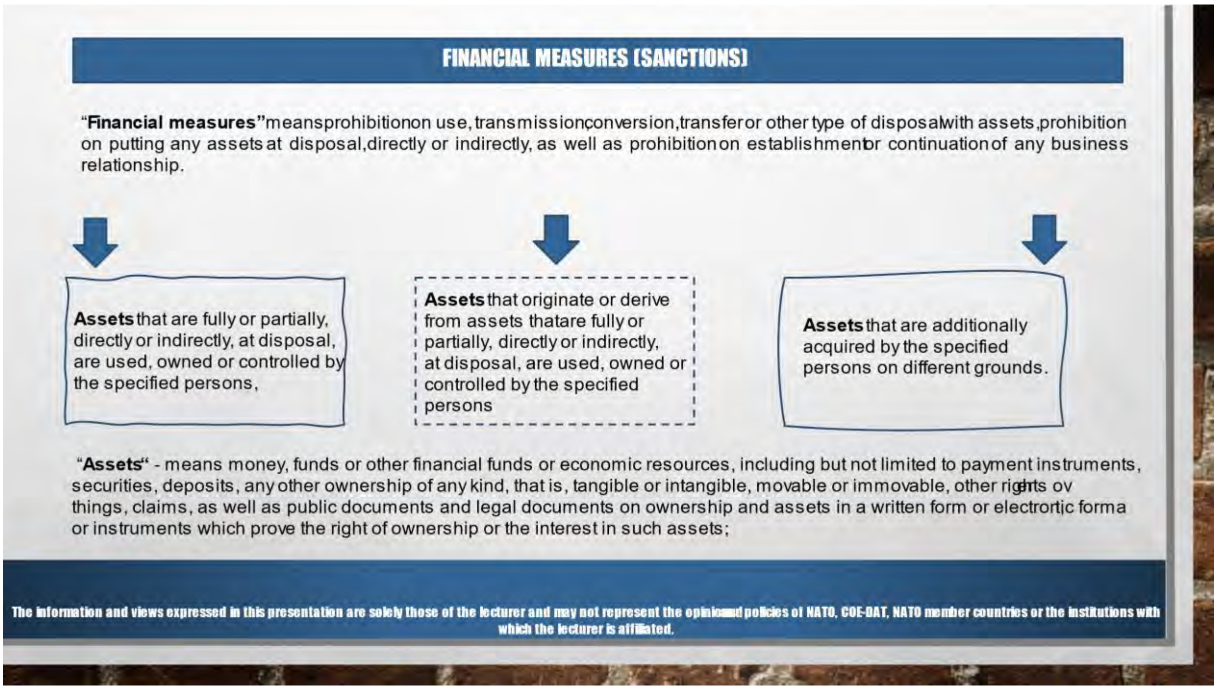
c) Dismantling terrorist financing networks by encouraging designated persons or entities to disassociate themselves from terrorist activity and renounce their affiliation withterrorist groups.

d) Terminating terrorist cash flows by shutting downthe pipelines used to move terrorist related funds or other assets.

e) Forcing terrorists to use more costly and higher risk means of financing their activities, which makes them more susceptible to detectionand disruption.

f) Fostering international co-operation and compliance with obligations under the Al-Qaida/Taliban sanctions regimes, and resolution 1373(2001).

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinionand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



FINANCIAL MEASURES (SANCTIONS)

“**Financial measures”**meansprohibitionon use, transmission,conversion,transferor other type of disposalwith assets,prohibition on putting any assets at disposal,directly or indirectly, as well as prohibitionon establishmentor continuationof any business relationship.

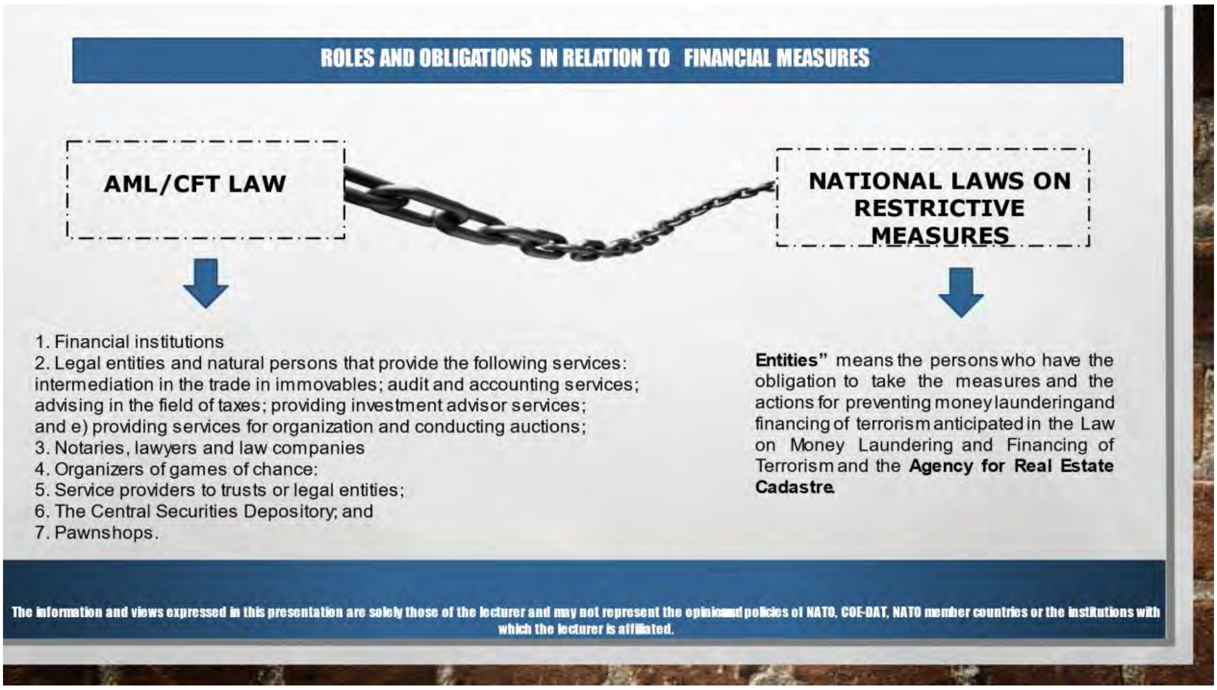
Assets that are fully or partially, directly or indirectly, at disposal, are used, owned or controlled by the specified persons,

Assets that originate or derive from assets thatare fully or partially, directly or indirectly, at disposal, are used, owned or controlled by the specified persons

Assets that are additionally acquired by the specified persons on different grounds.

“**Assets**“ - means money, funds or other financial funds or economic resources, including but not limited to payment instruments, securities, deposits, any other ownership of any kind, that is, tangible or intangible, movable or immovable, other rights ov things, claims, as well as public documents and legal documents on ownership and assets in a written form or electronic forma or instruments which prove the right of ownership or the interest in such assets;

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinionsand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



ROLES AND OBLIGATIONS IN RELATION TO FINANCIAL MEASURES

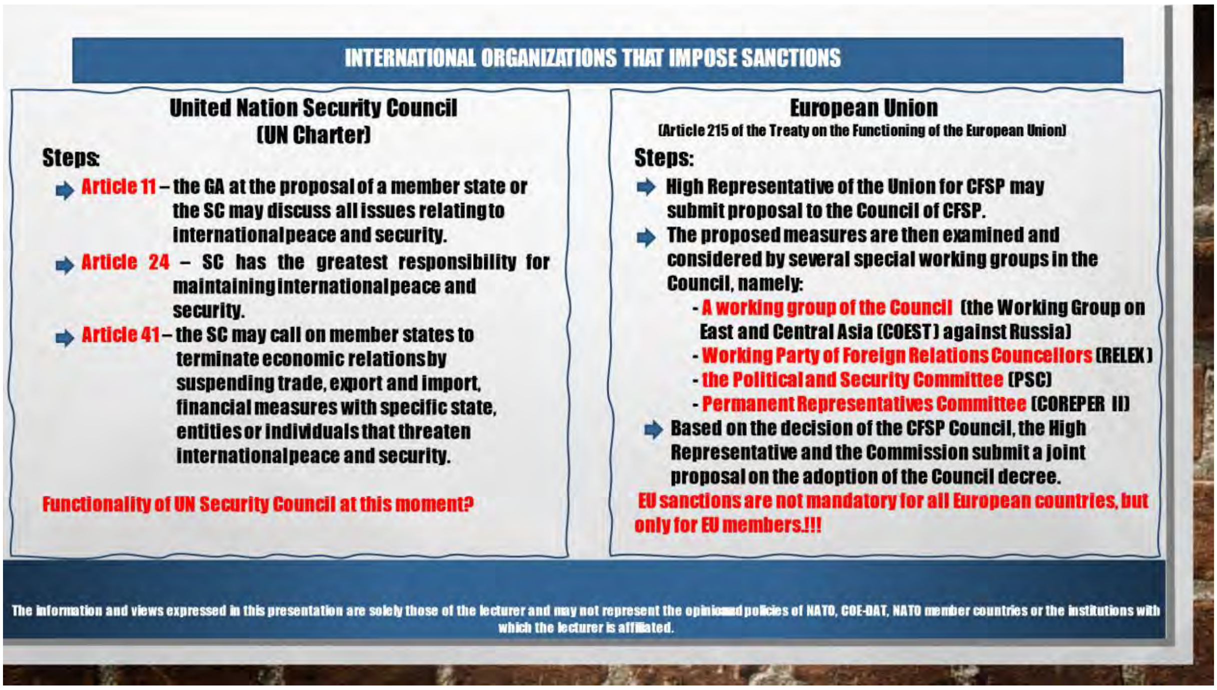
AML/CFT LAW

NATIONAL LAWS ON RESTRICTIVE MEASURES

1. Financial institutions
2. Legal entities and natural persons that provide the following services: intermediation in the trade in immovables; audit and accounting services; advising in the field of taxes; providing investment advisor services; and e) providing services for organization and conducting auctions;
3. Notaries, lawyers and law companies
4. Organizers of games of chance:
5. Service providers to trusts or legal entities;
6. The Central Securities Depository; and
7. Pawnshops.

Entities” means the persons who have the obligation to take the measures and the actions for preventing money launderingand financing of terrorism anticipated in the Law on Money Laundering and Financing of Terrorism and the **Agency for Real Estate Cadastre**.

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinionsand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



INTERNATIONAL ORGANIZATIONS THAT IMPOSE SANCTIONS

United Nation Security Council
(UN Charter)

Steps:

- **Article 11** – the GA at the proposal of a member state or the SC may discuss all issues relating to international peace and security.
- **Article 24** – SC has the greatest responsibility for maintaining international peace and security.
- **Article 41** – the SC may call on member states to terminate economic relations by suspending trade, export and import, financial measures with specific state, entities or individuals that threaten international peace and security.

Functionality of UN Security Council at this moment?

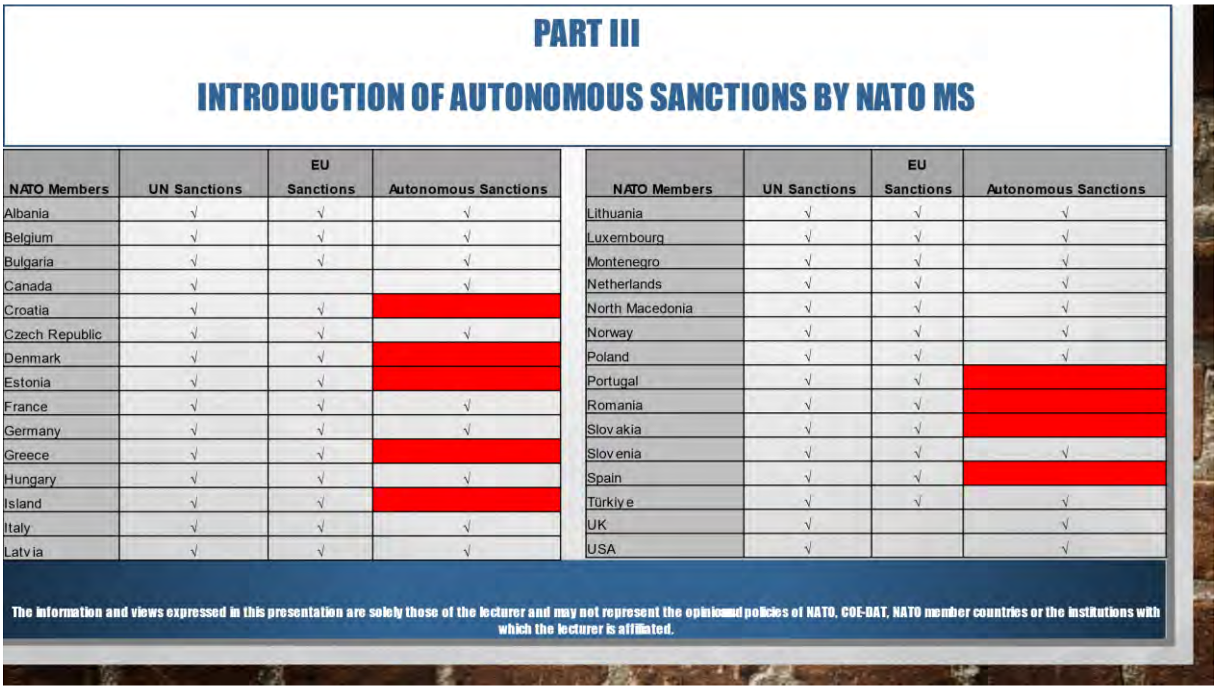
European Union
(Article 215 of the Treaty on the Functioning of the European Union)

Steps:

- High Representative of the Union for CFSP may submit proposal to the Council of CFSP.
- The proposed measures are then examined and considered by several special working groups in the Council, namely:
  - **A working group of the Council** (the Working Group on East and Central Asia (COEST) against Russia)
  - **Working Party of Foreign Relations Councellors** (RELEX)
  - **the Political and Security Committee** (PSC)
  - **Permanent Representatives Committee** (COREPER II)
- Based on the decision of the CFSP Council, the High Representative and the Commission submit a joint proposal on the adoption of the Council decree.

EU sanctions are not mandatory for all European countries, but only for EU members!!!

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinionsand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



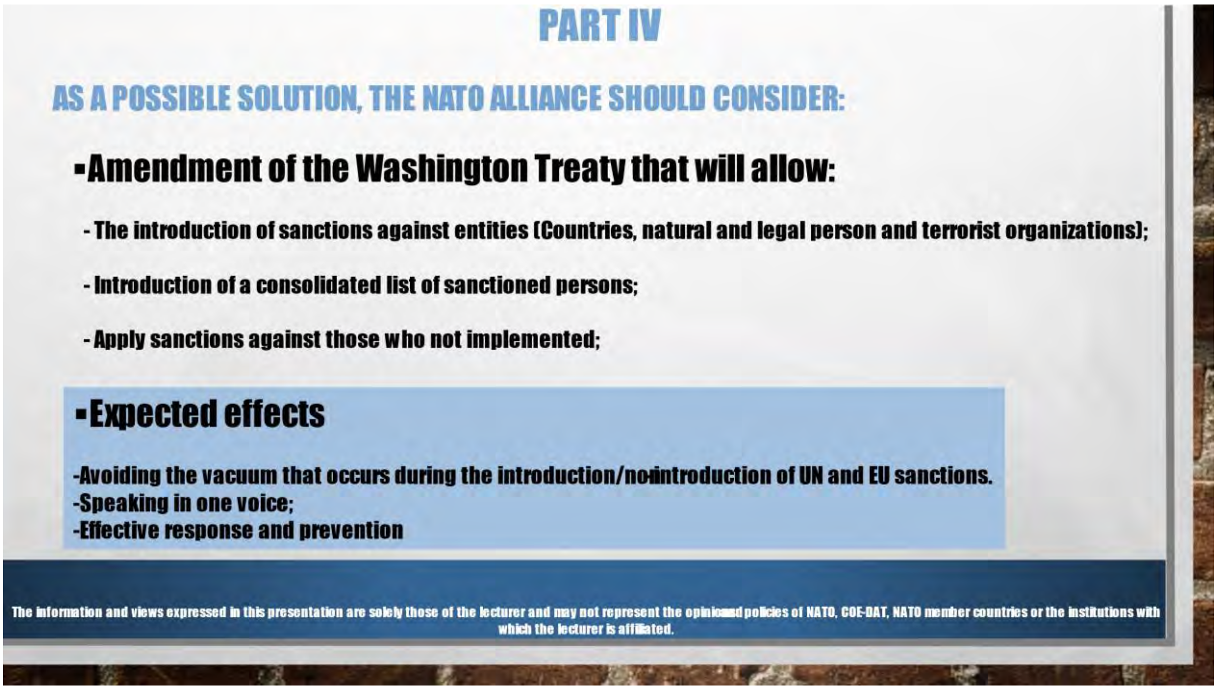
PART III

INTRODUCTION OF AUTONOMOUS SANCTIONS BY NATO MS

NATO Members	UN Sanctions	EU Sanctions	Autonomous Sanctions
Albania	√	√	√
Belgium	√	√	√
Bulgaria	√	√	√
Canada	√		√
Croatia	√	√	🟥
Czech Republic	√	√	√
Denmark	√	√	🟥
Estonia	√	√	🟥
France	√	√	√
Germany	√	√	√
Greece	√	√	🟥
Hungary	√	√	√
Island	√	√	🟥
Italy	√	√	√
Latvia	√	√	√

NATO Members	UN Sanctions	EU Sanctions	Autonomous Sanctions
Lithuania	√	√	√
Luxembourg	√	√	√
Montenegro	√	√	√
Netherlands	√	√	√
North Macedonia	√	√	√
Norway	√	√	√
Poland	√	√	√
Portugal	√	√	🟥
Romania	√	√	🟥
Slovakia	√	√	🟥
Slovenia	√	√	√
Spain	√	√	🟥
Türkiye	√	√	√
UK	√		√
USA	√		√

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinionsand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.



PART IV

AS A POSSIBLE SOLUTION, THE NATO ALLIANCE SHOULD CONSIDER:

- **Amendment of the Washington Treaty that will allow:**

  - The introduction of sanctions against entities (Countries, natural and legal person and terrorist organizations);

  - Introduction of a consolidated list of sanctioned persons;

  - Apply sanctions against those who not implemented;

- **Expected effects**

-Avoiding the vacuum that occurs during the introduction/non-introduction of UN and EU sanctions.
-Speaking in one voice;
-Effective response and prevention

The information and views expressed in this presentation are solely those of the lecturer and may not represent the opinionsand policies of NATO, COE-DAT, NATO member countries or the institutions with which the lecturer is affiliated.

THANK YOU FOR YOUR ATTENTION

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM
2004
TÜRKIYE

Ivica Simonovski PhD

DAY II

SESSION 2: Questions and Answers

Question to Dr. Sheelagh BRADY

1. *There is a question related to the cryptocurrencies and the work you have done on that. Clearly, this is a fantastic technology and offers many opportunities for the good, but it can also be used for evil purposes. But still you presented on the notion of using those technologies for the flow of resources. What about the flow of information and the storage of information? Because we are very close to the point in which he technology we are going to be able to store information in biological systems. What happens then and do we have any tools to deal with this kind of situation, because obviously we flow means that at one point has to become something else by yourself?*

   You make such an important observation because the when you combine the flow of value with the flow of information that is just a very potent combination. Therefore, I think this is where we come down to some of the points we heard in the panel earlier is the importance of the legal framework. At the moment when countries are not deliberating how you know cyber security measures, information storage, things like GDPR privacy controls that need to be put in place. Every country is doing its own thing, some are not doing anything at all. Some countries are creating a system that benefits maybe just the government or maybe benefiting a private sector. I know our perspective that we do not collect private data or private information. That data stays like with the bank it would stay with the bank, but this is a very big gap that at the moment it's really ad hoc and not uniformed. So, I agree with you, it's a big concern.

Questions to Ms. Liat SHETRET

1. *In my research, it was suggesting that cryptocurrencies may be as easy to create in the next couple of years as going on to make a PowerPoint presentation and would be available to anybody in their own home. Do you think that is realistic forecasting or do you think it is another one of these types of fear around the potential criminality?*

Anyone can create a crypto asset. We could have whatever coin we want. But what gives it value is the underlying piece of it. There is a community that gives a coin value and there is two elements of it. One is a community around it or something else that gives its value. We are really focused on investor protections and consumer protections to avoid this kind of exploitation of crypto and to avoid these big spikes around random coin or whatever is created by any one of us.

<u>Questions to Dr. Filiz KATMAN</u>

1. *What do you consider about the hawala system for money exchange role in modern terrorism and the ways of its prevention?*

In fact, my research does not cover specifically the analysis of each system, but there is one article which specifically deals with hawala system, by Ali Yurdakul, which is published in 2021, very recent research at business and economics research journal. And the name of the article is informal value transfer system as terrorism financing and money laundering. Like I mentioned, 9/11 is a milestone in countering terrorism financing, as well. Informal value transfer systems came under pressure to regulate and control hawala and alternative traditional remittance methods, often used by immigrant families. We have this flow of people from one country to another; therefore, it is going to be a further challenge indeed. It has been found to be vulnerable to abuse by criminal organizations and terrorist groups. While making arrangements for the informal value system, it is important that the service provision to those who use these systems is maintained without interruption. The Freedom to use for other purposes should be protected. For this reason, it has been concluded that it is important to synchronize economic factors.