CENTRE OF EXCELLENCE

DEFENCE AGAINST TERRORISM

COE DAT

STRENGTHENING THE SECURITY AND RESILIENCE OF NATO AND PARTNER NATION CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

Lessons Learned Workshop

Report

16-17 December 2019

Ankara, Turkey

Contents

General Information of the Workshop

Subject:	COE-DAT's "Strengthening the Security and Resilience of NATO and Partner Nation Critical Infrastructure Against Terrorist Attacks." Lessons Learned Workshop
Background:	Authorized in the COEDAT 2019 Yearly Activity Plan by the COEDAT Executive Steering Committee. Lessons Learned workshop was conducted between 16 and 17 December 2019 at COEDAT facilities in Ankara, Turkey.
Aim:	To discuss and validate a number of recent observations which suggest the current COEDAT's "Critical Infrastructure Protection Against Terrorist Attacks" (CIPATA) course should be: • Retitled as the "Critical Infrastructure Security and Resilience Against Terrorist Attacks" (CISRATA) course • That COEDAT develop and deliver a new "Advanced Critical Infrastructure Security and Resilience Against Terrorist Attacks" course, and • To identify the role of NATO in the field of security and resiliency for the protection of critical infrastructure.
Event OPR:	Col Attila CSURGO (HUN A) COEDAT's Chief of Knowledge Department
Academic Advisor:	Adjutant. Prof Ronald S. BEARSE at the Massachusetts Maritime Academy
WS Director:	Police Chief Oguz YURDAER (TUR State Police)
WS Assistant:	Ms. Aslihan SEVIM (TUR)
Rapporteurs:	Ms. Eylül ÖZYURT (TUR) and Ms. Alice LÖHMUS (EST)

Paper Overview

This lessons learned workshop report presents the overview of discussions and outcomes from the two-day event held in December 2019 at COEDAT's Ankara, Turkey facility. It starts with a letter from Professor Ron Bearse to COEDAT leadership with observations based upon his many years work on developing and instructing at COEDAT's Critical Infrastructure Protection Against Terrorist Attacks course with potential recommendations to improve and expand the course. This letter serves as the basis for the workshop and the projected follow-on workshop in June of 2020.

Our intent is to present an overview of the discussions during the event as if the reader were present in the room. This method was chosen to offer the reader an insight into what was discussed, what was agreed upon, and to spark the intellectual curiosity of the many experts who could not attend the workshop in person. With this report the reader may be able to read as if they were there in order to form their opinions and reach out to COEDAT with their views, opinions, and constructive suggestions to influence COEDAT's future work on Critical Infrastructure Protection / Critical Infrastructure Security and Resilience Against Terrorist Attacks.

The workshop report ends with observations, discussions, conclusions, and recommendations for inclusion into NATOs Lessons Learned portal. These observations, discussions, conclusions, and recommendations may be of use to the Alliance members, partner nations, and other actors in the global fight against terrorism to better develop more resilience for all of our critical infrastructure.

Col Daniel Stone, USAF

Deputy Director COEDAT

Background

NNSG

Nauset National Security Group, LLC

11 John Hall Cartway

Yarmouth Port, MA 02675

July 3, 2019

Dear Director GÖRGÜLÜ and Deputy Director STONE:

On behalf of my good friends and fellow COEDAT lecturers Dr. Carol Evans, Mr. Michael Lowder and Geoffrey French, I would like to convey our deepest appreciation to COEDAT and particularly to Major YAĞBASAN for developing and delivering the sixth iteration of the NATO COEDAT Critical Infrastructure Protection Against Terrorist Attacks (CIPATA) Course.

My colleagues and I have been helping many countries and organizations protect their critical infrastructure for decades; but one of our greatest satisfactions has been our involvement with COEDAT over the last six years as it effort to strengthen NATO and Partner Nation critical infrastructure protection (CIP) capabilities through education involving valuable information sharing, the discussion of important lessons learned, and challenging tabletop practicums.

COEDAT's prescient decision to develop and deliver the CIPATA course has produced real, measurable change – change within the minds of the 400+ students who have attended the CIP course over the last 6 years, and change within the nations and organizations many of these students represented. Last May's course convinced us that we are seeing material changes not only in Turkey, but also in other nations which are currently involved in developing and/or implementing their own strategic and operational approaches to CIP. COEDAT's investment in CIP education is essential to building national and economic security across the Alliance and Partner Nations[1] and also to improving industry efficiency, connectivity, and growth – all of which help these nations improve public confidence in governance. COEDAT's continued investment in developing and delivering state-of-the-art CIP education is just as important tomorrow as it has been for the last six years ago because the threat to critical infrastructure is evolving and likely to increase in the years ahead. We believe that effectively dealing with this challenge is of paramount concern in the new security environment and demands that COEDAT continue putting a premium on raising awareness of the growing threat; share valuable lessons learned in building and

[1] NATO cooperates with a range of international organizations and countries in different structures. It is including; Partnership for Peace (PfP) countries, NATO's Mediterranean Dialogue, Istanbul Cooperation Initiative (ICI), Partners across the globe. Source: https://www.nato.int/cps/en/natohq/51288.htm

maintaining demonstrable CIP capabilities; and providing concrete steps to secure NATO and Partner Nation critical infrastructure. We further believe the current security environment contains a broad and evolving set of challenges to the security of NATO's territory, infrastructure and populations which necessitates the continuing need to for COEDAT to offer CIPATA education.

COEDAT's CIPATA course serves NATO and Partner Nation long-term interests in supporting the development of essential capabilities for preventing, preparing for, responding to, mitigating the consequences of, and recovering from a terrorist threats and/or attacks which could easily threaten the proper functioning of critical infrastructure. When there are disruptions to the services critical infrastructure provide, such as energy, transportation, and communications, there is the potential for costly direct economic impacts, such as the cost of repairing damage to physical structures, and indirect economic impacts to society, such as disruption to global supply chains. This puts an enormous responsibility on Alliance and Partner Nations to collaborate with one another in the pursuit of coordinated global critical infrastructure security and resilience measures. By investing in CIP education and helping Alliance and Partner Nations build robust and redundant critical infrastructure protection capabilities across Alliance and Partner Nations, the length and magnitude of such disruptions can be minimized.

The May 2019 CIPATA course continued the recent tradition of providing a unique educational platform for discussing the protection of critical energy and other infrastructure with both military representatives of Alliance and Partner Nations and a few representatives from private industry, which was very important owing to the fact that most of the world's critical infrastructure is owned and operated by private sector corporations.

With the help of top notch speakers from around the world, this year's course was able to successfully:

- Expose students to the essential elements of modern national CIP policy and planning;
- Discuss how CIP supports national and economic security, as well as economic prosperity;
- Focus particularly on protecting critical energy (i.e., gas and oil pipelines, nuclear power and electrical power grid) and transportation infrastructures;
- Increase student knowledge and understanding of current and emerging issues, concerns and challenges in developing and implementing national CIP policy and plans;
- Identify the roles and responsibilities of government, the private sector, and non-government organizations (NGOs), international organizations and others in protecting critical infrastructure from the hazards they face, including terrorist attacks;
- Emphasize the need for clear and unambiguous methods for defining risk terms and risk methodologies for use in protecting critical infrastructure against terrorist attacks, and assessing the resilience of these assets;
- Provide students with concepts, methods and tools they can use to improve the security and resilience of critical infrastructures in their nations;
- Identify the need for public-private partnerships and information sharing mechanisms for protecting critical infrastructure; and

- Conduct an immersive practicum that enabled students to apply what they learned during the course in a tabletop exercise simulating terrorist threats and attacks against critical energy infrastructure.

With the course's conclusion, every student understood these important issues and nearly every student stated the course had met or exceeded their expectations. Many students provided updates on the status of national CIP planning and operations in their own countries, which confirmed that significant changes are taking place in a number of nations as they seek to establish and implement national CIP policies, plans and procedures.

After the course was over, the four of us got together to conduct a short net assessment of the last six years of our involvement in the CIPATA course and what we know is happening on the leading edge in the CIP arena. As a result of our analysis, we would like to provide some important observations and recommendations for improving COEDAT's position as a leader in providing important and useful education on protecting critical infrastructure against terrorist attacks.

Observations:

1. The current CIPATA course remains popular and particularly relevant in the new security environment. Over 400 students have graduated from the CIPATA course. Since its inception, the course has been fairly "introductory" in purpose and scope. However, we are now of the firm belief that COEDAT's mission can be better fulfilled by offering new types of presentations and more concrete protection solutions in future iterations of the CIPATA course.
2. The concept of CIP has matured to the point where it is now more commonly referred to as Critical Infrastructure Security and Resilience (CISR), not only in the West, but elsewhere around the globe. Focus on the "protection" of critical infrastructure began to turn to "resiliency" of critical infrastructure in the mid- 2000s because critical infrastructures need to be resilient (i.e., be able to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks, accidents, or other naturally occurring threats or incidents) due to the inability to provide absolute protection to all identified national critical infrastructure from all possible threats. Individuals and institutions responsible for the design, delivery and operation of critical infrastructure are now embracing and adopting resilience concepts and practices, so that engineered structures and infrastructure are not only safer (do not fail), but also better provide continuity of essential critical functions. Since "resilience" is one of NATO's seven key competencies, COEDAT should seriously consider changing the name of the current CIPATA course to the "CISRATA" course to support the broader NATO strategic objectives. Transforming the current CIPATA course to CISRATA would require adding a new concepts and practices providing the context for the CISR environment.
3. Additionally, we advise that a new "Advanced CISRATA" course should be designed and delivered to serve the "big thinkers" who have the responsibility for integrating CIP/CISR into the greater national security framework of a nation, and/or the "practitioners" who actually manage and directly work on CIP/CISR plans, policies, procedures and related activities. A number of students attending the May 2019 class specifically asked us if such a course(s) existed, which

indicates there is an appreciable interest in attending an Advanced CISRATA course. The development, marketing, and delivery of such a course are the logical next steps in pursuing desired CISR outcomes.

4. More recently, there has also been a movement toward conceptualizing, identifying, and modeling complex infrastructure interdependencies and their cascading effects. We know that computational models, sensor networks, big data, and self-healing systems are promising approaches to solving this challenge. These new approaches should be discussed in any future CISRATA course.
5. New materials offer promise for addressing infrastructure life-cycle issues because of their potential to improve resilience and extend system life expectancies. Sensing technologies allow for continuous system monitoring and more precise inspection. Advancements in computing techniques promise new approaches for data-informed simulations to explore critical infrastructure system performance in the face of changing conditions and threats, including the performance of aging infrastructure systems.
6. Research and development into the dynamics of interdependent systems and human/social factors in critical infrastructure systems is also gaining increasing interest.
7. As our team looks ahead, next-generation technologies may not only include self-healing materials and buildings, but also widespread 3-D printing of complex materials, and increased use of robotics. Current strategies and standards will have to be re-evaluated to more efficiently integrate innovative materials and technologies to improve CISR and move towards performance-based risk-management standards. Robust risk assessments are needed to better target and prioritize investments in CISR efforts. They are also needed to maintain and/or rebuild aging critical infrastructure.
8. The practicum we added to the course a few years ago to stress international communication and collaboration on CIP/CISR has been an effective education tool, as other Allies and Partner Nations face many of the same infrastructure challenges as the United States, including cyber infrastructure resilience in areas such as optical networking, the "Internet of Things," and big data. Partnerships between stakeholders in the telecommunications and computing industries are examples of how resilience can be improved through better communication. However, key challenges remain, including those of developing and maintaining a robust, diverse CISR workforce, and building and maintaining trusted cross-sector information sharing partnerships. Proactive partnerships designed to foster communication and collaboration across nations, regions, sectors, ministries, agencies, and communities are urgently needed to help ensure the timely and impactful integration of innovative solutions to common CISR challenges going forward, particularly with regard to the evolving terrorist threat.

Recommendations:

1. Develop and deliver both an in-house and mobile course entitled, "Critical Infrastructure Security and Resilience Against Terrorist Attacks" to expand the opportunity to educate more students from other nations on the basics of CISR focused primarily on defending critical infrastructure against terrorist attacks.

2. Develop and deliver a new in-house course entitled, “Advanced Critical Infrastructure Security and Resilience Against Terrorist Attacks” to serve strategic thinkers, senior managers, and practitioners responsible for developing and implementing CISR plans, policies, procedures, and related activities, including how such activities can be integrated with a more complex national security planning framework. This new course would be more focused on many of the topics identified in the observations noted above, but still retain a basic focus on the terrorist threat, in consonance with the COEDAT mission. A new Advanced CISRATA course would require issuing invitations to speak/lecture on these specific topics, including best practices and the results of ongoing research being carried out or applied by leading CISR research institutes, universities, and scientists from both the public and private sector. The course would also focus on educating students on concrete CISR capability- and capacity-building efforts currently being undertaken in NATO, European and Asian nations.

All of us would be very happy to assist COEDAT in building further developing and implementing either of these recommendations, and/or helping COEDAT build a solid business case for acquiring additional NATO funding to do so.

In closing, we are sincerely grateful to COEDAT and your leadership for providing us the opportunity to continue our involvement in the delivery of this year’s CIPATA course and being able to share our collective knowledge, experience, and domain wisdom with this year’s students. We thoroughly enjoyed discussing some of the key issues and challenges the Alliance and Partnering Nations face in strengthening the security and resilience of their critical infrastructure. We left Ankara having made new friendships, learning more about what NATO and Partner Nations are accomplishing in CIPATA/CISRATA, and having stronger appreciation for what (and how) COEDAT has accomplished by offering the CIPATA course for the last six years, and how its efforts are contributing to modern national and economic security planning.

On behalf of my colleagues, I wish both of you (and your staff) the very best of continuing success in providing key decision-makers with realistic solutions to meet current, emerging and over-the-horizon terrorist threats. Additionally, Dr. Evans and I look forward to further developing and institutionalizing an Academic Partnership between COEDAT and the U.S. Army War College and undertaking the book idea we discussed.

Very Respectfully,

Ronald S. Bearse

Ronald S. Bearse

Dramatis Personae

(In order of their appearance in the report)

Adjutant Prof. Ronald Sanford BEARSE (USA) (Academic advisor of the workshop) is an Adjutant professor at the Massachusetts Maritime Academy and Principal Consultant at Nauset National Security Group. Mr. Bearse is a former senior fellow at the George Mason University's Critical Infrastructure Protection and Homeland Security Center, and a distinguished graduate of the U.S. National Defense University. He has an undergraduate degree in Soviet Studies and an MPA from the George Washington University.

Mr. Bearse has held a wide variety of analytical, managerial and leadership positions with the U.S. Departments of Defense, Homeland Security and the Treasury, where he was the director of Security and Critical Infrastructure Protection on 9/11.

Col Mustafa Özgür Tüten (Turkish Army) Director of COEDAT

Col. Attila Csurgo, (Hungarian Army) COEDAT's Chief of Knowledge Department

Dr. Carol V. Evans (USA) is Research Professor of National Security Affairs at the Strategic Studies Institute, U.S. Army War College, in Carlisle, Pennsylvania.

Dr. Evans brings 25 years of expertise in the areas of mission assurance, defense critical infrastructure protection, crisis and consequence management, C4ISRT, asymmetric warfare, terrorism, maritime security, homeland defense, and homeland security. With that expertise, she has served as Advisor to the Director of Central Intelligence, Technical Advisor to the National Ground Intelligence Center, Department of the Army, and as Technical Advisor, the Defense Science Board, Office of the Secretary of Defense. Prior to joining the Army War College, Dr. Evans was Senior Program Manager, National Security Global Business Division, with Battelle Memorial Institute. Battelle is the largest non-profit applied research and development company in the world. At Battelle, she provided strategic planning support in the Pentagon to the Office of the Secretary of Defense, Washington Headquarters Services and the Pentagon Force Protection Agency, and to DHS' Office of Infrastructure Protection.

Mr. Malcolm Baker (UK) a Senior Counselor at ASERO Worldwide, is the former Head of the Counter Terrorism Security Advisors (CTSAs) for the New Scotland Yard in London, UK. Mr. Baker advices clients on relevant issues for homeland security such as identifying effective and cost efficient security solutions for complex environments involving strategic and operational planning and risk management.

As the Head of the Counter Terrorism Security Advisors, Mr. Baker was responsible for maintaining multi-agency relationships with both national and international partners, developing operational capabilities, counter terrorism strategies and policies and contingency plans for a number of relevant threat scenarios including those involving CBRN. Mr. Baker liaised with Government, military and Special Forces and other local partner agencies, including the MI5 Security Service, scientific advisers and the Joint Terrorism Analysis Centre (JTAC); devised and implemented business risk management

strategies for the Counter Terrorism Command (CTC) or SO15 operations for such events as the 2011 royal wedding and state visit by United States President Obama;

Mr. Baker holds an MSc in Resilience, including Risk and Crisis Management, Corporate Security, Strategy, and Business Continuity from Cranfied University, the Defense Academy of the United Kingdom.

Dr. Alessandro LAZARI (ITA) Manager-Information Risk Management, KPMG Advisory, he is a specialist on Critical Infrastructure Protection, Resilience and Cybersecurity.

Dr. Lazari, between 2010 and 2018, was a Project Officer for the European Commission. He worked on policy support to the "European Programme for Critical Infrastructure Protection", to "Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry", as well as on research and development of pre-normative support to standards, establishment of certification schemes for security products and development of qualified training for security managers.

He has also assessed and analyzed the impact of security-related policies and regulations on European Union's Member States and extracted best practices and key performance indicators. He is author of the book 'European Critical Infrastructure Protection' published by Springer Inc. in 2014.

Assoc.Prof. A. Salih BIÇAKCI (TUR) Kadir Has University, Istanbul, is an Associate Professor of International Relations at Kadir Has University, Istanbul. He completed his B.A. on History at Marmara University Education Faculty in 1994, and his M.A. at Marmara University in 1996. Bıçakcı completed the Humanities Computing program at Bergen University in Norway in 1999 and received his PhD from Tel Aviv University in Israel in 2004. Dr. Bıçakcı began his academic career at FMV Işık University and took part in numerous academic projects on identity, security and terrorism. He has thought classes in several national and international universities on the Middle East in International Politics, International Security, International Relations Theory and Turkish Foreign Policy.

Michael W. Lowder (USA) is the Principal in Michael W. Lowder & Global Associates, LLC, which is an internationally recognized consulting firm, with expertise in the Critical Transportation Infrastructure Protection & Resilience, Crisis & Emergency Management, Security, Intelligence, Counterterrorism and Business Continuity fields.

Mr. Lowder served as the Director of the Office of Intelligence, Security & Emergency Response (S-60) for the U.S. Department of Transportation. He was a highly respected member of the Senior Executive Service (SES). He was designated as a National Security Professional (NSP) and as a Federal Senior Intelligence Coordinator (FSIC), where he served on the Advisory Board for the Director of National Intelligence (DNI). Mr. Lowder served as a senior advisor to the Secretary of Transportation, and was the Department's Emergency Coordinator, providing leadership for all departmental civil transportation intelligence issues, security policy, and emergency preparedness, response, and recovery activities related to emergencies that affect the viability of the transportation sector. He has also been sought out by senior members of the State Department, National Security

Council and the White House to provide advice and counsel on domestic and international emergency response and critical infrastructure issues.

Mr. Lowder served as the Deputy Director of the Response Division for the Federal Emergency Management Agency (FEMA) in Washington, D.C. Mr. Lowder has been designated and served as both a Principal Federal Official (PFO) and a Federal Coordinating Officer (FCO) on numerous Presidentially declared disaster and National Security Special Events. Mr. Lowder was a senior member of FEMA's National Emergency Response Team (ERT-N), and lead the Domestic Emergency Response Team (DEST).

In 2012 he was awarded the Presidential Rank Award – Distinguished Executive.

Col. Pavlin Raynov (Bulgarian Air Force) COEDAT Transformation Department Head

Ankara, February 21, 2020

Col. Attila CSURGO

Chief of KNOWLEDGE Department

Introduction

"To stay secure, we must look to the future together…. We will continue to increase the resilience of our societies, as well as of our critical infrastructure and our energy security."

London Declaration[2]

The London declaration by Allies Head of States and Government highlighted again two of the "Key Principles" formulated in MC 0472/1[3] such as:

- NATO's Support to Allies;
- Non-Duplication and Complementarity;

However, it is also important the concept has identified "Key Areas" in which the Alliance initiated the enhancement of prevention and resilience to acts of terrorism, including suitable capabilities to address the threat posed by it. Meanwhile, the concept also includes the engagement of partner countries and other international actors.

On the other hand, the resilience is identified as core element of the collective defense and on the globalized and complex world it is and it will remain a concern of the Allies. Resilience is first and foremost a national responsibility and each member country needs to be sufficiently robust and adaptable to support the entire spectrum of crises envisaged by the Alliance.

The principle of resilience is firmly anchored in Article 3 of the Alliance's founding treaty: *"In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."*

Building and maintaining the resilience of every Ally can reduce the vulnerability of NATO just as developing individual national defense not only strengthens the nation but NATO's overall resilience as well. Today many parts of the critical infrastructure is not under the direct lead of governments. Therefore, military forces, especially those deployed during crises and war, heavily depend on the civilian and commercial sectors for transportation, communications, and even basic supplies such as food and water, to fulfil their missions. It is clear now that, military efforts to defend Alliance territory and populations need to be complemented by robust civil preparedness. However, civil capabilities can be vulnerable to disruption and attack in both peacetime and during war, because today's security environment is unpredictable. Threats can come from state and non-state actors, including terrorism and other

[2] Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019. Source: https://www.nato.int/cps/en/natohq/official_texts_171584.htm
[3] NATO's policy guidelines on counter-terrorism. Source: https://www.nato.int/cps/en/natohq/official_texts_87905.htm?

asymmetrical threats, cyber-attacks and hybrid warfare, which blur the lines between conventional and unconventional forms of conflict[4].

In 2016, at the Warsaw Summit, allied leaders committed to enhancing resilience by striving to achieve seven baseline requirements for civil preparedness:

- Assured continuity of government and critical government services: for instance, the ability to make decisions, communicate them and enforce them in a crisis;
- Resilient energy supplies: back-up plans and power grids, internally and across borders;
- Ability to deal effectively with uncontrolled movement of people, and to de-conflict these movements from NATO's military deployments;
- Resilient food and water resources: ensuring these supplies are safe from disruption or sabotage;
- Ability to deal with mass casualties: ensuring that civilian health systems can cope and that sufficient medical supplies are stocked and secure;
- Resilient civil communications systems: ensuring that telecommunications and cyber networks function even under crisis conditions, with sufficient back-up capacity. This requirement was updated in November 2019 by NATO Defense Ministers, who stressed the need for reliable communications systems including 5G, robust options to restore these systems, priority access to national authorities in times of crisis, and the thorough assessments of all risks to communications systems;
- Resilient transport systems: ensuring that NATO forces can move across Alliance territory rapidly and that civilian services can rely on transportation networks, even in a crisis.

It is essential for NATO as well as all individual nations to prepare and develop their capabilities with the private sector in order to have proper and functioning critical services.

NATO conducts crisis management exercises (CMX) to prepare and train for disruptions in critical infrastructure; the last CMX 2019[5] took place between 9 and 15 May 2019 (the 22nd iteration of CMX since 1992). However, it is still a political – military exercise which provide vehicle for leaders on both side to enhance their ability to respond a crisis in a complex and uncertain environment. Although CMX 2019 included external participant like Finland, Sweden and it also incorporated staff-to-staff exchanges with the European External Action Service, the EU Commission and the General Secretariat of the Council of the European Union, the involvement of private companies, owning different part of critical infrastructure has not been integrated.

The COE DAT's Lessons Learned Workshop on "Strengthening the Security and Resilience of NATO and Partner Nation Critical Infrastructure against Terrorist Attacks" was initiated, based on the

[4] NATO: Resilience and Article 3. Source: https://www.nato.int/cps/en/natohq/topics_132722.htm
[5] https://www.nato.int/docu/review/articles/2020/02/07/nato-crisis-management-exercises-preparing-for-the-unknown/index.html?utm_medium=email&utm_campaign=NATO%20Review%20Crisis%20management%20exercises&utm_content=NATO%20Review%20Crisis%20management%20exercises+CID_0e2f2f41beb544ebc232b4aa6bc18093&utm_source=Email%20marketing%20software&utm_term=READ%20MORE

background information provided by experts, who work in the arena of critical infrastructure protection[6] by many decades and COE DAT's internal Lessons Learned Working Group's observations after 2019's CIPATA course.

Ronald S. Bearse

[6] For further information, see the Dramatis Personae of this report.

Welcome Address by COE DAT's Director

Distinguished Guests,

I'm Col Mustafa Özgür Tüten, director of COEDAT since September 2019. As the COEDAT Director let me cordially welcome you all to Ankara, Turkey, on behalf of my staff and I. It is my great pleasure to open our Lessons Learned workshop which supports the COEDAT's Mission "to provide key decision-makers with a comprehensive understanding of terrorism and Counter-Terrorism (CT) challenges, in order to transform NATO and Nations of interest to meet future security challenges."

Many of you travelled long distances to join us here in Ankara, so I would like to thank each of you individually for your support in fulfilling COEDAT's mission.

This NATO Centre of Excellence continues to build its expertise on topics related to Defense Against Terrorism. One of our main goals as a strategic think tank for NATO is to play a leading role in developing concepts and doctrine related to combating terrorism. [7]

The protection of our nations' critical infrastructure is a core requirement by our political leaders who in the recently released London Declaration said: "We will continue to increase the resilience of our societies, as well as of our critical infrastructure and our energy security." Therefore, I do not need to emphasize the importance of this workshop's focus on security and resilience of critical infrastructure. This workshop is also in line with NATO's commitment to provide support to partner nations ability to build their own capability to fight against terrorism by updating our existing course and the potential development of an advanced critical infrastructure protection course.

I officially open the workshop and I give the floor to our distinguished experts.

Thank you all once again, welcome, and I wish you a very successful workshop.

Col Mustafa Özgür Tüten

Director COEDAT

[7] COEDAT supports and contributes to NATO's CT efforts in the fight against terrorism in three main ways:

1. As NATO's Department Head for Alliance CT education and training (E&T), COEDAT is tasked to coordinate, synchronize, and de-conflict the growing quantity of NATO CT E&T on behalf of Alliance members,
2. As a strategic think tank for the development of concepts, doctrine, policy, analysis, and lessons learned to support NATO defense against terrorism activities, and
3. As a NATO Education and Training facility to deliver CT related E&T in response to identified training requirements to Allied and increasingly Partner Nation personnel .

Workshop Day 1, Session 1

(Discussion noted by Rapporteurs)

Col. CSURGO started the workshop by presenting the aim, main questions to answer, NATO CT Policy, and agenda:

1. What is the role of NATO on the field of security and resiliency in terms of protection of critical infrastructure and;
2. Developing and delivering a new advanced critical infrastructure security and resilience against terrorist attacks course.

The main questions to be answered in COE DAT's Lessons Learned Workshop are:

1. What can NATO do better on Security and Resilience to protect Allies' Critical Infrastructure?
2. What are the lessons to be learned in order to increase the resiliency of Allies' Critical Infrastructure?

NATO's policy guidelines on counter-terrorism lay out the principles to which the Alliance adheres. These principles are:

1. Compliance with international law: NATO will continue to act in accordance with international law, the principles of the UN Charter and the Universal Declaration of Human Rights.
2. NATO's support to allies: Individual NATO members have primary responsibility for the protection of their populations and territories against terrorism. NATO can enhance Allies' efforts to prevent, mitigate, respond to, and recover from acts of terrorism.
3. Non-duplication and complementarity: NATO will promote complementarity with and avoid unnecessary duplication of existing efforts by individual nations or other International Organizations.

Moreover, the outcome of this WS may be incorporated in the Military Concept for CT which is under review and re-write in 2020. The Alliance will coordinate and consolidate its counter-terrorism efforts by focusing on three key areas:

1. Awareness: NATO will ensure shared awareness of the terrorist threat and vulnerabilities among Allies. As such, NATO is working to improve information distribution among the Alliance and Partner Nations.
2. Capabilities: NATO will maintain its operational capacity and capitalize on the lessons learned in operations, training, education and exercises based on different threat scenarios will continue to improve interoperability by assimilating lessons learned and best practices. These capabilities may also be offered to Allies in support of civil emergency planning and the protection of critical infrastructure, particularly as it may relate to counter-terrorism, as

requested. Moreover, this is the area where NATO has a role to play in critical infrastructure protection even when the majority of the infrastructure is in the civilian sector - CIP is mostly outsourced by private and civilian companies. Therefore, within nations, they have to have good connection with civilian sector.

3. Engagement: To enhance Allies' security, NATO will engage with partner nations and other international actors in countering terrorism. Particular emphasis will be placed on raising awareness, capacity building, civil-emergency planning, and crisis management in order to respond to specific needs of partner countries and Allied interests.

In terms of NATO's baseline requirements to resilience, there are some principles (NATO's support to Allies) and key areas (capabilities, engagement) to focus on. In 2016, at the Warsaw Summit, Allied leaders committed to enhancing resilience by striving to achieve seven **baseline requirements** for civil preparedness:

1. Assured continuity of government and critical government services;
2. Resilient energy supplies;
3. Ability to deal effectively with uncontrolled movement of people (i.e. refugee and immigration issues);
4. Resilient food and water resources;
5. Ability to deal with mass casualties;
6. Resilient civil communications systems; and
7. Resilient civil transportation systems.

However, these key areas are often outsourced and in the hands of companies, not governments. Within this frame, **what should NATO do?** In terms of awareness, this could be sharing information and knowledge what the Nations know about different terrorist organizations and proxies as well as warn others. In capabilities and engagement sector, what should NATO do strategically?

Prof. Bearse highlighted the progress he has seen over the past six years teaching as part of COEDAT's CIP course in different countries and emphasized how Turkey has developed since 2014 in CIP. The lecturers have watched many countries developing, implementing plans and strategies. Since 2014, the lecturers have been sharing what the European and Western allies primarily have been doing in CIP and sharing their progress as well as allow NATO and Partner Nations to jump-start their CIP programs, while learning lessons along the way. 'We do know the lessons that we learned in the West and NATO has also realized that security and resilience are critical'. With respect to the CIP in terms of terrorism, it is time to move from providing a survey course of what CIP is and what CIP policy is and try to move towards the transformation and implement these things, do some assessments ourselves and talk to senior level people what is happening in different countries. A year ago, after leaving the course, the USA side made an assessment and came to some conclusions. What are the lessons we have really learned? How do we build a new course for senior level people? Not particularly for heads of governments but right below that level, where the responsibility for making big decisions actually lies. It should be a course for those senior people that are implementing policies and

continuing not with an introductory course, but by changing some things done before. As such, part of the CIP that is done in the COE DAT, could be done with a mobile training unit. It is a lot easier to bring people that are familiar in this area and that can lead the transformative discussion of implementation and as such, could be one the fastest way to start this transformational process. 'We want to share what the team has thought in the last six years' worth of effort - our goal here is to take what we have learned and structure these courses'.

Col. Csurgo suggested a way NATO could improve CIP E&T by bringing more senior personnel of nations personnel in order directly provide information to those who are influencing policy development. This could be accomplished during COEDAT in-residence courses and also by dedicated mobile training teams.

Dr. Evans further reiterated that Nations and participants have expressed interest that we should take these courses to them and tailor its specifically to the country's needs. One of the problems is that we have different countries with different CIP needs and capabilities. Some Partner countries are at the very beginning, while others are at a more advanced level. A way to go is to be able to mix and match the subject matter experts and tailor design a mobile course to their needs. This will also ease the burden on staff in the COE DAT in order not to have several mini-courses.

Mr. Baker stressed that rather than coming up with new things, we need to take and recognize good practices - there are a lot of good ideas out there and a lot of countries are already doing good things. However, it is mostly local solutions to local problems rather than trying to superimpose NATO's will. Many countries struggle with food, disease, health and running water - terrorism is often the least of their problems. We need to put it in the context. Mobile teams are a good idea to see things first handedly - **we need to do it with the countries, not to them.**

Mr. Lazari agreed with the need to have tailored courses. Due to the EU enlargement agenda, many new countries prepare for their national framework to be compatible with the EU. There are some strategies that are inspired by the EU's and the USA's experiences in terms of the CIP. However, these countries are often able to install the law but they are not able to progress them further with the implementation because they are missing capabilities. We can let them do it their own way but we need to show them a benchmark because often, below that framework, there is nothing.

Assoc. Prof. Bıçakcı added that the biggest problem that we have in CIP is that most of the facilities are **not run by governments but private companies.** NATO has to make **exercises and focus on the civil-military cooperation.** NATO sees the issue from a military perspective but private companies are 'far away' from governments. They need harmonization between the parties, especially in terms of **strategic communication. Flow of the information** is also an issue. Intelligence gets stuck in the governments due to security issues, and do not reach companies. We need to build a risk system which passes the information to relevant private companies. On the NATO level, we need a manual of the

civil critical information protection by explaining the main issues. Centre of Excellence of Cyber Security has published a similar thing - what do governments and private sector do, how do security policies have to be regulated, how the law enforcement and private companies have to be harmonized. Also, NATO should do **cyber intelligence** because they have the capabilities. Most energy attacks in recent years have been done on cyber weapon level (Saudi Arabia, Ukraine) - NATO has to form an understanding on this. NATO could focus on SCADA, CERT and cyber physical systems for computer emergency teams. Many countries do not have experience in this but this is relevant for us. **Decision-making ambiguity** is also an issue – we could create simulations of such exercises or see how we could make decisions under ambiguity. We can also capture the **flag exercises** - this could also be motivation for workers in the CIP sector as well as doing yearly meetings of best practices in regard to CIP with different sectors and partners. This could also be done online.

Prof. Bearse added that the transformation NATO is talking about is now civil-military fully. We have to bring people together with governments and work on this, i.e. have a roadmap or a type of plan what to give, but the worry is how long it may take for NATO to process this. We need to **publicize more** that CI can be disrupted by almost anything, not just terrorist attacks. NATO has made some announcements on highest level, but we need to step up a little bit more. Mr. Baker stressed that many of the industries in different Nations are already regulated, i.e. aviation sector and that is how states fulfill their treaties. 'Form follows function' - we need to work out what we want to achieve first, what are its functions. For instance, in-country teams, regional workshops or workshops held in the COE DAT or targeting specific countries? It always starts from threats – you look at the risks and vulnerabilities and try to work it out. What do you want the function of the COE DAT to be? This is what it is supposed to do, then we can work how this is best achieved.

Col. Csurgo added that for him, CIP is a CT issue. Within NATO there is no doctrine for the fight against terrorism - CIP is heavily regulated and NATO does not need to interfere or create a new NATO doctrine in regard to CI. However, **there is a need to collect best practices** and this could be a guideline for other Nations how to deal with such issues. We should think of a handbook that could be useful for Partner nations, for instance what are the thoughts of academicians and practitioners rather than creating a NATO doctrine.

Energy and water is a very conservative sector - they do not like change and new technology. We should be talking to the Chief Executive Officer (CEO) of the Chief Compliance Officer (CCO) because 'this guy will be on your side'. That person will introduce whatever you say and put every single regulation there. However, every single manager of every single plant will normally say 'that it is not in my budget'. Most of the energy companies already have their HQs in Europe and most of the energy comes outside of NATO countries - we also **need to address issues that are outside of NATO.** Key threat can come from Mali or Nigeria, for instance. We need to be able to explain issues to people - it is not NATO who deals with the supply of oil and gas. It is not an army but another organizational structure where a manager of a refinery, country or a company can block the delivery because he will

only think of his own budget. How will we address this issue, because this is not an army, the issue is much more difficult? NATO is already worried about integrating our systems but in oil and gas operations, see how many third parties are involved in cyber, for instance. It is way more difficult than inside of an army and these are the issues that NATO should be addressing, because it happens all over the world and is affecting us. In most of the world, you need to address water security and infrastructure because there is no oil without water.

Col Csurgo stated that it could be an issue to target those countries under the flag of NATO and therefore, we have to mention to them the need to train emergency units with civilian companies involved in different sectors, like energy and transport. They should not be thinking that NATO is trying to interfere in their life but NATO wants to help them because in such situations, they may need military help if something collapses. Targeting the nations and providing them with on-site training could be useful because experts that go to these countries can learn in advance in which stage the country is in CIP (i.e. advanced or beginning) and they can focus accordingly. Experts are agreed, the NATO flag can give the right to talk about this issue on-site.

Mr. Baker added that we should also focus on CIP overseas, not just within NATO. There is a role for the COE DAT in developing a **security culture.** But in the nuclear world, the part of security culture is getting senior leaders to believe that a credible threat exists. Half of the problem is that when you go to these countries, terrorism may not be part of their radar at the time but it might be in the future. As such, COEDAT's role could be thinking outside of the box and understanding other developing nations and the role they would play in the future as well as see the investment in terms of 'secure by design'. Let's get the message out there ahead of bad news arriving on their shores, not wait until something happens. We need to get people to understand the security culture and COE DAT can play a role in this.

Mr. Lowder emphasized that we cannot lose sight of a bigger picture - we talk about security and resilience around CI but **not all threats come from terrorism.** We need to go back to the basics - what do we need protection against? How can we make our infrastructure more resilient and more secure against everything, which would also include terrorism but not limit it to terrorism? There are other **natural hazards**, accidents that can be just as devastating to countries and their economies as terrorist attacks. **We cannot solely focus on terrorism.** That is where the transformation will come even more apparent when we look at the broader picture - what are the threats out there? If we can make our infrastructure more resilient overall, then it will be more secure from a terrorist attack as well from as other things. We should synchronize and harmonize all efforts to work together and address all threats. Col. Tüten agreed that we need to think in a more comprehensive way, not only from the army's perspective. It is not only terrorism, but also other issues that we need to focus on.

Col. Raynov questioned, **what is critical?** When almost everything is critical; nothing is critical. When it comes to threat, it is better to assess what is critical in terms of the threat and time for reaction, not in

terms of the country. It may be better for NATO to focus on single countries or proper response to single threats in terms of CI.

Mr. Lazari added that we cannot interfere with a nation's CIP. Security is about national sovereignty but NATO has a voice and role to play. NATO needs to assess threats and governments can assess if they are impacted. NATO can also add complexity. In today's world, there are new threats with asymmetric and unconventional tactics. We have to find a balanced way to convey messages that are good for civil servants, military personnel and IP officers, the ones that are in charge. They will understand according to their areas where they can intervene and show them case studies to analyze better the measures, planning etc. What can the government do? We can show the operators how this is done - they pursue the law of business and 6 are privately owned. **Preventing is better than recovering or rebuilding.** Indeed, we have to focus on also natural events, not just terrorism. It is also about earthquakes, i.e. in Albania and Turkey, not just a terrorist with a weapon who is a threat. We should focus on **case studies**, in which we can convey messages to certain people, i.e. explain why something went wrong in real cases.

Mr. Lowder agreed that using case studies makes it from hypothetical into reality. It conveys a message of what could have happened, what went right or wrong, what could have been done differently. Mr. Baker added that the COE DAT could help assist nations develop national risk assessments. Link between security and resilience is fine, this will develop capability requirements.

Dr. Evans added that risk assessment is complicated. Often, people who come to the courses are introduced to risk assessment for the first time, it is an area that must be expanded. In a graduate course, we need much **more detailed risk assessment and risk management -** risk is really important.

Workshop Day 1, Session 2

(Discussion noted by Rapporteurs)

The second session started with the following questions:

Where should NATO interfere in the CIP sector and what could NATO do in regard to common exercises with civilian governments and industry?

- What should COE DAT do?
- How to reform COEDAT's CIP course?
- What should COEDAT be teaching and what to communicate to senior leaders?
- Who is it for, what are the key components, what will COEDAT say?
- Does the course that COEDAT has taught for the past six (6) years need to change?

Mr. Lowder pointed out that the existing course is important and as an introductory course, it helps people to understand why CI is important, why we need to protect it, and goes back to the basics. However, the exercise for the current course is quite high level and involves multinational, cross-border, political issues that many people may not be familiar with - we should re-focus that. That level exercise would be very good for an advanced course. It is important to help the senior leaders to understand that CIP has to be risk based and is something that the implications for not doing it, will have consequences for their economy, country and business. If you lose a portion of your CI, what is the ripple effect? We have to make sure that they have a clear understanding of the risk and what are the implications of that risk. We have to get to the policy people, people who can and will have to make decisions that will affect the broader level of industry, company or a government. If we want to affect the cultural change and build resilience, it has to come through the top, it has to be driven down.

The participants further agreed that inviting Vice Presidents, Senior Vice Presidents in private sector on a high level could be a way forward.

Mr. Baker added that we should also go wider and talk to policymakers and local authorities who would start writing national policies or strategies.

Assoc. Prof. Bıçakcı added that in such high level events with high level people, they may be kept concentrated only for about two to three hours. You have to **give them something new and exciting,** otherwise they will neither focus nor come.

Mr. Baker added, NATO could think of doing something at the beginning of a session of where these people go anyway (i.e. another conference), why not going and targeting businesses as you want, where certain companies' divisions come together? CI is not an amorphous entity - it is about telecoms, transport, health, emergency services. NATO may want to do a more focused effort - **take the product to them.**

How do we target these countries?

Col. Raynov suggested that we can stay focused on single countries who need these exercises, senior level may be too ambitious. **We could use the NATO CMX exercise that involves governments of NATO countries and involves interaction of national institutions.** We can involve the private companies' leaders in this exercise, however as a first step should be to invite them for the Distinguished Visitors Day (DVD) of the exercise. The important thing is not the numbers of participants but it is more about who is there. Experts agreed that it is essential to keep these leaders focused with added value for them. Let's think that we are presenting the participants in the East Mediterranean Security problem, for instance - how to protect CI? First it is NATO, secondly national interest.

Dr. Evans highlighted that we may be stuck on the risks of repeating the discussion of what are the threats. However, for the advanced course the focus has to be **giving people the actual tools of how they will protect the CI** (threat based, understanding, impacts). It should be more focused on crisis response management and be very 'nitty-gritty' and have real time solutions. Dr. Evans pointed out that she and her team are responsible for the CIP of Pentagon and other facilities that Pentagon manages - we have a lot of expertise in the National laboratories that are used in exercises. We should be showcasing some of the tools that are out there, whether corporate based or government laboratories and focus on the means that we can share that capability is very important - that is why we have to **go back to the tools.**

Col. Csurgo reiterated that the COE DAT still has a mission and a vision to fulfill as well as satisfy the eight Nations who are sponsoring the subject matter. When you have a basic course, of course, captains and majors are not right now policy makers of their countries but many of us were majors once. This is the right time to start teaching them. Perhaps majors from Gambia, Zambia and Burkina Faso will be policy makers in about 10 years later and can make an impact. We should separate how we want to influence high leaders and **use tools what NATO can provide us.** That is why we started our workshop as what NATO should do, and what the COE DAT should do. Therefore, we should keep the basic course, renew it and then do an advanced course for people who are getting closer to influencing their countries and use the seminar tools that Brussels or Norfolk could provide us and interfere only for couple of hours and deliver them the key messages. To keep the basic and the advanced course in our facilities that the participants can think they were thought once they become the decision-makers. **We should separate the issue and keep, in the COE DAT the focus on junior ranks in order to start their education on Critical Infrastructure (CI) as early as possible.**

The participants reiterated that the basic course should be here but the question is what could be the tool to address the advanced level course.

Mr. Baker highlighted that we should not be over ambitious. You have the NATO brand and your own departmental missions. In time, you could start partnering with companies, depending who the audience is. When we talk about the future leaders, you want to pilot this project and you already have the alumni who have been through the foundation course. Perhaps, for the more strategic course, it is for those 'high fliers' that have been through the alumni and this gives a variety of career pathway or academic pathway and revisit the people who already came here before. You can also invite the most active people from the foundational course later to the strategic course.

Prof. Bearse added that although the participants of the future course have to understand what the CIP/CISR is, we have to talk to the people who do not have the capabilities for the CIP. We have to talk not what it is about, but the transformative side.

Workshop Day 1, Session 3

(Discussion noted by Rapporteurs)

The third session focused on what the **content** of the upcoming advanced course should be.

Mr. Lazari pointed out that the course should be interactive and make people focus, this could be made as a roundtable. If the people in the course are CEOs and decision-makers, you need to present in an appropriate manner, i.e. have an operations room and work through crisis. Mr. Baker emphasized that there are other ways to be interactive. Counter-terrorism also needs to evolve because terrorism evolves - the bad people know what we are going to do and how we will react. We need to embrace more **diverse thinking** how to tackle terrorism - each terrorist strategy is different. What is NATO's response? What is the outcome? The content is mutually inclusive, it is very hard to protect CI and it may be easy for the terrorists to attack. A lot of our infrastructure is by design to be open and is there to serve people.

Prof. Bearse added that we have to be clear of what we want and try to find people who are engaged in CIP and that need some help from us and to implement some component of those courses. The goal would be a demonstrable CIP course. Mr. Baker questioned how do we know that they need help? We have to empower them and stop saying what they need to do but give them rules of the games. Mr. Lowder agreed - **local problems need local solutions.** Col. Raynov highlighted that it may be good to run a course or a training that would be solution based. It could be a one course with one nation and then a seminar that comprises the results, i.e. what we have achieved from different nations. When we mix people from different nations, they have different approaches. The training has to be based on a scenario and all participants could discuss what could be done, have one role or be in teams in different institutions. Dr. Evans agreed but where do you get the cross-sharing of lessons learned between different countries? Sometimes in a country, they do not know that they do not know. There are some setbacks to one-country focus - how do we bring that lessons learned in a whole of community issue? Perhaps, when they go back to their countries they can start implementing this.

Why is the content important at the first place? The tools are important – **strategic communication, crisis response, crisis management, threat intelligence.** In terms of mapping out their infrastructure, you really want some planning tools so that you are doing that risk assessment and figuring out where those resources need to be.

Mr. Lowder emphasized the need for a **case study** and go through things that have happened in reality. To give them some exercise and a problem to solve, get them engaged and find a solution. What other people have looked at and have them solve it, i.e. say that 'here is what they did and this is how they did it' or say it was a total failure. Helping them to see what has happened through a case study and let them know what are some of the landmarks, what kind of political things they need to think about. Most people do not do it every day.

Dr. Evans pointed out that **communication is the key;** the **importance of information sharing and intelligence**, i.e. ISAC[8] centers concept within the USA that is meant for both private and public partnerships - it is a tool of how we flow information between public/private partnerships.

Mr. Lazari shared his experience over summer schools and the content. It is important for people to understand the critical infrastructure complex into the role supply chain. Let them understand what the time scales are between planning, designing and reacting to things. There was also a night session within the summer school where people discussed catastrophic scenarios.

Assoc. Prof. Bıçakcı added that the biggest problem is leveling because some audience come here to learn something, but often have no idea what we are talking about - it may be the first place where they hear these terms, i.e. risk management. We are touching it, but not going into details like in the literature. Either we have to have an assessment after the course to see what they have learned or have an assessment prior to the course as a sort of a test to see the level of the people. We have to be separating things - health, finance, cyber. Transportation and telecommunications, for instance, have different expectations. Even health is infrastructure, it is also relevant to cyber and other sectors. We can make separate courses, but this may be costlier. We can also have two different tracks divided into two days that people would follow to have a multidisciplinary approach.

Col. Csurgo added that there are different Centre of Excellences of NATO and we could cooperate with them, i.e. in health because these centers already know who the experts are. We can include others, not always worry of the financial aspect. Prof. Bearse stressed that if we will target senior level people and have 20 people come from health/medical/financial services but when we are thinking about the strategic part of the Critical Infrastructure Security and Resilience (CISR), we are teaching the basic building blocks in ways that we can articulate the senior people and let them do the critical thinking. Give them examples from particular things but it is more generic, rather than specific.

The discussion shifted to the tools to be used as well as continuing to discuss course content.

Mr. Baker reiterated on the need of **self-assessment** - how do you know that you do well? Where are we - how do we do it? This should be outcome based - how to put trust into the CFO/CEO[9] because we also teach them self-assessment, it should be evidence based.

[8] An **Information Sharing and Analysis Center** or **(ISAC)** is a nonprofit organization that provides a central resource for gathering information on cyber threats to critical infrastructure and providing two-way sharing of information between the private and public sector.

[9] Within the corporate office or corporate center of a company, some companies have a chairman and chief executive officer (CEO) as the top-ranking executive, while the number two is the president and chief operating officer (COO); other companies have a president and CEO but no official deputy. Typically, senior managers are "higher" than vice presidents, although many times a senior officer may also hold a vice president title, such as executive vice president and chief financial officer (CFO).

Dr. Evans reiterated that a good **exercise** is important - we could give great marketing advice for mobile teams.

Col. Tüten questioned the protection measures - does NATO or any NATO body have such a website/meeting point to merge the cyber security threats, cyber security measures/lessons/samples identified and the same thing for CIP? We have to merge CIP and cyber security protection in a hub (i.e. COE DAT) or an institution and correlates all the data/analysis/exhibits the outputs to all NATO command and force structure.

Dr. Evans emphasized that there is not such a body in NATO but there is in the Department of Defense (Mission Assurance), it is a policy by directive – every service must comply and develop a mission assurance program as well as all of our agencies are required by the DoD law to do that. Now, you do assessments combining concerns about physical force protection with the cyber component. There are actual teams that go out who do risk assessment not about the facility but the mission essential functions - it is no longer about assets but about what is the function you are trying to protect. However, the content usually is not shared, nor on the websites of companies, excluding the information about the vulnerabilities.

Mr. Lazari pointed out that from his own experience, they look at how liquid goes back into gas and pump to the national grid. 'We take the availability of gas and split it into sub-processes'. From the moment the ship goes back to the terminal, there is an instrumentalization of maneuvering to make sure that the ship goes close to the terminal without damages. Then there are hooks that keep the ship close to the terminal, unload arm, and stock the tank. All of these services, we go through and inspect that the storage tank has no leakage/damages. **The new paradigm of cyber security is to look where we have to cyber secure something in the room**. We start from making sure the ship does not hit the terminal until delivering gas to another operator (National Transmission operator). This is done with risk analysis that is tailored. Is this program using programmable computer in coupled with other sensor - yes. Then we apply what is needed to secure that. What is it that can arm cyber architecture? Can they go manual - we consider all. **We still consider that everything can be managed manually** - certain things are still simplified.

Prof. Bearse added that CIP in the modern age is related to a cyber-security threat - there is a physical and a cyber-side. Now, **the lesson learned is that we can show them how focus on the function rather than the asset**. It emphasized that the industry is still focused on the plant level and saying that 'I am protecting my asset'. However, **if one asset is not working, it affects all**. There are new agencies built in the West but cyber security and any other assessment goes hand in hand of what is going on - there is that cohesion.

Col. Tüten emphasized that NATO is moving very slowly in these areas, but the adversary is not - they are quick, efficient and are really harming us. If we say we are NATO, we have Istanbul Initiative,

Partnership for Peace, Global Partnership, Mediterranean Dialogue - we have the responsibility to at least warn them and this center could be a hub for it.

Col. Csurgo added that we use references from NATO documents, it would be good if we can add some that we can use and are available openly that we could deliver to partner nations also. This would help us to prepare content better than it is now. The MC 472/1 is still under revision. Hopefully we can include our Lessons Learned WS result to the new Military Concept next year. The participants reiterated that a lot of CI sits in the private sector, the references should include international standards, good practices - bridging the gap between the business world and military doctrine. **Assess the function is very important.** Instead of protecting assets, the functions, interoperability and sustainment matter.

Prof. Bearse highlighted the progress made in the last course and the focus was on the security resilience, we started asking what CIP, risk assessments - getting it right is. The whole of community approach is important - local solutions to local problems. Changing the course name to include resilience is one thing but where do we need to provide some extra input?

Mr. Baker highlighted that you can never reduce risk to zero. The idea of resilience was born out from the state having the responsibility to counter the terrorist threat but the state cannot do it alone - it has to gain support from private and public sector. Now, service providers have legal responsibilities. Resilience building is important; the private sector has a role to play. It is not just terrorism but other hazard to focus on. During the floods, the electrical companies make a handsome profit. How does the military/NATO become more resilient? What if you cannot protect or you choose not to because the costs are high? Can you become more resilient by having distributed network of power stations?

Prof. Bearse highlighted that the course usually starts off with the keynote and explaining the state of CI in the world, what is going on within NATO/EU and partners. Now we are talking about merging security resilience, we should tell what the COE DAT is telling you and NATO statements now in CI. Then we talk about **risks, sectors, transformation, essence of the key elements of CI, case studies, table talk.**

According to Dr. Evans, a lot of time has been descriptively being spent on threats to sectors without case study analysis. **Analysis has to be done with a case study framework** rather than descriptive presentations what the threats to CI is - it must be focused. We did that for five days and the value added is 0. The water sector has never been touched and we could use this. We have never done a good job right up front in explaining what NATO's role is in this. **Why this issue is important for NATO?** Last time was the first time this was done. There is a marriage between the EU and NATO - where are the vulnerabilities, where is the convergence? How is that being shaped? The participants agreed to approach the industry and business, have both NATO and business angle. Then, go back to

tools - how is the information shared? Are there more tools to bring to the toolkit? However, people may not be prepared to do an exercise in right positions and use that time to do other things.

Col. Raynov pointed out that CIP is NATO's job. It is governmental assessment what is critical for governments not for businesses. Maybe NATO looks at CIP as protection of spots on the ground, nothing else.

Mr. Lazari reiterated the importance of including of natural events that are still predictable but having influence on CI. We cannot go into earthquake scenarios because they are unpredictable. Under certain circumstances, certain CI and certain countries can be more vulnerable therefore may receive another attack on top those.

Dr. Evans added that the feedback of this presentation was strong because it was very operational and had clear examples of where the infrastructure has been affected and how are adversaries deliberately weaponizing CI to attack us. That clear message needs to run throughout the course to keep the attention. Dr. Evans further reiterated that she wants to avoid description from the first course for it to be more impactful, i.e. have climate change and this brings it more contemporary. **Climate change** affects NATO basing - this would pull the military together. We need more military participants in this course.

Mr. Baker agreed to have the emphasis on the **role of NATO.** A lot of people would look at pure statistics of terrorist attacks but one of the difficulties is that there are simply not enough terrorist attacks for people to do trainings etc. But there are lots of examples - national security is important. If you are a developing nation you may be mistaken think that CIP is all about guns, cars and gates - it is about maintaining and growing a prosperity of a nation or a group of nations, it is about cooperation and interoperability. The main question is, why is CIP important for NATO? Civil-military cooperation is important. Who was it who went to recover 6 dead bodies in New Zealand - it was the military. Military is also helping with flooding. It plays nicely into the role of military in supporting the civil power. Military is playing an assisting role. **What about the CI as part of the military industrial complex?** What does it take for the military to fight a war from a critical infrastructure perspective? CI allows the military to fight a war and also the military is part of CI as well as own CI. Current President Trump administration has a presidential directive that is examining the defense industrial bases and have a major report. In the intelligence world, we have done a classified assessment of different vulnerabilities to map it out and understand where Chinese investments are, looking from a global supply chain. Experts agreed that there needs to be some extra focus on ports and Chinese (third party) investments in CI. **Human factor** (relations) and inside actors need to be focused on. These are issues in the army but also within companies. There is a blurred line of pointing out who a terrorist is in a group. Also, **global warming and climate change** should be in the course. Climate change will also change the role of NATO in the future - it will destabilize a lot of countries in the future. Climate change is an issue and it is also an issue outside of the NATO that will affect the NATO itself. The

course issues are mostly focused on inside of NATO, but NATO is getting more involved in protecting CI outside of NATO and this will increase. Also, natural disasters in India or South Africa, if we will help them as NATO, we are already involved. These issues need to be taken into account. In the course, take an example of every sector from recent events within past months or last year and work that out - it always will involve what is an issue.

Prof. Bearse pointed out that if NATO would do things in a perfect world, what we are talking about would be taking place in a civil-emergency planning committee. When you ask people there, what they do in CIP, they tell you what they do in Crisis Planning and Respond - it is not what we are doing and that is why the role in NATO in CIP it was just clarified for the most part a month ago. They are now committed to doing something and moving towards resilience - they have collectively agreed on it in the London Summit. Before that, there was no clear answer. If they are not doing it, and we are the only group doing it, then what are we missing here. We have to be involved with civil emergency planning and involve the civil part, i.e. companies who own the transportation and communications to understand that when we have interruption in the communications line, who will be in charge - the Chief CIS of the armed forces or the CEO of the company or someone from the government side? This needs to be practiced, then we at least know who will be in charge if something happens. When we talk about resilience, we are talking about **exercising together** whoever needs to be involved, both civil and military sector.

Key Points from Day 1

- Importance of deploying **mobile training units** that are tailored to the country's needs and capabilities.
- NATO should work **with** the countries and not dictate to them; NATO should work by, with, and through the countries.
- There is a need for **better information sharing** and better civil-military cooperation. This also needs to be extended with private companies.
- NATO should also focus on the issues **outside of NATO**, not just inside. Partner Nations needs and requirements must be addressed.
- NATO needs to **publicize more** on CIP issues.
- NATO should look at the bigger picture, **not solely focus on terrorism (need to take natural hazards into consideration).**
- Training and education events should **include case studies** and real life lessons learned.
- Need to focus on **global warming and climate change** in the training and education events.
- NATO should practice and conduct **exercises together with both the civil and military sector.**

Workshop Day 2

(Discussion noted by Rapporteurs)

"As the inability to provide absolute protection to all types of national critical infrastructure has been observed until the mid-2000s, the focus on the protection of critical infrastructure needed to adapt a perspective based on resiliency."

Ronald Sanford BEARSE[10]

What is our national critical infrastructure focus?

Professor Ronald Bearse touched upon some relevant takeaways from the day before:

1. Sharing of information with partners and governments, and letting them know about what's going on is essential to switch the focus from international level to national one.
2. Importance of the ISAC concept and strategic communication has been highlighted.
3. The use of case studies in the scope of risk analysis and risk management needs to be encouraged.
4. In terms of the national level of critical infrastructure protection, the importance of self-assessment which needs to be prepared independently from other countries' approaches has been raised by Prof. Bearse, Dr. Evans, and Mr. Baker.

Regarding the risk-assessment, what Col. Csurgo proposed is to prepare a check list for countries to **identify what critical infrastructure in fact is for them in the first place.** As a guidance, analytical tools can be given to the countries to conduct their own risk-assessment for critical infrastructure.

Within this scope, Mr. Lazari touched on the definition of criticality of assessment as almost 80% of the assets prove to be critical at the end of the day.

Col. Csurgo suggested that when countries identify their critical infrastructure and prepare risk assessment there is a floor under the NATO flag **to provide training and education focusing on exactly what they need rather than what other authorities think they need**.

Dr. Evans suggested that this has been depicted as a transformational agenda for NATO.

In addition to that, Col. Raynov raised a comment on that the country itself has to recognize the need for such kind of an activity and analysis before it is organized for them. The request must come from them instead of imposing what others think they need which addresses the first point of this workshop, the role of NATO on the field of security and resiliency in terms of protection of critical infrastructure.

[10] Principal Consultant - NAUSET National Security Group and Adjunct Professor at the Massachusetts Maritime Academy.

It has been discussed that prevention and protection is what has been desired, yet it is impossible to protect everything in today's world as we witness the complexity of threats. **That's why resilience is gaining importance over protection, when threat comes we have to be prepared to get through it**.

Mr. Lazari pointed out that resilience is in fact the result of business continuity, and by retitling the course in that particular way actually means that we are embracing this concept.

Mr. Lowder added into that renaming and refocusing these courses bring out **transformation and we are looking at things from a new perspective**. We are transforming the whole process for basic course as well as the executive level course.

On this approach, Prof. Bearse raised that transformation is on the scene because critical infrastructure comes out as a **global commodity** where countries and corporations involved in a cross-border level which, therefore, needs to be protected and made resilient.

Dr. Evans suggested that it is doable by starting a process to work with the **EU hybrid warfare** where NATO can work through an exercise. Energy can be given as an example of **tabletop exercise** working with private sector, all of the key nations, and private sector entities to focus on key vulnerabilities. She added that stage approach can be taken and that would be a separate effort which COEDAT has adequate resources for that. It is to highlight that this advice refers to the role of NATO on the field of security and resiliency as we go through it from what it is to what it should be.

Mr. Lazari emphasized the significance of **case studies** in teaching and modelling other nations to identify their own critical infrastructure and risk-assessment. By going through case studies and relevant experiences other countries have already involved in, countries can connect the dots in their own dimension. As one size would not fit all, they will start to see it from their own dimension and will possibly upgrade their certain procedures.

Col. Raynov questioned the effectiveness of the variety in education and training for other countries. As it goes in many different directions it in fact hardens the process to come up with practical solutions. Hence, it needs to be kept as simple as possible in the very beginning.

Mr. Baker raised that when it comes to capability and capacity building, what proves significant is not what it is done, but how it is done. The audiences may get tired of listening to recommendations on what to do. At this point, it is vital to show them how to make them real and put into practice, in other words by which means these are supposed to be effective.

Prof. Bearse addressed the question of what makes a transition referring to the key points for restructuring the current course.

Dr. Evans commented that the terrorist threat comes from **kinetic, cyber, climate, and hybrid**. These are the areas that must be covered. According to her, it is better to start with kinetic, cyber, and hybrid, and climate comes as the last one. Addressing it as climate rather than climate change is better because it incorporates both the changes occurring and natural disasters.

Prof. Bearse summarized **the overarching concepts as energy, communication, water, and transportation**. He highlighted the earlier discussion on what the required capacities are.

Dr. Evans reminded the audiences of **the importance of tools that need to be provided with and further improved for information sharing, crisis response, and crisis management**. It is also important to allocate some time to consider if there is any missing tool that needs to be provided.

Mr. Baker emphasized horizon scanning; we should not constrain ourselves by just looking at past case studies; we need to look at future threats because this is what resilience is all about.

Mr. Lazari talked about **"Sectorial Resilience Plan"** which is in the UK and publicly available for anyone to see. In the plans, they are basically saying that these are the challenges we are currently facing, yet we do have targeted plans for them. Particularly **banking and finance, electricity, and communication sectors** become prominent for the government. This might be a consideration for the advanced level course on critical infrastructure security and resilience.

Col. Csurgo mentioned the need for **references**. It is to say that NATO does not need to produce doctrines for everything. For the basic courses, there are certain sources available for everybody but those need to be read and analyzed.

In addition to that, Dr. Evans pointed out it would be transformational to **use a website** for critical infrastructure protection and have relevant links there for those who both take the course and are interested in the topic.

Col. Tüten also raised that there might be **the creation of a platform** where participants can scrutinize all the documents and presentations before the courses begin. Col. Tüten pointed out that even if some of the participants are of junior ranks, they might become the head of important departments of critical infrastructure protection in the future.

Prof. Bearse asked how COEDAT selects, develops, organizes, and conducts mobile education and training with partner nations.

In 2019, COEDAT conducted five mobile education and training team courses focused on CT in the Middle East and North Africa. The five courses were focused on four individual nations (Morocco, Algeria, Jordan, and Kuwait) and one regional organization (African union). The nations/organizations

were nominated by either NATO Joint Force Command-Naples (responsible for the Middle East and North African region) and/or NATO HQ International Staff Emerging Security Challenges Division section. Significant challenges for COEDAT faced in regard to mobile training teams were: lack of NATO common funding, lack of defined requirements from the requesting nations/organization, and the lack of direct lines of communication with the requesting nation to define requirements and coordinate the activities. COEDAT funded three of the mobile education teams through funds received by the eight nations that comprise COEDAT and with the approval of the eight nations. The funds were authorized only for 2019 in order to accomplish the objectives in support of NATO's strategic look to the South and to provide NATO force structure to secure NATO funding for future mobile training teams in support of Alliance missions. The remaining two were funded through grants by NATO's Science for Peace and Security.

Mr. Lowder highlighted an important aspect of countries sending a request to NATO in need of improvement in critical infrastructure protection. It is possible that **they do not actually know what to ask for and where to start,** therefore they may end up not asking at all.

Concluding Remarks

Col. Tüten praised **the participation of the scholars in this subject** by raising that soldiers are not keen on details and they sometimes cannot go beyond three dimensions. For this subject, forth and even fifth dimension may be needed which academicians can very well provide by going deeply.

Col. Csurgo listed what has been agreed on with respect to retitle and reshape the content of the current COEDAT's "Critical Infrastructure Protection against Terrorist Attacks" course as the "Critical Infrastructure Security and Resilience against Terrorist Attacks". For this year, due to the fact that everything has been settled and approved for the course, the course will be kept as it is. However, based on the recommendations during the workshop there is this possibility to modify the course content and teaching point. As well as the basic course, it is agreed to have an advanced level course and use the executive level seminar targeting the high representatives of different countries to advertise the capabilities of COEDAT and bring their very attention to critical infrastructure and what can be done for them in the future. For that, it is agreed that getting the NATO approval is a must in order to show the capabilities of COEDAT outside of the NATO borders as well as within. As the specific topics of the upcoming executive level seminar of 2020 are yet to be determined, critical infrastructure can be added into agenda.

Director of COE DAT, Col. Tüten has come to an end by reminding the experts of the **significance of combined education teams and a proposal draft with regard to that**. Once again, COEDAT as an education and training facility does not lack equipment, capacity, or budget. **What is highly needed is qualified man-power** and this will be surely overcome in the upcoming period of COEDAT's works, activities, and education and training programs.

As the last words, Mr. Lowder expressed how important to hold such a workshop by COEDAT consisting of different experts for the efficiency and effectiveness critical infrastructure protection studies.

Observation

Overall observations:

1. The concept of CIP has matured to the point where it is now more commonly referred to as Critical Infrastructure Security and Resilience (CISR), due to the inability to provide absolute protection to all identified national critical infrastructure from all possible threats.
2. NATO understands this change because "resilience" is one of NATO's seven key competencies. Although, protection of national critical infrastructure is primarily individual Ally's responsibility, protecting key global critical infrastructure is a strategic security concern and challenge which needs a comprehensive approach.
3. Crisis Management Exercise (CMX) is a tool for political and military leaders to prepare for potential disruptions in CI, within and in some cases outside of the NATO boundaries. Most critical infrastructure is owned by private companies.
4. The goals of the senior political and military leaders is to build a robust and resilient critical infrastructure in order to protect and provide essential services without significant interruption to their citizens. Private companies main goal is profit and in case of emergency to reduce losses which means protecting their assets rather than the function of a critical service.
5. Nations to strengthen their security and build a resilient critical infrastructure without direct involvement of the private sector is almost impossible.
6. NATO partner nations are also building their capabilities and developing their security plans in terms of critical infrastructure. Considering that global critical infrastructure (e. g. global transportation chain, energy supply chain) is a strategic security concern, NATO needs to provide, up to date training and education for its partners.

Observations for COE DAT:

1. The current Critical Infrastructure Protection Against Terrorist Attacks (CIPATA) course is providing basic knowledge for participants. The current security environment contains a broad and evolving set of challenges to the security of NATO's territory, infrastructure, and populations which necessitates the continuing need to for COEDAT to offer CIPATA education.
2. In the last decade, the concept of protection of critical infrastructure has changed to security and resilience of critical infrastructure. COE DAT needs to develop an advance course to provide further education on the concept and practices of critical infrastructure security and resilience (CISR) beyond the basics to aid Alliance and Partner Nations develop their own security and resilience plans for critical infrastructure.
3. COE DAT needs to find other means/forum to deliver education to decision makers and practitioners who actually manage and directly work on CIP/CISR plans, policies, procedures and related activities.
4. There is a need to collect information case studies and best practices CISR, in order to provide solid and standardized platform for training and education.

Discussion

COEDAT's prescient decision to develop and deliver the CIPATA course has produced real, measurable change: within the minds of the over 400 students who have attended the CIP course over the last six years and change within the nations and organizations these students represented. COEDAT's investment in CIP education is essential to building national and economic security across the Alliance and Partner Nations and also to improving industry efficiency, connectivity, and growth; all of which help these nations improve public confidence in governance. COEDAT's continued investment in developing and delivering state-of-the-art CIP education is just as important tomorrow as it has been for the last six years because the threat to critical infrastructure is evolving and likely to increase in the years ahead. COEDAT continues placing a premium on raising awareness of the growing threat; sharing valuable lessons learned in building and maintaining demonstrable CIP capabilities; and providing concrete steps to secure NATO and Partner Nation critical infrastructure. COEDAT's CIPATA course serves NATO and Partner Nations long-term interests in supporting the development of essential capabilities for preventing, preparing for, responding to, mitigating the consequences of, and recovering from a terrorist threats and/or attacks which could easily threaten the proper functioning of critical infrastructure. The recent CIPATA course, with the involvement of experts on different field of CI was able to successfully:

- Expose students to the essential elements of modern national CIP policy and planning;
- Discuss how CIP supports national and economic security, as well as economic prosperity;
- Focus particularly on protecting critical energy (i.e., gas and oil pipelines, nuclear power and electrical power grid) and transportation infrastructures;
- Increase student knowledge and understanding of current and emerging issues, concerns and challenges in developing and implementing national CIP policy and plans;
- Identify the roles and responsibilities of government, the private sector, and non-government organizations (NGOs), international organizations and others in protecting critical infrastructure from the hazards they face, including terrorist attacks;
- Emphasize the need for clear and unambiguous methods for defining risk terms and risk methodologies for use in protecting critical infrastructure against terrorist attacks, and assessing the resilience of these assets;
- Provide students with concepts, methods and tools they can use to improve the security and resilience of critical infrastructures in their nations;
- Identify the need for public-private partnerships and information sharing mechanisms for protecting critical infrastructure; and
- Conduct an immersive practicum that enabled students to apply what they learned during the course in a tabletop exercise simulating terrorist threats and attacks against critical energy infrastructure.

With the course's conclusion, many students provided updates on the status of national CIP planning and operations in their own countries, which confirmed that significant changes are taking place in a number of nations as they seek to establish and implement national CIP policies, plans and procedures.

However, the concept of CIP has matured to the point where it is now more commonly referred to as Critical Infrastructure Security and Resilience (CISR), not only in the West, but elsewhere around the globe. Focus on the "protection" of critical infrastructure began to turn to "resiliency" of critical infrastructure in the mid- 2000s because of the inability to provide absolute protection to all identified national critical infrastructure from all possible threats therefore, critical infrastructures need to be resilient. Individuals and institutions responsible for the design, delivery, and operation of critical infrastructure are now embracing and adopting resilience concepts and practices, so that engineered structures and infrastructure are not only safer (do not fail), but also better provide continuity of essential critical functions. Since "resilience" is one of NATO's seven key competencies, as it was reinforced in the London Summit declaration, NATO should seriously consider its involvement in this arena. NATO should reconsider its strategic objectives in a new concept to provide appropriate answers on the field of critical infrastructure security and resilience. Recent events such as the drone attacks against Saudi oil refinery and the outbreak of Coronavirus pointed out how the critical infrastructure, such as energy supply or global transportation chains, are vulnerable. NATO has the responsibility for integrating CIP/CISR into the greater national security framework of a nation, and/or the "practitioners" who actually manage and directly work on CIP/CISR plans, policies, procedures and related activities.

It is important to note that most of the world's critical infrastructure is owned and operated by private sector corporations. Although NATO has conducted CMXs since 1992, it is still just a political and military exercise to handle and practice issues in a crisis situation without involvement of the private sector. When there are disruptions to the services critical infrastructure provide (such as energy, transportation, and communications) there is the potential for costly direct economic impacts, such as the cost of repairing damage to physical structures, and indirect economic impacts to society, such as disruption to global supply chains, as was observed recently after the drone attacks against Saudi oil refinery and the outbreak of Coronavirus. By investing in CIP education and helping Alliance and Partner Nations build robust and redundant critical infrastructure protection capabilities across Alliance and Partner Nations, NATO builds resiliency in the very same CI NATO relies on to conduct its mission.

Conclusion

The concept of protecting critical infrastructure is shifting its focus to Critical Infrastructure Security and Resilience. Focus on the "protection" of critical infrastructure began to turn to "resiliency" of critical infrastructure because it has been recognized by practitioners that, critical infrastructures need to be resilient (i.e., be able to prepare for and adapt to changing conditions and withstand and recover rapidly from deliberate attacks, accidents, or other naturally occurring threats or incidents) due to the inability to provide absolute protection to all identified national critical infrastructure from all possible threats. NATO understands this change because "resilience" is one of NATO's seven key competencies. Although, protection of national critical infrastructure is primarily individual allies' responsibility, protecting the key Global Critical Infrastructure is a strategic security concern and challenge for the Alliance. The deterrent and credible value of NATO forces is essential. It is based not just on credible military capabilities, force structure and force projection but also on NATO infrastructures (transportation, energy, water, communications) to support short fused response and reinforcement timelines and means of sustainment. Meanwhile, many of critical infrastructure services are owned by private companies. If NATO needs to launch a major overseas operation, then 90% of military transport is chartered or requisitioned from the commercial sector. On the other hand, 50% of satellite communications used for defense purposes are provided by the commercial sector. Moreover, 75% of host nation to support to NATO operations is sourced from local commercial infrastructure and services.

Therefore, strengthening the security and resilience of critical infrastructure is a shared responsibility between NATO; critical infrastructure owners and operators; various government entities; and non-government organizations (including industry associations). Roles and responsibilities for maintaining or improving the security and resilience of infrastructure vary widely. Engagement at all levels of government and industry fosters mutual understanding and trust, promotes information sharing, and practical exchanges. Engagements that promote planning, prioritization of resources, exercises, and training greatly contribute to the success of national preparedness efforts and effective and timely responses. Such engagements also galvanize support for joint public-private efforts.

Terrorism poses a direct threat to the security of the citizens of NATO countries, to international stability and prosperity, and will remain a threat for the foreseeable future. Through the Alliance Strategic Concept, Allies reaffirmed that the Alliance must "deter and defend against emerging security challenges where they threaten the fundamental security of individual Allies or the Alliance as a whole". Allies have, therefore, decided to review NATO's approach to counter-terrorism and to enhance both the political and the military aspects of NATO's contribution to national and international efforts.

NATO has unique capabilities in the field of training and education. These capabilities, should be offered to partner nations in cooperation with other international organizations in order to enhance

NATO's security. The military concept on countering terrorism can provide possibility to engage with partner nations on their defense capability development including critical infrastructure.

The CMX series is a good opportunity to practice and prepare the political and military leadership for crisis situations. If NATO were to incorporate the involvement of private critical infrastructure owners from the planning through execution of these exercises, NATO has the opportunity to ensure greater security of and resilience of the critical infrastructure NATO relies on but does not own or operate.

COE DAT must continue its efforts to provide efficient training to Allies and partner nations on protection of critical infrastructure by adapting the findings of this workshop into the CIPATA/CISRATA course content. It is also important to provide advanced educational opportunities to educate the future leaders on CI.

Recommendation

For NATO consideration:

1. The review and update of MC 0472/1 military concept for counter terrorism should emphasize the importance of building Allies and Partner Nations Critical Infrastructure Security and Resilience (CISR).
2. NATO organize seminars and conferences to engage the owners of the global strategic critical infrastructure.
3. Provide a forum for strategic thinkers, senior managers, and practitioners responsible for developing and implementing CISR plans, policies, procedures, and related activities, to determine how such activities can be integrated with a more complex national security planning framework
4. Crisis Management Exercises (CMXs) should be a tool to harmonize the resiliency of different sectors of CI, including private stakeholder's involvement, in order to build a collaborative resilient CI.
5. NATO should increase cooperation with partner nations and not only provide E&T in NATO's ETFs but also on-site team visits to help identifying and building nations secure and resilient capabilities on critical infrastructure.

For COE DAT consideration:

1. Adapt the current Critical Infrastructure Protection Against Terrorist Attacks (CIPATA) course to the current security environment. Shift the course's focus from protection to security and resilience.
2. Develop an advance course to provide further education on the concept and practices of critical infrastructure security and resilience (CISR) for those whose are accomplished the basic course.
3. Provide forum (i.e. seminar, conference) to deliver education for decision makers and practitioners who actually manage and directly work on CIP/CISR plans, policies, procedures and related activities.
4. Generate a project for writing a handbook on best practices of CISR, in order to provide a commonly agreed to and standardized platform for training and education.

ANNEX – A Workshop Program

Lessons Learned Workshop on "Strengthening the Security and Resilience of NATO and Partner Nation Critical Infrastructure against Terrorist Attacks"

(16-17 December 2019 COE DAT, Ankara/TURKEY)

Arrival Day (15.12.2019)		
16.00 – 19:00	Initial discussion with experts in Holiday Inn Hotel	COL CSURGO
Day One (16.12.2019)		
08.20 – 09.00	Transportation to the Centre	Workshop Assistant
09.00 – 09.20	Registration and Welcome Coffee	Workshop Director, Workshop Assistant
09.20 – 09:35	Welcome address and Briefing on COE-DAT Activities	Director of COE DAT
09.35 – 10.00	Administration brief and group photo	Workshop Director
10.00 - 11.00	**Introduction of LL CISR WS Subject and Aim** *This session is in one hand to introduce the aim of the workshop and on the other hand design the main objectives of WS.*	Prof. Ronald S. Bearse (USA) Academic Advisor of the WS. COL Attila Csurgo COE DAT Chief of Knowledge department
11.00 – 11.10	*Break*	Workshop Assistant
11.10 – 12.00	Observations made by the experts on their area of expertise *This session is designed to elaborate on the recent observations made by lecturers on CIPATA course, conducted in this year May by COE DAT. It is open discussion moderated by the Academic Advisor*	Prof. Ronald S. Bearse (USA)
12.00 – 13.30	*Lunch at Merkez Officers Club*	
13.30 – 15.10		Prof. Ronald S. Bearse (USA)

	Observations made by the experts on their area of expertise *This session is designed to elaborate on the recent observations made by lecturers on CIPATA course, conducted in this year May by COE DAT. It is open discussion moderated by the Academic Advisor*	
15.10 – 15.35	*Break*	
15.35 – 17.00	Conclusions and Recommendations *This session is design to summarize the observations and drafted all possible way ahead for NATO as well as for COE DAT too. Moderated discussion with all participants.*	Prof. Ronald S. Bearse (USA) Rapporteurs
Day Two(17.12.2019)		
08.20 – 08.40	Transportation to the Centre	Workshop Assistant
08.40 – 09.00	*Welcome Coffee*	Workshop Director, Workshop Assistant
09.00 – 10.20	**Observations made by the experts on their area of expertise** *This session is designed to elaborate on the recent observations made by lecturers on CIPATA course,*	Prof. Ronald S. Bearse (USA)

	conducted in this year May by COE DAT. It is open discussion moderated by the Academic Advisor	
10.20 – 10.40	*Break*	
10.40 – 12.00	**Observations made by the experts on their area of expertise** *This session is designed to elaborate on the recent observations made by lecturers on CIPATA course, conducted in this year May by COE DAT. It is open discussion moderated by the Academic Advisor*	Prof. Ronald S. Bearse (USA)
12.00 – 13.30	*Lunch at Merkez Officers Club*	Workshop Assistant
13.30 – 15.10	Conclusions and Recommendations *This session is design to summarize the observations and drafted all possible way ahead for NATO as well as for COE DAT too. Moderated discussion with all participants.*	Prof. Ronald S. Bearse (USA) Rapporteurs
15.10 – 15.25	*Break*	Workshop Assistant
15.25 – 16.10	Wrap-Up, Path forward and closing remarks.	Prof. Ronald S. Bearse (USA) COL Attila Csurgo (HUN A)
16.10 – 16.30	Transportation to hotel	Workshop Assistant