

Terrorism Experts Conference

&

Executive Level Defence Against Terrorism

Seminar

(TEC 2021)

Combined COE-DAT Event

12-13 October 2021

Ankara, Turkey

DISCLAIMER

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

Contents

TEC 2021 Team	4
TEC 2021 Concept	5
Terrorism Experts Conference & Executive Level Defense Against Terrorism Seminar (TEC 2021) Combined COE-DAT Event Program	6
Main Outcomes and Common Points of TEC 2021	11
Opening Remarks – Welcome Address.....	15
Closing Remarks	17
DAY I –Session 1: Good Practices in Counter-Terrorism Volume 2	19
Special Courts and Prosecution Asst. Prof. Omi HODWITZ (CA).....	19
Presentation	27
Reconciliation Mr. Stephen HARLEY (GBR).....	33
Presentation	35
Community Policing Dr. Richard WARNES (GBR).....	41
Presentation	44
Gender Specific CT Policies Dr. Zeynep SÜTALAN (TUR).....	49
Presentation	54
DAY I – SESSION 1: Questions and Open Discussion.....	59
DAY I – SESSION 2: COE-DAT Research	67
Terrorist Implications Arising From COVID-19 and Predictions to Future Terrorist Implications Dr. Richard WARNES & Mr. Stephen HARLEY	67
Presentation	70
Border Security in Contested Environments Col. Daniel Wayne STONE	75
Presentation	78
Terrorism Threat during Peer to Peer Conventional War Mr. Krisztián JÓJÁRT.....	85

Presentation	88
Why is Gender Important in Counter-Terrorism? Col. Daniel W. STONE.....	98
Presentation	104
DAY I – Session 2: Questions and Open Discussion.....	108
DAY II – Session 1: Critical Infrastructure Security and Resilience Book Volume 1	115
CI Overview, Policy Definitions & Importance Prof. Ronald Sanford BEARSE.....	115
Presentation	120
Terrorist Threats to CI Mr. Raymond MEY & Mr. Malcolm BAKER.....	128
Presentation	131
Hybrid Threats to NATO CI Dr. Carol V. EVANS	135
Presentation	139
Crisis Response & Consequence Management Mr. Malcolm BAKER.....	146
Presentation	150
DAY II – Session 1: Questions and Open Discussion	157
DAY II – Session 2: Critical Infrastructure Security and Resilience Book Volume 1	162
Aviation – Post-9/11 Case Studies Mr. David HARELL.....	162
Presentation	165
Water – Washington DC Metro Case Study Mr. Steven E. BIEBER.....	170
Presentation	173
Cyber & Hybrid – Electric Grids/Ukraine Dr. Theresa SABONIS-HELFF	185
Presentation	189
European Policy Framework Mr. Alessandro LAZARI	196
Presentation	201
DAY II – Session 2: Questions and Open Discussion	209

TEC 2021 Team

Seminar Director

Col. Bayram Mert DEVECİ (TUR A)

Assistant Director

Maj. Ali MAVUŞ (TUR A)

CIS Specialist

Mrs. Selvi KAHRAMAN (TUR Civ.)

Seminar Assistant

Mrs. Özge ERKAN (TUR Civ.)

Speakers

Mr. Alessandro LAZARI (ITA)

Dr. Carol V. EVANS (USA)

Col. Daniel STONE (USA)

Mr. David HARELL (GBR)

Prof. Haldun YALÇINKAYA (TUR)

Mr. Krisztián JÓJÁRT (HUN)

Mr. Malcolm BAKER (GBR)

Dr. Omi HODWITZ (CAN)

Mr. Raymond MEY (USA)

Dr. Richard WARNES (GBR)

Prof. Ronald Sanford BEARSE (USA)

Mr. Stephen HARLEY (GBR)

Mr. Steven E. BIEBER (USA)

Dr. Theresa SABONIS-HELFF (USA)

Dr. Zeynep SÜTALAN (TUR)

Rapporteurs

Elif Merve DUMANKAYA (TUR)

Alice LÕHMUS (EST)

TEC 2021 Concept

COE DAT is developing projects like The Good Practices in Counter Terrorism book volume-2 in coordination with TOBB-University in Ankara, Turkey; Critical Infrastructure Security and Resilience books volume 1 and 2 in coordination with US Army War College; COVID-19 implications in terrorism; and gender aspects to terrorism and counter terrorism. COE DAT's intent is to provide examples of what has worked in countering terrorism from the Strategic and Operational levels focusing on what militaries and NATO can do to support the Whole of Government and Whole of Society's efforts.

Both flagship COE DAT activities – the Terrorism Experts Conference and the Executive Level Defence Against Terrorism Seminar for 2021 were planned to support the two book projects and other research activities conducted by COE-DAT. Because of the COVID pandemic, the Terrorism Experts Conference and Executive Level Defence Against Terrorism Seminar were conducted as a joint hybrid conference between 12 and 13 October 2021 on the topic of “The Military Role in Countering Terrorism”. The duration of the working day was 5 hours between 15.00 and 20.00 local (Turkish) time.

The aim of this combined event was to underline the role of the military in different dimensions of countering terrorism. Combining Terrorism Experts Conference and Executive Level Defence Against Terrorism Seminar provided an opportunity to review the included topics from the point of view of academicians and executive level officers from NATO and Partner Nation's countries who are involved in the development of national policies related to countering terrorism.

**Terrorism Experts Conference
&
Executive Level Defense Against Terrorism Seminar
(TEC 2021)
Combined COE-DAT Event Program**



Conference Program
Terrorism Experts Conference 12-13 October 2021



OCTOBER 12, 2021

14.30 - 15.00	Communications Check	
15.00 - 15.05	Welcome Address, Director of COE-DAT	
15.05 - 15.10	Admin Remarks, TEC Director	
15.10 - 15.15	Opening Remarks by Keynote Speaker	
15.15-15.20	Session 1: Good Practices in Counter Terrorism Volume 2 Moderated by: Prof.Dr. Haldun YALÇINKAYA (TUR), International Relations Department, TOBB ETU University Ankara, Turkey	Speaker
15.20-15.40	Special Courts and Prosecution	Asst.Prof. Omi HODWITZ (CA) Department of Culture, Society, and Justice, University of Idaho
15.40-16.00	Reconciliation	Mr. Stephen HARLEY (GBR) UK Foreign Office Advisor- British Embassy Mogadishu
16.00-16.20	Community Policing	Dr. Richard WARNES (GBR) Senior Consultant ad Vedette Consulting
16.20-16.40	Gender Specific CT Policies	Dr. Zeynep SÜTALAN (TUR) Atılım University
16.40 - 17.30	Questions and Discussion	
17.30 - 17.45	Break	

17.45-17.50	Session 2 : COE-DAT Research Moderated by: Col. Daniel Wayne STONE (USAF), Deputy Director, COE-DAT	Speaker
17.50- 18.10	Terrorist Implications Arising From COVID-19 and Predictions to Future Terrorist Implications	Dr. Richard WARNES (GBR) Senior Consultant at Vedette Consulting & Mr. Stephen HARLEY (GBR) UK Foreign Office Advisor- British Embassy Mogadishu
18.10 - 18.30	Border Security in Contested Environments	Col. Daniel Wayne STONE (USAF), Deputy Director, COE-DAT
18.30 - 18.50	Terrorism Threat during Peer to Peer Conventional War	Mr. Krisztián JÓJÁRT (HUN), National University of Public Service, Budapest
18.50 - 19.10	Why the Gender in CT Topic is Important for NATO	Col. Daniel Wayne STONE (USAF), Deputy Director, COE-DAT
19.10 - 20.00	<i>Questions and Discussion</i>	
20:00	<i>End Day 1</i>	



Conference Program
Terrorism Experts Conference 12-13 October 2021



OCTOBER 13, 2021

15.00 - 15.05	Session 3: Critical Infrastructure Security and Resilience Book Volume 1 Moderated by: Dr. Carol V. EVANS (USA) Director, Strategic Studies Institute and US Army War College Press	Speaker
15.05 - 15.25	CI Overview, Policy Definitions & Importance	Prof. Ronald Sanford BEARSE (USA) Nauset National Security Group, LLC, Hyannis, MA
15.25 - 15.45	Terrorist Threats to CI	Mr. Raymond MEY (USA) & Mr. Malcolm BAKER (GBR)
15.45 - 16.05	Hybrid Threats to NATO CI	Dr. Carol V. EVANS (USA) Director, Strategic Studies Institute and the USAWC Press U.S. Army War College
16.05 - 16.25	Crisis Response & Consequence Management	Mr. Malcolm BAKER (GBR)
16.25- 17.15	<i>Questions and Discussion</i>	
17.15- 17.30	<i>Break</i>	

17.30-17.35	<p align="center">Session 4: Critical Infrastructure Security and Resilience Book Volume 1</p> <p align="center">Moderated by: Dr. Carol V. EVANS (USA) Director, Strategic Studies Institute and US Army War College Press</p>	Speaker
17.35 - 17.55	Aviation – Post-9/11 Case Studies	<p align="center">Mr. David HARELL (GBR) Lecturer Berlin School of Economics and Law Master’s Program for Security Management, Berlin, Germany</p>
17.55 - 18.15	Water – Washington DC Metro Case Study	<p align="center">Mr. Steven E. BIEBER (USA) Metropolitan Washington Council of Governments, Program Director, Water Resources</p>
18.15 - 18.35	Cyber & Hybrid – Electric Grids / Ukraine	<p align="center">Dr. Theresa SABONIS-HELFF (USA) Georgetown University Masters of Science in Foreign Service Program</p>
18.35 - 18.55	European Policy Framework	<p align="center">Mr. Alessandro LAZARI (ITA) Centre for Interdisciplinary Research on CISR</p>
18.55 - 19.45	<i>Questions and Discussion</i>	
19.45 - 20.00	Closing Speech & Final Remarks Dir. COE-DAT	
20:00	<i>End Day 2</i>	

Main Outcomes and Common Points of TEC 2021

- Based on research on court records in the United States, the **criminal justice model is more effective** than the military justice model at deterring re-offending, particularly when court proceedings and programming are available. Specifically, it appears that the **criminal justice model may be more effective at reducing re-engagement and recidivism in comparison to the military model.**
- It is important to **include everyone in a negotiated settlement.** Also, bringing in a country that is not particularly involved in the conflict matter but has an interest instead, has proven to be useful.
- **Community policing** includes focusing on personal relationships and engaging with communities with the **goal of gaining and maintaining popular support to ultimately develop local community intelligence.** If the police are engaging with the community and if the transactions with the community are fair and just, it can help build a level of trust with the community, enhancing the legitimacy of the police as well as enhance the level of institutional authority. However, if engagement with the police within the community is poor and unjust, this destroys trust building and weakens institutional authority. **Engagement with the local communities and information sharing is the key.**
- Gender matters in counter terrorism because: **diversity produces better policies,** gender is directly linked to the analysis and response to the terrorist threat and **represents a security threat** to NATO and nations around the world, and understanding gender increases the effectiveness of preventing and countering violent extremism. There are disparities in criminal prosecutions and whether women are prosecuted at all.
- When it comes to gender-sensitivities and gender-responsiveness in counter-terrorism, it is important to underline **what gender is and what gender is not.** Gender is a socially constructed set of roles based on biological sex in a given society and time. Gender perceptions shape power dynamics, opportunities, and norms between men, women, boys, and girls. Gender roles change over time and within different groups. Gender is far more than just women.

- In order to understand and efficiently respond to the gender aspects of terrorism, it is critical to recognize the **different roles played by women in terrorism** and evaluate these roles in the broader context of gender, ranging from victims to perpetrators. Moreover, gender-sensitive CT policies should be **tailored according to the gender-specific needs** and be human rights compliant.
- When it comes to the **gender dimension of prosecution**, research indicate that there is a gender disparity in the criminal justice processes, such as women escaping prosecution or receiving more lenient sentences compared to their male counterparts. The starting point is the **criminalization of terrorist offences**.
- It is important to increase women's representation at all levels in the security sector. The recruitment, retention, and advancement of women across the security sector to bolster the capacity of forces to mitigate potential terrorist threats should be addressed. CT policies should be tailored to the needs of women, men, boys, and girls in terms of prosecution and rehabilitation programs.
- The COVID-19 pandemic **opened up the potential of bioterrorist attack** and illicit procurement of a biological weapon by terrorist groups. This is something NATO and nations need to start preparing for - **terrorists learn constantly** and they exploit technology.
- In terms of specific policy recommendations to NATO, it can include provision of field hospitals as well as help with medical evacuation. There is a need to challenge inadequacies of terrorist groups in terms of contradictions in messaging, fallacy and promises. Moreover, there is a need to **increase focus on human security and enhance civil preparedness**. This means renewing focus on transnational human security threats and **closer cooperation of military with civilian emergency services**.
- In terms of more general recommendations, NATO should **improve information sharing** of best practices and lessons. As COVID-19 challenged NATO's strategic

communications, there is a need for **more innovative and coordinated strategy** as well as to **strengthen defence cooperation and integration of military and civil capabilities**.

- In the context of preventing cross-border movement of terrorist fighters and transnational groups, **information sharing and holistic CT strategy** which covers land, air, and maritime domains is key to identifying and disrupting networks that facilitate their travel.
- **Militaries have expertise in operational planning** that is often not matched by any other organizations. The military also has a capability to be called-in as first responders and capable to operate in very remote areas. However, the **military cannot provide long-term replacement to law enforcement** in emergency services.
- With regards to the definition of terrorism, there is no distinction between war and peacetime, civilian and military targets as well as state or non-state actors.
- Regarding COVID-19 – **we must engage with the fake news** rapidly and bring in legal measures. **If people can think critically and are media literate, that is how we have a longer-term solution** – it is about being more **prepared**.
- **Promoting and supporting civilian counter terrorism initiatives**, as well as **civil society**, is beneficial as different views can come up with new solutions.
- Over the last twenty years, most national critical infrastructure (CI) policies focused solely on “protection” of CI to make it more secure and resilient. This is primarily a function of the evolution. The number of threats directed to the CI are continuously increasing. As a result, states initiate policies and strategies in order to meet the expectations to overcome those threats. Under the **Critical Infrastructure Security and Resilience (CISR) Construct the focus has shifted from protection to recovery (resilience)**; the terms *security* and *resilience* certainly support the idea of protection.

- 85% of Critical Infrastructure is in the private sector. Government in partnership with the private sector should **adopt an All Hazards Approach** to securing and preparing to recover from critical infrastructure interruptions.
- We need to understand **relativity of the threat** to the CI that we are trying to detect and which threats or hazards could manifest themselves on our radar.
- Over years, many different policy documents stressed the importance of critical infrastructure. In this regard, NATO holds a position which enables the Alliance to possess a **deterrent value** and makes its role even more crucial.
- Understanding how the characteristic of a crises helps to understand the approach of different countries. For instance, an emergency can in long term turn out to be a global crisis that requires a global solution. Therefore, we need to track the process. In order to do so, we should understand the “*Anatomy of a Crisis*” sometimes referred to as a strategic surprise.
- Critical infrastructure operators, owners, and the government should be involved in the **process of developing a crisis management capability**. In that sense, militaries are good at creating crisis management frameworks.
- In most of these cases in aviation security, the anti-terrorism effort’s failure was exacerbated by intelligence/counter-terrorism failures.
- In the conflict between Ukraine and Russia, energy has been used as a tool. More research is needed concerning risk factors with regards to cyber-attacks and what kind of economical as well as human loss this can lead to.

Opening Remarks – Welcome Address

Dear Generals and Admirals,

Dear Distinguished speakers and participants, Ladies and gentlemen,

I would like to present a warm welcome to you all and thank you for your participation in our TEC conference.

The interest this conference has received made me quite pleased, for we have been preparing for a long time.

Before we get started, I would like to express my sincere appreciation to all of you who generously helped us make this event come together to become a success.

TEC 2021 will draw nearly 200 well-known terrorism experts, academics, and practitioners. The goal of TEC is for the presenters and participants to have a venue to share their expertise, experience, and research works so that NATO and its partner countries can transform together in the fight against terrorism.

This year's TEC explores "Military Considerations in Countering Terrorism (CT)" in four sessions drawn from original COE-DAT research. The first session examines CT policy issues concerning special courts and prosecution, reconciliation, community policing, and gender implications in CT. Session two examines NATO's role in pandemic/bioterrorism support to civil government, potential good practices in military border security, the terrorism threat to NATO during peer to peer conventional war, and why gender is important in CT. The third and fourth sessions introduce Critical Infrastructure Security and Resilience by tracing the threat to NATO critical

infrastructure (CI); exploring case studies on the aviation, water, and electric sectors; and modelling infrastructure dependencies to present a tool to protect and make CI resilient.

Generals and Admirals,

Ladies and gentlemen, distinguished participants,

To be brief, I would like to wish all of us to have an interesting, challenging, dynamic, and fruitful conference.

Oğuzhan PEHLİVAN

Colonel (TUR A)

Director COE-DAT

Closing Remarks

Dear Generals and Admirals,

Dear Distinguished speakers and conference participants,

Ladies and gentlemen,

After two days of hard work, it is time to close this year's "Terrorism Experts Conference".

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

I'd also like to specifically thank our moderators and for their dedicated and valuable work.

As you have noticed, we have two Rapporteurs among us, Ms. Alice LOHMUS and Ms. Elif Merve DUMANKAYA, who are not just focusing their studies on Terrorism, but who tremendously helped to COE-DAT, by diligently taking notes during the activity. Thank you.

Many thanks to our CIS team and especially to Mrs. Selvi KAHRAMAN. Without you, this unusual but successful conference would not be possible.

I would also like to thank all of to my COE-DAT Staff, without which this activity would not have been likely.

Last but no least I want to thank all of you in the audience. It is thanks to your valuable contributions and your vast expertise that this activity was such a success – a success we want to build on in future events, for which I hope to see you all again.

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

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

Oğuzhan PEHLİVAN

Colonel (TUR A)

Director COE-DAT

DAY I –Session 1: Good Practices in Counter-Terrorism Volume 2

Moderated by: **Prof. Dr. Haldun YALÇINKAYA** (TUR), *Political Science and International Relations Department, TOBB University of Economics and Technology, Ankara, Turkey*

Special Courts and Prosecution

Asst. Prof. Omi HODWITZ (CA)

Department of Culture, Society, and Justice, University of Idaho

Overview

Dr. Hodwitz is a criminologist who looks at how different policies and practices influence criminal behaviour, in particular, political violence. The purpose of the presentation was to assess different methods of processing, prosecuting, and detaining extremists who are in custody with the goal of identifying practices with positive outcomes. These methods may be grouped into two models of counterterrorism: the military model and criminal justice model. The presentation includes an introduction to these models paired with a description of model goals and metrics of success, including deterrence (goals) and reengagement or recidivism (metrics). As a means of gauging effectiveness, the presentation provides a general assessment or meta-analysis of model applications and effects in select nations around the world. It also includes a data-driven case study assessment of the practices and outcomes of each model in the United States. The outcomes of these assessments indicate that the criminal justice method of prosecution and detainment is the more effective means of deterring terrorism, as measured by rates of recidivism and reengagement, particularly when paired with transparent and definitive court proceedings and in-prison programming. The results are persistent across case studies, despite the variability in their application of the criminal justice and military models.

Context

The start of the 21st century was marked by several isolated high-profile terrorist incidents, including the attacks in the United States on September 11, 2001 which served as a reminder to a counter terrorism community that there was a great deal of effort to be done in order to curb terrorism. In response, the counter terrorism community implemented a series of policies and

practices designed to thwart and punish extremist behaviours around the world. These measures resulted in extensive investigative growth and a dramatic increase in the number of extremists taken into custody. Twenty years later, many of these alleged and/or convicted terrorists are being released back into the community, subject to repatriation or reintegration. These individuals are being released either because they have served out their court-ordered sentences or being repatriated back to their home-countries. The influx of released extremists raises concerns among practitioners and policymakers alike regarding their ability to disengage and desist. These concerns stem from the fact that there is a deficit in empirical research examining re-entry success among this unique group of offenders. Often, we do not know what to expect from these individuals as they are returning to their communities, whether they are going to desist, re-engage or recidivate. Desistence relates to separating from any kind of deviant attack, whereas re-engagement is engaging in ideologically motivated activities. Recidivism relates to engaging with any kind of deviant attack whether it is ideologically motivated or not. Up until now, there have not been enough information of individuals in aggregate numbers to collect data in order to understand what re-entry looks like for them.

A lack of information on re-entry stems, at least in part, from a lack of data. Until recently, there simply were not enough extremists re-entering the community to allow for the collection of aggregate data and, thus, the formation of evidence-based predictions. The increasing wave of recent releases, however, have mitigated this issue, providing the numbers necessary to begin the examination of aggregate extremist re-entry outcomes. At this early stage, the results from these projects are inconsistent but promising. Of the handful of preliminary data collection efforts that have arisen in the last five years, most report low rates of re-engagement (terrorist activity) and recidivism (criminal activity of any kind); estimates indicate that between 1-20% of political extremists re-offend within the first few years of release. This is in sharp contrast to apolitical releases who report recidivism rates of 30-70% within the same timeframe. Unfortunately, researchers do report some outlier studies, with re-engagement or recidivism rates comparable to apolitical populations, falling somewhere between 40-60%. This begs an important question: what factors facilitate desistance versus re-engagement or recidivism? What is driving this inconsistency in data results? Do our counter-terrorism responses help facilitate desistance? The research community has begun to explore this, focusing on demographics, psychological characteristics, location, and geo-political dynamics. There is, however, a notable lack of focus on the very measures that are designed to affect terrorism: counter-terrorist efforts.

State Responses to Terrorism

State responses to terrorism may be grouped into two counterterrorism models: **the criminal justice model** and **the military model**. The military model is a proactive model, driven by the goal of thwarting terrorism before it occurs or, if it does occur, deterring future incidents of terrorism. Within this model, terrorism is viewed as an act of war, triggering the rules of engagement and often displacing considerations of due process and civil liberties with the strategic use of violence. The criminal justice model on the other hand, is a reactive model that requires plotting and/or the execution of terrorist events before it can be triggered. It serves to punish extremists for their violent engagement as well as deter future incidents. Terrorism is viewed as a criminal act, thus requiring rules of due process and civil protections. Although the two models may overlap in some practices and policies, they differ considerably in their strategies and guidelines. Despite these differences, both models seek to stop extremist violence and, thus, assessments of re-engagement should consider the presence and influence of each of these models.

Within each model type, there are a handful of factors that are actively employed that can influence their effectiveness. Research with apolitical populations point to, for example, the importance of transparent and definitive court proceedings, convictions, and sentencing, along with detention-based programming. Regarding the former, studies have found that a lack of court proceedings can lead an offender to question the legitimacy of their detainment and to embrace a sense of injustice. For a political population, this may incite animosity, leading to future offending. Regarding the latter, apolitical offenders consistently demonstrate the importance of programming, particularly in prison. Appropriate programming can reduce recidivism considerably, suggesting that the same may be true of a politically motivated population. Therefore, not only should model type be considered, but so too should the presence of court proceedings and programming options.

Empirical Analysis

Informed by the considerations outlined above, this presentation examined the effectiveness of the counter-terrorism model type, particularly related to prosecution and detainment, on the recidivism and reengagement rates of extremist offenders re-entering society. In addition, it also explored the impact that court proceedings and in-prison programming had on successful re-entry. A two-stage analysis was conducted to accomplish this task, beginning with a meta-

analysis of the pre-existing research on terrorist re-offending and an in-depth case study of re-entry in the United States.

Meta-Analysis

The meta-analysis consisted of recent empirical studies that included assessments of terrorist re-engagement and recidivism. Studies that were not data-driven or had mixed model types were excluded. This resulted in nine different empirical analyses, including six samples processed through the criminal justice model and three processed through the military model. Both sets reported low recidivism rates, but the former were consistently in the 1-20% range while the latter reported rates between 1-40%, suggesting that it was less consistently effective at facilitating desistence. Program availability also appeared influential, at least within the criminal justice samples. Criminal justice samples that reported the highest rates of re-offending were denied programming or had very limited access while those that reported the lowest rates were offered programming, particularly focused on de-radicalization. Unfortunately, there was not enough diversity in court proceedings to form any conclusions about its relationship to desistence; only one sample was denied transparent and definitive court rulings. However, criminal justice model does seem to have a more consistent desistence rate than the military model, this is particularly evident when it comes to the use of programming.

Stage 1: Existing Research						
AUTHOR	LOCATION	TYPE OF REOFFENCE	REOFFENDING RATES	YEARS OF STUDY	COURT PROCEEDINGS AND PROGRAMMING	MODEL TYPE
Cragin (2017)	Indonesia	Reengagement	40%	1980s-1990s		No Model
Cragin (2017)	Algeria	Reengagement	90%	1980s-1990s		No Model
Carmel et al (2020)	Israel	Reengagement	6.8% - 17.3%	2004-2017	Court convictions and sentencing No programs	Criminal Justice Model
Van der Heide and Schuurman (2018)	Netherlands	Recidivism and reengagement	4.2% (reengagement) 5.8% (all recidivism)	2008-2012	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Ministry of Justice (2020)	England and Wales	Reengagement	3.1%	2013-2016	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Renard (2020)	Belgium	Recidivism and reengagement	2.3% (reengagement) 4.8% (all recidivism)	1990-2019	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Hecker (2021)	France	Reengagement	0%	2016-2020	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Ismail and Sim (2016)	Indonesia	Reengagement	15%	Prior to 2013	Court convictions and sentencing Limited programming	Criminal Justice Model
Boucek (2010)	Saudi Arabia	Reengagement	1-20%	2003-2008	Mixed court convictions and sentencing Deradicalization programs	Military Model
Seifert (2010)	Yemen	Reengagement	40%	2002-2005	Limited court convictions and sentencing Deradicalization programs	Military Model
Azam and Fatima (2017)	Pakistan	Reengagement	1%	2009 to unknown date	No court convictions and sentencing Deradicalization programs	Military Model

Figure 1— Existing Research on Criminal Justice Model and Military Model

One criticism that could be levied at this first stage of analysis is the claim that differences in recidivism rates reflects factors inherent in the culture of the sample, rather than the model type. For example, an argument could be made that country-specific practices that differ between samples explain differences in desistance. This is an ‘apples-to-oranges’ concern; perhaps the samples are simply too different to allow comparison. This is a fair concern but one that is easily circumvented. To address this, the next stage of analysis included an examination of recidivism rates over time within countries as they experienced changes in model type or programming availability, thus providing an ‘apples-to-apples’ comparison. Israel, for example, transitioned from a majority military model to a majority criminal justice model in the beginning of the new millennium. Three studies examining recidivism before, during, and after this shift in model type report decreasing rates of recidivism. As for programming, the United States offered a ready within-country example. Specifically, the United States introduced programming to its detention facilities in Iraq in the late 2000s, a shift that was marked by a significant decrease in re-engagement and reoffending. These within-country shifts and their impact on desistance support the conclusion that model type and programming may be influential for successful re-entry outcomes.

Stage 1: Existing Research

Author	Location	Type of Reoffence	Reoffence Rates	Years of Study	Court Proceedings and Programming	Model Type
Ganor and Falk (2013)	Israel	Reengagement	12.4%	1993-2003	Court convictions and sentencing No programs	Mixed Military and Criminal Justice Model
Walk and Berman (2008)	Israel	Reengagement	7.9%	Prior to 2008	Court convictions and sentencing No programs	Mixed Military and Criminal Justice Model
Carmel et al (2020)	Israel	Reengagement	6.8%	2004-2017	Court convictions and sentencing No programs	Criminal Justice Model
Rubin (2008)	United States in Iraq	Reengagement	<1%	2007-2008	No court convictions and sentencing Deradicalization programs	Military Model
Rubin (2008)	United States in Iraq	Reengagement	5-10%	Prior to 2007	No court convictions and sentencing No programs	Military Model

Figure 2 — Existing Research on Criminal Justice Model, Military Model and Mixed Model

Case Study

In addition to the meta-analysis summarized above, the presentation also focused on an in-depth case study analysis of the United States. The United States provides a rich contrast between the two model types as they run parallel to each other but rarely overlap. In addition, while court proceedings and access to programming is an inherent part of the U.S. criminal justice model, it is notably absent in large part from the military model, thus providing a clear point of comparison between these two models. In other words, if recidivism rates are lower among one sample versus the other, this may be attributed to the model type and to the role of court proceedings and programming.

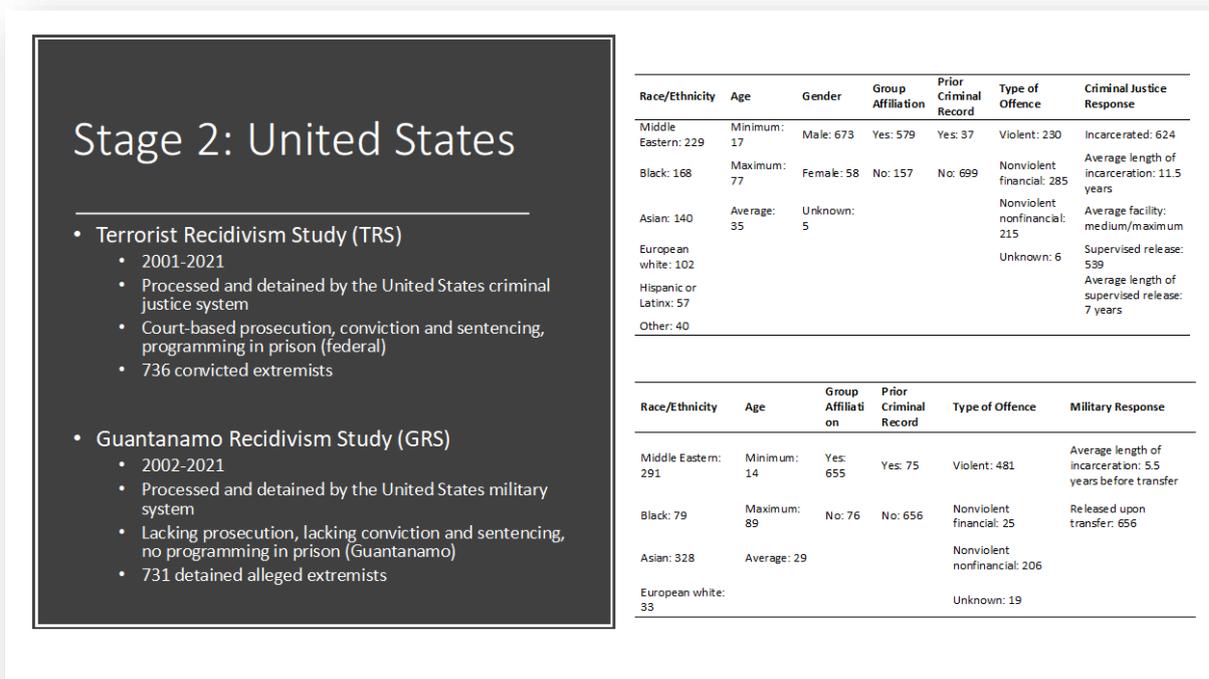


Figure 3-- The United States' Model

The analysis relied on two different datasets that tracked alleged and convicted extremists through each model and upon release. Each sample, between 700-800 individuals detained and processed between 2001 and 2021. Results are striking. Individuals processed by way of the criminal justice model (and, thus, granted access to transparent and definitive court proceedings and programming) reported reengagement rates of approximately 0.2 percent and recidivism

rates of approximately 3.2%. This is in stark contrast to those processed by way of the military model (and, thus, denied court proceedings and programming); these reported rates of 3.6% and 5.6% respectively. While still low, the rates in the military sample were notably larger than the criminal justice sample (twice as high for recidivism and eighteen times as high for re-engagement). This suggests that, once again, the **criminal justice model is more effective at deterring re-offending**, particularly when court proceedings and programming are available.

Despite these promising results, critics could still point to the ‘apples-to-oranges’ concern. The criminal justice sample consisted of both males and females, the majority of which were U.S. citizens who, upon release, were exposed to limited domestic surveillance. In addition, their offenses tended to be less violent than the military sample. To address this concern, a final stage of analysis involved matching the two samples on several key factors. Specifically, the criminal justice sample was reduced to males who were non-U.S. citizens, subject to deportation upon release with offenses that matched those found in the military sample. The resulting matched criminal justice sample consisted of 102 individuals who were then compared to the full military sample. Results, although less stark, were still informative. The matched criminal justice sample reported re-engagement rates of 1% and recidivism rates of 2%; this was in contrast to the military model sample that reported rates of 3.6% and 5.6% respectively. This indicated that, even with a matched sample, the military model produced rates of re-engagement and recidivism that were approximately three times higher than those produced by the criminal justice model.

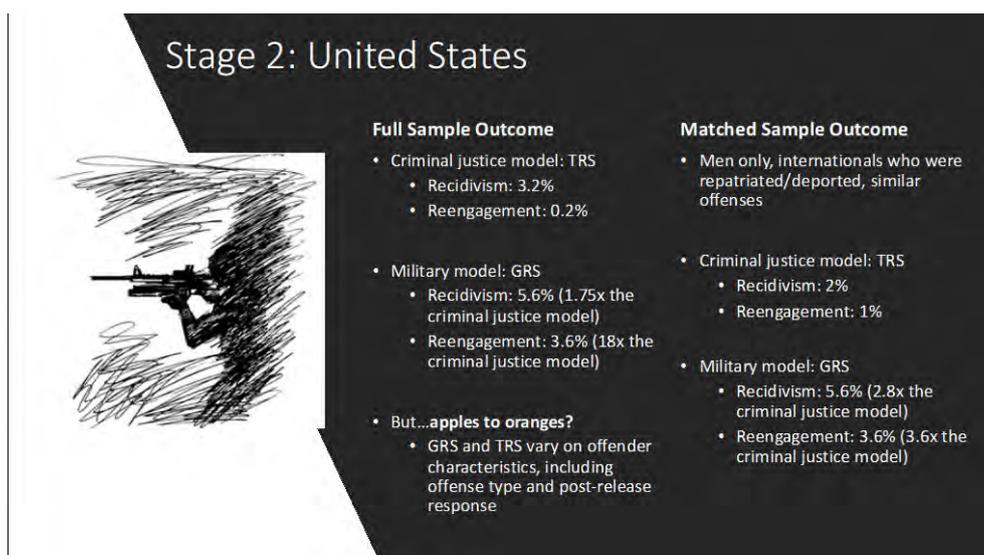


Figure 4 —The United States Sample

Implications

The results from the various studies included in the presentation point to a number of implications. First, recidivism rates among political releases are low, particularly when compared to apolitical releases. However, there is some diversity, suggesting that there are specific factors that may facilitate a more positive outcome. Both between-country and within-country analysis point to the conclusion that model type may be influential. Specifically, it appears that the **criminal justice model may be more effective at reducing re-engagement and recidivism in comparison to the military model**, especially when it comes to detainment, prosecution, and release. However, it is not to say that the criminal justice model is the better model per say, however, they do use a variety of policies and practices that help to facilitate the systems.

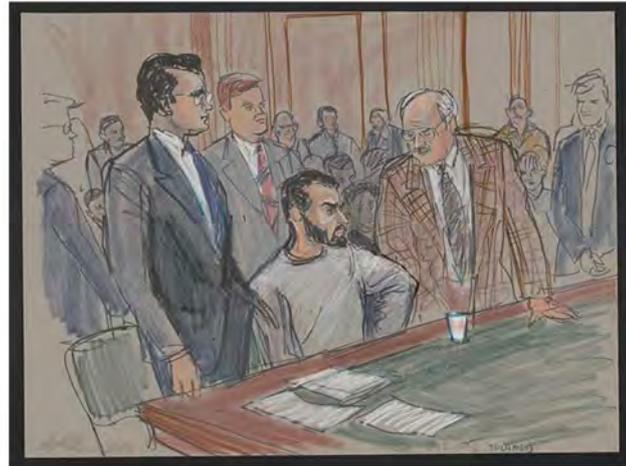
Although model type may be important, the practices and policies employed by each model seem to be particularly salient for successful re-entry. Specifically, the presence of transparent and definitive court proceedings has been linked to successful outcomes in apolitical offenders and the results suggest that this may be an important factor for political offenders as well. In addition, program availability also appears influential, demonstrating a significant impact in both the meta- and case-study analyses.

Therefore, although the criminal justice model appears more effective at reducing re-engagement and recidivism, the military model, if to be used for the purposes of post-capture processing and detainment, would be well served to incorporate those elements that have shown positive results in a variety of contexts, including court proceedings and programming.

Presentation

Special Courts and
Prosecution:
Criminal Justice and Military
Models

Omi Hodwitz
University of Idaho
Department of Culture, Society & Justice



Background and Context

- 9/11 and the new millennium
 - Increase in counterterrorism measures
 - Increase in detainments, arrests, prosecution, and incarceration
- Present day
 - Increase in extremist release and/or repatriation
 - Increase in legislator, practitioner, and public concerns regarding desistance
 - Increase in data collection and analysis examining desistance

A photograph of a tall skyscraper, likely the Empire State Building, viewed from a low angle looking up, with a blue sky and clouds in the background.



Military model

- Proactive model
- Military is central figure; employs displays of force
- Views terrorism as an act of war
- Adheres to rules of engagement

• Criminal justice model

- Reactive model
- Police/courts/corrections is central figure; employs legal proceedings
- Views terrorism as a crime
- Adheres to the rule of law

The State Response: Counterterrorism Models

Empirical Framework

- Central to both counterterrorism models:
 - Detainment/incapacitation → desistance
- But mechanisms of detainment and incapacitation vary dramatically between models
- Research question: which model is more effective at facilitating desistance?
- Factors to consider
 - Court proceedings
 - Conviction and sentencing
 - Program availability
 - Reengagement versus recidivism
- Empirical analysis
 - Stage 1: what does the existing research indicate? Meta-analysis of empirical studies from countries around the world.
 - Stage 2: what do data indicate? In-depth case study in the United States.



Stage 1: Existing Research

AUTHOR	LOCATION	TYPE OF REOFFENCE	REOFFENDING RATES	YEARS OF STUDY	COURT PROCEEDINGS AND PROGRAMMING	MODEL TYPE
Cragin (2017)	Indonesia	Reengagement	40%	1980s-1990s		No Model
Cragin (2017)	Algeria	Reengagement	90%	1980s-1990s		No Model
Carmel et al (2020)	Israel	Reengagement	6.8% - 17.3%	2004-2017	Court convictions and sentencing No programs	Criminal Justice Model
Van der Heide and Schuurman (2018)	Netherlands	Recidivism and reengagement	4.2% (reengagement) 5.8% (all recidivism)	2008-2012	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Ministry of Justice (2020)	England and Wales	Reengagement	3.1%	2013-2016	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Renard (2020)	Belgium	Recidivism and reengagement	2.3% (reengagement) 4.8% (all recidivism)	1990-2019	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Hecker (2021)	France	Reengagement	0%	2016-2020	Court convictions and sentencing Deradicalization programs	Criminal Justice Model
Ismail and Sim (2016)	Indonesia	Reengagement	15%	Prior to 2013	Court convictions and sentencing Limited programming	Criminal Justice Model
Boucek (2010)	Saudi Arabia	Reengagement	1-20%	2003-2008	Mixed court convictions and sentencing Deradicalization programs	Military Model
Seifert (2010)	Yemen	Reengagement	40%	2002-2005	Limited court convictions and sentencing Deradicalization programs	Military Model
Azam and Fatima (2017)	Pakistan	Reengagement	1%	2009 to unknown date	No court convictions and sentencing Deradicalization programs	Military Model

Stage 1: Existing Research

Author	Location	Type of Reoffence	Reoffence Rates	Years of Study	Court Proceedings and Programming	Model Type
Ganor and Falk (2013)	Israel	Reengagement	12.4%	1993-2003	Court convictions and sentencing No programs	Mixed Military and Criminal Justice Model
Walk and Berman (2008)	Israel	Reengagement	7.9%	Prior to 2008	Court convictions and sentencing No programs	Mixed Military and Criminal Justice Model
Carmel et al (2020)	Israel	Reengagement	6.8%	2004-2017	Court convictions and sentencing No programs	Criminal Justice Model
Rubin (2008)	United States in Iraq	Reengagement	<1%	2007-2008	No court convictions and sentencing Deradicalization programs	Military Model
Rubin (2008)	United States in Iraq	Reengagement	5-10%	Prior to 2007	No court convictions and sentencing No programs	Military Model

Stage 2: United States

- Terrorist Recidivism Study (TRS)
 - 2001-2021
 - Processed and detained by the United States criminal justice system
 - Court-based prosecution, conviction and sentencing, programming in prison (federal)
 - 736 convicted extremists
- Guantanamo Recidivism Study (GRS)
 - 2002-2021
 - Processed and detained by the United States military system
 - Lacking prosecution, lacking conviction and sentencing, no programming in prison (Guantanamo)
 - 731 detained alleged extremists

Race/Ethnicity	Age	Gender	Group Affiliation	Prior Criminal Record	Type of Offence	Criminal Justice Response
Middle Eastern: 229	Minimum: 17	Male: 673	Yes: 579	Yes: 37	Violent: 230	Incarcerated: 624
Black: 168	Maximum: 77	Female: 58	No: 157	No: 699	Nonviolent financial: 285	Average length of incarceration: 11.5 years
Asian: 140	Average: 35	Unknown: 5			Nonviolent nonfinancial: 215	Average facility: medium/maximum
European white: 102					Unknown: 6	Supervised release: 539
Hispanic or Latinx: 57						Average length of supervised release: 7 years
Other: 40						

Race/Ethnicity	Age	Group Affiliation	Prior Criminal Record	Type of Offence	Military Response
Middle Eastern: 291	Minimum: 14	Yes: 655	Yes: 75	Violent: 481	Average length of incarceration: 5.5 years before transfer
Black: 79	Maximum: 89	No: 76	No: 656	Nonviolent financial: 25	Released upon transfer: 656
Asian: 328	Average: 29			Nonviolent nonfinancial: 206	
European white: 33				Unknown: 19	

Stage 2: United States



Full Sample Outcome

- Criminal justice model: TRS
 - Recidivism: 3.2%
 - Reengagement: 0.2%
- Military model: GRS
 - Recidivism: 5.6% (1.75x the criminal justice model)
 - Reengagement: 3.6% (18x the criminal justice model)
- But...**apples to oranges?**
 - GRS and TRS vary on offender characteristics, including offense type and post-release response

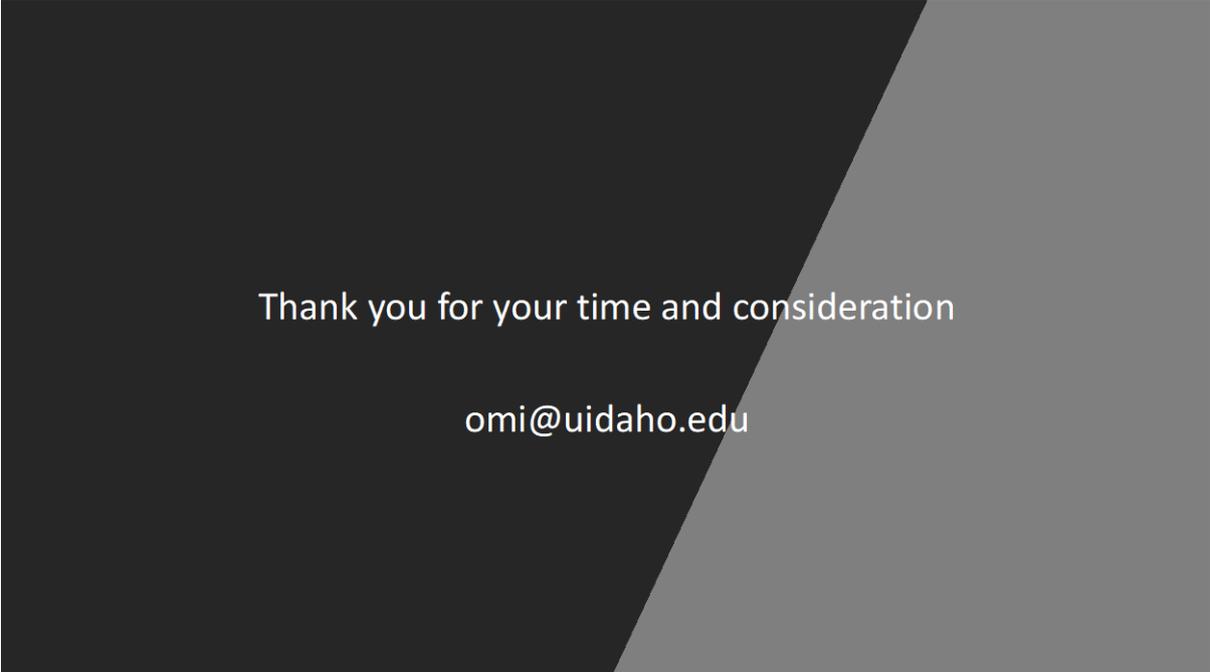
Matched Sample Outcome

- Men only, internationals who were repatriated/deported, similar offenses
- Criminal justice model: TRS
 - Recidivism: 2%
 - Reengagement: 1%
- Military model: GRS
 - Recidivism: 5.6% (2.8x the criminal justice model)
 - Reengagement: 3.6% (3.6x the criminal justice model)

General Implications and Recommendations

- Results indicate that lower rates of reengagement and recidivism are evident in:
 - The criminal justice model
 - Facilities that offer in-prison programming
 - Proceedings that involve court convictions and sentencing
- Therefore, if the goal of counterterrorism measures is to facilitate desistance, extremists will likely fare better if:
 - Processed through the criminal justice model rather than the military model
 - Subject to court proceedings, conviction, and sentencing (regardless of model type)
 - Given access to programming (regardless of model type)





Thank you for your time and consideration

omi@uidaho.edu

Reconciliation

Mr. Stephen HARLEY (GBR)

UK Foreign Office Advisor, British Embassy Mogadishu

Introduction

Negotiated settlement sits primarily under the soft power approach. It is still an area which is being learned and studied. It is also a very controversial issue. While many people believe that we do not negotiate with terrorists, Mr. Harley argues in his chapter of the Good Practices in Counter-Terrorism Handbook 2 that we do negotiate with terrorists and if we are to negotiate with terrorists, let's do it right. However, there are multiple countries where it is illegal to negotiate with terrorists. However, there are also multiple examples of negotiations with different terrorist groups, i.e. the FARC and Northern Ireland.

This presentation is a follow-up and an update of Dr. Harmonie Toros', "Terrorism, Counter-terrorism and Conflict Resolution: Building Bridges" paper, written for the NATO COE DAT in 2015. Mr. Harley has simplified the terminology for his chapter in the Counter-Terrorism Handbook as "before the shooting starts, once the shooting has started and after the shooting has ended". Conflict Resolution is a process whereby to avoid the conflict. While it is not always possible to avoid political conflict, it might be possible to avoid a conflict that branches into political violence and therefore, terrorism. Peace-making is often done in the middle of terrorist campaign while peacebuilding is a neglected area, done after violence has ended. Nevertheless, there is still much work to be done.

In terms of literature review, there are several updates on the subject matter since 2015, providing key developments in understanding negotiated settlement in counter-terrorism, including Sarah V. Marsden "Re-integrating Extremists: De-radicalization and Desistance" (2017); Sophie Hasperslar "Proscribing Peace" (2021); Jonathan Powell and Inter Mediate. Overall, preventing and countering violent extremism (PCVE) and how it integrates with the rest of the broader counter-terrorism campaign is still an issue to be studied on.

Case studies

In terms of case studies between 2015 and 2021, an example of “success” is seen in Columbia with the FARC while examples of “ongoing efforts” include Somalia’s al-Shabaab and South Sudan. Mr. Harley has previously led the British Government’s efforts in negotiating with the senior members of al-Shabaab and seen it work in limited sense. Examples of “no success” are seen in Yemen with the al Qaida; Boko Haram in Nigeria as well as Daesh in Iraq and Syria. Afghanistan and the Taliban is still an ongoing and a controversial case, which could be seen in a context of a negotiated settlement, however, the issue is still very new to comment on. Nevertheless, Mr. Harley sees the Taliban as an insurgency, not as a terrorist organization.

Conclusions

In terms of good practices in counter-terrorism and negotiated settlement, the first thing that needs to be done is to **shape the environment**. This means that we should shape both the state and the population. Therefore, we need to shape certain concepts for a negotiated settlement to take place. Another issue is defections, which can offer an insight to the organization, they damage the organization as well as damage the reputation of the organization.

Remote negotiations can be a useful approach – putting terrorist organizations out of their environment, i.e. negotiations with FARC as well as negotiations with the Taliban in Doha. Furthermore, negotiations are usually conducted in secrecy. One of the reasons for this is the approach of “we do not talk to terrorists” but also, these issues are overall delicate to discuss in public. There are negotiations which do not benefit from interference or observation or unwanted inputs of politicians, news media and the population itself.

Another important aspect of a negotiated settlement is who to include? The answer is – **everyone**. If you exclude anyone from a negotiated process, it will not work. This has been known already from the 1970s and 1980s with the example of Northern Ireland and is also apparent with the FARC. In terms of the role that individual states can play, sometimes bringing in a country that is not particularly involved in the issue but has an interest, has proven to be useful in negotiated settlements. For instance, Cuba provided support to the talks with the FARC while Switzerland and Norway provided neutral observers and interlocutors. The European Union has recently been looking into viable interlocutors to talk with the al-Shabaab in Somalia. In case of South Sudan, both neighboring countries, Kenya, and Ethiopia, have

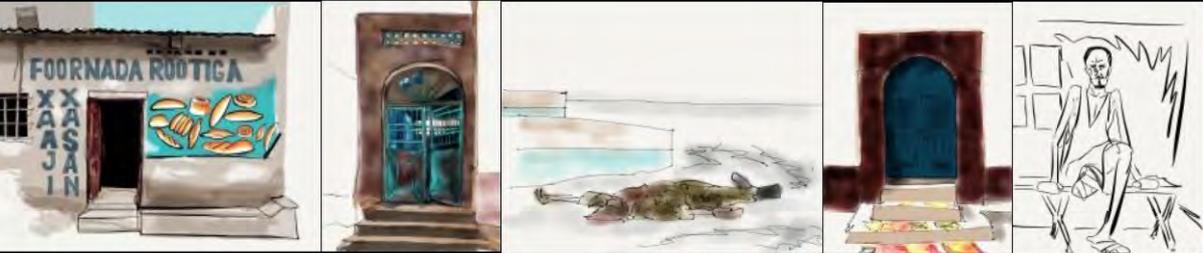
supported the negotiating process with symbolic results. The international community also has a strategic role in negotiations. The EU has been supporting Somalia and was willing to payroll the process by engaging a country like Pakistan or Indonesia.

In terms of peacebuilding, this has been a neglected concept. As such, good practice is involvement in the political process of the former terrorist – we cannot isolate them from the process. However, this has been proved to be very difficult in Columbia (FARC) and Northern Ireland. Moreover, the need for justice is often neglected and this continues to be so in Northern Ireland. An aspect that continues to be and issue is the forgiveness, amnesties, and justice. How to reconcile that with the prosecution of former soldiers or historic defenses? These are issues that need to be considered in a negotiated settlement. In terms of amnesty, the question is who gets and does not get amnesty? When we talk about amnesty, there is a level of risk, the level of seniority as well as issues with national and international law.

In terms of next steps, this is a challenging long-term process. Finally, there will be setbacks and resistance. There will be people trying to resist the process, i.e. members of states and political parties in the country who may not want the process to succeed. In the UK and Northern Ireland, Brexit vote has already had ramifications in the peace process. There have also been missed opportunities – exploring why some terrorist groups do not want to negotiate as well as why we want to negotiate with some groups and not with others.

Presentation

Stephen Harley
CT/Strat Comms Consultant,
Somalia Area Specialist



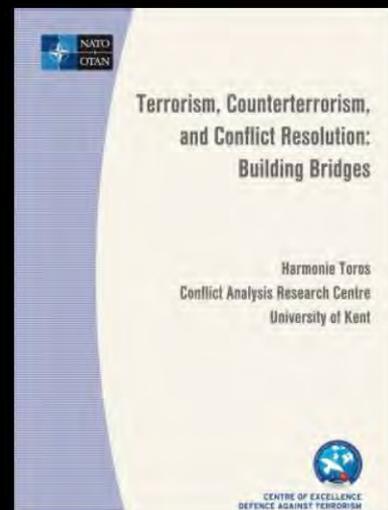
stephenharley@me.com
Twitter/Tumblr/WordPress: OurManontheHorn

Good Practices in Counterterrorism: Negotiated Settlement with Terrorist Groups



Introduction

- **Dr Harmonie Toros, 'Terrorism, Counterterrorism and Conflict Resolution: Building Bridges' (NATO COE DAT 2015)**
 - **Brief summary of key concepts:**
 - **Conflict Resolution**
 - **Peacemaking**
 - **Peacebuilding**
 - **Reference to Case Studies**
 - **Return to the Northern Ireland 'Good Friday Agreement' Case Study**
 - **Summary of previous recommendations**



Introduction

- **Key developmens in understanding Negotiated Settlement in Counterterrorism**
- Sarah V Marsden, 'Reintegrating Extremists: Deradicalisation & Desistance' (2017)
- Sophie Hasperslar, 'Proscribing Peace' (2021)
- Jonathan Powell & Inter Mediate
- Preventing & Countering Violent Extremism
- **BEYOND THE SCOPE OF THE PAPER**



CASE STUDIES

EXAMPLE OF SUCCESS

- **COLUMBIA: the FARC**

EXAMPLE OF ONGOING CHALLENGES

- **SOMALIA: al-Shabaab**
- **SOUTH SUDAN**

EXAMPLES OF NO SUCCESS

- **YEMEN: al-Qa'ida**
- **NIGERIA: Boko Haram**
- **IRAQ/SYRIA: Da'esh**

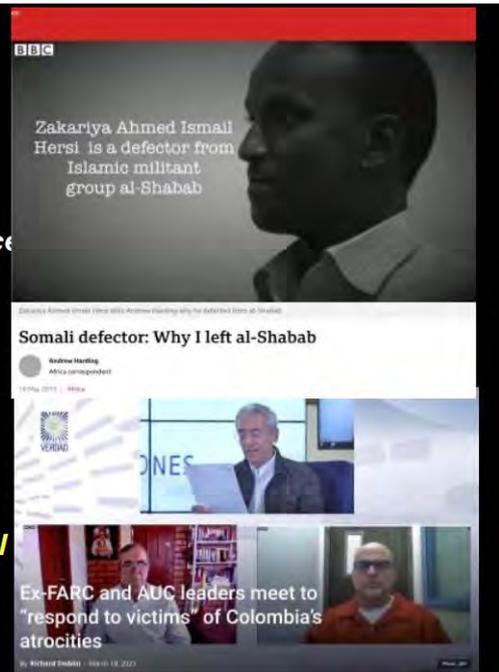
AND...

- **AFGHANISTAN: the Afghan Taliban**



CONCLUSIONS

- **Shaping the environment for negotiated settlement:**
 - Terrorists, the state and the populace
 - Defections
- **Remote negotiations**
- **Secrecy:**
 - Engagement, exploratories, negotiation, agenda, deals
- **Inclusion**
- **The role of individual nation states**
- **The strategic role for the international community**



CONCLUSIONS

- **Shaping the environment for negotiated settlement:**
 - Terrorists, the state and the populace
 - **FARC, Somalia**
 - Defections
 - **Somalia**
- **Remote negotiations**
 - **FARC, the Afghan Taliban**
- **Secrecy:**
 - Engagement, exploratories, negotiation, agenda, deals
 - **FARC**



CONCLUSIONS

- **Inclusion**
 - **FARC**
- **The role of individual nation states**
 - **FARC, Somalia, South Sudan**
- **The strategic role for the international community**
 - **FARC, South Sudan, Somalia**



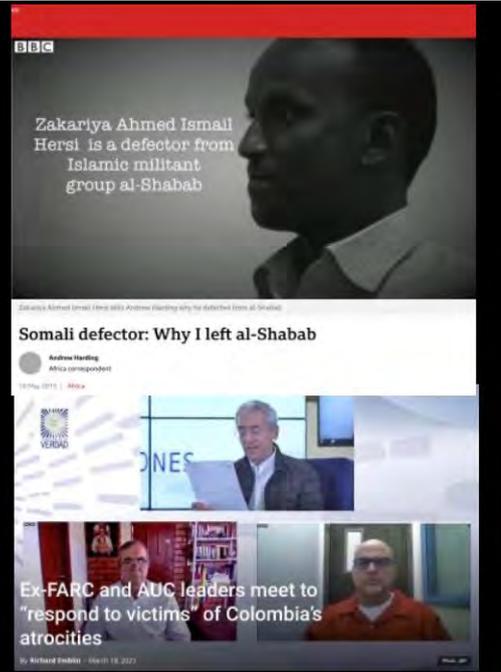
CONCLUSIONS

- **The next steps**
 - **Involvement in the political process**
 - **FARC, Northern Ireland**
 - **Justice**
 - **FARC, Northern Ireland**
 - **Amnesty**
 - **Somalia**



CONCLUSIONS

- **Setbacks**
- **Resistors**
 - **FARC, Northern Ireland**
- **External events**
 - **Northern Ireland**
- **Missed opportunities**
 - **Iraq/Syria, Niger Delta, Yemen**



Community Policing

Dr. Richard WARNES (GBR)

Senior Consultant at Vedette Consulting

Dr. Warnes gave a comprehensive overview of the Community Policing chapter to the Good Practices in Counter-Terrorism Handbook 2, in particular, engagement with local communities in order to build a level of trust as well as building a relationship with that community. Closely associated with this, is the concept of the “procedural justice model”, arguing that if the police engage with community and if the transactions with the community are fair and just, that itself can help build a level of trust with the community, enhancing the legitimacy of the police as well as enhance the level of institutional authority. However, if engagement with the police within the community is poor and unjust, this also destroys trust building and weakens institutional authority. This model is transferrable to military and military aid to civilian authorities’ operations and overseas counter-terrorism/counter-insurgency. Overall, we are talking about individuals, personal relations and engaging with communities overseas with the goal of gaining and maintaining popular support to ultimately develop local community intelligence.

Examples

In terms of CT policing, in France, there have been couple of examples in which local landlords were suspicious about the behaviour or actions of people staying in their properties, i.e. a Spanish couple paying rent three months in advance in cash, which later led to an investigation and a Franco-Spanish counter-operation, leading to the arrest of the couple later on as well the incident with ETA military wing leaders in 2002, that was done in cooperation with local intelligence and suspicion by the local community. In terms of counter-radicalization, understanding local communities and building engagement, there is a better chance of preventing and understanding people who may be vulnerable to radicalization. Domestic military aid has been used in Ireland and later in France in 2015 in which military was seen as being deployed on the streets after attacks for public reassurance and security protection while in Spain in 2004, Spanish military was deployed in working on public transport while the public felt more secure during those times.

However, there is a flip side to this and negation of trust such as historical legacies. In Ireland, police have a close relationship with much of the community but why? Mostly, because of the white male background, but the level of trust is not the same with minority populations or having the right language skills. In France, even now, there is particularly older generation who are worried to talk to the police because of what happened during the WWII. In Spain, there have been previous issues of police enforcing the regime, i.e. the Francoist 'Legacy of Fear'. However, the issue is not only with the police but the military as well. In the UK, the Operation BANNER and al-Qaeda related concerns in the Heathrow Airport in 2003, engagement of military around the airport and land was not welcomed by the local population.

Overseas Counter-Insurgency

In terms of transferability of overseas counter-insurgency, one of the main pillars is to gain and maintain popular support. Unless security forces gain and maintain level of support and confidence, the chance of success is greatly reduced. Building trust helps to increase influence and generate influence. However, a negative side arises when military takes the whole population overseas as hostile, and this reduces support from the local community. As such, lack of understanding of the local community can build in fear from the side of the military. For instance, in Bosnia and Herzegovina, the UK military deliberately did not wear full body armour and helmets as this would have decreased the chances of understanding the situation on the ground and building trust within the community.

In terms of enablers, the use of community and culture, it is critical to take advantage of local community and culture – “cultural asymmetry”. That means, learning as much as possible of their culture and language, even if it is basic greetings. If there are members from the security forces who speak the same language, they are invaluable. For instance, in Afghanistan, officers were trained to speak Pashto, i.e. what the local people called the *Queen's Pashto*, but they did not know some of the local words or nuances. In Turkey, there is a “cultural understanding of terrorism.” However, sometimes police forces are far better in understanding religious aspects than understanding leftist terrorist groups and where their views are coming from and their mind-set. In Israel, the use of *Mista'Aravim*, who often speak Arabic in home environment, coming from different communities and able to disguise themselves to look like Palestinians. This has been similar to France and Spain, having a “Military Cultural pool”. Security forces

have also supported local community members becoming additional “eyes and ears”, like the local security guards, i.e. in Turkey, the “Temporary Village Guards” to provide additional security in the community.

HUMINT and Surveillance

Ultimately, with all these enablers, the ultimate aim is to develop human intelligence and capabilities. The understanding of local communities is critical in providing covert intelligence methodologies of HUMINT and Surveillance and see who is active in the community, who is supporting terrorist elements etc. Hence, understanding the community and understanding threats and dangers is important.

Conclusion

Best practices include building up trust from the bottom upwards – training and understanding of culture and history; community engagement; use of “cultural asymmetry,” understanding of “human terrain” where you are operating, recruitment of “unlikely counter-terrorists”, as well as the development of HUMINT and surveillance. One of the examples of this includes Andrew ‘Isa’ Ibrahim in 2008, about to carry out a suicide attack in Bristol on which the local community reported him to the police beforehand.



NATO COE-DAT
Terrorism Experts Conference (TEC)

Community Policing

12-13 October 2021

Dr. Rich Warnes (Senior Consultant, Vedette)

1

Intro - Community Policing & Transferability

Community Policing: Engagement with local communities –
Development of relationships – Building of Trust

“Community policing is, in essence, a collaboration between the police and the community that identifies and solves community problems. With the police no longer the sole guardians of law and order, all members of the community become active allies in the effort to enhance the safety and quality of neighbourhoods.” US Bureau of Justice Assistance 1994

Procedural Justice Model: Engage community → fair & just
→ build trust → enhance legitimacy → institutional authority

Transferability: Military - Domestic MACA - Overseas CT /
Counter-Insurgency

‘Gain & Maintain Popular Support’: Legitimacy & Engage
population to develop local community intelligence



2

Intro - Community Policing & Transferability

Community Policing: Engagement with local communities –
Development of relationships – Building of Trust

“Community policing is, in essence, a collaboration between the police and the community that identifies and solves community problems. With the police no longer the sole guardians of law and order, all members of the community become active allies in the effort to enhance the safety and quality of neighbourhoods.” US Bureau of Justice Assistance 1994

Procedural Justice Model: Engage community → fair & just
→ build trust → enhance legitimacy → institutional authority

Transferability: Military - Domestic MACA - Overseas CT /
Counter-Insurgency

‘Gain & Maintain Popular Support’: Legitimacy & Engage
population to develop local community intelligence



2

Examples: CT Policing & Domestic MACA

CT Policing:



- France – Local Landlords –
 - ARB Explosives 1999
 - ETA Military wing Leaders 2002
- UK – Operation Crevice 2004 - Storage Worker

- Counter-Radicalisation – P/CVE – Prevent & ‘Safety Houses’

Domestic MACA:

- Ireland – ATCP during the ‘Troubles’
- France – *Vigipirate & Sentinelle*
- Spain – CNI & post Atocha 2004



3

Examples: Negation of Trust – Police/ Military

Police:

- Ireland – Republican understanding... But lack of minority 'Cultural Interface'
- France – Historical 'Legacy of Fear' from collaboration
- Spain – Francoist 'Legacy of Fear'



Military:



UK – Op BANNER - MACA support to RUC not mainland – Heathrow 2003 *al-Qaeda* threat

US – *Posse Comitatus* 1878 – Hence FBI HRT

Israel – Conscription & *Milum*... 'Right of passage' –

Different perspectives from Palestinian community



4

Overseas Counter-Insurgency



- 'Gain and Maintain Popular Support':

"Gaining and maintaining popular support is an essential objective for successful counterinsurgency. It gives authority to the campaign and helps establish legitimacy. Unless the government gains its people's trust and confidence, the chances of success are greatly reduced." British Army Field Manual, *Countering Insurgency*, 2010

- **Application:** Influence, Separate insurgents from community, Reduce support, Generate intelligence
- **Community Engagement vs. Force Protection**

"Rather than working with the population so as to protect them from the insurgents, some units, because of their lack of situational awareness and personal relationships with the people, tended to treat all Iraqis as a potential threat and thus adopted a high-handed approach that alienated the population. This exacerbated the backlash against their presence, discouraged people from coming forward with information about the insurgents and thus further reduced these unit's situational awareness, leaving them trapped in a vicious cycle of intervention and rejection."

Kilcullen, *The Accidental Guerrilla*, 2009



5

Enablers: Culture & Unlikely Counterterrorists

- **Community & Culture:** 'Cultural Asymmetry' - Linguistic, cultural, religious & historical understanding of 'Human Terrain' –
 - UK – Queen's Pashto
 - Turkey – Cultural understanding of terrorism
 - Israel – *Mista'Aravim*
 - France & Spain – 'Military Cultural pool' – Foreign Legion & Spanish Legion

- **Unlikely Counterterrorists:** Support of local community members becoming additional 'eyes & ears'

- Local Security Guards
- Business, especially 'dual purpose technology'
- Turkey – GKK 'Temporary Village Guards'



6

HUMINT and Surveillance

- **Human Centric Intelligence:** Such community support can benefit more covert intelligence methodologies of HUMINT and Surveillance –

- **HUMINT**

- UK – FRU vs. PIRA
- CT HUMINT
- Afghanistan – Legacy Programme



- **Surveillance**

- France & Spain – Franco-Spanish Teams vs. ETA
- UK – RUC E4A & 14 Intelligence Company vs. PIRA
- Ireland – Garda NSU vs. Crime-Terrorism Nexus



7

Best Practice & Conclusion

- **Best Practice:**

- Training & understanding of culture & history
- Community engagement
- Application of PJM principles
- Use of 'Cultural Asymmetry'
- Understanding of 'Human Terrain'
- Recruitment of 'Unlikely Counterterrorists'
- HUMINT & Surveillance



- **Examples**

- Andrew 'Isa' Ibrahim 2008
- Gen. Rupert Smith – 'War Amongst the People'- Intelligence to target the insurgents and minimise collateral impact on local community

- **Conclusion**

Ultimately, it is argued that such approaches can assist in the identification of terrorists, insurgents and their support networks, exploiting and operating inside local communities.



8



Thank You – Any Questions?



vedetteconsulting.com

Gender Specific CT Policies

Dr. Zeynep SÜTALAN (TUR)

Atılım University

Introduction

In the presentation, Dr. Sütalan focused on gender-specific counter-terrorism policies with cumulative insights from NATO COE DAT's "Gender in Terrorism and Counter-Terrorism: Data, Analysis, and Responses Workshop" in June 2021. Gender-specific counter-terrorism policies are the policies which are formulated and implemented through prioritizing gender differences in efforts to prevent and respond to the terrorist threat and incidents. Within the broader framework of gender, this presentation focuses primarily on women. Therefore, it is intended to present a picture to what extent women, their roles and needs are taken into consideration in countering-terrorism and what should be done to overcome existing shortcomings.

Before underlining the need for gender-sensitiveness and gender-responsiveness in counter-terrorism, it is important to underline **what gender is**. Even in case one focuses on women, it is not possible to reduce it to women, because gender is not only about "being a woman" or "a man", but about expectations, opportunities, and norms about being a man and being a woman. Gender also encompasses the relationship between men and women including the power relations between men and women, so gender is 'relational', and one cannot talk about women without their relation to men and masculinities. Gender is socially constructed, but "seeing gender as a social construction does not mean it is not real or not experienced in social and political life. Instead, gender as a social construction is a crucial element of how people go through their lives."

Additionally, since gender is one of the many identities of individuals, it is much better to consider how gender intersects with other identities like race, religion, ethnicity, and class. As such, being an educated woman in a middle-class society does not correspond for the same thing as being from uneducated, poor refugee woman in the same society. These two women can both become terrorists as there is no profile of a woman terrorist as we do not have a profile of male terrorists but reintegration of these two women into the society significantly differs once they are disengaged from terrorism. Therefore, it is this kind of awareness that should be

promoted and integrated in terms of policy-making and programming of CT. Moreover, mainstream security thinking sees terrorism as a “young man’s adventure” and women’s involvement in terrorism as coerced or duped, by seeing primary motivation of female involvement in terrorism as personal. However, women have always been involved in terrorism.

What we should also be aware of is that there are gender dynamics at play, between terrorist organizations and states; between states; as well as among members of same terrorist organizations. Research indicate that women tend to be drawn more to domestic terrorist groups (notable exception of Daesh), also as leaders and in combat roles. In order to understand and then efficiently respond to the gender aspect of terrorism, it is critical to recognize the different roles played by women in terrorism and evaluate these roles in the broader context of gender. Women’s ‘other’ roles in terrorism as sympathizers, supporters, radicalizers, recruiters, facilitators, and financiers are not acknowledged like the fact that historically women have always been part of terrorism. From a threat analysis perspective, turning a blind eye to the agential power of women in terrorism leads to security gaps and insufficient CT programming.

Gender-Specific CT Policies

In terms of how the international community started talking about gender-sensitiveness and for what the gender-responsiveness in CT is concerned, it is important to underline that few developments have reinforced the need for gender perspectives in CT, i.e. the need for deploying women officers on a tactical level. In line with the counter-insurgency (COIN) perspectives of winning the hearts and minds of people, women as mothers had a critical role in societies, having a critical value for intelligence gathering and community engagement. Moreover, one of the first developments of the subject matter was the onset of the global framework of Women, Peace and Security (WPS) by the adoption of the United Nations (UN) Security Council Resolution 1325 in 2000. Admitting the differential impact of armed conflict on women, girls and children, the international community recognized the need to include women in building and maintaining peace and security. With the UN Security Council Resolution 2242 in 2015, the WPS agenda joined together with the CT and countering violent extremism (CVE) efforts.

Another development that reinforced recognition of the need to have gender-responsive CT policies was the challenge posed by returning and relocating Foreign Terrorist Fighters (FTFs).

Daesh terrorist organization became a global threat, and the issue of individuals going to Syria and Iraq to join Daesh led the issue of FTFs to become a concern for most of the nations in the world. The threat became more visible with the issue of returning or relocating FTFs. Returnees are perceived to pose a threat to the national security of individual nations. However, it was predominantly male FTFs who engaged in terrorist acts that are thought to be the source of the threat, but if women travelled to the conflict zone to somehow join the terrorist organization pose a security threat differed according to national perceptions, because the approach to the women in Daesh issue was very much dominated by the gender stereotypes. The acuteness of the threat and the challenges of responding to FTF threat, especially the question of how to deal with the women, girls and boys associated with Daesh upon the end of the Daesh control over territories in Iraq and Syria compelled the individual nations and the international community to revise their approaches to CT, particularly the neglected gender dimension of the present terrorist threat and the response lacking gender-sensitive approach.

Gender Dimension of Prosecution

When it comes to the gender dimension of prosecution, research indicate that there is gender disparity in criminal justice processes. Often, women escape prosecution processes or get softer sentences compared to their male counterparts. The starting point is the **criminalization of terrorist offences**. There comes in the importance of the awareness on the different roles played by women in terrorism. What we know as of today is that women are predominantly performing ‘support roles’ in transnational terrorist networks especially the ones based on religious extremist ideologies as in the case of Daesh. These support roles can be defined as functional roles performed to help planning, preparation or perpetration of terrorist acts by providing logistical and financial support or assisting in recruitment. Therefore, it is highly important to criminalize such roles. In some national legislations, acts other than conducting terrorist act is not criminalized. This turns out to be one of the reasons why women associated with terrorism escape prosecution. Moreover, Dr. Hodwitz has pointed out in the NATO COE DAT’s 2021 “Women in Terrorism and Counter-Terrorism Workshop” that present research is based on particular case studies and qualitative research. However, we need to have more quantitative research based on sex-aggregated data to come up with definitive conclusions.

Once women’s engagement with terrorism is regarded as a security threat and their acts are criminalized in legislation, women convicted of terrorist or terrorism-related offences are getting lenient sentences because their criminal intent is thought to be tempered by emotional

drivers or misguided beliefs. These kind of gender-stereotypes are also exploited to escape prosecution by the female terrorist suspects to escape prosecution by building the defense on the argument of being deceived. Therefore, it is important to note that gender-stereotypes based on the victimhood of women create blind spots that works in favor of the women who are not only victims in their association with terrorism, paving the way for re-radicalization and further recruitment.

Gender-Responsive Rehabilitation and Reintegration

Gender-responsiveness in Disengagement, Rehabilitation, and Reintegration (DRR) of former terrorists is no better compared to the problems about gender disparity in the prosecution of suspected terrorists. What is meant by gender-responsive DRR is gender-specific disengagement, rehabilitation and reintegration measures which are tailored according to the needs of women, girls, men, and boys, and guarantee equal access of these different groups to the support and services provided. While these measures should take into account the different sexes, femininities and masculinities, they should also ensure the protection of the rights of these different groups.

Today women do not have access to de-radicalization, rehabilitation, and reintegration programs, because they were tailored to men, women may be convicted of crimes not directly linked to terrorism – which is a requirement for program entry or there is no perceived threat from potential radicalization of female detainees. Gender-responsive rehabilitation and reintegration programs is a prerequisite in order to eliminate the terrorist threat including the prevention of recidivism and further terrorist recruitment.

While developing gender-responsive Disarmament, Demobilization and Reintegration (DRR) programs in CT, it is critical to bear in mind the historical global experiences and lessons learned from similar processes such as the past or continuing DDR programs. Experience with DDR programs have shown that when they are not gender-sensitive or gender-responsive, they do not work for women or they are not embraced by women. Apart from the DDR experiences, the Nigerian experience with Boko Haram displays those similar problems apply to the CT context. It was reported that some women who survived Boko Haram and went through de-radicalization programs go back to the terrorist organization, because they faced social marginalization, stigmatization and they neither have security nor minimum economic standards to pursue a life in dignity. One of the points that should be raised is analysing social status and power of women before and after they are part of a terrorist group in DRR processes

is essential to provide them with suitable skills for their reintegration into the society. It is also important to keep in mind that effectiveness of the reintegration policies is dependent on the elimination of the socio-economic, political conditions as well as discriminations and injustices that are conducive to breeding violent extremism that leads to terrorism.

Recommendations

When it comes to the recommendations, gender-sensitive CT policies should **recognize women's agency and different roles in terrorism and CT**. Such policies should be **tailored according to the gender-specific needs** and be human rights compliant. For that, gender-sensitive CT policies should be based on assessment of gender dynamics in societies before and after terrorism and gender roles of individuals in and out of the terrorist organization. Therefore, gender sensitive CT policies should **include efforts for criminalization of offences other than the conduct of a terrorist act** as well as **gender training for the professional groups** including judges, prosecutors, law enforcement personnel, military personnel, social services personnel.

Moreover, gender-sensitive CT policies should ensure the implementation of “whole of government approach” and “whole of society approach” as well as consider the value of “whole of person” approaches to rehabilitation and reintegration. It should also ensure **inclusion of diverse stakeholders** including women's organizations; representation of women at all levels of security sector as well as ensure meaningful representation of women. It should also include efforts to prevent the ground that terrorism might flourish together with efforts of rehabilitation and reintegration.

Gender-specific Counter-Terrorism Policies

Dr. Zeynep Sotalan
zeynepsotalan@gmail.com
COE-DAT Terrorism Expert Conference
12 October 2021

CONTENT

- Gender Aspect of Terrorism
- Gender Dimension of Prosecution
- Gender- Responsive Rehabilitation and Reintegration
 - with special emphasis to FTF challenge
 - including good practices (present initiatives-not many) and recommended good practices

Gender ...

“ [...] genders are the characteristics associated with expectations of “being a man” or “being a woman”. Gender, then, describes the socially constituted behavioural expectations, stereotypes, and rules that construct masculinity and femininity. These socially constituted differences are intersubjective and constantly evolve as they are intentionally manipulated or affected by changing social norms. [...] Seeing gender as a social construction does not mean it is not real or not experienced in social and political life. Instead, gender as a social construction is a crucial element of how people go through their lives.”

Laura Sjoberg, Grace D. Cooke, and Stacy Reiter Neal, “Introduction: Women, Gender and Terrorism” in Laura Sjoberg and Caron E. Gentry (ed.s), *Women, Gender, and Terrorism* (Athens & London: The University of Georgia Press, 2011), 6.

Gender Aspect of Terrorism

- Terrorism is gendered.
- Mainstream security thinking sees
 - terrorism as “young man’s adventure carried out by the band of brothers”
 - Katherine E. Brown, “Once a Terrorist, Always a Terrorist? How to Respond to the Women of Daesh?” *RUSI Newsbrief* 39, no.1 (January/February 2019).
 - women’s involvement in terrorism as coerced or duped
 - primary motivation of female involvement in terrorism is seen as personal.
- Women’s different roles in terrorism should be recognized and evaluated in the broader context of gender.
 - We are accustomed to view women as victims in their links with terrorism
 - We are less mindful of the other roles play by women as sympathisers, supporters, radicalizers, recruiters, facilitators, perpetrators, ...
 - Historically, women have always been part of terrorism

Gender Dynamics

“Gender relations happen among members of terrorist organizations, between terrorist organizations and their target audiences, between terrorist organizations and states, and between states.”

Laura Sjoberg and Caron E. Gentry, *Women, Gender and Terrorism*, (University of Georgia Press, 2011), 7.

- In line with different gender dynamics at play, research indicate that women tend to be drawn more to domestic terrorist groups (notable exception of Daesh);
- In domestic groups do engage as leaders and in combat roles
- In transnational groups, fewer numbers, more likely as support roles, service roles, sympathisers, spies, logistical roles.

Gender-Specific CT Policies

- How did international community start talking about gender-sensitiveness and/or gender-responsiveness in CT?
- Few developments have been reinforced the need for gender perspectives in CT
 - Operational needs
 - Tactical level: need of searching women
 - Community engagement, intelligence gathering
 - UNSCR 1325 and the Women, Peace and Security (WPS) Agenda
 - UNSCR 2242 merged CVE, CT and WPS
 - The challenge posed by returning and relocating Foreign Terrorist Fighters (FTFs)

Gender Dimension of Prosecution

- Women escape prosecution processes or get softer sentences compared to their male counterparts
 - gender stereotypes: underestimating women's agency
 - national legislations do not criminalize support roles
 - difficulties in evidence- obtaining
 - place of the offence
 - women exploit gender-stereotypes to escape prosecution- they built their defence upon the argument that "they are deceived".
- Gender-stereotypes based on the victimhood of women create blind spots that works in favour of the women who are not only victims in their association with terrorism.
 - Re-radicalization, further recruitment, returning back

Gender Responsive Rehabilitation and Reintegration

- Women do not have access to de-radicalization, rehabilitation and reintegration programs;
 - Tailored to men
 - Women may be convicted of crimes not directly linked to terrorism –which is a requirement for program entry
 - No perceived threat from potential radicalization of female detainees
- LL should be inferred from DDR (Demobilization, Disarmament and Reintegration) processes, even to be adopted in CVE
 - Obstacles to access assistance
 - Fighting against stigmatization
 - Providing women with vocational training and jobs
 - Ensuring their security and physical well-being
 - ...

Recommendations

- Gender-sensitive CT policies should;
 - Recognize women’s agency and different roles in terrorism
 - Avoid gender-stereotyping as well as gender essentialism
 - Assess gender dynamics in societies before and after terrorism and gender roles of individuals in and out of the terrorist organization
 - Be tailored to gender-specific needs and human rights complaint
 - Include efforts for criminalization of offences other than the conduct of a terrorist act
 - Include gender training for the professional groups including judges, prosecutors, law enforcement personnel, military personnel, social services personnel

Recommendations

- Gender-sensitive CT policies should;
 - Ensure the implementation of “whole of government approach” and “whole of society approach”
 - Consider the value of “whole person” approaches to rehabilitation and reintegration
 - Ensure inclusion of diverse stakeholders including women’s organizations
 - Ensure representation of women at all levels of security sector
 - Ensure meaningful representation of women
 - Include efforts to prevent the ground that terrorism might flourish together with efforts of rehabilitation and reintegration

DAY I – SESSION 1: Questions and Open Discussion

Asst. Prof. Omi HODWITZ

- 1. What is your opinion about poor/tolerant CT legislation? Is it taken into account by terrorists' individual/groups, in order to plan/prepare/recruit/fund/execute their actions?**

Dr. Hodwitz stressed that all academics would say that more research is needed. However, as a criminologist, Dr. Hodwitz focuses on data that applies to both political and apolitical deviant positions. Within the first question, there is notable difference between political and apolitical deviance. Apolitical deviance tends to focus on legislative repercussions for themselves, but we do not see the same for political population, with the latter focusing mostly on success and their ability to accomplish their goals. With the limited research of what we have, indicates that regardless of the nature of the CT legislation applied, it only influences individual and group level decision-making rather than survival of the group.

- 2. Is there a difference between the rates of male and female extremists re-engaging with the terrorist organization? If yes, what are the ratio differences according to the counter-terrorism models?**

As for the second question, there is also a huge deficit here. We do not know much about differences between male and female re-engagement. We have limited qualitative data that allows us to examine re-engagement between the two gender groups but on an aggregate level the research simply is not there. Dr. Hodwitz' previous research has been focused on primarily males while her own dataset includes also female offenders, however, on a small level. Therefore, on an aggregate level, it is not possible to make conclusions out of it.

Mr. Stephen HARLEY

- 1. In the military perspective, the Centre of Gravity (CoG) is “the source of power that provides moral or physical strength, freedom of action, or will to act. Analyzing CoG to understand the critical capabilities and vulnerabilities of terrorist organizations, is there any example using CoG approach in the reconciliation process?”**

The answer is yes, in particular, when it comes to the shaping period of a negotiated settlement. In Somalia, we have changed terminology compared to Iraq and Afghanistan and now work on understanding the organization and dynamics instead. **Understanding the organization** is the important element that we as negotiators prioritize. “Clearing”, “building” and “holding” will not achieve long-term security – we now understand “negotiate secure”. That fits the CoG – you need to understand the organization.

In terms of understanding terrorist groups, we are not only shaping terrorist groups but also shaping ourselves and elements of the state. We need to recognize that terrorist groups are not homogenous, they do not point to the same direction, all the members do not have the same reasons for entering, i.e. money, revenge, excitement and ideology – we need to understand all these dynamics. If we understand the group, we have a better chance in identifying elements that can be negotiated with. The Centre of Gravity can then easily be adapted to the group. We as NATO nations would not get away with same approaches that were used against the Tamil Tigers or the Chechens – we need to think about it differently. We need to think about the continuum that leads to negotiated settlement, i.e. defections. A broader organizational settlement is the most useful aspect. However, this does not only relate to terrorist groups – we also need to understand ourselves. One of the reasons that we did not do well in Afghanistan is the fact that some individual nations did not do particularly well in that mission is that they did not understand themselves, let alone terrorist organizations.

- 2. We say that terrorist organizations are acting in irrational way, in your personal negotiation period, did you experience that level of irrationality?**

We often act irrational as well - know ourselves as well as know our enemy. Often, the enemy is us. We have to think about – irrational to who? My experience with terrorist organization is that they act quite predictably, sometimes it is us who act irrational.

- 3. As a case study, MILF (Moro Islamic Liberation Front), Philippines, is good for research because this terrorist organization got agreement with the Philippines government through long negotiations. What is your opinion on this?**

This is a very good case study and is mentioned in Dr. Toros' 2015 COE DAT paper. But this is now a more historical example. There are two elements to point out – one is to do with spoilers coming from within state politics. Either agreeing with the process or elements seeking political gain. Some elements in the Philippines asked the United Nations not to list the MILF as a terrorist organization, indicate that the Philippines' authorities themselves can decide whether it is a terrorist organization or not. There will always be domestic local issues, even with groups like al-Qaeda. Therefore, we need to look things on a global strategic and tactical level.

- 4. Powell has said that there are many difficulties to negotiate with terrorists. One of the difficulties is the separation. Even though a government may get an agreement with a terrorist group, some people who do not agree with such negotiation, may create another terrorist organization. What is your opinion on this?**

I completely agree – this is another end of the spoilers-defectors aspect. We have plenty of historical examples splitting up from the terrorist group, i.e. ETA. It is all about familiarizing ourselves what are the historical examples and what to expect. The issue in Northern Ireland is still an ongoing issue.

- 5. What is the current influence of al-Qaeda to the Taliban movement, Boko Haram and al-Shabaab?**

In terms of observation, I would steer you towards a podcast of “The Long War Journal”. They highlight that one of the key elements they pointed out was that Taliban should disconnect from al-Qaeda. In terms of al-Shabaab, they have very clear links with al-Qaeda. They swore allegiance to al-Qaeda in 2012. Many senior al-Shabaab commanders have fought in Afghanistan with al-Qaeda. Nowadays its relationship is different – al-Shabaab sends third of its money to al-Qaeda to be left alone, basically provide money to al-Qaeda. Al-Shabaab does not take foreign fighters and does its own thing. There is always a local element. As for the Boko Haram, they swore allegiance to Daesh in 2015. Al-Qaeda has no influence of it as far as I know. There is also another mysterious group in Mozambique, one day they are call al-Shabaab, the next day something else. No one is quite clear but there seems not to be any al-Qaeda link to it, but perhaps with Daesh.

Dr. Richard WARNES

1. What do you consider as Best Practice, in switching what is considered by community as “snitching” to collaboration?

The first factor you need to consider is that you may be dealing with different communities and this thinking will differ significantly between different communities – this comes back to “cultural understanding”? How would a community react to cooperation with security forces? No one size fits all. Some communities would react very violently, or other communities would not respond in the same way. As such, understanding different responses from the community is the key.

The second point is the criticality, the need to do firewall between the wider community engagement with the intelligence collection – they have the carefully be firewalled. Source protection is important – if you do not protect the source, who else would give you information? But it is also trying to maintain that level of trust with the community. So, firewalling those two aspects is absolutely critical. An example of this is the UK Prevent Strategy, designed as part of four responses, including the UK’s CT Strategy. The program is aimed at trying to stop or prevent radicalization but also to help with

disengagement and desistance. There is lack of trust within the Muslim community in the UK to such an extent that Prevent is referred as having toxic associations. As such, “snitching” collaboration has to be done very carefully. For instance, in Spain, when you are from certain Basque villages, it is very difficult to go into other Basque villages because you are immediately seen as being a suspect. In Spain, it was a complex mixture of human and technical intelligence used.

Overall, it is a long-term approach – you need the firewalling, you need the separation, but you also need to engage with that community and use information operations to build wider community trust over a longer time. But the criticality of that is that you cannot wait until long-term relationship building and in shorter term, you may have to develop covert intelligence sources in legal terms. The flip-side of this is an example from Kilcullen – if you do not build trust within a community, you will not get any information.

- 2. By the term “cultural understanding of terrorists”, do you mean “the separation of terrorists and community?” If so, what is your advice?**

Separation of terrorists in the community is one aspect, one tool of it but by developing an understanding of the community, you can also develop a cultural understanding of the terrorists and their motivations, their operations, and how they exploit the community, i.e. with violence or financially, and how do they recruit people in that community. As such, cultural understanding is one aspect of a wider overarching thing that helps you with separation of terrorist community. It may help to separate terrorists from the community. Moreover, intelligence means to attempt to target specifically the terrorist. If you use intelligence correctly, it helps mitigate the collateral impact on a wider community and are less likely to create “accidental guerillas”. By using carefully controlled intelligence, you can mitigate those risks.

- 3. How to use the “cultural asymmetry” most effectively? Is it possible to produce a working method in few steps that the cultural asymmetry can mark the possible terrorist or to recruit an agent in terrorist?**

There is not a specific method done in a few steps because it would again be different within communities. However, any understanding of communities is of benefit. Any person from an organization who is from that community or has that cultural or language understanding is an absolute force multiplier and can assist as being a force multiplier in that community. In Afghanistan, we worked with cultural advisors as contractors, not as military and these people spoke the language and understood the culture. It was the cultural advisers telling you when not to say something and what not to do – it is also about what not to do in that community as well as the linguistic and cultural understanding that matter.

4. Could you comment on the community policing and the integration process of al-Qaeda's activity?

The original core al-Qaeda group was quite exclusive in terms of approach. An individual would show interest for certain websites and would be asked to do small tasks and then would get recruited. However, Daesh's approach is quite inclusive. For instance, Daesh would put out a message to everyone and say that anyone could be a member of Daesh and give tactical advice of what to do, i.e. on knife attacks. In terms of countering al-Qaeda networks, the main thing is community engagement and build up understanding within the community. Overseas counter-insurgency is critical because it allows you to target terrorist organizations without significant collateral damage. Therefore, one aspect to it is community engagement for understanding the community and the second, development of intelligence to understand the community domestically.

Dr. Zeynep SÜTALAN

1. By the term, “terrorism is gendered,” could you please explain your idea in broader terms, with example if possible?

The issue of terrorism being gendered may be better understood when I give an example of recruitment. Even if we talk about men’s recruitment, we should take it from a gendered perspective, otherwise we won’t understand it. If we talk about far right groups, they also used gendered norms in societies and reinforces narratives. Thinking of Daesh, they exploited unemployed but educated young men without hope for future, claiming to provide them with an opportunity to become a “real man”. When it comes to understanding why women get involved in this because their perception is being liberated from “immoral culture” or being protected in certain societies, especially in terms of hyper-masculine ideologies. When it comes to leftist organizations, terrorists discourse attacks the patriarchal order and terrorist organization claims to provide egalitarian social order, including gender equality and economic benefits. Terrorism being gendered is very much prevalent if you think of recruitment processes and the roles men and women play in terrorist organizations, they are not immune from gendered norms. Power relations do exist in the realm of terrorism as well, being gendered.

2. Women are more “emotional and intuitive than men”. Do you think that this is a disadvantage when women are involved in counter-terrorism?

I can congratulate the person who asked this question, but my answer is “no” – this is not a disadvantage. If it was a disadvantage, we would not have any women officers, for instance. Thinking of neuroscience, women’s brains function differently than men’s, but this does not necessarily mean that women are too emotional to take rational decisions. The system of women’s brain is much more complicated, but this does not mean that women are prone to take emotional decisions. We should accept these differences but in terms of intuition, this works better for women compared to men. This intuition is something we need to include in CT. When we talk about artificial

intelligence, we are saying that we need gendered perspectives, otherwise it is too dependent on male perspective which lacks certain nuances.

3. **Comment:** Terrorism is no more a domestic issue. There is a more prudent example that people are influenced with the rise of extreme ideology and fanaticism through various means, such as social network, media etc. Sometimes, this may be a proxy act of certain vested groups to de-stabilize a community or a country. How coherently this act of influencing can be countered in a comprehensive manner?

DAY I – SESSION 2: COE-DAT Research

Moderated by: Col. Daniel Wayne STONE (USAF), *Deputy Director, COE-DAT*

The main questions for the session two were intended to answer questions of what is the military's role in countering-terrorism, COVID-19 pandemic and with regards to the civil society? What are the potentially good practices for the military environment? What is the terrorism threat during peer-to-peer conventional war? Why is gender important for NATO and what does it mean to the military?

Terrorist Implications Arising From COVID-19 and Predictions to Future Terrorist Implications

Dr. Richard WARNES & Mr. Stephen HARLEY

Senior Consultant at Vedette Consulting & UK Foreign Office Advisor, British Embassy
Mogadishu

Within this research, the key overarching factors that emerged were COVID-19 pandemic and its impact on different sectors, including social and economic issues. During the worst stages, the economic indicators were worse than during the Great Depression of 1929 acting as a catalyst for radicalization and racism. We have seen a revival, to some extent, in terrorism, increase in violent extremism and ethnic separatism. In terms of counter-terrorism, there is an economic impact on CT funding - many nations that would normally give support to the Middle East and Sub-Saharan Africa, are now constrained how much budget they have available. Now, the priority for the public would go to hospitals, social care, and other domestic measures, not necessarily to CT support. In terms of bioterrorism, COVID-19 exposed a window on the potential of a bioterrorist attack – global travel, urbanization, technological advances, terrorist interest in weapons of mass destruction (WMD), state proxy. COVID-19 itself does not have a particularly high lethality compared to biological weapons. Nevertheless, terrorist groups are interested in WMD.

Threats

In terms of how terrorist groups responded to COVID-19 pandemic, they did not all respond in the same way but there are clear patterns that run across a number of groups. Most terrorist groups initially denied the existence of COVID-19, pretended it did not affect them or only affected their enemies or said that it was God's punishment on those who offended Islam. Some groups like far-right extremists, racially or ethnically motivated violent extremists (REMVE) saw COVID-19 as a conspiracy theory. As such, there was a commonality among terrorist groups – they denied it.

However, as time passed, some of the groups started to set up treatment centers as well as replace state provision, offering advisories. In terms of terrorist activity, most groups maintained or increased their operational tempo. At that point, state and security forces were doing less because they were occupied with COVID-19. At the same time, communications matched these activities and terrorist groups used the pandemic to highlight incompetency and corruption of government responses. This was not unique to terrorist groups - political opposition groups were doing the same thing. However, terrorist groups did take advantage of it. In terms of exploitation, the REMVEs exploited COVID-19 with conspiracy theories and racist narratives linking the narratives of COVID-19 to their existing narratives, i.e. the white supremacists. Most terrorist groups exploited lockdown in terms of recruitment.

Terrorist outliers

Taliban was one of the groups who are seen as outliers during the COVID-19 pandemic. They agreed to allow health workers such as NGOs to operate in the area, they agreed for ceasefire, they also established treatment and quarantine centers. Why would Taliban do that? Perhaps they were preparing themselves to be a government or alternatively recognize the threat and did not want refugees from Pakistan, Iran, or Central Asia. We may say that the Afghan Taliban is now not the same as it was in the 1990s but in the past two and a half months ago, a lot has happened since this research was done. In terms of the REMVEs, they deliberately targeted out groups and took out issues linked to race, sexuality, and political beliefs. They also had links with mainstream populist political parties. Moreover, the REMVEs wanted to weaponize the virus and call for violence, i.e. attack synagogues and mosques. Overall, both Taliban and REMVEs took different approaches in terms of COVID-19. However, REMVEs took advantage of those who were isolated and on the Internet.

What could we predict in terms of what happens next? Already now, criminal-terrorism nexus exists in which terrorists and criminals cooperate for mutual benefit. Nevertheless, terrorism is an expensive “hobby” – it requires funding. In Somalia, al-Shabaab is making money over cigarettes and goods, fake vaccines, and counterfeit printer-cartridges. In the short-term future, we are likely to see such collaboration to control illicit stocks and COVID-19 vaccines. In terms of nightmare scenarios, COVID-19 pandemic has opened the potential of bioterrorist attack and illicit procurement of a biological weapon. This is something that we need to start preparing for - **terrorists learn constantly** and they exploit technology, and it seems that this is exactly what they do amid COVID-19 pandemic.

Policy recommendations to NATO

In terms of specific policy recommendations to NATO which support and help to prepare, include provision of field hospitals as well as NATO’s help with medical evacuation. There is a need to challenge inadequacies of terrorist groups in terms of contradictions in messaging, fallacy and promises. There is a need to prepare and respond to biological weapons attacks. This includes lessons learned from COVID-19 response, coordination, and logistics as well as indicators and warnings. Moreover, there is a need to increase focus on human security and enhance civil preparedness. This means renewing focus on transnational human security threats and closer cooperation of military with civilian emergency services. Also, maintaining collective security from both hostile sub-state and state actors exploiting COVID-19 pandemic by remaining focused on core task of collective security against both hostile sub-state and state threats.

In terms of more **general recommendations**, NATO should improve information sharing of best practices and lessons: NATO could focus on being a strategic level platform for sharing best practices during COVID-19 and need for improved information sharing amongst member states and partners. Another recommendation is to consolidate and innovate strategic communication. As COVID-19 challenged NATO’s strategic communications, there is a need for more innovative and coordinated strategy. Another recommendation is to strengthen defense cooperation and integration of military and civil capabilities. COVID-19 pandemic highlighted transnational nature of such emerging threats, showing the need for increased international cooperation and integration of military and civilian responses around ‘Total Defense’ whole of society concepts.

Conclusion

In conclusion, COVID-19 is one of the biggest challenges of our generation since 9/11. It has impacted terrorism and CT responses. It is important to understand, analyse and prepare for the effects of COVID-19 and what might come next, such as bioterrorism, natural calamities, and social and political impact.

Presentation

The slide features a white background with a faint, light blue diamond-shaped grid pattern. In the top right corner, there is a logo consisting of a diamond shape with a smaller diamond inside, containing a red and blue square, with the word 'VEDETTE' written below it. The main text is centered and reads: 'NATO COE-DAT Terrorism Experts Conference (TEC)' in blue, followed by the title 'COVID-19: Developments in Terrorism & Counterterrorism & Implications for the Future' in a larger, bold blue font. Below the title, the dates '12-13 October 2021' are listed in black. At the bottom, the names 'Mr. Stephen Harley & Dr. Rich Warnes' are written in purple. A small number '1' is centered at the very bottom of the slide.

NATO COE-DAT
Terrorism Experts Conference (TEC)

**COVID-19: Developments in
Terrorism & Counterterrorism &
Implications for the Future**

12-13 October 2021

Mr. Stephen Harley & Dr. Rich Warnes

1

COVID-19 Terrorism & CT: Environment

- **Impact of C-19:** Across Range of Phenomenon
- **Economic:** Indicators worse than 'Great Depression' 1929 acting as a catalyst for radicalisation and racism
- **Terrorism:** Revival in terrorism, violent extremism and ethnic separatism
- **Counterterrorism:** Impact on CT funding & support particularly in MENA and SSA
- **Bioterrorism:** C-19 exposed a window on the potential of a bioterrorist attack – Global travel, Urbanisation, Technological Advances, Terrorist interest in WMD, State proxy
- **NATO responses:** MACA & C-19 responses – medical & PPE



2

COVID-19 Terrorism & CT: Threat part 1

- **Initial Denial:** Didn't exist or only affected enemies
- **Volte Face:** Treatment centres, PPE, replace state provision
- **Terrorist Activity:** Most groups maintained or increased tempo
- **Communication:** Initially ignored, but increasingly used to highlight incompetence & corruption of government responses
- **Exploitation:** REMVE exploited C-19 with conspiracy theories & racist narratives
- **Recruitment:** Exploitation of lock downs, captive audiences & use of internet



3

COVID-19 Terrorism & CT: Threat part 2

- **Terrorist Outliers:**

- **Taliban:**

- Agreed a ceasefire
- Allowed health workers into their areas
- Campaign of public awareness
- Established treatment centres & quarantine system

- **REMVE:**

- Targeted 'out groups' – racial, sexuality, political beliefs etc.
- Links with mainstream populist political parties
- Calls for violence, weaponisation of virus, conspiracy theories, rising populism
- Culmination in QAnon Conspiracy aligning C-19 to Jewish conspiracy
- Tailored communications just within bounds of political discourse



COVID-19 Terrorism & CT: Threat part 3

- **Crime-Terrorism Nexus:**

- Terrorism requires funding
- Crime-Terrorism nexus where terrorists & criminals cooperate for mutual benefit
- Example of *al-Shabaab* in Somalia and counterfeit printer-cartridges, cigarettes and goods
- Short term future, likely to see such collaboration to control illicit stocks of PPE and C-19 vaccines

- **Nightmare Scenario:**

- Impact of C-19 pandemic
- Potential of bioterrorist attack
- Illicit procurement of a biological weapon
- Development & deployment of new capability



COVID-19 Terrorism & CT: Policy part 1

• Specific Recommendations

- **NATO core military tasks that prepare for bioterrorism/global pandemics:** Medical evacuation, field hospitals, transport PPE, stockpile PPE & future preparedness
- **Challenge inadequacies of Terrorist Groups:** Contradictions in messaging, inconsistency, fallacy of promises
- **Prepare to respond to threat & impact of Bioterrorism:** Lessons from C-19 response, coordination & logistics, indicators & warnings
- **Increase focus on human security & enhance civil preparedness:** Renew focus on transnational human security threats & closer cooperation of military with civilian emergency services
- **Maintain collective security from both hostile sub-state and state actors exploiting C-19 pandemic:** Remain focused on core task of collective security against both hostile sub-state and state threats



6

COVID-19 Terrorism & CT: Policy part 2

• General Recommendations

- **Improve information sharing of best practices and lessons:** NATO as strategic level platform for sharing best practice during C-19 & need for improved information sharing amongst member states & partners
- **Consolidate and innovate strategic communication:** C-19 challenged NATO's strategic communications – Need for more innovative & coordinated strategy
- **Increase MACA capabilities and preparedness:** NATO MACA during C-19 played a key role – Learn lessons & seek to improve capability
- **Strengthen defence cooperation and integration of military and civil capabilities:** C-19 pandemic highlighted trans-national nature of such emerging threats, showing the need for increased international cooperation and integration of military & civilian responses around 'Total Defence' whole of society concepts



7

Conclusion

The COVID-19 Pandemic has presented a generational challenge impacting on all aspects of geopolitical and policy landscapes, including counterterrorism. Consequently, it has become necessary to understand, analyse and prepare to counter the effects of COVID-19, including the potential threat of bioterrorism and terrorist exploitation of social and political factors

Border Security in Contested Environments

Col. Daniel Wayne STONE

(USAF), Deputy Director, COE-DAT

The main question behind this presentation is what the military's role is and what are the potential good practices to learn from, based on the 2020 NATO COE DAT's Lessons Learned workshop report. Moreover, it looks at why NATO COE DAT has been interested in this issue, what it tries to do, as well as give an overview of the UNCCT-Global Counter-Terrorism Forum Good Practices in Border Security and Management (BSM).

Security is a priority area for NATO. NATO focuses on military aspects to border security, from a CT perspective, especially as its borders have been tested from the extraordinary movement of people escaping from violence and poverty from parts of Africa, the Middle East, and Asia. NATO has been faced with large migration flows and terrorist groups; transnational criminals using porous borders for illicit trade; weapons movement as well as moving terrorist operatives around to conduct attacks to do intelligence gathering. All these activities affect NATO but also our Partner Nations because our borders are being used for organizing crimes and terrorist attacks.

UNCCT Good Practices on BSM

While NATO is not a lead player in border security, the alliance is dramatically affected by political and security developments not only on NATO's borders but also at our allies and Partner Nations' borders. In 2019, NATO HQ International Staff Emerging Security Challenges Division (ESCD), COE DAT and the United Nations Centre of Counter-Terrorism (UNCCT) conducted the "Best Practices on Border Security" Workshop with Jordanian Armed Forces (JAF), which showed the recognition of importance of Border Security and Management (BSM). These practices were then tailored to secure Jordan's border security. In this workshop, the UN focused on civil law enforcement and 15 good practices for border security management in that environment. What the COE DAT and the UNCCT today are looking at is how do we complement those 15 good practices for civil law enforcement and put them to the military perspective of what are the practices that military can use in terms of border security.

These 15 good practices aim to increase Member States' capacity on CT on a national and regional level to prevent those cross-border activities in porous borders. What was particularly emphasized was the good practice on cross-border cooperation and border community engagement. Although these practices are non-binding, they are intended to guide nations' border policies, guidelines, and programs to secure their borders. The UNCCT particularly wanted the COE DAT to highlight good practices number 7 and 13.

UNCCT Good Practices (GP) in Border Security and Management

- GP 1: Enhance intra-agency cooperation
- GP 2: Enhance inter-agency cooperation
- GP 3: Enhance international cooperation
- GP 4: Develop and establish comprehensive remote border area surveillance programs
- GP 5: Engage with empower border communities as key contributors in BSM
- GP 6: Develop and implement Border Community Policing programs
- GP 7: Develop and implement BSM information exchange programs and mechanisms
- GP 8: Establish Border Cooperation Centers
- GP 9: Nominate and assign Border Liaison Officers
- GP 10: Conduct joint and coordinated cross-border patrols, as well as joint multiagency and interdisciplinary operation exercises
- GP 11: define parameters for cross-border operational engagement
- GP 12: Conduct and effective risk analysis assessment
- GP 13: Create National Border Management Strategies and Action Plans
- GP 14: Establish Joint Border Crossing Points
- GP 15: Identify corruption as a serious risk for effective and robust BSM

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/goodpractices_bsm_english_2018_0.pdf
4 / 11
UNCLASSIFIED

Figure 5--UNCCT Good Practices (GP) in Border Security and Management

In the context of preventing cross-border movement of terrorist fighters and transnational groups, **information sharing and holistic CT strategy which covers land, air, and maritime domains are key to identifying and disrupting networks that facilitate their travel.** These 15 good practices are designed for law enforcement. However, do these good practices apply or not apply to the military and how? Are there ones that militaries can or cannot use or are there any additional ones to apply?

In collaboration with the UNCCT, the COE DAT developed a Concept to Develop Military Good Practices in Border Security that would be complementary and support law enforcement that already had good practices. Militaries can provide a central role in border management. **Militaries have expertise in operational planning** that is often not matched by any other organizations. The military also has a capability to be called-in as first responders and capable to operate in very remote areas. Nevertheless, the military cannot provide long-term replacement to law enforcement in emergency services, but the military has capabilities to provide these services to civil agencies in extremist situations.

COE DAT's Initiation of Border Security Practices

Good Practice (GP) 1: enhance intra-agency cooperation; and Good Practice 2: enhance inter-agency cooperation can be especially highlighted. In GP 2, military practices are not often well defined in civilian areas. GP3 is about developing and establishing comprehensive remote border area surveillance programs. Nevertheless, in all aspects, **engagement with the local communities is the key** – just like law enforcement in order to understand their needs and concerns in order not to seem as a threat but more of an ally. **Information sharing is the key.** But to what level can the military share intelligence, an aspect of security classification needs to be paid attention to.

Another aspect is to put military liaison officers not only to borders but having liaison capabilities as well as having effective security risk management strategy. It is important to know who is doing what, to have authority in place before the event. Moreover, GP 10 refers to conducting joint and coordinated border patrols with law enforcement as the lead agency as well as joint multiagency and interdisciplinary operation exercises, with the legal authority to make arrests. As such, COE DAT is looking for further refinement of these Good Practices and conduct further events on the subject matter and cooperate with Partner Nations to make these practices better. NATO does not do military border against on day-to-day basis while many Partner Nations do. This can help assist the COE DAT and NATO further.

In terms of the way forward, we really have to focus on what is the military's role in this and is there such a role; provide universal information, not tied to a specific Nation for global use and have executive level expertise, not involving special political issues. We also have to focus on an operational and strategic level. COE DAT intends to hold additional workshops with the

UN, Partner Nations, and academia and to eventually publish non-binding good practices on the military role on border security.

Presentation



Agenda



- Background to the project and report on border security in contested environments
- UNCCT-Global Counter Terrorism Forum Good Practices in Border Security and Management
- COE DAT's initiation on Border Security Program aligned to UNCCT Border Security and Management Programme
- The 13 potential good practices based on COE-DAT's Lessons Learned workshop report
- Request for Support from Partner Nations to validate the outcome of the report.

2 / 11

UNCLASSIFIED

Background



- Border Security is a priority area for NATO
 - NATO focuses rightly in military aspects to border security, from a CT perspective
 - Partners also highlighted in their framework documents, BS is one of the priority area for cooperation with NATO
- Science for Peace and Security Best Practices on Border Security Workshop NATO HQ IS ESCD, COE DAT and Jordan Armed Forces (JAF) in 2019 - DCB.
 - The event, hosted by JAF shown the recognition of importance of BS and Management (BSM)

3 / 11

UNCLASSIFIED

UNCCT Good Practices (GP) in Border Security and Management



- GP 1: Enhance intra-agency cooperation
- GP 2: Enhance inter-agency cooperation
- GP 3: Enhance international cooperation
- GP 4: Develop and establish comprehensive remote border area surveillance programs
- GP 5: Engage with empower border communities as key contributors in BSM
- GP 6: Develop and implement Border Community Policing programs
- GP 7: Develop and implement BSM information exchange programs and mechanisms
- GP 8: Establish Border Cooperation Centers
- GP 9: Nominate and assign Border Liaison Officers
- GP 10: Conduct joint and coordinated cross-border patrols, as well as joint multiagency and interdisciplinary operation exercises
- GP 11: define parameters for cross-border operational engagement
- GP 12: Conduct and effective risk analysis assessment
- GP 13: Create National Border Management Strategies and Action Plans
- GP 14: Establish Joint Border Crossing Points
- GP 15: Identify corruption as a serious risk for effective and robust BSM

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/goodpractices_bsm_english_2018_0.pdf

4 / 11

UNCLASSIFIED

Concept to Develop Military GP in BS



- Existing good practices focused on civilian law enforcement in permissive environments
- A gap exists for the role militaries can fill in border security management in contested environments
- Militaries have capabilities that can support civil law enforcement
- COE-DAT and UNOCT-UNCCT initiated project with academia and Partner Nations to collect, analyze, and identify potential military good practices in border security

5 / 11

UNCLASSIFIED

COE DAT's Initiation on BS



Potential good practices for militaries in border security based on the outcome of COE DAT's WS

- GP 1: Enhance intra-agency cooperation (GP1 GCTF)
- GP 2: Enhance inter-agency cooperation (GP2 GCTF)
 - **Military expertise in operational planning is not often matched by other agencies. The military can facilitate a combined, interagency environment with the capacity to interconnect multiple agencies to coordinate effort**
- GP 3: Develop and establish comprehensive remote border area surveillance programs (GP4 GCTF)
- GP 4: Engage with and empower border communities as key contributors in BSM; recognizing continuity to understand local issues is a key contributor in BSM (GP5 GCTF)

6 / 11

http://www.coedat.nato.int/COEDAT_LLWSreport_BorderSecurityinContested_Environment.pdf UNCLASSIFIED

GPs for Militaries in Border Security



- GP 5: Develop and implement BSM information exchange programs and mechanisms (GP7 GCTF)
 - **Providing on-the-ground intelligence collection, exploitation, and assessments to enhance overall situational awareness;**
 - **Sharing of relevant counter-terrorism information with key non-military actors (law enforcement and emergency services);**
 - **Maintaining a system of indicators and warnings to facilitate early detection of imminent threats;**
- GP 6: Nominate and assign military Border Liaison Officers to Border Cooperation Centers (linked to GP6 GCTF)
- GP 7: Conduct an effective risk analysis (GP12 GCTF)
- GP 8: Create National BM Strategies/Action Plans (GP13 GCTF)
- GP 9: Identify corruption as serious risk for effective BSM (GP15 GCTF)

7 / 11

http://www.coedat.nato.int/COEDAT_LLWSreport_BorderSecurityinContested_Environment.pdf UNCLASSIFIED

GP's for Militaries in Border Security



- GP 10: **Conduct joint and coordinated border patrols with law enforcement as the lead agency, as well as joint multiagency and interdisciplinary operation exercises.** (mostly GP10 GCTF)
- GP 11: **Develop policies and procedures for military support during crisis periods to provide support as first responders during mass casualty events, and reinforce civil law enforcement**
- GP 12: **Build physical infrastructure to support border security**
- GP 13: **Training, advising, and assisting host nation security forces**

RFS from Partner Nations



Request for Support from Partner Nations:

- Validate the outcome of the report;
- PNs experience in BSM;
- What are PNs key priorities in BSM;
- Integrate expertise of PNs on BSM in contested environment.

COE-DAT Lessons Learned Report:

http://www.coedat.nato.int/COEDAT_LLWSreport_BorderSecurityinContested_Environment.pdf

Accomplishments and Way Ahead



- Border Security in Contested Environments military good practices with UNOCT&INTERPOL
 - COE-DAT, UNOCT-INTERPOL, and academia endeavor to collect, analyze, and share lessons learned to develop best practices on border security and management within the context of counter-terrorism in contested environments,
 - Focus on the military's role in CT relating to Border Security
 - Provide universal information, not tied to a specific Nation, for global use. Executive level expertise, not involving specific political issues
 - Operational and strategic outlook, focusing on executive level military and lessons learned.

Achievements:

- LL report to JALLC
- NATO PC WG & MD countries' representatives were briefed
- METs to MENA (e.g. Mauritania with NSHQ & JCNP)

Questions?



Thank You For Your Attention!

Terrorism Threat during Peer to Peer Conventional War

Mr. Krisztián JÓJÁRT

National University of Public Service, Budapest

The focus of this presentation was how Russia may use the tool of terrorism during peer-to-peer conventional war with NATO, based on a study authored by Tamás Csiki, Krisztián Jójárt, András Rác and Péter Tálás.

As there is no unified definition of terrorism, this research used NATO Military Committee Concept for Counter-Terrorism which states that terrorism is “the unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives”. With regards to the definition of terrorism, there is no distinction between war and peacetime, civilian and military targets as well as state or non-state actors. However, **NATO’s definition of terrorism is applicable to investigate how a peer competitor may use the tool of terrorism.**

In terms of how Russia sees terrorism, there is an assumption that Russian use of illegal armed forces formations (including terrorists and other proxies) is centered around grey-zone conflicts is unsubstantiated, as seen in Ukraine and Syria. The Russian understanding of war and peace is not as binary as the West may think. Western actions that are regarded as measures short of war, i.e. economic sanctions, can be understood by Moscow as part of war.

It is also important to see **how Russia sees contemporary wars**. As such, the line between war and peace is blurred; there are no clearly defined frontlines or recognizable distinction between combatants and non-combatants. This perception of the general character of war legitimizes the use of unlawful means and methods by Russia too. Deputy Defence Minister of the Russian Federation, Andrey Kartapolov, has said that the new type of wars consists of 20 percent propaganda, 80 percent armed confrontation but 90 percent are civilians, non-combatants.

In Russia, there is a term, “interstate (*mezghosudarstveniy*) terrorism” used as a Russian military thought, saying that it is “a method of intimidating an adversary state by an aggressor state influencing it with means of terrorism. The purpose of this kind of action is the physical elimination of the representatives of the political leadership and military command of the adversary state or provoking mass panic and chaos via organizing terrorist acts against the

civilian population” (*War and Peace in Terms and Definitions. Military-Political Dictionary. Ed. by Dmitry Rogozin*). Within this research, **five types of terrorist attacks** were identified, used in peer-to-peer conventional war, including terrorist attacks implying strategic effects; attacks on political/military leadership; targeted killings; sabotage attacks and attacks aimed at stirring up social tension.

Terrorism with strategic effect

In terms of terrorism with strategic effect, it aims to compel the enemy to fulfil our political will or provokes the enemy to act in a certain way, which is beneficial for us. This is what the Russian terminology calls “reflexive control.” There are numerous references to those type of attacks in the Russian literature. However, in practice, there have been references to an alleged Soviet plan to poison the Potomac River as well as the mysterious Russian apartment bombings in September 1999 which serves as *casus belli* for the Second Chechen War. However, it seems that the actual perpetrators were not Chechen terrorists but actually Russia’s authorities.

Attacks on political-military leadership

In theory, Russian thinkers have expressed that Russia should use the method of targeted killings against key decision-makers and key military personnel as part of countering an air offensive. When we look at the practice, we see the KGB’s assassination of *Hafizullah Amin* preceding the Soviet invasion of Afghanistan in 1979 as well as the failed Montenegro coup attempt in 2016 to prevent Montenegro’s NATO accession.

Targeted killings

In terms of targeted killings, we see this in practice by the poisoning of *Alexander Litvinenko* and *Sergey Skripal* as well as the failed poisoning of Bulgarian arms trader *Emilian Gebrev* who supplied Ukraine with ammunition in 2014. This strategy can also be seen on political opposition, i.e. *Aleksey Navalny*. In Ukraine, Russian security services assassinated numerous Ukrainian high military and security officials.

Sabotage attacks

In terms of sabotage attacks, in theory, *Chekinov* and *Bogdanov* have referred to inflicting unacceptable damage to the enemy in non-military security areas like attacking economy and critical infrastructure. In practice, in 2014, Russian GRU targeted Ukraine crucial ammunition locations. There have been numerous cyber-attacks against Ukrainian critical infrastructure. Moreover, GRU's Unit 29155 has been dedicated to carry out sabotage and destabilization activities and stands out as a special unit for these types of activities.

Attacks aimed at stirring up social tension

In theory, Russian military literature has referred to West sowing chaos in their target countries - this thought embedded in the Russian military theory. In practice, there was an arson attack in 2018 against the cultural center of the Hungarian minority in Ukraine but it turned out that the perpetrators were Polish citizens, paid by a German journalist with close relations to Russian intelligence services.

In terms of **blowbacks and unintended consequences**, this is the case with the downing of the MH-17 in which Buk air defence system was supplied to separatists to deny the operation of Ukrainian air force. The unintended shot down of the MH-17 civilian flight resulted in the acceptance of tougher Western sanctions against Russia. Another case with unintended consequences was the case of NotPetya cyber-attack, targeting Ukraine but which spiralled out of control, causing an estimated 10 billion USD damage worldwide, being the most devastating cyber-attack in history.

Conclusions

Terrorism and other unlawful forms of violence constitute an integral part of Soviet/Russian military thinking. Russian perception of contemporary wars testifies about a blurring distinction between peace and war, combatant and non-combatant, civilian and military. Russian military thinkers openly propagate the use of asymmetric means against a technologically superior enemy. Ukraine has seen a number of actions that may be qualified as acts of terrorism. These actions are indicative of how Russia would use terrorism in a conventional war fought with a peer competitor. However, from the Russian perspective, this was a localized war. It is likely that civilian objects of NATO countries would constitute free targets for Russian special services and proxies in case of a conventional war.

Presentation



Remarks and disclaimers

- This presentation is based on a study authored by **Tamás CSIKI**, **Krisztián JÓJÁRT**, **András RÁCZ** and **Péter TÁLÁS**.
- This presentation relies exclusively on open sources.
- The views expressed are those of the authors and do not reflect the position of the ISDS or the Hungarian government.

The scope of the presentation

How would Russia use the tool of terrorism during a peer to peer conventional war?

- The presentation **will not cover**
 - escalation to a nuclear war,
 - use of terrorism by other potential peer competitors (China)
 - the likelihood of actual occurrence
 - possible ways of defense or deterrence against such threats

The definition of terrorism

Terrorism

“The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives.”

(NATO Military Committee Concept for Counter-Terrorism)

The definition of terrorism

No distinction between

- war and peacetime
- civilian and military targets
- state or non-state actor

Therefore, NATO's definition of terrorism is applicable to investigate how a peer competitor may use the tool of terrorism.

Terrorism and Russian military thought

- The assumption that Russian use of illegal armed formations (including terrorists and other proxies) is centered around grey-zone conflicts is unsubstantiated.
- The Russian understanding of war and peace is not binary. Western actions that are regarded as measures short of war (such as economic sanctions) can be understood by Moscow as part of war.

Terrorism and Russian military thought

In contemporary wars

- the line between war and peace is blurred,
- there are no clearly defined frontlines,
- or recognizable distinction between combatants and noncombatants.

This perception of the general character of war legitimizes the use of unlawful means and methods by Russia too.

Terrorism and Russian military thought

Interstate (*mezhgosudarstveniy*) terrorism

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

(War and Peace in Terms and Definitions. Military-Political Dictionary. Ed. by Dmitry Rogozin)

Main possible types of terrorist attacks

- Terrorist attacks implying strategic effects
- Attacks on political/military leadership
- Targeted killings
- Sabotage attacks
- Attacks aimed at stirring up social tensions

I. Terrorist attacks with strategic effect

To compel or provoke the enemy to act in a certain way

Theory

- *Doulnev and Orlansky*: threatening with the destruction of an ecologically hazardous object (eg. a nuclear power plant).
- *Bartosh*: use of proxies to carry out provocations in a hybrid war
- *Kiselyev*: ethnic cleansing of Kosovar Albanians, as an example of provoking the NATO bombing of Yugoslavia.

I. Terrorist attacks with strategic effect

To compel or provoke the enemy to act in a certain way

Practice

- Alleged Soviet plans to poison the Potomac River
- Mysterious Russian apartment bombings in September 1999, which served as casus belli for the Second Chechen War

II. Attacks on political/military leadership

Theory

- *Glebov, Mikheev and Oleinik*: assassination of key decision-makers and military personnel as part of countering an air offensive

Practice

- Assassination of *Hafizullah Amin* preceding the Soviet invasion of Afghanistan
- Failed coup attempt in Montenegro in 2016
- Killing of Chechen leaders *Dudayev* and *Yandarbiev* in 1996 and 2004

III. Targeted killings

Practice

- Poisoning of *Alexander Litvinenko* and *Sergey Skripal*
- Assassination of separatist leaders in the Donbas and Ukrainian military and intelligence officers
- Failed poisoning of Bulgarian arms trader *Emilian Gebrev*

IV. Sabotage attacks

Theory

- *Chekinov and Bogdanov*: inflicting unacceptable damage to the enemy in other (nonmilitary) security areas

Practice

- Explosion of an arms depot in Vrbetice by GRU agents in 2014
- Numerous cyber attacks against Ukrainian critical infrastructure
- GRU's Unit 29155 dedicated to carry out sabotage and destabilization

V. Attacks aimed at stirring up social tensions

Theory

- *Evgeny Messner's* concept of *myatezhvoina* (mutiny war): criminality, subversion and terrorism to break the enemy's fighting morale
- Russian perception of "color revolutions" and contemporary wars

V. Attacks aimed at stirring up social tensions

Practice

- Arson attack against the cultural center of the Hungarian minority in Ukraine

Blowbacks and unintended consequences

The case of MH17

- Buk air defense system supplied to separatists to deny the operation of Ukrainian air force
- The unintended shot down of MH17 resulted in the acceptance of tougher Western sanctions against Russia

Blowbacks and unintended consequences

The case of NotPetya

- A cyber attack targeting Ukraine spiraled out of control, causing an estimated 10 bn USD damage worldwide.

Conclusions

- Terrorism and other unlawful forms of violence constitute an integral part of Soviet/Russian military thinking
- Russian perception of contemporary wars testify about a blurring distinction between peace and war, combatant and non-combatant, civilian and military
- Russian military thinkers openly propagate the use of asymmetric means against a technologically superior enemy

Conclusions

- Ukraine has seen a number of actions that may be qualified as acts of terrorism
- These actions are indicative of how Russia would use terrorism in a conventional war fought with a peer competitor
- It is likely that civilian objects of NATO countries would constitute free targets for Russian special services and proxies in case of a conventional war

Why is Gender Important in Counter-Terrorism?

Col. Daniel W. STONE

(USAF), Deputy Director, COE-DAT

It is often asked, why does gender matter in counter-terrorism (CT) and what does gender really mean? There are three main reasons why gender matters in CT. First, **diverse groups provide better solutions and policies to address terrorism and its root causes**. Gender is not only about biological sex; gender is also about the social norms associated with biological sex and power dynamics between and amongst the sexes. Second, gender matters because it is directly linked to the analysis and response to the terrorist threat and **represents a security threat** to NATO and nations around the world. There is a visible rise of women in terrorism as well as women's hidden roles in terrorism. If gender is not accounted for in threat assessments, it could lead to deficient understanding of the threat and insufficient responses to the threat. Third, gender is critical to Preventing/Countering Violent Extremism (P/CVE) and CT by increasing the efficiency of CT efforts. **Women can play various roles supporting CT efforts such as being predictors, preventers, and security actors.**

What is “gender”?

We often have a misconception that gender equals women. Gender is more than women. Gender refers to a socially constructed role based on sex, intersecting with other identities. Gender is consistently used against both men and women by terrorist organizations. Attributes such as sex, religion, race, ethnicity, age, and social class need to be addressed when considering gender. These identity markers impact how men and women should act in a society and most importantly affects power dynamics, relationships between people, as well as access to resources.

Perceptions of gender roles create a “blind spot” for CT practitioners and policy makers. Three simplified and misleading assumptions concerning the gendered roles of women in terrorist organizations are that women join to be “brides” of a terrorist and are viewed through their affiliation with men, that women are mothers and therefore non-violent by nature, and women are victims with no agency who are forced into terrorism against their will. All three of these

assumptions are wrong and indicate the need to mainstream gender and the many different roles women and men play in terrorist organizations.

Terrorism affects men and women differently, i.e. their unequal ability to recover from attacks or leading terrorist organizations. We also need to understand how CT policies affect men, women, boys, and girls. Since most CT practitioners are male and most violent terrorists are male it is easy to overly focus on males and fail to understand that women fill exactly same roles in terrorist organizations as men do: victims, supporters, and perpetrators of terrorism.

Diversity produces better policies

The more inclusive a society is linked to the production of better policies and solutions in general and CT in particular. Women visible in society is a sign of inclusion. There is a correlation between **women and lower levels of corruption**. The exclusion of women from society correlates to societies with **greater levels of institutionalized violence and are far less likely to negotiate**. Women provide distinct insights, different views, and concerns. As such, diversity results in more comprehensive solutions.

Security Threat: The Rise of Women in terrorism

As mentioned earlier, **gendered aspects of terrorism present a security threat to NATO, Partner Nations**, and the International Community because **gender is directly linked to the analysis and response to the terrorist threat that represents a security threat** to NATO and nations around the world. **If gender is not accounted for in threat assessments, it could lead to deficient understanding of the threat and insufficient responses to the threat.**

More and more women are visibly involved in terrorist organizations. Between April 2013-June 2018, 13 percent of FTFs in Iraq and Syria were women. Across Europe, women accounted for 22 percent of arrestees suspected of terrorism in 2018, as compared to 16 percent in 2017, and 26 percent in 2016. We are also seeing the increase of women in far-right terrorist organizations in Europe. However, we do not have the data to truly understand the level of impact of women in terrorist groups because many states do not track their data on FTFs, underscoring the need to develop the data to better understand and come up with more nuanced solutions.

Moreover, **armed groups supported by women are more likely to control greater territory and achieve victory over government forces**. Terrorist organizations truly understand the importance of gender and they understand gender stereotypes. They try to seek people through

tailored recruitment, such as looking at frustrated men in societies and tailor a recruitment accordingly. Terror organizations use the notion of **male hyper-aggression** and the **subjugation of women** to men to **entice males to the organization as a place those frustrated males can meet the expected gendered norms for a man.** We saw that ISIS successfully recruited educated young men, offering all the traditional things of “manhood” (job, wife, money, power) that these disaffected men wanted to have. Similarly, they reached out to females, “liberating” them from “beauty-oriented” West. All these things were attractive to women as they were disillusioned by the gendered expectations of them in the Western societies.

Women are used as **recruiters** of both males and females. Daesh uses women to recruit males by calling on males to be “men” and defend the women who have joined Daesh as well as **question their “manhood”** since women are fighting because they were not “man” enough. Women are also great recruiters for Daesh on social media and calling for their **“sisters” to meet their “roles” to populate the state as baby factories.**

The move to recruit women into terror organizations is a pragmatic decision to regain the strategic advantage. Women are a perfect demographic as gendered perceptions will reduce any scrutiny CT forces apply to women enabling women terrorists to remain hidden.

Why do women join terrorist organizations?

For the same reasons as men do, i.e. poverty, discrimination, political marginalization, exclusion. Women are pulled to terrorism by the same factors as men are. When there is economic disparity, coupled with some kind of social alienation, it leads to extremism. Anger over government and security forces over-reach are also factors that drive people to join terror organizations. According to a UN Development Program report, **71% of African based/convicted terrorists indicated the arrest or killing of a family member by government forces was what pushed them into joining a terrorist organization.**

As more and more women join and support men’s militancy by **nurturing committed violent extremist families** a **generational threat is emerging.** FTFs pose a significant security threat.

Furthermore, there are **disparities in criminal prosecutions** and whether women are prosecuted at all. In many countries due to the prevailing gendered views that women are victims with no agency, **many women are not prosecuted, and if they are prosecuted, women receive sentences that are far more lenient than men.** The gendered affect is women

do **not receive equal access to de-radicalization programs**, as these are typically part of prison sentences for males. This **could lead to women never de-radicalizing and lead to a second generation of terrorists as women FTFs pass on their ideologies.**

Security Threat: Women's Hidden Roles in Terrorism

We are accustomed to view women as victims in their links with terrorism, such as sex-slaves or “Jihadi Brides”. We are less mindful that women are involved in the same activities as men such as **sympathizers, supporters, radicalizers, recruiters, facilitators, perpetrators and enablers.**

Women predominately are active in support capacities for terrorist organizations enabling the violent actions of male terrorists. **Fundraising** is one way in which women provide operational support to terrorist organizations

While men remain the largest number of perpetrators of terrorism and receive the greatest scrutiny, this causes the **role of women as perpetrators** to not be recognized nor addressed, even as the **numbers of female perpetrators are increasing.** Since the 1950s, approximately 60% of armed groups have included women in their ranks. In the 1950s women in **Algeria** transported and deployed bombs at strategic targets, in the 1990s all female battalions gained reputations as fearsome fighters in **Sri Lanka**, and in Columbia **almost 40% of the FARC** (Revolutionary Armed Forces Columbia) were female to include fighters and combat leaders.

Women are increasingly leading violent attacks. Women are seen especially dangerous in terms of suicide bombings. Terror organizations see women as a “strategic” asset within the realm of suicide terrorism, often being able to slip through security. On average, female suicide bombers count 8.3 vs 5.4 average deaths. Between 2014 and 2018, over 1,200 attacks were done by female suicide bombers. The Taliban used males dressed up as women as to escape targeting by security forces and not be searched.

We should also be mindful of the historical involvement of women in terrorism. For instance, in Japan, the Japanese Red Army was created with female leadership support and the Baader-Meinhof Gang in Germany. From the threat analysis perspective, we often turn blind eye to their roles.

Women as agents in P/CVE and CT

Women can play different roles in CT as: 1) **predictors**: Women have a critical role in early identification of radicalization in families and communities. Moreover, attacks on their rights and physical autonomy are often the first indication of a rise of fundamentalism in the society. 2) **Preventers**: women as mothers can contribute to building resilience in these families and communities by influencing their husbands and children away from extremist views, i.e. Mother Schools. Women can offer credible counter-narratives to the terrorist organizations recruitment propaganda as mothers, rehabilitators and community leaders, like the Murshidat Program in Morocco. In Nigeria, women support each other in community policing. 3) **Security actors**: Women in security forces are a force multiplier that builds trust with local communities and increases security (i.e., more engagement, more intelligence, greater situational awareness, and force protection). Women have a much easier time to build trust in societies, and perceived different by their male peers. This allows greater trust as well as more awareness and intelligence. Globally, about 15 percent of law enforcement are women. Unless we change these structures, women terrorists remain to have influence in terms of being involved in terrorism.

Recommendations

It is important to **increase women's representation at all levels in the security sector**. It should be about the **meaningful participation** of women, **not only about numbers**, and **not only having female gender advisors**. Moreover, we should **improve recruitment, retention, and advancement** of women across the security sector to bolster the capacity of forces to mitigate potential terrorist threats. We should also ensure that CT programming is inclusive and gender-responsive; solutions done are best through a Whole of Government Approach and Whole of Society Approach. We should take into consideration of gendered impacts and needs as well as **acknowledge women's agency in terrorism and counter-terrorism**. We should also look at CT policies – how do we tailor the needs to women, men, boys, and girls in terms of prosecution and rehabilitation programs? These programs should take into account the special skills that people have. **Otherwise, women may go back to terrorist organizations to resume to their power-status**.

As such, NATO COE-DAT has been involved in research on gendered aspects of terrorism since the first workshop on women and CT conducted in 2019.



CENTRE OF EXCELLENCE DEFENCE
AGAINST TERRORISM

COE-DAT'S WORK ON GENDER

- COE-DAT series of Gender in Terrorism and Counterterrorism Workshop
 - **1st Workshop:** Women in Terrorism and Counterterrorism (27-28 May 2019)
 - **Report:** https://www.tmmm.tsk.tr/publication/workshop_reports/08-WomenInTerrorismAndCounterterrorism.pdf
 - **2nd Workshop:** Gender and Counterterrorism: Enhancing Women's Role and Empowering Women (22-24 September 2020)
 - **Report:** https://www.tmmm.tsk.tr/GENDER_AND_COUNTERTERRORISM_REPORT.pdf
 - **3rd Workshop:** Gender in Terrorism and Counterterrorism: Data, Analysis and Response (15-17 June 2021)
 - **Report:** [https://www.tmmm.tsk.tr/GENDER_AND_COUNTERTERRORISM_REPORT\(2021\).pdf](https://www.tmmm.tsk.tr/GENDER_AND_COUNTERTERRORISM_REPORT(2021).pdf)
- **Good Practices in Counter Terrorism Handbook**
 - **Vol 1 (2021)** : Contains a chapter on "Good Practices in Integrating a Gender Perspective to Countering Terrorism" Full text (whole book) is available at; https://www.tmmm.tsk.tr/GOOD_PRACTICES_INCOUNTER_TERRORISM.pdf
 - **Vol 2 (2022):** research in process
 - is to contain a chapter on Gender-Specific CT Policies.

Figure 6—COE-DAT'S work on gender

Presentation



CENTRE OF EXCELLENCE DEFENCE
AGAINST TERRORISM

Why is Gender Important in Counter-Terrorism

TEC 2021

Col. Daniel W. Stone (USAF)

COE-DAT Deputy Director



CENTRE OF EXCELLENCE DEFENCE
AGAINST TERRORISM

Why does gender matter in counterterrorism?

1. **Diversity produces better policies**
2. It is directly linked to the **analysis and response to the terrorist threat** that represents a **security threat** to NATO and nations around the world.
 - a. Rise of women in terrorism
 - b. Women's hidden roles in terrorism
3. **Critical to P/CVE and CT, increases the efficiency** of the efforts since women can play various roles as;
 - a. Predictors
 - b. Preventers
 - c. Security actors



CENTRE OF EXCELLENCE DEFENCE
AGAINST TERRORISM

Gender...

... more than women...

... socially constructed roles based on sex

... intersects with other identities

- “the **social attributes and opportunities associated with being male and female** and the **relationships** between women and men and girls and boys, as well as the relations between women and those between men.”
- “These attributes, opportunities and relationships are **socially constructed** and are learned through socialization processes.”
- “They are **context/ time-specific** and changeable.”
- “**Gender is part of the broader socio-cultural context.** Other important criteria for socio-cultural analysis include class, race, poverty level, ethnic group and age.”

Gender roles create a “Blind Spot”

See <https://www.un.org/womenwatch/osagi/conceptsanddefinitions.htm>



CENTRE OF EXCELLENCE DEFENCE
AGAINST TERRORISM

Diversity Produces Better Policies

- **More inclusive** the society equates to **better policies**
- Women in society is a sign of inclusion
 - Correlation between **women and lower corruption**
 - **Exclusion of women** from society correlates to societies with **greater levels of institutionalized violence**
- Women provide distinct insights
 - Different views and concerns
 - **Diversity** results in **more comprehensive solutions**



CENTRE OF EXCELLENCE DEFENCE
AGAINST TERRORISM

Security Threat: Rise of Women in Terrorism

- **Numbers of women in terrorism increasing**
 - **13%** of FTFs in Iraq and Syria (April 2013 - June 2018) were **women**.
 - Across Europe, women accounted for **22%** of arrestees suspected of terrorism in **2018**, as compared to **16 % in 2017**, and **26 % in 2016**.
 - 20,000 reported FTFs from the **OSCE region**; **3,400 (17%)** were **women**.
- **Increase in women's participation in far-right organizations and the increase in far-right women's groups in Europe**
- **Armed groups supported by women** more likely to:
 - **Control greater territory**
 - **Achieve victory over government forces**
- **Gendered recruitment strategies**
- **Disparity in criminal prosecutions**



CENTRE OF EXCELLENCE DEFENCE
AGAINST TERRORISM

Security Threat: Women's Hidden Roles in Terrorism

- We are accustomed to view **women as victims** in their links with terrorism
 - Sex-slaves, Jihadi Brides
- We are less mindful that women involved in the same activities as men such as **sympathisers, supporters, radicalizers, recruiters, facilitators, perpetrators, enablers** etc.
- Terror organizations see women as a **“strategic” asset**
 - Female suicide bombers 8.3 vs 5.4 average deaths
 - Slip through security
- We should be mindful of the **historical involvement** of women in terrorism.
 - 1878- Vera Zasulich (Naraodnaya Volya)- attempted to assassinate governor general of St. Petersburg
 - 1970s- Ulrike Meinhof (Red Army Faction)- co-founder



Women as Agents in P/CVE and CT

- Women can play different roles in CT as;
 - **Predictors**
 - Women have a critical role in early identification of radicalization in families and communities.
 - Attacks on their rights and physical autonomy are often the first indication of a rise in fundamentalism in the society
 - **Preventers**
 - Women as mothers can contribute in building resilience in these families and communities **by influencing their husbands and children away from extremist views.** (e.g. Mother Schools)
 - Women can offer credible counter-narratives to the terrorist organizations recruitment propaganda as mothers, rehabilitators and community leaders. (e.g. Murshidat Program in Morocco)
 - **Security actors**
 - Women in security forces is a force multiplier that builds trust with local communities and increases security. (e.g. more engagement, more intelligence, greater situational awareness, force protection)



Recommendations

- Women's Representation at all levels in the Security Sector
 - Meaningful participation of women
 - Improve the recruitment, retention, and advancement of women across the security sector to bolster the capacity of forces to mitigate potential terrorist threats
- Ensure that CT programming is inclusive and gender-responsive
 - Solutions are best through a Whole of Government Approach + Whole of Society Approach
 - Consideration of gendered impacts and needs
- Acknowledge women's agency in terrorism and counterterrorism

DAY I – Session 2: Questions and Open Discussion

Dr. Richard WARNES & Mr. Stephen HARLEY

1. **Comment:** NATO Allies stand in solidarity in response to the COVID-19 pandemic. NATO and Allied military personnel have been supporting civilian efforts - providing military airlift, setting up field hospitals, sharing medical expertise, and helping to develop innovative responses. The Euro-Atlantic Disaster Response Coordination Centre (EADRCC) is NATO's main civil emergency response mechanism. The Centre operates on a 24/7 basis, coordinating requests and offers of assistance. It is helping to coordinate assistance, including medical and financial support. In June 2020, NATO Defence Ministers decided on a new Operations Plan to ensure that the Alliance is ready to help Allies and partners. This plan can be activated at any time during this crisis, for future pandemics or other large-scale medical emergencies. NATO also established the Pandemic Response Trust Fund that maintains a stockpile of medical equipment and supplies to be able to provide immediate relief to Allies or partners in need.
2. **Do you think that NATO was able to react collaboratively, as an organization and in a coordinated manner, against COVID-19? According to positive or negative aspect, could this hamper or reinforce international posture? Is NATO ready for similar and probable social threats?**

Yes, that is already answered by the above comment but logistically, NATO did play a very effective role in terms of shipment of movement of medical equipment, vaccines, also in the provision of air transport. In that sense, NATO did perform well. Setting up an establishment of a stockpile in response of any future threats, having that stockpile already prepared, was a good thing. Also, NATO acted as a supranational agency to keep best practices on different medical-focused COEs in Europe, are examples of that to be able to provide best practice.

However, what NATO did not do well, was that it did not counter what terrorist organizations said about governments and NATO, it did not inform people as it should

have. Nevertheless, the response did discuss what it was doing, especially logistically. Yes, NATO did respond in a number of ways but there is clearly room for improvement.

- 3. Talking about COVID-19, there is a big threat about fake news. For example, vaccines that can make human body metal, vaccines that prevent pregnancy etc. So, it is important for us to counter this fake news under the cyber area. On the other hand, at the beginning stage, we did not know much about COVID-19. Is it important for us to counter this fake news at the beginning?**

According to Mr. Harley, fake news did not appear during COVID-19 pandemic nor in 2016. Fake news has been around forever and terrorists are natural experts on it. It is one of these things that terrorists do – it is not a new phenomenon. Now, a lot more people are aware of the term of “fake news”. There is a general consensus among academics and analysis done that overall, around 30 percent of the population are vulnerable to fake news. People are vulnerable to fake news. 3 out of 10 people naturally like conspiracy theories but within that 30 percent – people fall into three different groups: “Vulnerable” people try to answer the question of “why”, i.e. why did we lose jobs and these are the ones we can deal with quite easily – they are the victims of circumstances. There are also the “gullible”, who are seen as being “daft” – it can be about having not enough educational opportunities or not enough travel. However, they can also be dealt with if right information is available for them. However, the third group, the “risible,” is the most concerning. They share, invent and store conspiracy theories.

What to do about it? The approach should be about 1) direct engagement, 2) diverting away, 3) distract the subject, 4) diffuse or 5) do nothing. **In case of COVID-19 – you must engage with the fake news rapidly and bring in legal measures**, i.e. stop people sharing these messages and fake news. However, this is a short-term fix. **But how do we really fix it?** How do we diffuse the situation before it happens? Generating higher level of critical thinking and media literacy within your population helps. It is interesting to know which societies have been vulnerable to fake news and which have not? Those societies with higher education levels, create more awareness. How do I work out where has it been published, what is the message? Why would someone post this? We need to be more prepared. How do I analyse a media product, how do I figure out the audience

and source of this? **If people can think critically and are media literate, that is how we have a longer-term solution to this – it is about being more prepared.**

Mr. Krisztián JÓJÁRT

- 1. With regards to war and terrorism, lots of questions emerge, but these are two separate issues. There are lots of similarities to unconventional warfare or state terrorism. Soon after 9/11 attacks, war on terrorism was objected by scholars. 1999 attacks in Moscow were to some extent terrorism, yet we can still describe this as state terrorism. Is it possible to differentiate war and terrorism to some extent?**

Dr. Jójárt agreed and stressed that it was not an intent to develop a new notion in the case of Russia. However, Russia could possibly use measures of terrorism for tactical or strategic reasons, but this would not mean that it would be as state terrorism. It could also use methods labelled as terrorism, like using proxies, as in the case of Ukraine – for Ukraine, these are seen as terrorists, but for Russia, it was a campaign against anti-terror operations. But the overall logic, is about political will.

- 2. Can we say that the line between terrorist activities and information warfare is getting blurred depending on your examples? What's the difference between terrorism and the asymmetric approach used by the military?**

Yes, there is a blurred line between these two. If we take the cyber domain, cyber-attack taking out infrastructure, like in Ukraine in 2015 to take out Ukrainian power grid, people died in hospitals because of no electricity – there was human loss and actual casualties due to cyber-attacks. On the other hand, warfare information domain serves as an intermediate and therefore, for terrorist attacks - this can amplify one another.

If we see how Western behaviour is viewed in Russia, from the Russian perspective, the CIA meddling has happened in Venezuela, Ukraine, Libya. Again, warfare information

domain serves as an amplifier and can lead to physical violent acts. Nevertheless, what Russian means under asymmetrical approach is different how the West sees it. War is something cheap, i.e. President Putin says frequently that Russian behaviour to the West is symmetrical not asymmetrical. Some issues are also about negotiations for Russia, i.e. when it comes to arms reduction. What Russia sees as asymmetrical warfare, is also about the use of non-military means. In the Western approach, this is related to an “indirect approach”, i.e. try to counter technological superiority of the West by technological means. In this sense, Russian military has behaved differently compared to the West, Russia has deliberately bombed hospitals in Syria – it has a lot less moral constraint compared to the West. The third aspect that Russia has focused on is the exploitation of vulnerability with regards to the adversary. We have seen that the Russian intelligence is developing certain weapons, i.e. possibly taking out the West’s internet or satellite systems.

- 3. There is a terminology “pyro-terrorism” to explain terror threat to nations with Arson-induced Forest Fires. The fire’s devastation could overwhelm suppression resources, weaken regional economies, destroy critical infrastructure, effect readiness in military forces, and put political pressure on national leadership. Could the “pyro-terrorism” become common tactics of terrorist organizations to create strategic effects?**

Dr. Jójárt stressed that he is not an expert on terrorism but if Russia could use pyro-terrorism, it certainly would, i.e. for neutralizing or mitigating threats before they hit Russia.

- 4. Sponsored terrorism and hybrid threats are increasing in pursue of national interest. Russia's military effort to influence different domains, such as cyber in Ukraine was evident but it failed raise substantial resistance. In your brief, you delineated the fact how a military crafted and blended terrorism with military operations. At this backdrop, in your view, what should have been done by the country to counter State Sponsor Hybrid threat?**

In 2014, Ukraine was particularly in a bad situation in terms of Crimea, *Maidan* protests etc. Given those disadvantages Ukraine had, Russia did not manage to reach its goals of relying only on non-military means. From the summer of 2014, Russia had to intervene with regular forces. In the case of Crimea, this was not the same as Eastern Ukraine. Later, Ukrainian leadership realized that Russia was into military confrontation and Ukrainian forces stepped up in Eastern Ukraine. There is a lot to learn from Ukrainians – they are the ones who faced with modern weapons techniques, especially with regards to electronic warfare and in terms of cyber domain. The main conclusion here is that what Russia did in Ukraine, could not be repeated. Security services, counter-intelligence, resilience in critical infrastructure should recognize early on such threats. The problem was that it was not seen as normal peace time operation unless first shots were fired in Ukraine.

Col. Daniel Wayne STONE

- 1. Organized crime and terrorism use one another to fulfil their goals. Since organized crime has no physical boundaries, it has infiltrated and corrupted officials on both sides of the borders, what should be our approach and tackle this “partnership” be?**

To tackle the partnership between terrorist organizations and organized crime, it is needed to look at anti-corruption measures, also identified by the UN. It is about linking nations with organizations such as Interpol and putting in place systems and laws to punish. These systems are especially important in terms of border-management. The inter-relationships between multiple organizations is required to share information and maximize the capabilities and assets of various law enforcement, governmental, and military organizations. This is an area where military expertise at setting up and running cross governmental organizations should be used to support civil border security agencies and law enforcement. The international community also has experience in this area and can offer advice more to tackle this issue.

2. What about women in the role of mothers to avoid joining the terrorist activities? Would better educated mothers prevent recruitment of the terrorist organizations by nature?

Women's roles as mothers to counter terrorism are important. Women are able to influence and keep their children and families out of terrorism and often, they are the first line of defence. An example of this is the "Mother Schools" model developed in 2018 by Women Without Borders, and used in Pakistan, India, Tajikistan, Nigeria, and Tanzania. If we keep supporting such models and civil society, they can come up with answers we could never think of. Thus, we should promote these types of activities. It also depends for NATO whether it is an operational mission. When on an operational mission, it opens more opportunities to engage with civil society groups and promote such kind of activities.

3. Is there a policy against recruiting children in terrorist organizations?

This is rolled up in the whole gendered process. Here, we are talking also about boys and girls, not only men and women, and how they are affected by terrorist organizations. Terrorist organizations are more willing to recruit younger people and are also willing to use children, manipulating gendered norms. Just as they are using Western perceptions of gender as a strategic tool, they are also willing to use children as strategic assets. For example, US forces in Iraq were confronted on a number of occasions by children. The terrorists chose children because they understood US forces' values that children are non-combatants and should be protected. The issue is about how to look at the role of gender and how gendered norms are understood by the various sides to understand how gender can be used against security forces and also understand how security forces can operationalize gender norms to support the government. We have to be cognizant that gender norms change over time, based on conditions.

4. If “gender is socially constructed role based on sex,” does it mean that the society has special expectations which are the basic disadvantage to identify and prevent terrorism?

The question is, are there specific advantages and disadvantages to recognize and prevent terrorism? When we look at the root causality, how does an organization manipulate, use a person and how they define “me as me”? How do I see myself as biological male or female? But doing this by only looking at biological sex is not feasible because women in terrorism join the organization for same reasons as men do; women don’t join based on biological sex, but rather based on gender, power, economics, and ideology – areas in which terrorist organizations operate. We typically look at religious based organizations which tend to be very fundamentalist, i.e. declaring what men and women should wear and what they should not wear. In terms of right-wing terrorist organizations, they also include women and have similar fundamentalist views with slight variations. If we understand how terrorists think about gender, this can be very important for us to understand how they operate and how we can then develop strategies to counter their views.

Dr. Warnes added that traditional groups would use young people for rioting, i.e the *Intifada*, and use this as a selection process, identifying courageous youngsters for terrorist groups. Also, there is an exploitation of gaming platforms, i.e. “gamifications”, which are now appealing to radicalizing young people. As such, some of the messages and symbolism out there is very worrying. Religious terrorist groups have also started to use this, being corrupted, and using game platforms for this.

DAY II – Session 1: Critical Infrastructure Security and Resilience

Book Volume 1

Moderated by: Dr. Carol V. EVANS (USA), *Director, Strategic Studies Institute and US Army War College Press*

CI Overview, Policy Definitions & Importance

Prof. Ronald Sanford BEARSE

Nauset National Security Group, LLC, Hyannis MA

The very first chapter of the handbook authored by Prof. Ronald Sanford Bearse is entitled “*An Overview of Critical Infrastructure, its Importance, and Key Policy Terms*”. This chapter covers several questions regarding the issue as follow:

- What is critical infrastructure?
- Why is it important?
- What is the difference between critical infrastructure protection (CIP) and critical infrastructure security and resilience (CISR)?
- What are some of the key terms defined in national CISR policy?
- What are the core areas of activity or (work streams) involved in implementing CISR policy?

Although there is not a universal definition of *Critical Infrastructure* (CI), many nations that have national policies and plans for protecting their critical infrastructure define CI as:

“...the physical and cyber systems and assets that are so vital to the country that their incapacity or destruction would have a debilitating impact on its physical, economic or national security or public health or safety.”

Most countries that have established a national CIP or CISR policy have identified several sectors as Critical Infrastructure Sectors. Some nations have identified other sectors -i.e. industrial or economic- as critical. However, the figure below points out the vast majority of sectors which are considered as CI sectors. On the other hand, it should be recalled that these

elements or sectors are only representative and just exemplifies some of the mostly-argued aspects.



Figure 7—Representative List of Critical Infrastructure Sectors

The figure below exemplifies some typical CI sectors and highlights the special status of the communications, energy, transportation and water sectors as *lifeline infrastructure sectors*. Lifelines infrastructure sectors have defining characteristics that separate them from other CI sectors. They provide necessary services that support every home, business, or government agency, every single part of daily life in general. However, disruption of this service has the potential to develop life-threatening situations. They involve complex physical, electronic networks that are inter-connected within and across multiple sectors. As a result, disruption of just one lifeline unavoidably holds the potential to threaten the other lifeline and non-lifeline sectors in a cascading effect.

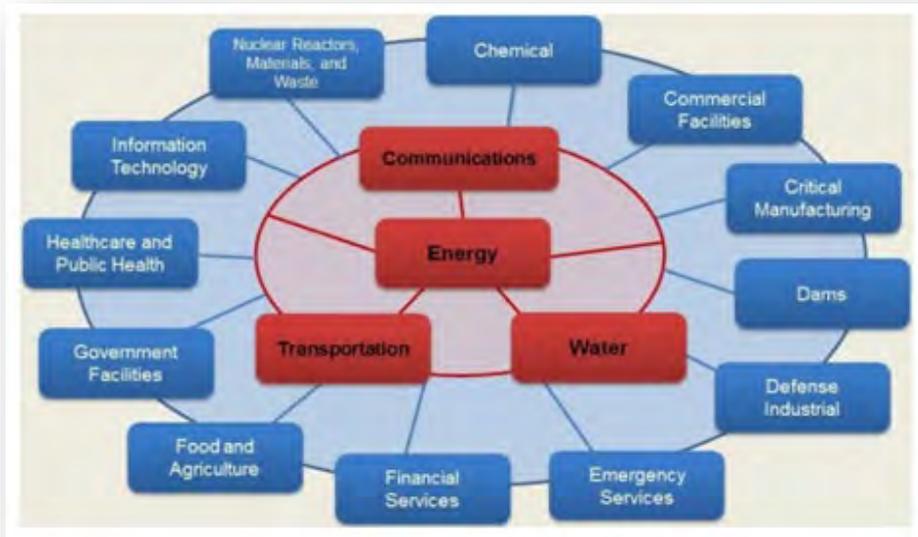


Figure 8—Critical Infrastructure Sectors (Blue) and Lifeline Sectors (Red)

In addition to nations' definitions of CI, Prof. Barse drew attention to NATO's CI definition. He stressed that within NATO, CI is a general term. NATO considers CI as *a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political and/or social life on which a nation and/or the Alliance depends*. On the other hand, there are many definitions even across NATO in order to clarify the area of operation. For instance, from an Allied Command Operations (ACO) perspective, Critical Infrastructure is categorized into three different sub-categories:

1. Critical National Infrastructure (CNI).
2. Mission-Vital Infrastructure (MVI).
3. Key Infrastructure (KI).

Critical National Infrastructure (CNI) is assets, facility systems and networks identified by territorial host nations that are integral to continue delivery and integrity of the essential services upon a nation relies. The destruction of these will led to severe military, economic, political, and social consequences to the nation.

Mission-Vital Infrastructure (MVI) is infrastructure within a joint operations area which NATO and troop contributing nations' forces rely on to build capability. Again, the destruction of MVI singularly creates a decisive disadvantage to a NATO mission.

Key Infrastructure (KI) contains facilities, systems, and networks within the joint operations area which host nations, NATO, or troop contributing nations forces rely on to develop capability.

At this point, a question arises. How much of NATO's mission readiness depends on the assured availability of critical infrastructure? CI is mostly provided by private sectors or with private sectors' cooperation. Today, this issue is something to carefully consider. During operations or exercises, for instance, about 90% of military transport relies on civilian ships, railways, and aircraft. Lacking an available critical infrastructure could result in catastrophic consequences for a nation's safety, a nation's well-being, environment, national security, and economy.

Prof. Barse highlighted some other reasons that address the importance of critical infrastructure. First of all, the public requires/demands/expects critical functions that are available for 24/7/365. Second, failure to provide all-time service can be catastrophic locally, regionally, nationally, and globally. Moreover, adversaries are penetrating and disrupting various parts of our CI with little or no repercussions. Prof. Barse recalled that a small group of hackers launching a ransomware attack on *Colonial Pipeline* just a couple of months ago. This example indicates the possible level of destruction in case of such an unexpected attack that was able to damage one of the world's greatest supply chains. Therefore, the Colonial Pipeline attack should be the turning point for why nations should pay greater attention to **resilience**. An organization's ability should not only used to improve the security of these critical infrastructure systems, but they should also increase their ability to respond and spring back after a disruption. Increasing this ability also strengthens the resilience part of CISR. At this point, **Smart Systems** and **Internet of Things (IoT)** deliver efficiencies and savings, but they may also create massive new vulnerabilities.

Over the last twenty years, most national critical infrastructure policies focused solely on "protection" of CI to make it more secure and resilient. This is primarily a function of the evolution. Because today, the number of threats directed to the CI is continuously increasing. As a result, States initiate policies and strategies in order to meet the expectations to overcome those threats. Under the **Critical Infrastructure Security and Resilience (CISR) Construct**, the terms *security* and *resilience* certainly support the idea of protection. Security refers to a notion that covers reducing the likelihood of attacks against CI and securing CI sectors from terrorist attacks or any kind of disasters. The term resilience, means the ability of the CI to resist, absorb, recover from, or successfully adapt to continuing changes. A resilient

infrastructure is robust, agile, and able to adapt and recover rapidly from the disruptions. Resilience increasingly applies to larger social and technical systems.

CISR informs policies that mitigate the consequences of such events and speak to the vital need to develop and implement a comprehensive risk management strategy. Prof. Bearse also stated that CISR further requires change in focus of education and training to ensure that core CISR work streams are completed and well-managed.

When it comes to CISR Planning and Operations, Prof. Bearse stressed several key work streams that has to be taken into consideration:

1. Defining Clear Roles and Responsibilities for all Stakeholders,
2. Identifying and Determining the Criticality of National Infrastructure and or Critical National Functions,
3. Mapping Critical Infrastructure Dependencies and Interdependencies,
4. Determining Critical Infrastructure Vulnerabilities,
5. Defining Clear Roles and Responsibilities for all Stakeholders
6. Identifying and Determining the Criticality of National Infrastructure and or Critical National Functions,
7. Mapping Critical Infrastructure Dependencies and Interdependencies,
8. Determining Critical Infrastructure Vulnerabilities,
9. Developing and Exercising Continuity of Operations and Information Technology Disaster Recovery Plans,
10. Providing Physical and Cyber Security and Resilience Measures,
11. Ensuring the Integrity, Security and Continuity of Critical Infrastructure Supply Chains
12. Expanding opportunities to develop and deliver CISR education and training
Implementing a robust Test, Training and Exercise Program.

All in all, Prof. Ronald S. Bearse warns that while these aforementioned points define much of “**what**” needs to be done, the extent to which a nation effectively develops and implements the “**what**” is a function of “**how**” well the people responsible for leading and managing CISR work streams foster the *collaboration, cooperation, coordination, communication, and concentration* which are indispensable to building and sustaining a viable, risk based, CISR posture.

An Overview of Critical Infrastructure, its Importance, and Key Policy Terms

For 2021 NATO COEDAT TEC

Presented by Ronald S. Bearse
Principal, Nauset National Security Group, USA
Adjunct Professor, Massachusetts Maritime Academy USA

Chapter 1 “Sets the Stage” By Asking:



What is critical infrastructure?

Why is it important?

What is the difference between critical infrastructure protection (CIP) and critical infrastructure security and resilience (CISR)?

What are some of the key terms defined in national CISR policy?

What are the core areas of activity or (work streams) involved in implementing CISR policy?

What is Critical Infrastructure (CI) ?

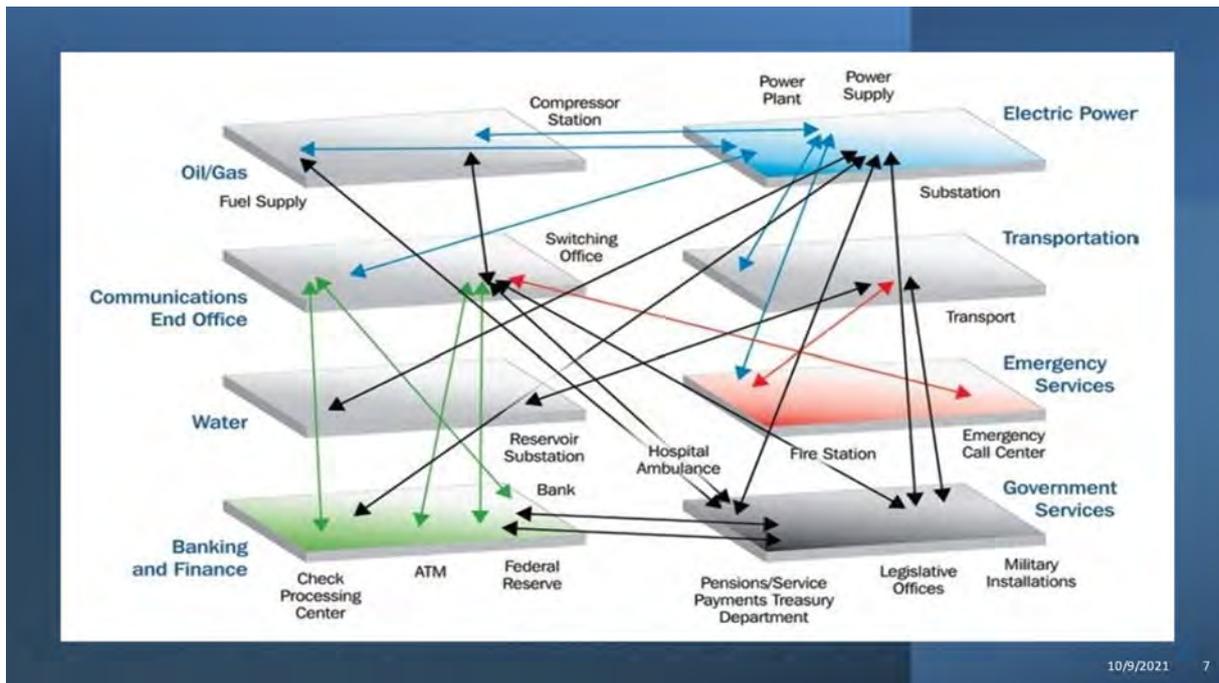
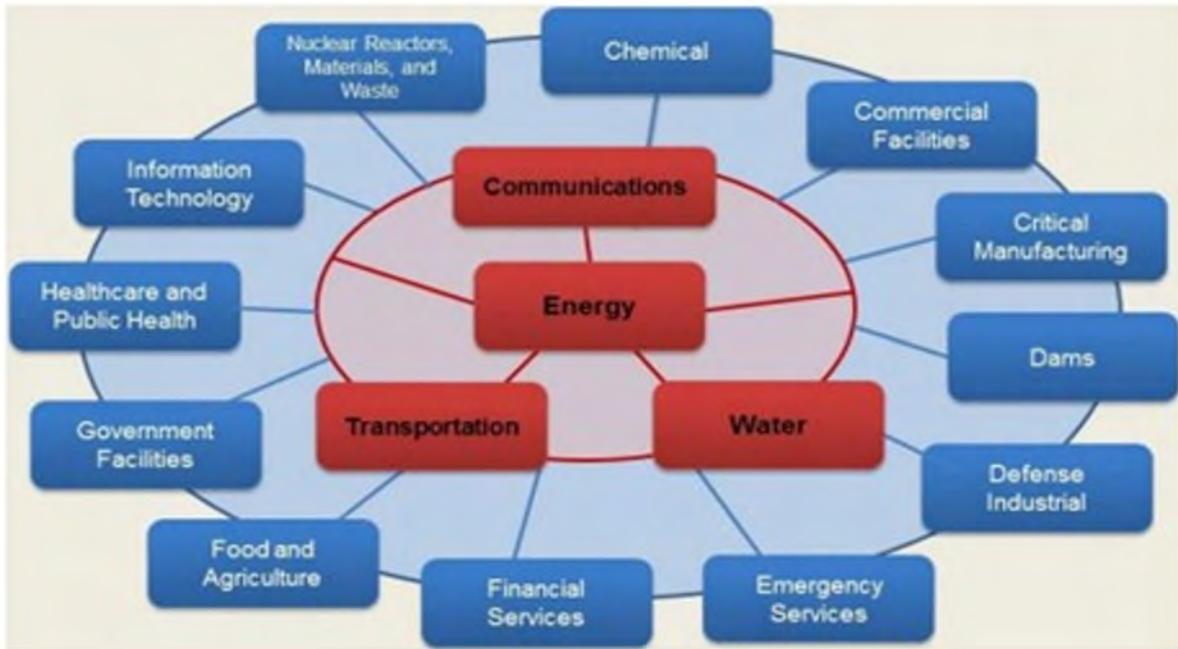
No universal definition, but most countries that have national policy and plans for protecting their critical infrastructure define CI as:

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

Representative List of Critical Infrastructure Sectors



10/9/2021 5



Definition Used by Allied Command Operations (ACO)

Critical Infrastructure. Within NATO Critical Infrastructure is a general term describing a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political and/or social life on which a nation and/or NATO depends.

Again, from an ACO perspective, Critical infrastructure is categorized into three different sub-categories:

1. **Critical National Infrastructure (CNI).**
2. **Mission-Vital Infrastructure (MVI).**
3. **Key Infrastructure (KI).**

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

Why is Critical Infrastructure Important?

- Public demands/expectations that critical functions be available 24/7/365.
- Failure can be catastrophic locally, regionally, nationally and globally
- Adversaries are penetrating and disrupting various parts of our CI with little or no repercussions
- “Smart Systems and IoT” deliver efficiencies and savings, but also create massive new vulnerabilities.
- Ensures national security, economic competitiveness, and public health and safety.

Bottom Line: CIP/CISR should be considered the most serious national security concern since the development of the atomic bomb.

What is the Difference between CIP and CISR?

- The reality is you cannot protect all CI against all threats
- The Critical Infrastructure Security and Resilience (CISR) Construct
 - CISR is the “vision”
 - The terms “security” and “resilience”
 - Resilience increasingly applies to larger social and technical systems
 - CISR informs policies that mitigate the consequences of such events and speak to the vital need to develop and implement a comprehensive risk management strategy
 - Requires change in focus of education and training to ensure that core CISR work streams are completed and well -managed.

Key Work Streams in CISR Planning and Operations

- Defining Clear Roles and Responsibilities for all Stakeholders
- Identifying and Determining the Criticality of National Infrastructure and or Critical National Functions
- Mapping Critical Infrastructure Dependencies and Interdependencies
- Determining Critical Infrastructure Vulnerabilities

Key Work Streams in CISR Planning and Operations

- Using Applicable Risk Assessment, Analysis and Management Approaches
- Establishing Crisis Management Capabilities
- Establishing Public Private Partnerships between Government and Private Sector Owners of Critical Infrastructure
- Establishing and Implementing Collaboration and Information Sharing Mechanisms between Government and Critical Infrastructure Owners and Operators

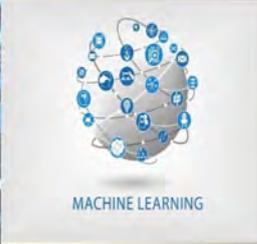
Key Work Streams in CISR Planning and Operations

- Developing and Exercising Continuity of Operations and Information Technology Disaster Recovery Plans
- Providing Physical and Cyber Security and Resilience Measures.
- Ensuring the Integrity, Security and Continuity of Critical Infrastructure Supply Chains
- Expanding opportunities to develop and deliver CISR education and training Implementing a robust Test, Training and Exercise Program

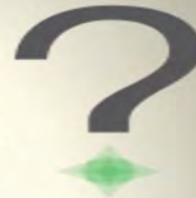
Key Lesson Learned this Century

While the last three slides define much of “what” needs to be done, the extent to which a nation effectively develops and implements the “what” is a function of “how” well the people responsible for leading and managing CISR work streams foster the **collaboration, cooperation, coordination, communication, and concentration** which are indispensable to building and sustaining a viable, risk based, CISR posture.

Looking Back and Looking Ahead



Any
questions



Contact: rbearse@nnsllc.com or
rbearse@maritime.edu
USA Phone #: +1 (703) – 928-5779

Terrorist Threats to CI

Mr. Raymond MEY & Mr. Malcolm BAKER

Mr. Raymond Mey and Mr. Malcolm Baker authored the second chapter of Critical Infrastructure Security and Resilience Book Volume 1. The concept of threat is a quite diverse topic with many different definitions. Therefore, Mr. Mey states that a growing need for evaluating the concept of threat with regard to the critical infrastructure security emerged. In order to meet this need, for the chapter they co-authored, they have come up with a comprehensive definition of threat which also reflects the aspects of CI. According to Mey and Baker, the threat is

“A possible capability, strategic objective, criminal behavior or intent which could cause significant harm to the continuing area of operations and ability, a CI to support its national welfare and interest.”

Nowadays, the concept of threat has become “**All Hazards**” when it comes to addressing CI. All hazards encapsulate three different areas of interest:

1. ***Consideration of Natural Disasters***

Tsunamis, floods, hurricanes, etc. These disasters are more or less specific to certain areas. Depending on the part of the world that you live in, one of these disasters may influence one area more than the other. However, the challenge of the natural disasters is much more difficult to prevent compared to other threats related to All Hazards.

2. ***Accidental Events***

These incidents may occur due to a human error or organizational deficiencies and they can certainly contribute to threats that can make significant impact on the CI.

3. ***Types of Threats Emanating from Manmade Aspects***

Majority of the threatened CI sectors’ future lies in the operators’ hands. They have to consider every single aspect to tackle the issue and this is the rationale for adopting All Hazards Approach.

Businesses are also facing challenges that threaten their supply chains, especially after COVID-19. The business sector is also concerned about terrorist or manmade threats. At this point, All Hazards Approach indeed provides a very sound return on investment that is asked of the

operators of CI, because all of this actually costs a great amount of money and making profit is also taken into account. If the companies are encouraged to spend money on this and invests on facilities, structures, systems, components, they need a guarantee to secure their investment from any possible threats.



Figure 9—Risk/Threat Radar

The figure above exemplifies the variety of threats we are facing at different times and underline the point that one-size-fits-all approach does not function very well to deal with these threats. Therefore, we need to understand the threat relative to the CI that we are trying to protect and which threats or hazards could manifest themselves on our radar.

In order to clarify the issue, Mr. Mey and Baker have conducted detailed research on different case studies across the world i.e.

- Westgate Mall in Nairobi/Kenya,
- Westminster Bridge, London/ UK,
- Amenas Gas Facility Attack, Algeria,
- Aramco, Saudi Arabia

Mr. Mey explains that it is very critical to have a process in terms of determining where the threats are coming from in order to engage and have an appropriate security program from a

risk-based perspective. In order to do so, authorities should follow a process that the CI owner should utilize by looking at information and intelligence and try to take counter-measures against possible vulnerabilities and conduct gap analysis. As a result, they should come up with a plan testing the reliability of their threat and vulnerability detection and they could conclude with an idea whether the plan is implementable. This process is a continuous one and never ends. A good program of threat assessment within a CI should be focused on this continuing process to look at the threats. This allows one to constantly be in position to see the threat coming over the horizon.

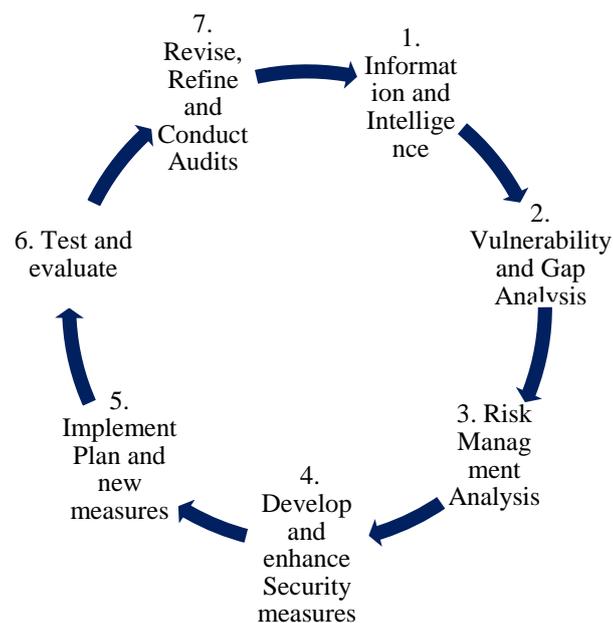


Figure 10—Threat Assessment Process

Mr. Mey and Mr. Baker's concluded with the potential role of NATO and COE-DAT in securing CI in terms of threat assessment. They recommend that COE-DAT can think about how to

- Generate joint intelligence,
- Develop CISR communications,
- Develop CISR "Fusion Cell",
- Learn from experience.

Presentation



Introduction



- Chapter 2 – Threat
- Authors:
 - Raymond Mey – former US Federal Bureau of Investigation (FBI)
 - Malcolm Baker – former UK New Scotland Yard counter-terrorism policing

Chapter 2 - Threat



- Understanding threat and security
- Definitions of 'threat'
- Threats versus hazards
- Adopting an 'All threats, all hazards' approach
- Relevance to Critical Infrastructure



3 / 30

UNCLASSIFIED

Critical Infrastructure Security & Resilience



- What are the threats?
- What are the hazards?
- Developing a 'risk radar'
- Lessons Identified
- Use of Case studies



4 / 30

UNCLASSIFIED

Threat Assessment Process



5 / 30

UNCLASSIFIED

Summary and comments



- Role of the State in CISR
- CI Operators
 - Return on Investment
 - Security AND Resilience
- Defining NATO's role



6 / 30

UNCLASSIFIED



- COE-DAT's role
 - Joint Intelligence
 - Develop CISR communications
 - Develop a CISR 'Fusion Cell'
 - Learning from Experience



Hybrid Threats to NATO CI

Dr. Carol V. EVANS

Director, Strategic Studies Institute and US Army War College Press

Protecting key global critical infrastructure is a NATO Strategic Security Concern and Challenge. Over the years, many different policy documents stressed the importance of critical infrastructure. NATO provides a deterrent to armed attack that depends on critical infrastructure. NATO's role in the protection of critical infrastructure is not only based on credible military capabilities, force structure and force projection, but it is also based on Continental United States (CONUS) and Outside the Continental United States (OCONUS) and NATO infrastructures (transportation, energy, water, communications) to support short fused response, reinforcement timelines and means of sustainment.

To provide an understanding of adversarial hybrid threats to CI and the innovative ways in which the US and NATO are countering them, this presentation is structured in three sections. The first section addresses the evolution in the nature of the threat to CI. The second provides an analysis of several hybrid threat vectors to US and NATO warfighting, force projections, and sustainment capabilities. The third section highlights measures that NATO may take in order to enhance Critical Infrastructure Security and Resiliency (CISR).

The nature of the threat to the critical infrastructures in US and NATO countries has evolved significantly from one that was based primarily on kinetic attacks by terrorist organizations, to the exploitation of cyber and hybrid means by nation states, proxies and other adversaries. . As seen from a cyber-perspective, or in other words cyber and space domains, connectivity is now between information and communications systems, and Internet of Things has proliferated the use of cyber as a means of attacking critical infrastructure. In that sense, the Ukraine became a testing ground for hybrid warfare, with Russia using a sophisticated mix of physical, cyber, and information warfare modes of attack.

The term "*hybrid warfare*" became a domain of discussions in academia questioning if there is anything new in the term justifying its use or if it is just a component of asymmetric warfare under hybrid threat activity. . NATO utilizes hybrid threats as an overarching framework (hybrid warfare as a subset) to include other activities such as disinformation, economic

pressure, use of irregular forces that are not expected to trigger Article 5 but which undermine and destabilize civil societies.

Adversaries are targeting NATO's critical infrastructure capabilities, particularly those provided by the US in order to support the Alliance's force projection, sustainment, and warfighting capabilities. Three different areas are considered to be greatest vulnerabilities to the Alliance in terms of critical infrastructure:

1. Target US/Euro electric grids that power U.S. installations and NATO bases,
2. Degrade mobility and sustainment operations by targeting logistics nodes for forward deployed/deploying forces,
3. Penetrate and erode U.S. & NATO Defense Industrial Bases.

Electric Grids

The US Department of Homeland Security/Federal Bureau of Investigation (DHS/FBI) confirmed in March 2018 that Russian government cyber activity targeting energy and other critical infrastructure sectors were occurring in the U.S.. U.S. Department of Defense (DoD) bases and installations are dependent upon continuous and assured power to support its varied missions for CONUS and OCONUS expeditionary operations. Underinvestment in U.S. base facilities, combined with increased DoD reliance on "outside the fence" private sector owned infrastructure, means CONUS-based operations can be seriously degraded.

Mobility & Sustainment Impacts

From a force projection issue, we are relying on United States Transportation Command (USTRANSCOM) to provide NATO with strategic mobility and deployment capabilities. USTRANSCOM relies heavily on commercial air, ground, and maritime transportation support which are vulnerable to cyberattacks and energy disruptions. Therefore, rebalanced U.S. force structure in Europe requires secure transportation, energy supplies, and communications, **to project and sustain rapid power anywhere in theatre.**

Impacts to US/Euro Defense Industrial Base (DIB)

Analysis needs to be directed on the degree and impact foreign direct investments by Russia and China particularly in Europe may have on NATO mobility and sustainment operations. The importance of foreign direct investments in strategic sectors is discussed in NATO's review of "*Resilience: The First Line of Defense*":

"The degree and impact of foreign direct investment in strategic sectors – such as airports, sea ports, energy production and distribution, or telecoms – in some Allied nations raises questions about whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military."

This strategy can be seen as a tool to penetrate U.S. and European Defense Industrial Base. In this regard, Dr. Evans examines Chinese investments in controlling in Southern European electric grids particularly in Portugal, and Greece. She also analyzes Russian and Chinese foreign investments on key strategic locations such as San Diego, Finland, and Scotland for intelligence gathering and other types of activities. She further conducted research on maritime affairs and found that China pays great attention to maritime transportation facilities as well Russian and Chinese joint maritime exercises.

NATO CISR Measures

NATO's initial efforts to secure CI have focused on developing "*organizational capacity*". NATO has built institutions via the establishment of NATO Centres of Excellence to support CISR such as:

1. 2004 COE-DAT (Defense Against Terrorism) Ankara Turkey
2. 2008 CCD-COE (Cooperative Cyber Defense) Tallin, Estonia
3. 2012 COE-ENSEC (Energy Security) Vilnius, Lithuania
4. COE Maritime Security Istanbul, Turkey. Established in 2012, and awaiting formal NATO accreditation.

NATO also comments on the significance of CISR and protective measures in summit releases. In particular, the 2018 Brussels Summit stated:

“We are committed to strengthening our ability to deploy and sustain our forces and their equipment, throughout the Alliance and beyond, and aim to improve military mobility by land and air as soon as possible but no later than 2024.”

In line with that commitment to strengthen the protective capacity, NATO created two NATO Commands:

1. NATO Headquarters Joint Forces Command – Norfolk (JFCNF) for protection of sea lines of communication in the Atlantic,
2. Joint Support and Enabling Command (JSEC) in Ulm, Germany for mobility and sustainment in support of rapid movement of troops and equipment across Europe (FOC/2021).

NATO CISR Measures include:

- Raising awareness through intelligence sharing, consultations with the EU, and the private sector,
- Enhancing DoD/NATO military energy efficiency and use of microgrids for U.S. installations,
- Strengthening cyber defenses through the deployment of CERT teams within NATO member countries, new Cyberspace Operations Centre,
- Integration of military energy and cyber requirements within NATO exercises (DEFENDER-21 21/Locked Shields 2018) and war games.
- 2016 NATO Warsaw Summit enhancing CI resiliency with seven baseline requirements for civil preparedness.



THE UNITED STATES ARMY WAR COLLEGE



Protecting Key Global Critical Infrastructure is a NATO Strategic Security Concern and Challenge

STRENGTH-WISDOM



THE UNITED STATES ARMY WAR COLLEGE



The deterrent value of NATO forces is critical

It is based **not just** on credible military capabilities, force structure and force projection **but on U.S. CONUS/OCONUS and NATO infrastructures** (transportation, energy, water, communications) to support short fused response and reinforcement timelines and means of sustainment

STRENGTH-WISDOM



Agenda

- A Hybrid Threat Framework for NATO CI
- CI Threat Impacts to NATO Missions & Capabilities
- NATO Measures to Enhance Critical Infrastructure Security and Resiliency (CISR)

STRENGTH-WISDOM



Evolution of Threats to NATO CI

- Prior attacks against NATO host country CI required the attackers to be physically present.
- Connectivity between information & communications systems, and IoT has proliferated the use of cyber as a means of attacking CI.
- Ukraine became a testing ground for hybrid warfare, with Russia using a sophisticated mix of physical, cyber and information warfare modes of attack.
- NATO now utilizes hybrid threats as an overarching framework (hybrid warfare a subset) to include other activities such as disinformation, economic pressure, use of irregular forces etc that are not expected to trigger Article 5 but which undermine and destabilize civil societies.

STRENGTH-WISDOM



CI Vulnerabilities on Missions & Capabilities

- Undermine NATO force projection, sustainment and warfighting capabilities:
 - Target US/Euro electric grids that power U.S. installations and NATO bases
 - Degrade mobility and sustainment operations by targeting logistics nodes for forward deployed/ing forces
 - Penetrate and erode U.S. & NATO Defense Industrial Bases



STRENGTH-WISDOM



Base/Installation Vulnerabilities

- March 2018 DHS/FBI confirmed Russian government cyber activity targeting energy and other critical infrastructure sectors in the U.S.
- DoD bases and installations are dependent upon continuous and assured power to support its varied missions for CONUS and OCONUS expeditionary operations
- Underinvestment in U.S. base facilities, combined with increased DoD reliance on "outside the fence" private sector owned infrastructure, means CONUS -based operations can be seriously degraded.



U.S. bases increasingly used to conduct specialized warfighting activities, such as anti-ISIS/AQ UAV operations .

STRENGTH-WISDOM



Mobility & Sustainment Impacts



- Rebalanced U.S. force structure in Europe requires secure transportation, energy supplies, communications, **to project and sustain rapid power anywhere in theatre.**
- USTRANSCOM provides strategic mobility and deployment capabilities but relies heavily on commercial air, ground and maritime transportation support which are vulnerable to cyberattacks and energy disruptions
- June 2017 Russian-launched NotPetya attack brought down the entire port, shipping, logistics, container operations of major USTRANSCOM provider, Maersk.

USTRANSCOM

Commercial and Military shipping support for...

	Contingency Operations		Steady-State Operations	
	Passenger	Cargo	Passenger	Cargo
Air	High	High	High	High
Sea	Low	High	Low	High
Ground	Low	Low	Low	High

Source: <https://fas.org/sgp/crs/natsec/IF10840.pdf>

STRENGTH-WISDOM



Impacts to US/Euro DIB



“The degree and impact of foreign direct investment in strategic sectors – such as airports, sea ports, energy production and distribution, or telecoms – in some Allied nations raises questions about whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military.”

NATO, “Resilience: The First Line of Defence.”



STRENGTH-WISDOM



NATO CISR Measures

- Institution building via the establishment of NATO Centres of Excellence to support CISR:
 - 2006 COE-DAT (Defence Against Terrorism) Ankara Turkey
 - 2008 CCD-COE (Cooperative Cyber Defense) Tallin, Estonia
 - 2012 COE-ENSEC (Energy Security) Vilnius, Lithuania
 - COE Maritime Security Istanbul, Turkey. Established in 2012, and awaiting formal NATO accreditation



STRENGTH-WISDOM



NATO CISR Measures

- 2018 Brussels Summit:

“We are committed to strengthening our ability to deploy and sustain our forces and their equipment, throughout the Alliance and beyond, and aim to improve military mobility by land and air as soon as possible but no later than 2024”
- Creation of two NATO Commands:
 - NATO Headquarters Joint Forces Command – Norfolk (JFCNF) for protection of sea lines of communication in the Atlantic
 - Joint Support and Enabling Command (JSEC) in Ulm, Germany for mobility and sustainment in support of rapid movement of troops and equipment across Europe (FOC/2021)



STRENGTH-WISDOM



NATO CSIR Measures

- Raise awareness through intelligence sharing, consultations with the EU, and the private sector.
- Enhance DoD/NATO military energy efficiency and use of microgrids for US installations
- Strengthen cyber defenses through the deployment of CERT teams within NATO member countries, new Cyberspace Operations Centre,
- Integration of military energy and cyber requirements within NATO exercises (DEFENDER -21 21/Locked Shields 2018) and war games.
- 2016 NATO Warsaw Summit enhancing CI **resiliency** with seven baseline requirements for civil preparedness
- *"NATO must remain prepared for both conventional and hybrid threats: from tanks to tweets,"* NATO Secretary General Jens Stoltenberg

STRENGTH-WISDOM



U.S. Policy CISR Measures

- Presidential Executive Order 13805.
- FY 2018 & 2019 National Defense Authorization Acts
- Committee on Foreign Investment in the United States (CFIUS)
- 2012 OSD Mission Assurance Strategy, 2016 DoD Directive 3020.40 and 2018 MA Construct 3020.45
 - Improve the resilience of critical defense missions via strengthening partnerships with private sector infrastructure owners/operators



STRENGTH-WISDOM



THE UNITED STATES ARMY WAR COLLEGE



**Forward Presence,
Combat Operations, Stability
Operations, Counter Insurgency,
Crisis Response contribute to the
deterrence of would be
adversaries and to the assurance
of allies.**

**ALL depend on secure CI
protection**

STRENGTH—WISDOM



THE UNITED STATES ARMY WAR COLLEGE



**Questions?
Feedback!**

Contact Information

carol.evans@armywarcollege.edu

STRENGTH—WISDOM

Crisis Response & Consequence Management

Mr. Malcolm BAKER

Crisis response and consequence management are quite significant. From NATO's perspective, the Alliance's, member states' and partner countries' roles are increasing in order to manage crisis. In this regard, NATO even documented the "*Strengthened Resilience Commitment*" (NATO 2030), including the NATO Article 3 "Resilience and Crisis Management". The idea was to learn mainstream crisis management processes and whether they can empower the Alliance.

The words incident, emergency and crisis are often used erroneously as interchangeable or synonymous terms to describe an event that occurs or a scenario. Each of these terms are different but are often used to describe negative or unwelcome consequences. Incidents, emergencies, and crises can not only bring about negative outcomes but may also provide positive consequences or opportunities for organizations.

As **Error! Reference source not found.** illustrates an initiating event or 'trigger' starts the response process, but the event could be a 'slow burn' or incremental event rather than a 'sudden impact' event. The diagram represents a general depiction to illustrate the key phases. Achieving 'consolidation and control' could take some time as shown by the recent outbreak of the Covid-19 Coronavirus pandemic, together with the latter stages of public inquiries and hearings that will follow.

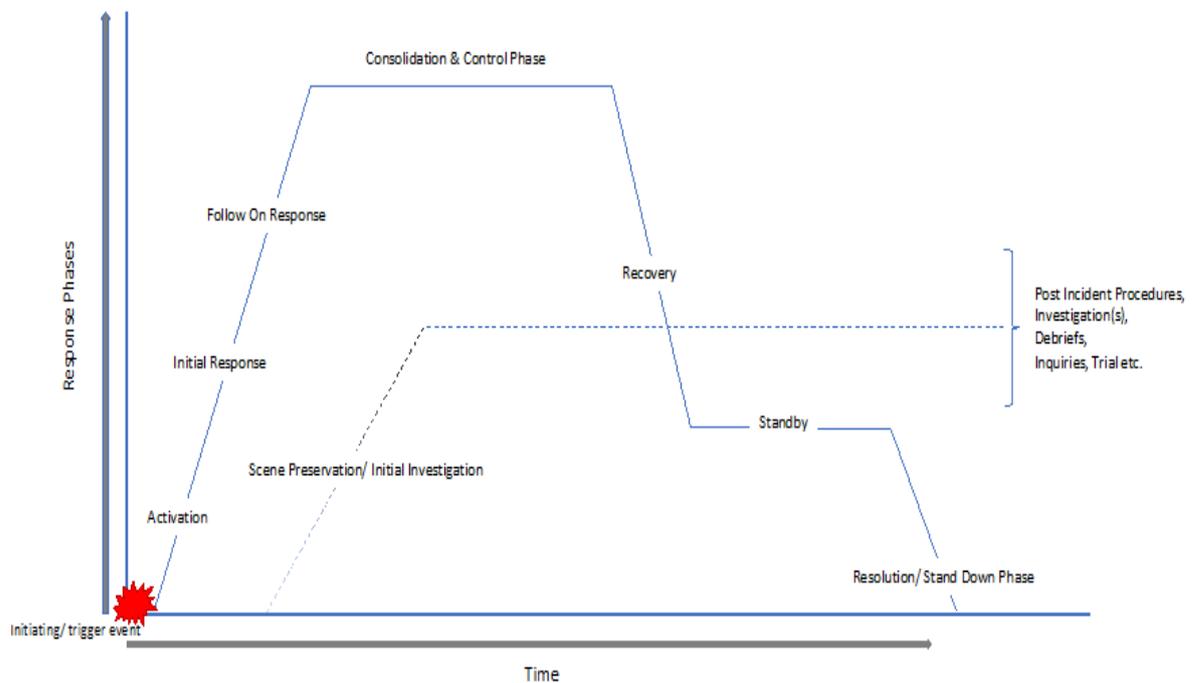


Figure 11—Anatomy of a Crisis

At this point, it is quite useful to comprehend the definition of crisis. Since NATO provides a clear definition for crisis management as “*coordinated actions taken in order to defuse crises, prevent their escalation to armed conflict and/or containing resulting hostilities*”. This may not be what the critical infrastructure is dealing with. Therefore, first we need to understand the crises. Under the document entitled “Crisis management - Guidance and good practice”, NATO simply puts the definition of crisis as

“*...abnormal and unstable situation that threatens the organization’s strategic objectives, reputation or viability.*”

Mr. Baker further explains several key standards that could also be implemented in national level:

1. **Predictability**: Generally foreseeable, although timing, nature and detail may be unpredictable.
2. **Onset**: Short notice/ no-notice.
3. **Urgency and pressure**: Incident response usually spans a short time frame of activity. Resolution prevents longer-term exposure/ significant impacts.
4. **Impacts**: Adverse events – reasonably well understood. Predefined responses work well.

5. **Media scrutiny**: Positive when well managed but can be negative if an incident escalates into a crisis.
6. **Manageability through established plans and procedures**: Resolution often achieved by applying appropriate, predefined procedures and plans, including adequate resources.

In crisis management, there are also core concepts and principles that needs to be shed light on as well:

1. **Predictability**: Often unique, rare and unforeseen; or poorly managed incidents/ events.
2. **Onset**: Sudden onset/ no-notice, or ‘rising tide’.
3. **Urgency and pressure**: Higher sense of urgency; Scale, Duration and Impact.
4. **Impacts**: ‘Strategic shock’; crises can disruptor affect an entire organization, transcend geographical and sectoral boundaries. Complexity, uncertainty together with incomplete/ ambiguous information.
5. **Media scrutiny**: Crises create significant public and media interest, with potential to negatively affect reputation. Inaccurate media coverage and social media networks may lead to reputational damage/ escalation.
6. **Manageability through established plans and procedures**: Rarely resolved through application of predefined procedures. Crises require flexible, creative, strategic and a dynamic response.

Therefore, the idea is that critical infrastructure operators, owners and other possible actors should be involved in the process of developing a crisis management capability. In that sense, militaries are really good at creating crisis management frameworks and by scrutinizing these procedures, Mr. Baker argues, one can easily understand how states need to build a crisis management capability to manage crises, respond effectively and manage the possible consequences. In terms of the intent, what does a state want to achieve? Are we going back to normality? In this regard, the COVID-19 pandemic is quite interesting. We are not only witnessing a global health crisis, but we also see the difficulties and transformation in supply chains. To deal with a crisis in a proper manner, “*policy, planning and priorities*” are significant but understanding roles and responsibilities, authority and accountability, and situation awareness are even more important.

Mr. Baker states that there are some challenges in terms of crisis leadership. For instance, crisis management is not “*business as usual*”. Usual plans will not possibly work. Therefore, the leadership is absolutely pivotal and top-down resolution in many respects. Crisis leadership also requires rigorous, realistic, and repeated training. The authorities in charge of crisis management should consider the tempo or battle rhythm of a crisis, decision-making, complexity (scale, duration and impact), severity and seriousness, and uncertainty and ambiguity.

In order to better manage the process, in his chapter Mr. Baker brings out several questions with regard to situation, direction and action.

1. ***Situation***

What is happening? What are the impacts? What are the issues? What are the risks?
What might happen? What is being done about it? How bad could it get?

2. ***Direction***

What end-state is desired? What is the aim and objectives of the crisis response?
What overarching values and priorities will inform and guide this?

3. ***Action***

What needs to be decided? What needs to be done to resolve the situation? What
needs to be done to achieve the desired end-state? How will you monitor actions, events
and outcomes? What reporting structures are required?

In conclusion, Mr. Baker’s presentation explains the importance of effective crisis management in the context of NATO and Critical Infrastructure Security & Resilience; analyzes and interprets the differences between incidents, emergencies and crises; describe the different characteristics of crises; identify recognized good practice in NATO, and other crisis management techniques; describes how NATO member states and partner countries can develop more effective crisis and consequence management arrangements.

Presentation

Aim & Objectives



Aim:

To understand Crisis Management in the context of NATO Critical Infrastructure Security & Resilience (CISR) and the NATO handbook chapter.

Learning Objectives:

- 1) Explain the importance of effective crisis management in the context of NATO and Critical Infrastructure Security & Resilience.
- 2) Analyse and interpret the differences between incidents, emergencies and crises.
- 3) Describe the different characteristics of crises.
- 4) Identify recognised good practice in NATO, and other crisis management techniques.
- 5) Describe how NATO member states and partner countries can develop more effective crisis and consequence management arrangements.

UNCLASSIFIED

Issues for Consideration



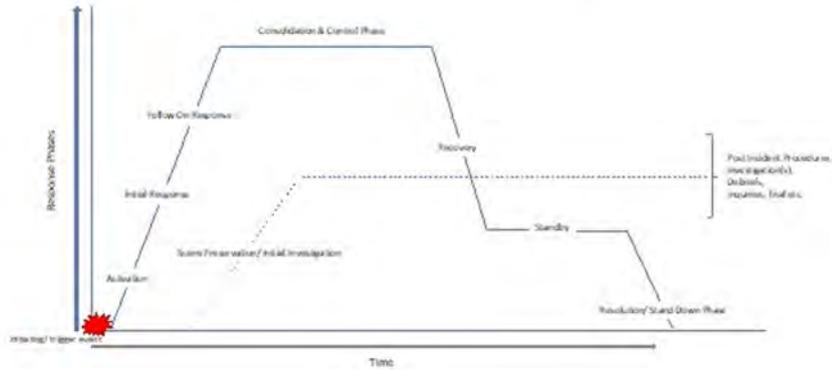
- Role of NATO member states and partner countries in crisis management
 - 'Strengthened Resilience Commitment' (NATO 2030)
 - NATO Article 3 Resilience and crisis management
- How do incidents and emergencies differ from crises?
- What characteristics are inherent in crises, and how do crises manifest themselves in Critical Infrastructure Security & Resilience (CISR)?
- Why do crises require a different management approach from incident and emergency management?
- How can NATO assist CISR and develop more effective crisis management?

UNCLASSIFIED

Phases of an incident or crisis



The Anatomy of a Crisis – “a strategic surprise”



UNCLASSIFIED

Crisis - Definition



“... abnormal and unstable situation that threatens the organization’s strategic objectives, reputation or viability.”

[Source: BS 11200: 2014 Crisis management- Guidance and good practice]

UNCLASSIFIED



Incidents (Emergencies – threat to life/ property)

- **Predictability:** Generally foreseeable, although timing/ nature and detail may be unpredictable.
- **Onset:** Short notice/ no -notice.
- **Urgency and pressure:** Incident response usually spans a short time frame of activity. Resolution prevents longer -term exposure/ significant impacts.
- **Impacts:** Adverse events – reasonably well understood. Predefined responses work well.
- **Media scrutiny:** Positive when well managed but can be negative if an incident escalates into a crisis.
- **Manageability through established plans and procedures:** Resolution often achieved by applying appropriate, predefined procedures and plans, including adequate resources.

UNCLASSIFIED

Crisis Management: Core concepts & principles



Crises

- **Predictability:** Often unique, rare and unforeseen; or poorly managed incidents/ events.
- **Onset:** Sudden onset/ no -notice, or 'rising tide'.
- **Urgency and pressure:** Higher sense of urgency; Scale, Duration and Impact.
- **Impacts:** 'Strategic shock'; crises can disruptor affect an entire organization, transcend geographical and sectoral boundaries. Complexity, uncertainty together with incomplete/ ambiguous information.
- **Media scrutiny:** Crises create significant public and media interest. Potential to negatively affect reputation. Inaccurate media coverage and social media networks may lead to reputational damage/ escalation.
- **Manageability through established plans and procedures:** Rarely resolved through application of predefined procedures. Crises require flexible, creative, strategic and a dynamic response.

UNCLASSIFIED

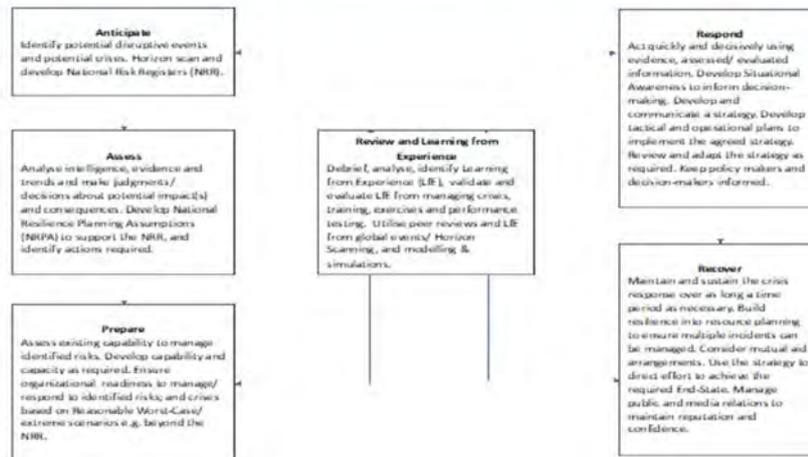
Developing a crisis management capability



- Setting a Crisis Management Framework
 - Objectives in managing a crisis
 - Intent – how will the objectives be realized?
 - Organizational commitment
- Policy, Planning and Priorities
- Roles and responsibilities
- Resources
- Authority and Accountability
- Situational Awareness/ Common Recognised Information Picture
- Decision support and decision-making
- Subsidiarity
- Develop a Crisis Management Plan

UNCLASSIFIED

Crisis management framework



UNCLASSIFIED

Crisis leadership



Challenges:

- This is not 'Business as Usual'
- Requires rigorous, realistic and repeated training
- Challenge organizational culture
- Plausibility and 'what if'?

Consider:

- Tempo or battle rhythm of a crisis
- Decision-making: critical and timing
- Complexity – Scale, Duration and Impact
- Severity and seriousness
- Uncertainty and ambiguity

UNCLASSIFIED

Strategic crisis decision -making



• Situation:

What is happening? What are the impacts? What are the issues? What are the risks? What might happen? What is being done about it? How bad could it get?

• Direction:

What end-state is desired? What is the aim and objectives of the crisis response? What overarching values and priorities will inform and guide this?

• Action:

What needs to be decided? What needs to be done to resolve the situation? What needs to be done to achieve the desired end -state? How will you monitor actions, events and outcomes? What reporting structures are required?

UNCLASSIFIED

Crisis communications



- Pre-crisis preparation
- Management of reputation and interested parties/ stakeholders
- Response:
 - Be prepared
 - Move fast
 - Monitor continuously
 - Maintain the flow
 - Speak with one voice
 - Be transparent
 - Accuracy is key
 - Build a strategy
 - Manage the timing
 - Be human
 - Sign off

UNCLASSIFIED

Training, exercising and learning from crises



- Developing people and rehearsing Crisis Management arrangements
- Training, Exercising and testing – know the difference
- Training for Crisis Management roles
- Skills development
- Methods of instruction
- Rehearsing crisis management arrangements
- Exercising
- Post-crisis debriefing and exercise activity

UNCLASSIFIED

Summary & concluding remarks



- Crisis management is one of NATO's fundamental tasks
- NATO's response relies on military/ non -military measures
- NATO's Strengthened Resilience Commitment
- CI as High Reliability Organisations
- Links to Civil-Military Cooperation (CIMIC)

UNCLASSIFIED

Further reading



- Crisis Management: Planning for the inevitable - Steven Fink
- Managing The Unexpected: Resilient Performance in an Age of Uncertainty – Karl E. Weick and Kathleen M. Sutcliffe
- Crisis Management in a Complex World – Gilpin and Murphy
- Risk, Crisis and Security Management – Edward Borodzicz
- Soft Targets and Crisis Management – Fogel and Hesterman
- Securing the State – David Omand

UNCLASSIFIED

DAY II – Session 1: Questions and Open Discussion

Prof. Ronald Sanford BEARSE

- 1. Is there any difference between Critical Infrastructure (CI) and Key Point Installation (KPI)?**

In many countries, including the US, there are different definitions. The quick answer to this question would be simply “no”. Prof. Bearse states that nations have KPI which is a facility providing some kind of “key” functions that are able to respond several threats, namely targeting the critical infrastructure. Therefore, the answer is there is no distinction between these two terms. Countries name these notions as they want to and this simply does not mean that these concepts have nothing in common.

- 2. Do you think Artificial Intelligence (AI) could be a useful asset in order to ensure or improve CISR? If yes, how? Are there any positive or negative effects for protection?**

There is not a crystal-clear answer to this question. If we use artificial intelligence to help us identify the unknowns to enhance our capabilities, the answer is yes. It possesses great potential. We really hope, as artificial intelligence is continuously developing, it will envision our understanding of CISR. However, Prof. Bearse recommends to be more cautious about the negative effects of the artificial intelligence.

- 3. Could be rational to consider religious sites and monuments CI, since possible destruction could trigger riots and destabilization under specific circumstances. Thank you.**

Yes, religious sites and cultural can be considered as critical infrastructure, especially when the destruction of these sites could trigger riots and destabilization under specific circumstances. We should take it as a responsibility to protect these kinds of sites, we have quite concrete reasons to make sure that we are securing them. On the other hand,

this may not be a concern of every country, however it depends on the country's choice and culture.

Mr. Raymond MEY & Mr. Malcolm BAKER

1. In the threat assessment process circle, where should we evaluate the opportunities which threats provide?

In the process of conducting a threat assessment, a lot of information that we rely on has to come from the entities gathering the intelligence. There are some difficulties in this process while determining where the threats are, at what stage. Mr. Rey reminds of a general's addressing on the issue. Mr. Rey conveys that general's advice on concentrating the focus on vulnerabilities as opposed to information and intelligence. That is because many times we are not getting that information and intelligence in order to conduct appropriate level of threat assessment. Therefore, if there is enough information out there, there will not be potential disruption or threatening situations that could impact critical infrastructure. As a result, we need to focus on our ability to counter all of these threats even in the absence of intelligence and information.

On the other hand, Mr. Baker reminds of every step of threat assessment process and he contends that opportunities lie within every step of the process circle. When you start to seek for information at community intelligence as an opportunity, when you start to look at vulnerabilities at gap analysis, gaps will always provide you with opportunities. Therefore, risk management is full of opportunity. Developing and enhancing security measures, and innovation do provide opportunities.

2. Should we also include social media as critical infrastructure as a part of information security since false news can also be a part of misinformation campaign?

Mr. Rey states that he is not so sure about considering social media as a pillar of critical infrastructure. However, he points out that the impact of social media on critical infrastructure needs to be considered. He reminds of the attacks occurred during the recent elections in the US and the use of social media utilized by nation-states directed

at the elections. The fact that social media can present a lot of information that is not credible can have a detrimental impact on critical infrastructure. Certainly, social media should be considered in our assessment in terms of preparations, and security.

On the other hand, Mr. Baker adds that social media could be a subset as we have it as a part of telecommunications. We cannot think of a world without television, e-mails which are not evaluated as parts of critical infrastructure. He clearly states that the social media is quite significant to him. How fast you get the message, decides how fast you can get situational awareness. We can all use social media to build situational awareness.

- 3. When we do the cycle, information - risk assessment - security plan - test - modification (you explained 7 steps), for CISR improvement continuously, I think it takes a long time. If you have any idea to shorten this span, please let me know. Or if you have any important point for this cycle management by your experience, please let me know.**

Mr. Baker states that this is not a modal, this is a “process”. You have to ideally follow every step of it; however, you do not have to complete each particular stage in turn. You might decide you can move through it to shorten the time and frame. By doing so, you can have a rapid procedure to see what you get in turn. You may identify what you do not know about the process. This process is actually implemented round and round, the process is cyclical. Therefore, the first detect or round might be quick, but not necessarily a rush. It might accelerate the cycle to start with. It will give you a great coverage. And then, you are going to come back to the round again, you will find more time to think about it. Therefore, do not think that it is about shortening the process and missing the steps. Move forward step by step; unless you make sure that you completed every single thing, do not move to the second one. This gives you the simultaneous effect.

- 4. NATO defined “crisis” as “disruption of the equilibrium within a nation or among several nations, creating tensions which might lead to serious turmoil or to a conflict”, and “crisis management” as “the coordinated actions taken to defuse crises, prevent their escalation into an armed conflict and contain hostilities if they**

should result.” We should not confuse “crisis management” with consequence management.

Mr. Baker does not think they are mutually exclusive. He contends that he issued this in the chapter and tried to make a link between these two concepts. Crisis management process refers to cyclic procedure that functions getting an unstable process to stable levels. On the other hand, there must be a strategic intend to return to normality, that is, pre-crisis stage. We should accept that it will be really hard to change things in long term. Take COVID-19, for instance. It has really changed the way we do business. You cannot manage a crisis without recovery and recovery is all about managing the consequences. Yes, these concepts are two different things. However, they are linked together in the same way as the risk analysis process is separate from threat assessment process. We have to link them together. We want to reach the harmony in the system.

Dr. Carol V. EVANS

- 1. You are suggesting more awareness and information/intelligence sharing related to CISR for NATO. This is a general suggestion as well as a general challenge for NATO. Do you think that this recommendation could be implemented easily or with more difficulties in comparison with the one which refers to the regular military duties?**

Intelligence and information sharing come from many different sources particularly in NATO environment. We do not only have NATO capabilities, but we also have Five-Eyes capabilities, and transactional intelligence capabilities. How we bring them together to harness a complete picture of the threat to critical infrastructure is a huge challenge, of course. Dr. Evans states she is pleased with NATO’s own efforts to look deep into the issue and where the aversion of the military industrial base is and where the key strategic investments are. The Alliance also works on the possible impacts of some scenarios on NATO.

However, there are many different efforts on the way. Dr. Evans strongly believes that NATO has played an important role in unifying this collaboration particularly between

EU host countries and private sector in order to build situational awareness and NATO's leadership does matter in that sense.

When the critical infrastructure is the issue, the private sectors steps in, even in the military perspective. Therefore, there needs to be a great coordination among different actors. This is a sector where the information of private sector is highly desired. On the other hand, it is also very crucial for military to understand how private sectors operate in this field.

- 2. Hybrid threats were evident throughout history, maybe the means were different. It's a significant concern considering the blend of technology, cyber etc. in the present hybrid spectrum. As an expert, Hybrid may be an option to counter hybrid threat? Then, how to legitimate that course of action?**

The word "legitimate" needs more clarification here. Are we referring to NATO or individual countries countering hybrid threats? On the other hand, if we are talking about the offensive cyber domain, there are great developments that NATO has been working on. Dr. Evans used the US as an example, having a Cyber Command and conducting offensive and defensive cyber actions.

Dr. Evans underlines the importance of countering hybrid threats with innovative hybrid means. She resumes, we first have to understand the possible implications of these hybrid threats so we can then articulate very clearly coordinated hybrid strategy in response. We have to consider the involvement of many different entities within the NATO context that collaboration and coordination are going to be kept in order to deal with the arena full of hybrid threats.

DAY II – Session 2: Critical Infrastructure Security and Resilience

Book Volume 1

Moderated by: Dr. Carol V. EVANS (USA), *Director, Strategic Studies Institute and US Army War College Press*

Aviation – Post-9/11 Case Studies

Mr. David HARELL

Lecturer Berlin School of Economics and Law Master's Program for Security Management,
Berlin, Germany

An examination of significant terrorist attacks against Civil Aviation since 9/11, from the anti-terrorism and intelligence perspective, indicates the aviation security response has for the most part not been successful in detecting or preventing attacks.

While analysing numerous case studies, the conclusion can be drawn that responsible security actors were not able to detect or prevent an attack. In most of these cases, the anti-terrorism effort's failure was exacerbated by intelligence/counter terrorism failures. An analysis of aviation case studies identifies some of the reasons behind these outcomes and serve as the basis for recommendations based on best practices which will enable increased awareness and improve preparations and capabilities against possible attacks.

Identified characteristics of the aviation security (AVSEC) system:

- **Criticality.** These are really critical systems. What makes aviation so critical? Consider the current response to COVID-19 period. What would have been the response if there were not any possibilities to move supplies and medications from one place to another? Using ships to bring critical equipment would have increased the wait times.
- **Rigidity.** Rigidity of the system mainly refers to lack of ability to change in real-time when confronted with a threat. A lot of the equipment today is same as it was in 40-50 years ago i.e., X-rays, metal detectors used many years ago. Even if there are improvements in body scanners nowadays, the systems cannot detect every threats. As

a result, these systems are rigid. Consideration must be given about on how to change them.

- ***Predictability.*** The AVSEC system relies on technologies and processes that have been in place for more than 30 years. This is especially true for walk-through metal detector gates and dual source X-ray machines. Even the more advanced computed tomography scanning machines have been in service since 1995. Seasoned passengers typically understand why these scanners sound an alarm, what item they are wearing that triggered the alarm or which particular item in their carry-on baggage has attracted the screener's attention. If passengers understand this, then imagine what well-trained and determined terrorists, who have access to these detection technologies, understand about the capabilities and vulnerabilities in the system. There are global terrorism on-line forums that specifically discuss the vulnerabilities of such aviation detection technologies.
- ***Volatility and Sensitivity.*** The volatility relates both to economic factors and external geopolitical factors. The aviation industry is impacted by fluctuating demand, a rigid cost structure, competitive pricing, and changing and erratic fuel costs. In addition, the industry can be severely impacted by global events such as the 9/11 terrorist attacks, the SARS and COVID-19 pandemics, and the global economic recession in 2008. These factors lead to an industry with low profit margins which can cause airlines to move from profitability to loss in a very short space of time. For example, in 2019, prior to the COVID-19 outbreak, profit margins for most US carriers were between five and six percent, which are generally considered low and susceptible..
- ***An Attractive Target from the Terrorists'.*** There have been more than 1200 attacks against aviation systems in mid 1960s. The significant number of attacks demonstrates how attractive the aviation industry is for terrorists.
- ***Reactive to the Evolving Threats.*** Terrorists are really adaptive. They can learn new tactics which are in accordance with current technological innovations. Therefore, security always try to catch up with these developments and fill the gap to prevent the penetration of terrorist intentions.

The aviation security sector is focused on “*compliance*”. The aviation sector has to comply with the UN, ICAO, and other possible partners. However, compliance does not always mean that the threat will be eliminated. To comply with perimeter fences at airports, these fences have to

be at least eight feet tall. In addition, there should be CCTV coverage and patrols. Compliance does not tell you how to manage perimeter fences, CCTV coverage, and patrols in order to secure the area. It utterly depends on the preferred implementation of individual airport authorities. And if an individual with malicious intentions arrives at the airport and cuts the fences; the fences are not smart to tell you that there is something wrong. If the CCTVs are not on and security guys are not watching the place, this individual is now able to do whatever they like. This is not something desirable.

For instance, a 2013 incident at Brussels Airport involved eight criminals who cut through the fences, drove to where an aircraft destined for Switzerland was being prepared pre-flighted, and these men took control of the airplane and stole diamonds worth more than 50 million dollars and just vanished. The incident was quite shocking. Afterwards, spokesman of the airport stated that the security standards of the Brussel Airport is compatible with international standards. These men are just thieves, what would happen if these were terrorists carrying other heavy weapons?

Airport public areas are also vulnerable. While the airside is strictly and very well regulated in terms of screening processes, the ground side, where most attacks take place (for instance the suicide bombers in Brussels and attacks in Istanbul) are relatively in-secure and do not possess screening procedures until passing through security checks leading to departure gates. As a result, more focus should be placed on securing the ground side of airports.

Several recommendations for reducing vulnerabilities in terms of aviation security are:

- Continue to move to a more risk-based system including improving threat definitions in accordance with adversary capabilities,
- Utilizing airline passenger travel data (PNR) for risk-based screening purposes,
- The integration of behavioural detection programs into PNR analysis and risk-based screening,
- Design and implement airport community security programs. These programs should integrate into the airports' risk-based screening regimes. This has proven to be a significant force multiplier in Singapore (TOPSIS program),
- Hardening of airport perimeters,
- The need for more security regulation of airports' public areas,
- Creating and utilizing field intelligence,

- Avoid over reliance on indications and warning intelligence for determining security levels, and
- The importance of the human factor.

Presentation



NATO COE-DAT & USAWC SSI:CISR Conference October 12-13, 2021

Chapter 6 Civil aviation: A critical infrastructure, volatile industry, attractive target – the need to reduce its vulnerability.

David Harell



Introduction

- ▶ Almost every time civil aviation has been significantly challenged by terrorism since 9/11, the aviation security response, or lack of it, has not been too successful in detecting and preventing the attack. In most of these cases, the anti-terrorism failure was exacerbated by intelligence/counter terrorism failures.

Characteristics of the AVSEC System:

Criticality

Rigidity

Predictability

Volatility and
sensitivity

An attractive
target from the
terrorists'
perspective

Reactive to the
evolving threats

Additional challenges discussed

Adaptive adversary and evolving threats

In many cases threat definitions have been calibrated to meet technological limitations.

Compliance versus risk based/threat-oriented security operations

Securing airport public areas has been neglected/overlooked/avoided?



Compliance versus risk based/threat-oriented security operations



Compliance versus risk based/threat-oriented security operations

BRUSSELS AIRPORT DIAMOND HEIST
February 18, 2018

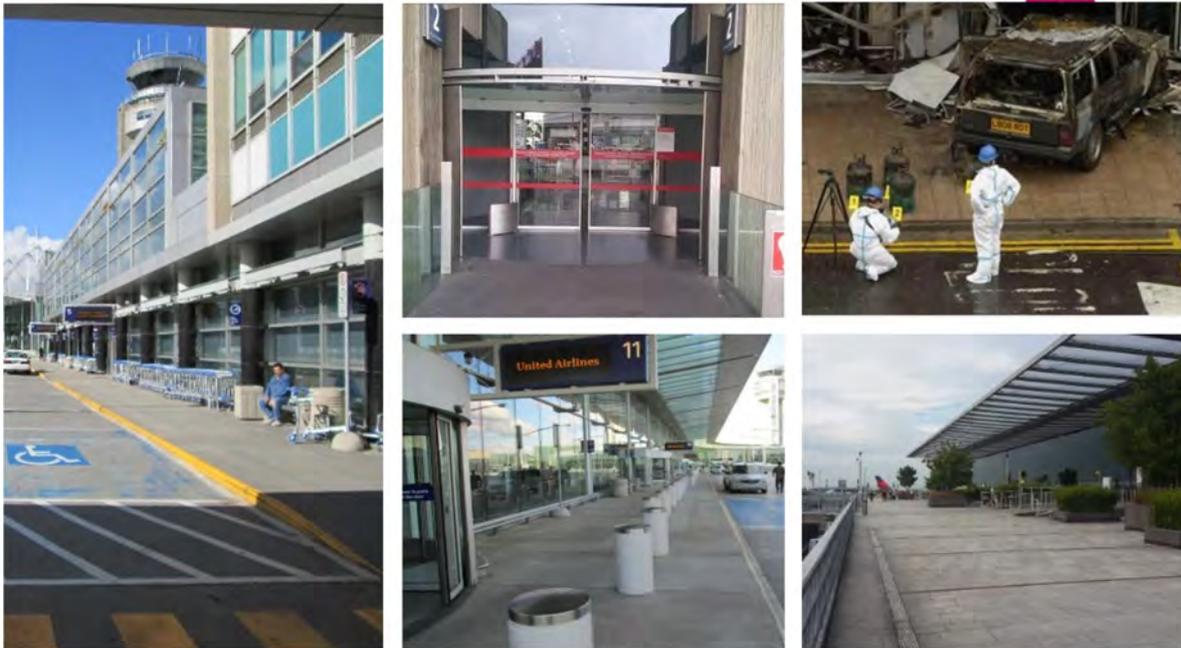
Additional challenges discussed

Adaptive adversary and evolving threats

In many cases threat definitions have been calibrated to meet technological limitations.

Compliance versus risk based/threat-oriented security operations

Securing airport public areas has been neglected/overlooked/avoided?



Recommendations for reducing discussed vulnerabilities:

- ▶ Continue to move to a more risk-based system including improving threat definitions in accordance with adversary capabilities.
- ▶ Utilizing airline passenger travel data (PNR) for riskbased screening purposes
- ▶ The integration of behavioural detection programs into PNR analysis and riskbased screening
- ▶ Design and implement airport community security programs. These programs should integrate into the airports' riskbased screening regimes. This has proven to be a significant force multiplier in Singapore (TOPSIS program).
- ▶ Hardening of airport perimeters.
- ▶ The need for more security regulation of airports' public areas.
- ▶ Creating and utilizing field intelligence
- ▶ Avoid over reliance on indications and warning intelligence for determining security levels
- ▶ The importance of the human factor

Thank you

Water – Washington DC Metro Case Study

Mr. Steven E. BIEBER

Metropolitan Washington Council of Governments, Program Director, Water Resources

In the U.S., drinking water for 80% of the population comes from about 400 water companies. In the Washington DC metropolitan area alone there are more than 14,500 miles of water pipes supplying water to more than five million consumers. The average daily demand is approximately 485 million gallons (MGD). The concern of a possible terrorist or cyber-attack should be on the considered to take necessary measures to counter these threats.

In Washington, cooperative planning and management process has historically been implemented. Since the 1970s, the idea of a Water Supply Coordination Agreement has been realized. This agreement constitutes a legally binding integrated system of water of the Potomac River. It also includes water supply capacity planning in long-term and possible operations to be carried out under the drought conditions. Following that agreement, other action plans have been created in order to increase the level of readiness for possible harsh conditions. Afterwards, Water Supply Emergency Plan is concluded in order to secure the water supply. These plans then evolved into a more general and extensive format that could address all other kinds of hazards.

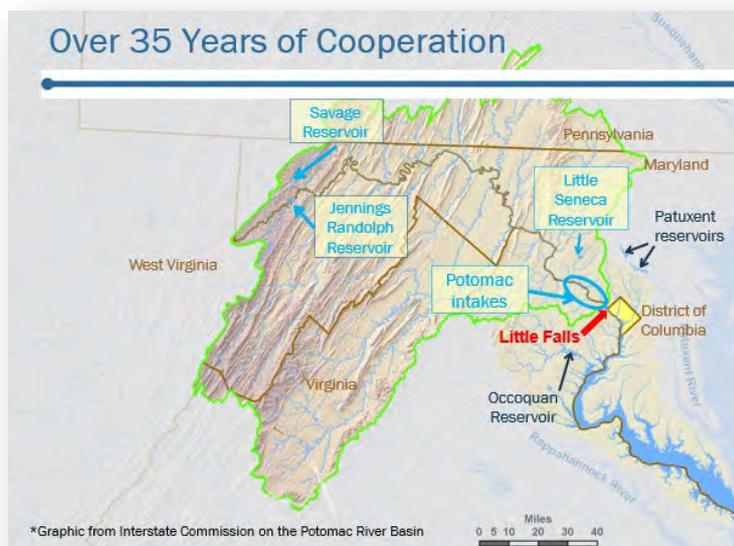


Figure 12--Potomac River Basin

In the figure above, there is a circle near the Potomac Intakes, all the bigger utilities and intakes are concentrated in the one part of the river. The reservoirs are also there and named in blue i.e., Jennings Randolph, Little Seneca and Savage Reservoirs. Those are actually reservoirs that are built by the water utilities so they can provide resilience against any possible threats. Therefore, it provides the capability of being able to meet average daily demand.

As in many sectors, water sector also faces many risks and threats. Intentional threats directed to a water sector can be listed as;

- Cyber-attacks,
- Destruction of parts of a system, such as bombing a pipeline,
- Intentional contamination of drinking source of water, and
- Intentional contamination of treated water in the distribution system.

Another perspective that follows intentional threats is about natural hazards or unintentional events as follow:

- Extreme weather and climate change,
- Aging infrastructure,
- Accidental contamination of drinking source water
- Accidental contamination of treated drinking water.

Water companies are very heavily regulated especially in areas such as Washington D.C. Investments to increase the level of resilience and protection against potential terrorism are taken into consideration and are continuously being developed.

There are some case studies concerning attacks on water resources, systems, and water-related terrorism. By examining these cases and possible outcomes of these incidents, the potential terrorist threat directed to water resources and the potential consequences of such attacks can be identified.

It is also noted that water supply systems are heavily dependent on electrical power. No electric power means no pumping which means no water. Even an attack on an electric grid could disable water treatment as well.

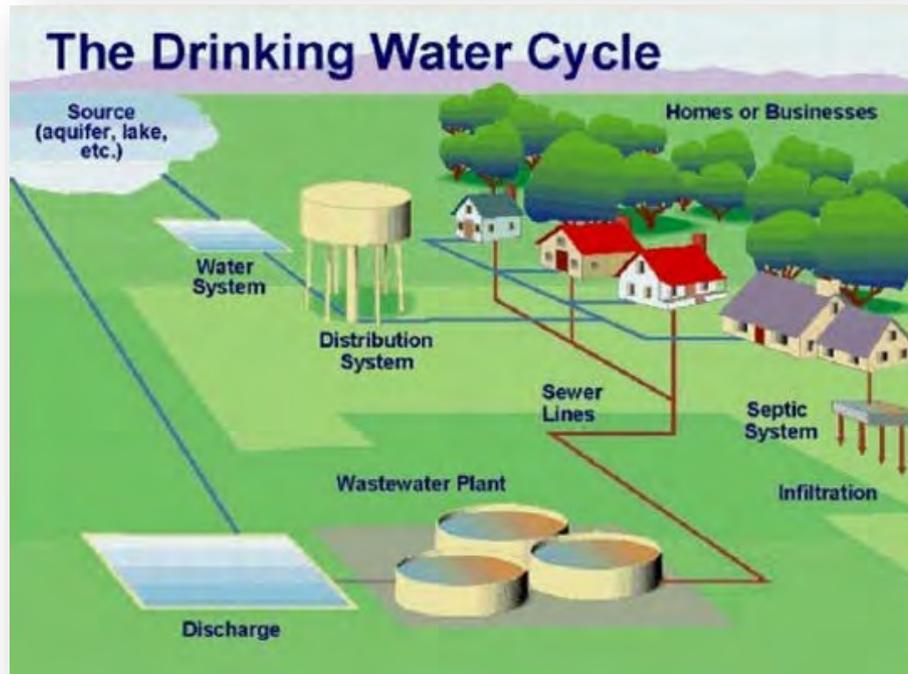


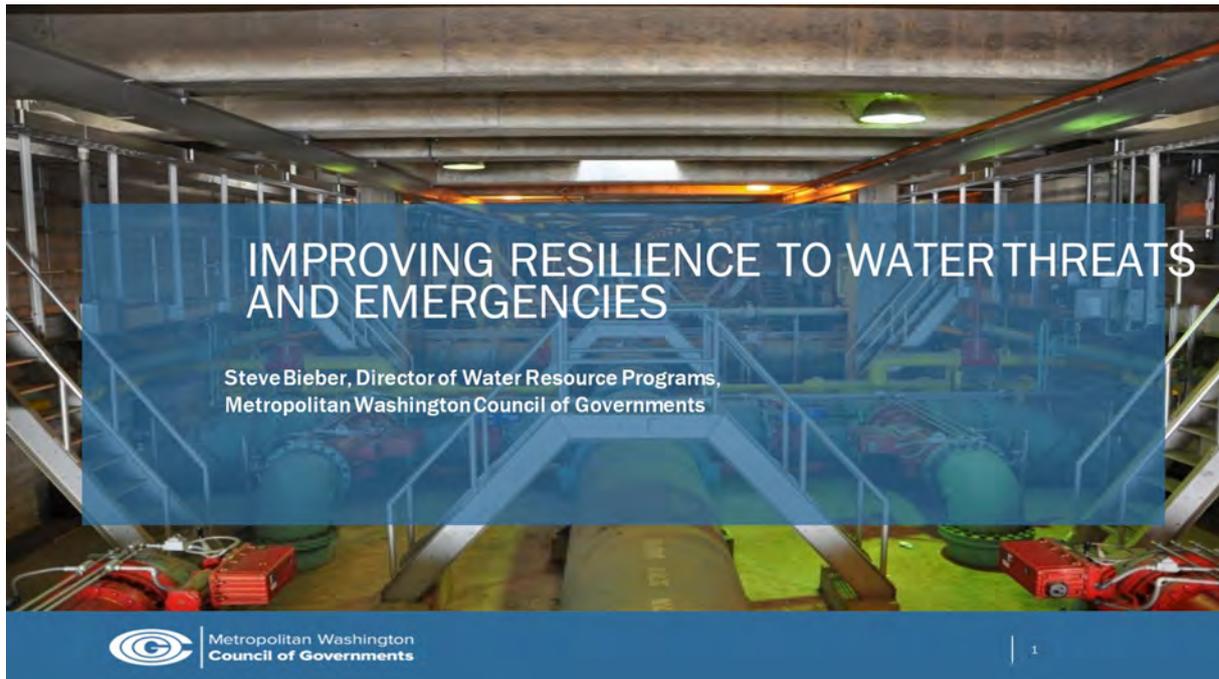
Figure 13--Drinking Water Cycle

An attack whether or not it is intentional or accidental against the water system can happen in lots of different areas in the water cycle. It can be in the septic system, source, or in the distribution system all of which could lead to devastating results. Therefore, analyses of possible vulnerabilities require different planning and detection process for each of these areas shown in the image.

Recommendations concerning regional collaboration to improve water security resilience by considering some important points as listed below:

- Regional-level planning and response - effective approach for enabling resilience,
- Regional goals, resource -sharing criteria, and performance metrics,
- Relationship building and knowledge transfer,
- Successful models for mutual-aid, such as WARN, and
- Coordinated regional water supply planning promotes the sharing of benefits, risks, and resource costs.

Presentation



Acknowledgments

- Many thanks to our partners in this regional project
 - Washington Suburban Sanitary Commission
 - Fairfax Water
 - Washington Aqueduct
 - DC Water
 - Loudoun Water
 - Arlington County
 - ICPRB
 - Black & Veatch

About COG

- An independent, nonprofit association founded in 1957.
- Brings area leaders together to address regional issues.
- Membership comprised of 300 elected officials from 24 local governments, the Maryland and Virginia state legislatures, and U.S. Congress.
- 125+ staff.
- Regional planning for transportation, water, air quality, and numerous other areas.



4





Metropolitan Washington Drinking Water at a Glance

- Average daily demand ≈ 485 million gallons (MGD)
- 14,500+ miles of water mains
- ≈ 114,000 fire hydrants
- 1,000,000+ metered accounts
- 5,000,000 + people served



Metropolitan Washington
Council of Governments

5

Long-term Cooperative Water Supply Planning & Management

- Cooperative regional monitoring of source & finished water
- Collaborative training, exercises & contingency planning
- Regional communication & coordination

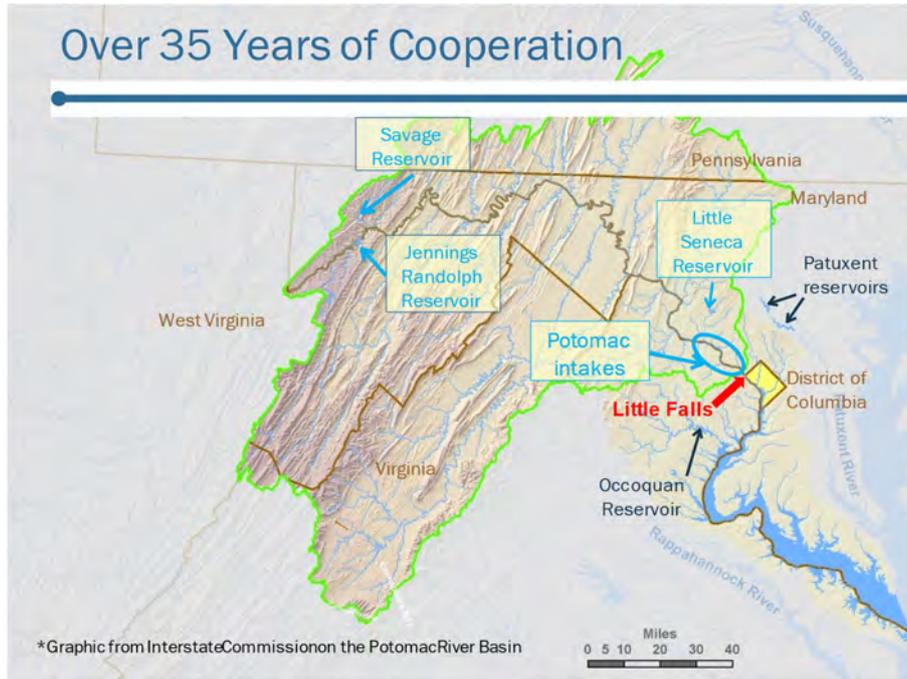
- | | |
|------------|--|
| 1970 | • Watersupply added to ICPRB scope |
| 1978 | • Low Flow Allocation Agreement |
| 1979 | • ICPRB Section for Cooperative Water Supply Operations |
| 1982 | • Watersupply storage at Jennings Randolph and Little Seneca |
| 1982 | • Water Supply Coordination Agreement |
| 1994/04/09 | • Water Supply Emergency Plan |
| 2000 | • Water Supply & Drought Response Plan |
| 2004 | • Potomac Drinking Water Source Protection Partnership |
| 2007 | • Regional Redundancy Study |
| 2008 | • NCR Water/Wastewater Agency Response Network |
| 2013-16 | • Emergency water supply planning |
| | • Updated source water assessment |
| | • Regional water system resiliency study |



Metropolitan Washington
Council of Governments

6

Over 35 Years of Cooperation



Water Sector Risks

Intentional threats such as:

- Cyber attacks
- Destruction of parts of a system
- Intentional contamination of drinking source water
- Intentional contamination of treated water in the distribution system



Natural hazards or unintentional events such as:

- Extreme weather and climate change
- Aging infrastructure
- Accidental contamination of drinking source water
- Accidental contamination of treated drinking water



Metropolitan Washington
Council of Governments

Terrorism and Black Sky Events are in the News

'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID (ANDY GREENBERG/HTTPS://WWW.WIRED.COM/STORY/CRASH-OVERRIDE/MALWARE/)

Florida hack exposes danger to watersystems
February breach at Oldsmar plant alarmed officials across the country

New Global Analysis Finds Water-Related Terrorisms On the Rise
May 8, 2018 By [Jennifer Veilleux](#) & [Shlomi Dinar](#)

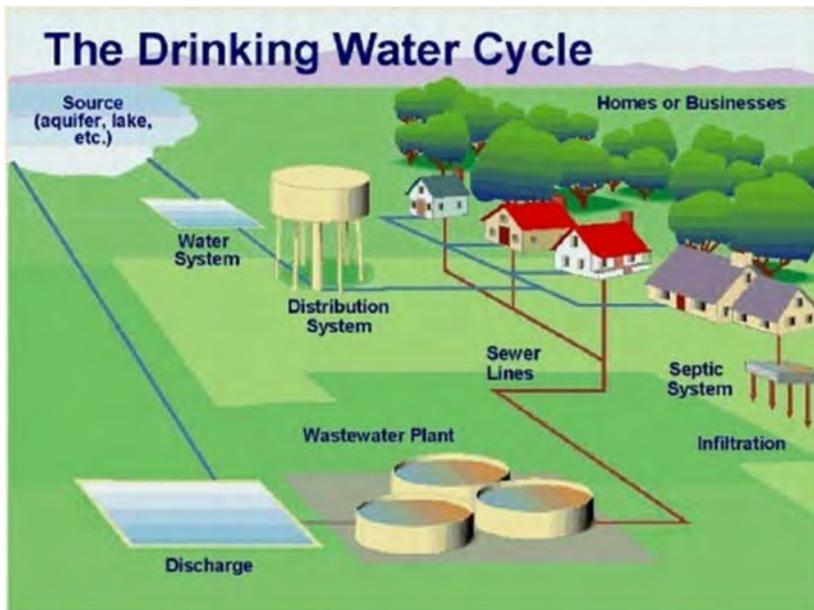
Assault on California Power Station Raises Alarm on Potential for Terrorism (Rebecca Smith/
<https://www.wsj.com/articles/assault-on-california-power-plant-raises-alarm-on-potential-for-terrorism-151915708791>)

Thousands Without Water After Spill in West Virginia
By TRIP GAMBEL July 16, 2014

Could North Korea turn America's lights out? We're living in the dark about our electric grid (John Moody/
<https://www.foxnews.com/opinion/could-north-korea-turn-america-into-dark-about-our-electric-grid>)

Department of Homeland Security
Emergency Operations

 Metropolitan Washington Council of Governments



 Metropolitan Washington Council of Governments

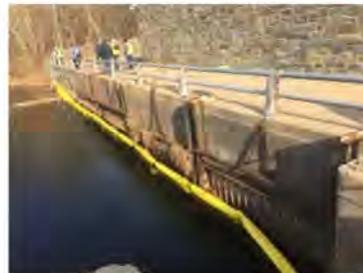
Regional Collaboration to Improve Water Sector Resilience

- Regional level planning and response-effective approach for enabling resilience
- Regional goals, resource sharing criteria, and performance metrics
- Relationship building and knowledge transfer
- Successful models for mutual-aid, such as WARN
- Coordinated regional water supply planning promotes the sharing of benefits, risks, and resource costs



Regional Resiliency Study - Overview

- Federal Urban Area Security Initiative (UASI) grant
- Metropolitan Washington Area serves 4.6M, 490 MGD
- Limited connections between water systems in metropolitan Washington to transfer raw or treated water to areas where shortfalls might occur
- Consequences of extended water outages include direct costs and related societal impacts from outage



Regional Resiliency Study - Overview

Objectives

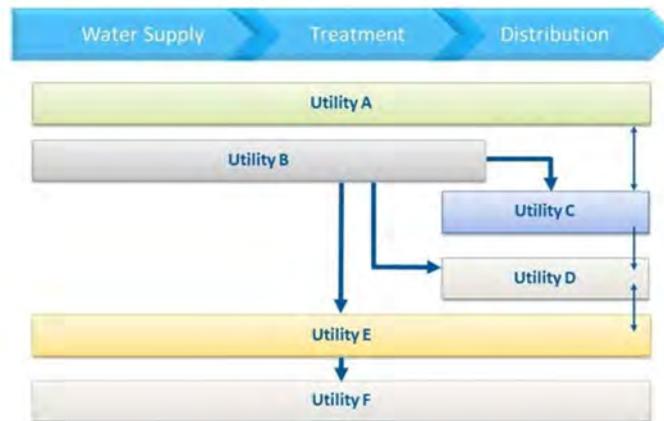
- Evaluate ability of region's water systems to withstand regional emergencies.
- Identify improvements to enhance the overall resilience and reliability of water system under emergency conditions.



System resilience approach to identify prioritized improvements



Understanding Existing Capabilities



Defining Risk Framework

- Target level of service
 - Ability to supply winter average demand
- Consider failure events of concern
- Likelihood of Occurrence
 - 1/10, 1/30, 1/100, 1/250 years
- Consequence of Occurrence
 - LoS impact (People - Outage Days)
 - Direct Costs
 - Economic Costs – value of loss of water service (source, FEMA)
 - Critical functionality of military installations



Inputs to Model – Failure Scenarios

Scenario	Duration, days	LOO	COO (PODs) x1000	Direct Cost, \$	Econ Impact, \$
Risk 1 – Main Break	14	1/30	435	DC1	EI1
Risk 2 – River Contam., all intakes	28	1/100	83,000	DC2	EI2
Risk 3 – River Contam., some intakes	3	1/30	5,400	DC3	EI3
Risk 4 – Fire at WTP	3	1/30	680	DC4	EI4
Risk 5 – Airplane Crash	0	1/250	0	DC5	EI5
Risk 6 – Reservoir Contamination	14	1/30	760	DC6	EI6

LOO: Likelihood of Occurrence
 COO: Consequence of Occurrence
 POD: Population Outage Days



Potential Improvements

- Raw water storage and transmission (5 alternatives)
- Raw water transfer (2 alternatives)
- New raw water intake
- Treated water transfer (7 alternatives)
- WTP pumping upgrade and associated network improvements
- Upgrade network interconnections

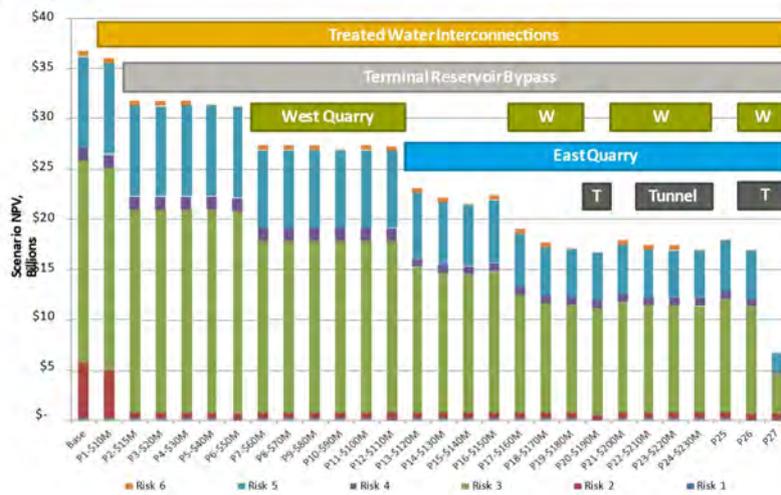


Risk Model

- Monte Carlo Simulation
 - Track mean values for capital, O&M, direct, and economic costs
- Evaluate improvements individually
 - Calculate Benefit Cost Ratio (BCR) for each project for initial ranking
- Choose capital spending ranges for portfolio analysis
 - \$0 to \$350M
- Evolver simulation
 - Evaluates all possible combinations of improvements within capital spending ranges for maximum BCR
- Top BCR portfolios brought to Monte Carlo model
 - Synergies calculated for top portfolios
 - Recalculate portfolio BCRs w/synergies



Major Improvements by Portfolio



Regional Resiliency Study Outcomes and Conclusions

- River contamination events are responsible for a substantial amount of total risk.
- Raw water storage combined with water transfer improvements are effective risk-mitigating initiatives.
- Need to plan with the long term vision in mind.
- Seeking optimum balance of risk reduction and cost.



Water sector risk and vulnerability assessment resources

- AWWA J100 - Risk Analysis and Management for Critical Asset Protection (RAMCAP®) Standard for Risk and Resilience Management of Water and Wastewater Systems (available here: <https://www.awwa.org/Store/ProductDetails/productId/37334446>)
- AWWA G430 - Security Practices for Operation and Management (available here: <https://www.awwa.org/Store/AWWAG430-09-Security-Practices-for-Operation-and-Management-/ProductDetail/20779>)
- AWWA G440 - Emergency Preparedness Practices (available here: <https://www.awwa.org/Store/AWWAG440-17-Emergency-Preparedness-Practices/ProductDetail/62471757>)
- Vulnerability Self-Assessment Tool - Web Enabled (VSATWeb) 2.0 (available here: <https://www.epa.gov/waterriskassessment/conductdrinkingwater-or-wastewater-utility-risk-assessment>)
- Climate Resilience Evaluation and Awareness Tool (CREAT) Risk Assessment Application for Water Utilities (available here: <https://www.epa.gov/crwu/climateresilience-evaluation-and-awareness-toolcreat-risk-assessment-application-water>)



Steve Bieber

Metropolitan Washington Council of Governments
sbieber@mwkog.org

777 N. Capitol St., NE
Suite 300
Washington, DC 20002

mwkog.org



Cyber & Hybrid – Electric Grids/Ukraine

Dr. Theresa SABONIS-HELF

Georgetown University Masters of Science in Foreign Service Program

Europe is currently in its third modern energy transition. The first transition was led by Lord Churchill in 1911, when he decided to change the United Kingdom's coal dependence to oil. The second transition began in the 1980s when Europe began a transition towards gas. Now, Europe has begun the third transition to move away from fossil fuels for the production of electricity. During each transition, access to energy supplies through multiple routes provided security.

Until Europe can make the transition from fossil fuels for electricity, a new problem has emerged; not only are numbers of sources required, but it is also important not to be dependent on one source of gas. During the Cold War, Europe agreed that it would never be more than 30 percent dependent on Soviet resources. In the 2000s amid new threats to gas structures, the European Union (EU) adopted a new legislation, the Third Energy Package of 2009, which required gas hubs, and construction of infrastructure to make states more capable of supporting each other in emergency to further reduce the risk of relying on Russian gas.

Electricity emerging

With the shift to electrification, the EU is expected to lead the energy transition. EU Climate Law (2020) requires a cut of Greenhouse Gases (GHG) emissions to 55 percent below the 1990 baseline by 2030. Moreover, electricity will become increasingly the main consumption in the world. Currently, electricity accounts for 19 to 20 percent of total world energy consumption. It is expected to meet greener energy requirements this will increase to 50 percent by 2040. This represents a huge shift to electricity. An advantage of electricity is that some of it can be produced domestically, i.e. renewables, which will lead to more cross-border electricity transfer and more infrastructure emphasis on electricity. There will be more trade in electricity. It will also move Ukraine towards the European grid. While this will provide climate advantages, it also brings new risks.

Crimea

In terms of the historical case of Crimea, it is important to understand that the war between Russia and Ukraine was certainly not about energy. There were many issues, including Ukraine's new energy policies that were not in Russia's interest and there was the issue of extensive offshore development in Crimea. Ukraine lost an estimated 80 percent of its oil and gas deposits in the Black Sea due to Russian annexation of Crimea. As such, energy serves as an objective in the war between Ukraine and Russia. Since energy was an objective in the conflict it can be concluded that Russia at least partially succeeded in achieving critical energy objectives in this conflict as Ukraine lost about 80 percent of its oil and gas deposits.

Both Ukraine and Russia focused on critical infrastructure in the conflict. During winter, Crimea was dependent for at least 80 percent of its electricity on Ukraine. In November 2015, saboteurs blew up key electrical pylons destroying the lines between Crimea and Ukraine. Ukraine was uninterested in restoring the connections. In fact, Ukraine cut off electricity and water to Crimea a month before the December 2015 cyber-attack against the Ukrainian grid.

Attacks on the Ukraine Grid

The attack on the Ukrainian grid was the first known cyber-attack that took down an electric grid, bringing 30 substations offline and left 230,000 residents without power. Although power was restored in 1 to 6 hours, grid control centers were not fully operational for several months. In December 2016, a second cyber-attack happened. Although it was restored more quickly, the attack was much more complex, dangerous, and sophisticated. It was clear that **energy was a tool** in the conflict.

When Crimea was plunged into darkness for the first time in 2015, it was realized that it had no connections to the infrastructure of Russia. Russia constructed undersea electric cables to supply Crimea with electricity and connect Crimea to the Russian mainland. Moreover, new electric power plants were completed in Crimea in November 2019. **Energy is an imperative in governance** – people hold government responsible when it fails.

Cyberwarfare in Ukraine

Cyberwarfare in Ukraine

Case study examines three events with direct impact on infrastructure, each with a distinct effect:

- **December 2015** (BlackEnergy & KillDisk). *First successful cyber-disruption of an electricity grid*
- **December 2016** (CrashOverride). *Attack with (unsuccessful) goal of long-term damage to infrastructure*
- **June 2017** (NotPetya). *Attack on Ukrainian business that leaked out to global commerce, resulting in \$10 Billion damage to global economy.*

US DoJ unsealed an indictment (Oct 2020) charging that the Russian Main Intelligence Directorate (GRU)- sponsored Sandworm Group was behind each of the three attacks.

NotPetya attack in 2017 was an interesting case in Ukraine in which Ukrainian business leaked out to global commerce, resulting in 10-billion-dollar damage to global economy. However, it was not supposed to be an attack on Ukrainian grid, but on Ukrainian business instead, with very high visibility. The U.S. Department of Justice concluded in 2020 that the Russian GRU was behind the attacks.

Ukraine and the EU

The European Union has fast-tracked Ukraine to be part of the European grid. Ukraine joined the EU Energy Community in 2011. Plans are underway for a full delinking from the Russian grid and subsequent integration into the EU grid in 2023. The Baltic grid is scheduled to happen in 2025. Therefore, the EU has planned that for Russia, such attacks would be more costly as Ukraine would be connected to the European grid.

Interestingly, Ukraine itself has a particular pattern and history of cyber behaviour. A lot has been learned from the Ukrainian case in terms of the cyber domain. Ukraine remains on the “Priority Watch List” of the U.S. Trade Representative in the 2020 Special 301 Report. One of the issues in Ukraine is about pirated software. Moreover, hacktivists remain active against

Russia and outside the control of the Government of Ukraine and regularly attack Russian systems. There is a very strong “hactivist network” in Ukraine, called the Ukrainian Cyber Alliance. In terms of attacks, they regularly attack Russian systems. It has been reported that the Ukrainian Cyber Alliance attacked the Russian Federation three times for every one time that pro-Russian groups attack Ukraine. In this conflict, aggressive cyber activity occurs in which government systems are regularly attacked back and forth. It is of concern that such risky activities occur outside of the control of the European Union as well as the Ukrainian Government.

Assistance to Ukraine Energy Security

It turns out that every actor, including NATO, European Union, and the USA are doing different things regarding the Ukrainian Energy Security. European Union has been focusing on infrastructure support as well to improve the electricity sector in order to move it into the European grid. NATO has been trying to assess and train how do to increase cyber defences. The U.S. Government has been focusing on strengthening Ukrainian Government and their expertise in cyber security. A lot of this has to do with engaging private sector and workforce.

In conclusion, each time the predominant form of energy is changed there are new security challenges that must be addressed.

Assistance to Ukraine Energy Security

NATO Support

- NATO Energy Security Centre of Excellence established 2012 (Vilnius)
- NATO Trust Fund on Cyber-Defence for Ukraine est. 2014
- NATO Science & Tech Board created a research task group on energy security/hybrid conflict in 2020

USA Support

- Cybersecurity dialogues
- (2017-2020) \$38 million program to support legal and regulatory reform, development of cyber workforce and private sector engagement.
- Total US support to Ukraine of \$198 million in 2019

EU Support

- Includes New Safe Confinement, completion of 3 nuclear reactors
- EU assistance to Ukraine in 2019 was \$413 million. Germany contributed an additional (bilateral) \$205 million and Poland \$81 million
- EU agreement to work towards full synchronization of the grid includes substantial investment (World Bank estimates the total for Ukraine and Moldova will be \$400 million)
- EBRD invested \$124 million in improving the grid 2015-2020.

European Energy Security, Infrastructure Resilience and the Case of Ukraine

Terrorism Experts Conference/ CISR Project
Theresa Sabonis-Helf
October 2021



1910s: Europe began a transition towards oil when Churchill traded coal for oil in pursuit of a more effective Navy



1980s: Europe began a transition towards gas by importing from the USSR

Present Day: Europe begins a transition away from fossil fuels



European Energy Transitions

- Shift from coal to oil (1910s)
- Shift from oil to gas (1980s)
- Shift to electrification (underway)

Each transition shifted the risk portfolio, each has different level of networkness (Balmaceda: “degree to which the overall functioning of the system may be dependent on the network working properly as a network.”)

EU legislation adopted to address the challenge of networkness– the Third Energy Package (2009), required gas hubs, and construction of infrastructure to make states more capable of supporting each other in emergency.

Electricity Emerging



- The EU is expected to lead the energy transition. EU Climate Law (2020) requires a cut of GHG emissions to 55% below the 1990 baseline by 2030.
- In 2018, electricity accounted for 19% of total world energy consumption. The IEA has set a target of 50% by 2040.
- This will lead to more crossborder trade in electricity, has already led to a prioritization of infrastructure projects that address electricity, and EU policy goal of >30 million electric vehicles by 2030.
- EU is pursuing movement of the Baltic states entirely into the European grid, and moving Ukraine as well.
- The shift towards electrification provides clear climate advantages but also brings new risks.

Energy and Crimea



- Ukraine lost an estimated 80% of its oil and gas deposits in the Black Sea due to annexation of Crimea (March 2014).
- Extensive offshore development underway would have reduced Ukraine's energy dependence on Russia.
- Coming shifts in Ukraine energy law negatively affected Kremlin interests.

see: Ariel Cohen, "As Russia Closes in on Crimea's Energy Resources" *Forbes*, Feb 28, 2019; and Todd Prince, "After Years of Stalling, Can Ukraine Finally Become Energy Self-Sufficient?" *RFE/RL* Sept 15, 2019, map from Columbia Univ

Attack on Crimea's Grid

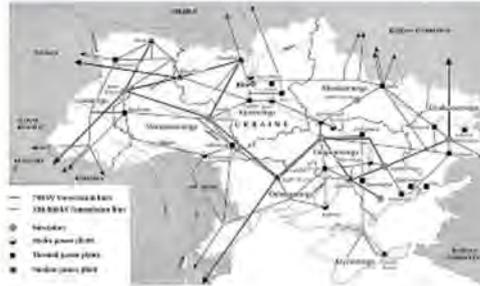


See: Anna Shamanskaa "Why Ukraine Supplies Electricity to Crimea, and Why it Stopped," *RFE/RL*, Nov 24, 2015, map from *Russia Insider*

- Crimea imported 80% of its electricity : 500-900 MW depending on the season.
- Two lines connected Crimea to the Ukrainian grid.
- Nov 20, 2015, saboteurs blew up key pylons, destroying the lines.
- Crimea is not connected to Russia by land, so Russia could not immediately replace the supply.
- Dec 23, 2015, Ukraine's power grid taken down by hackers

- Dec 23, 2015, a cyber attack took 30 substations offline in Ukraine, leaving 230,000 residents without power.
- Power was restored in 16 hours, but grid control centers were not fully operational for several months.
- December 2016, a second cyber attack caused a larger blackout than the first, taking down a significant portion of Kiev.
- Ukenergo rebooted the systems within an hour, but later analysis revealed a more ambitious attack.

Attacks on the Ukraine Grid

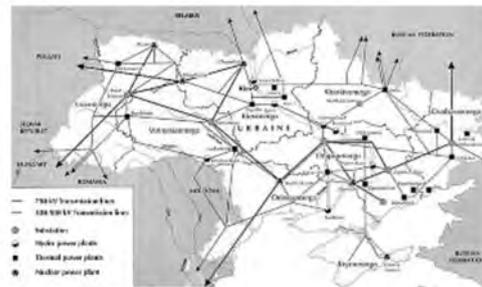


http://www.geni.org/globalenergy/library/national_energy_grid/ukraine/ukrainiannationalelectricitygrid.shtml

Grid Attacks in the Russo-Ukraine War



See: Anna Shamanska "Why Ukraine Supplies Electricity to Crimea, and Why it Stopped," RFE/RL, Nov 24, 2015, map from Russia Insider



Energy as tool in conflict

Russian Response in Crimea



The Economist

- Kerch Strait Energy Bridge: 4 undersea electricity cables connecting Crimea to the Russian mainland completed May 2016
- A 12-mile rail bridge connecting Crimea and Russia completed May 2018
- New power plants completed in Crimea November 2019

See: Tass "Crimea will be able to export electricity, first time ever," Nov 22, 2019 and Lyrychikova and Zverev, "Sanctions short-circuited Russia's electricity plans for annexed Crimea, Reuters April 27, 2017.

Russian Response in Crimea



The Economist

Energy as an imperative in governance

- Kerch Strait Energy Bridge: 4 undersea electricity cables connecting Crimea to the Russian mainland completed May 2016
- A 12-mile rail bridge connecting Crimea and Russia completed May 2018
- New power plants completed in Crimea November 2019

See: Tass "Crimea will be able to export electricity, first time ever," Nov 22, 2019 and Lyrychikova and Zverev, "Sanctions short-circuited Russia's electricity plans for annexed Crimea, Reuters April 27, 2017.

Cyberwarfare in Ukraine

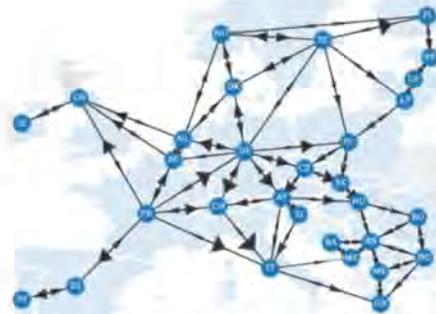
Case study examines three events with direct impact on infrastructure, each with a distinct effect:

- **December 2015** (BlackEnergy & KillDisk). *First successful cyber -disruption of an electricity grid*
- **December 2016** (CrashOverride). *Attack with (unsuccessful) goal of long - term damage to infrastructure*
- **June 2017** (NotPetya). *Attack on Ukrainian business that leaked out to global commerce, resulting in \$10 Billion damage to global economy.*

US DoJ unsealed an indictment (Oct 2020) charging that the Russian Main Intelligence Directorate (GRU)sponsored Sandworm Group was behind each of the three attacks.

Ukraine and the EU

- Ukraine joined the EU Energy Community in 2011
- The EU Energy Bridge is under construction, will bring one NPP (Khmelnitski-2) out of the Ukraine grid and into the European grid. One coal plant is already linked.
- Plans are underway for a full delinking from the Russian grid and subsequent integration into the EU grid in 2023 (The Baltic grid is scheduled to move in 2025)



- Ukraine a favored location to study Russian cyber behavior.
- Ukraine remains on the “Priority Watch List” of the USTR in the 2020 Special 301 Report
- Cybersecurity actors are funded and Ukraine’s capacity is improving...
- Hacktivists remain active against Russia and outside control of GoU.
- Hacktivists tabulated by Kostyuk and Zhukiv (2018) estimate that Pro-Kyiv forces originated 75% of attacks while Pro-Russia attacks constituted 22% of all attacks in 2014-2017.



The Cyber Alliance: CyberHunta, Falcons Flame, Trinity; and RUH8



Assistance to Ukraine Energy Security

NATO Support

- NATO Energy Security Centre of Excellence established 2012 (Vilnius)
- NATO Trust Fund on CyberDefence for Ukraine est. 2014
- NATO Science & Tech Board created a research task group on energy security/hybrid conflict in 2020

USA Support

- Cybersecurity dialogues
- (2017-2020) \$38 million program to support legal and regulatory reform, development of cyber workforce and private sector engagement.
- Total US support to Ukraine of \$198 million in 2019

EU Support

- Includes New Safe Confinement, completion of 3 nuclear reactors
- EU assistance to Ukraine in 2019 was \$413 million. Germany contributed an additional (bilateral) \$205 million and Poland \$81 million
- EU agreement to work towards full synchronization of the grid includes substantial investment (World Bank estimates the total for Ukraine and Moldova will be \$400 million)
- EBRD invested \$124 million in improving the grid 2015-2020.

European Policy Framework

Mr. Alessandro LAZARI

Manager, Resilience Assessment Group, Energy and Global Security Directorate

Definitions

Although the EU Council Directive 2008/114/EC of 08 December 2008 provides the identification and designation of the European CI and the assessment of the need to improve their protection, this does not imply that all Member States (MS) are currently at the same stage. Some MS are still catching up with elements that constitute the European Union while others are more advanced.

Definition of Critical Infrastructure (CI)

2

...means an asset, system or part thereof **essential for the maintenance of vital societal functions**, health, safety, security, economic or social well-being, and the destruction or disruption of which would have a **significant impact in a Member State** as a result of the failure to maintain those functions.

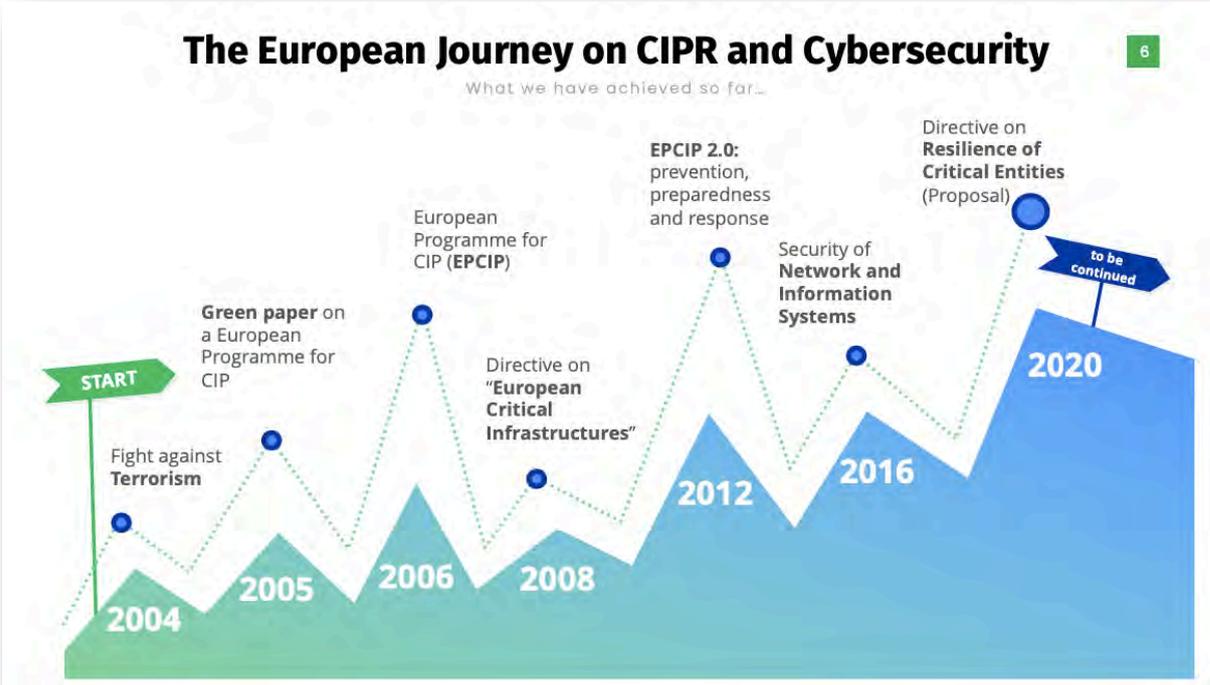
*COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

The Directive also includes the definition of European Critical Infrastructure (ECI), stating that “...a Critical Infrastructure located in one Member State, the disruption or destruction of which would have a significant impact on at least two Member States”. This Directive is still currently in force, but a new Directive is being developed to revert what is referred to as critical infrastructure and refer to the definition of “critical entity”. As such, “critical entity” is seen as

a means to a public or private body which has been identified as such by a Member State. This will be further referred towards “resilience”, meaning the ability to prevent, resist, mitigate, absorb, accommodate to, and recover from an incident that disrupts or has the potential to disrupt the operations of a critical entity. Previously, all the documents have mentioned “protection”, rather than “resilience” but this is now changing within the European Framework of CISR.

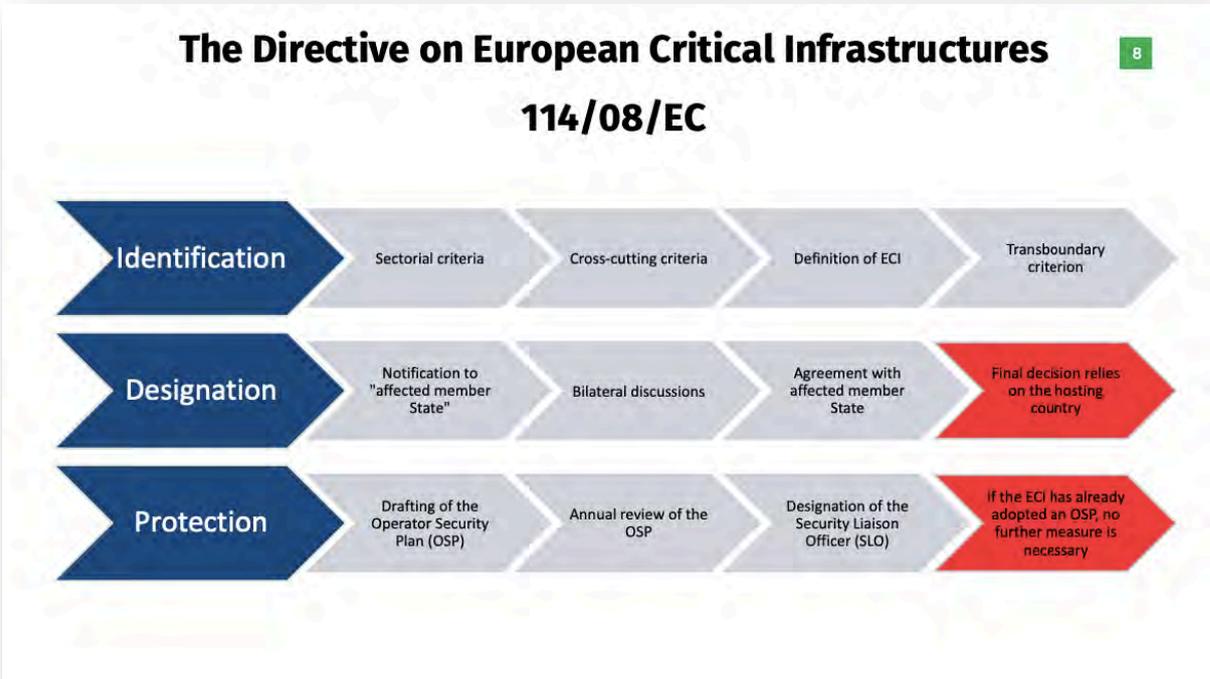
The European Journey on CIPR and Cybersecurity

Why is resilience only developed now and since 2020? This does not imply that MS have not worked on their resilience before. MS are solely responsible of protection and resilience of their CI. The start of this “journey” started in 2004 and has developed ever since. European Programme for CIP (EPCIP) and the Directive on “European Critical Infrastructure” are still very important documents in terms of MS’ discussion up to this day. In 2016, the focus shifted towards the Directive on Network and Information Systems. Now, cyber security is seen as one of the most important issues to focus on. However, we should also not forget about physical infrastructure and threats to it.

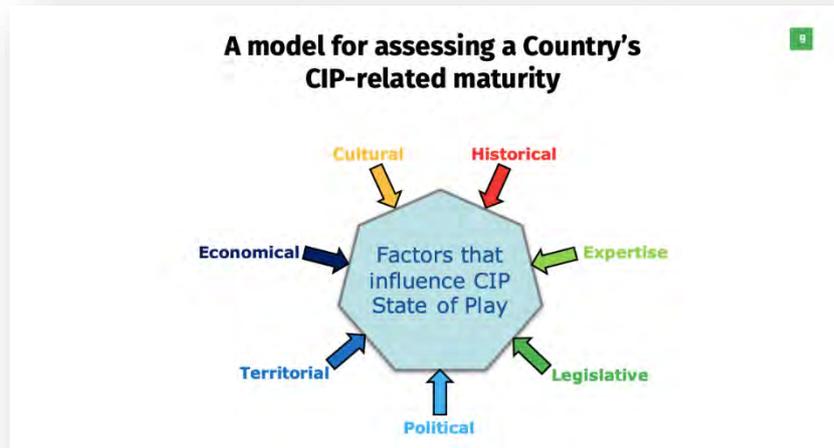


EPCIP also has an external aspect, i.e. looking at the framework of the USA and other neighboring countries. Moreover, countries on the EU enlargement agenda like the Western Balkans, are already looking towards the respective EU framework on CISR in order to align with it better.

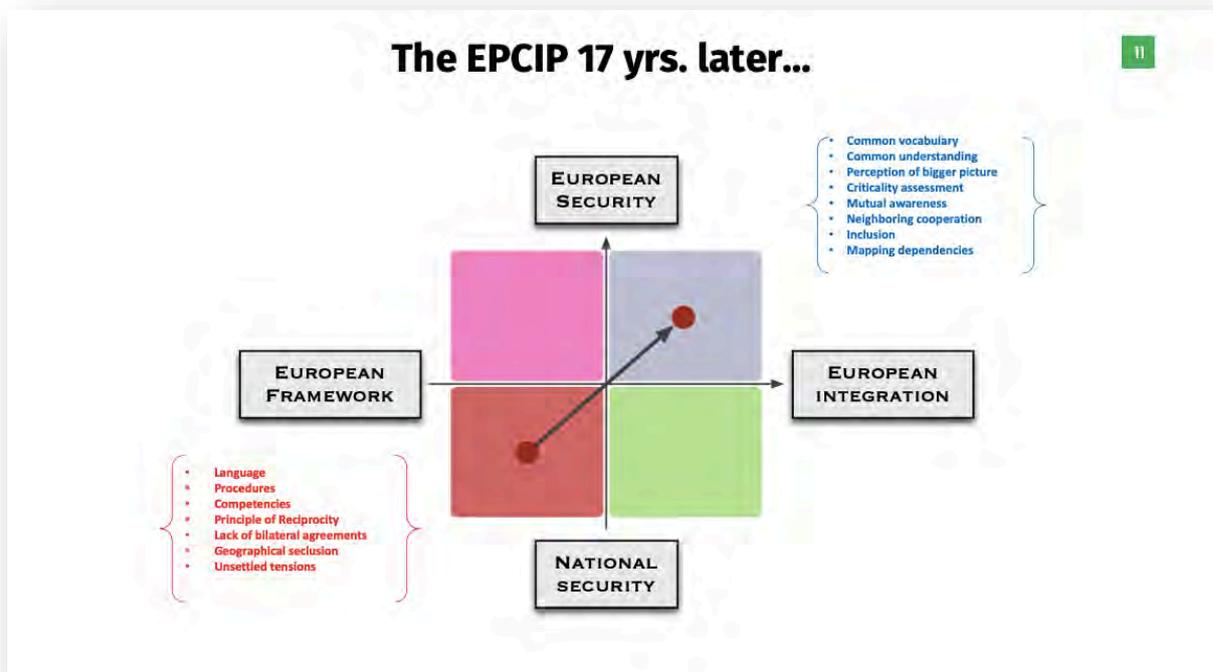
The following slide shows what are the main pillars and expectations of the Directive on European Critical Infrastructures – the identification, designation, and protection of critical infrastructure.



However, the CIP overall process was affected from the fact that 27 EU MS have different approaches, history, economies as well as culture, influencing the CIP-state of play. Therefore, differences in MS’ systems do play a role of how it approaches the CIP.

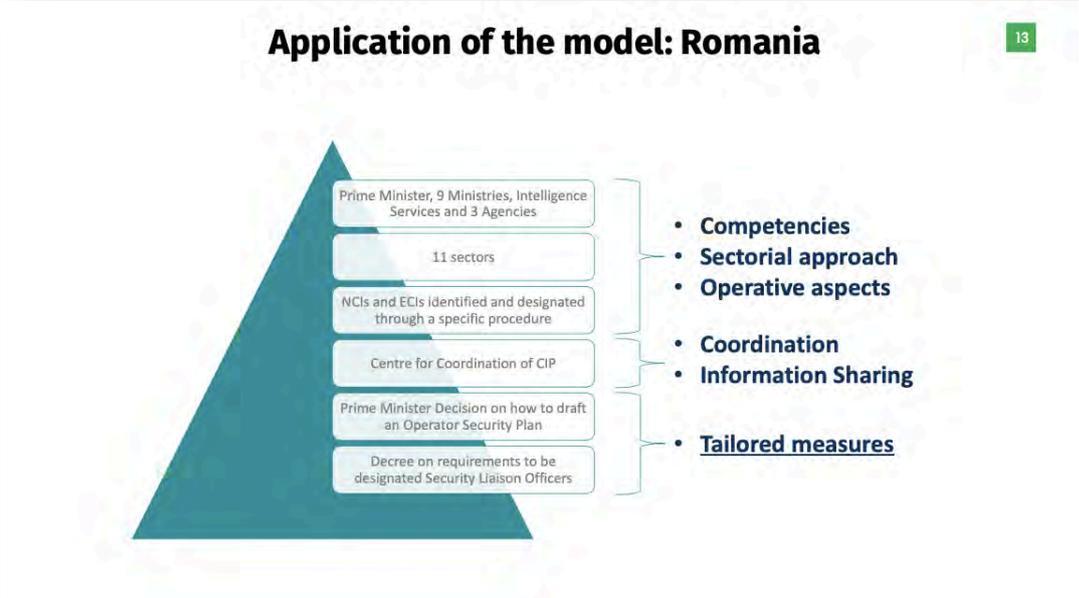


Overall, EPCIP 17 years later has been more standardized and MS work together for a common framework – the greatest value of what the framework has provided so far.



In terms of applying the “security pyramid” to a MS, it has worked well in the case of Romania as one of the MS to have understood the principles of the Directive back then. Now, it has very

comprehensive, tailored measures in place, serving as an example of the successful framework and Directive.



General overview of the European European Framework for CISR

Alessandro Lazari, Ph.D.
School of Law - University of Salento (Lecce - Italy)
TEC - COEDAT - 13th of October 2021

Definition of Critical Infrastructure (CI)

...means an asset, system or part thereof **essential for the maintenance of vital societal functions**, health, safety, security, economic or social well-being, and the destruction or disruption of which would have a **significant impact in a Member State** as a result of the failure to maintain those functions.

*COUNCIL DIRECTIVE 2006/114/EC of 8 December 2006 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Definition of European Critical Infrastructure (ECI)



...a Critical Infrastructure located in one Member State, the disruption or destruction of which would have a **significant impact on at least two Member States**.

*COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

Definition of Critical Entity



"critical entity" means a public or private entity which has been identified as such by a Member State



- (a) the entity provides one or more essential services;
- (b) (the provision of that service depends on infrastructure located in the Member State; and
- (c) an incident would have significant disruptive effects on the provision of the service or of other essential services in the sectors referred to in the Annex that depend on the service.

*Proposal for a Directive of the European Parliament and the Council on resilience of critical entities, COM(2023) 829 final, 16.12.2023

Definition of Resilience

30

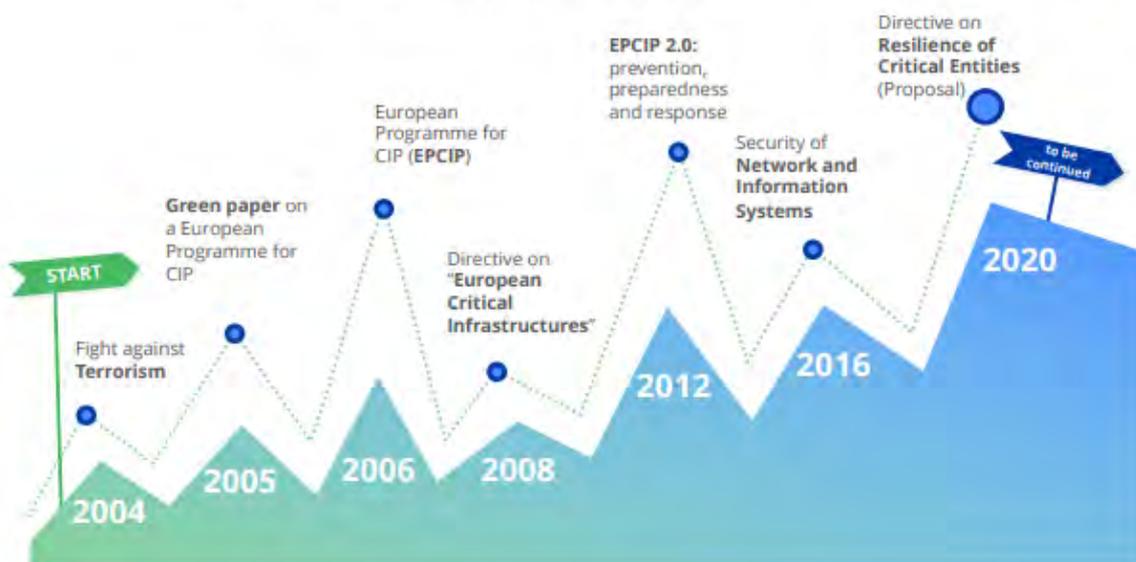
"resilience" means the ability to **prevent, resist, mitigate, absorb, accommodate to and recover** from an incident that disrupts or has the potential to disrupt the operations of a critical entity

*Proposal for a Directive of the European Parliament and the Council on resilience of critical entities (COM(2019) 620 final), 16.12.2019

The European Journey on CIPR and Cybersecurity

31

What we have achieved so far...



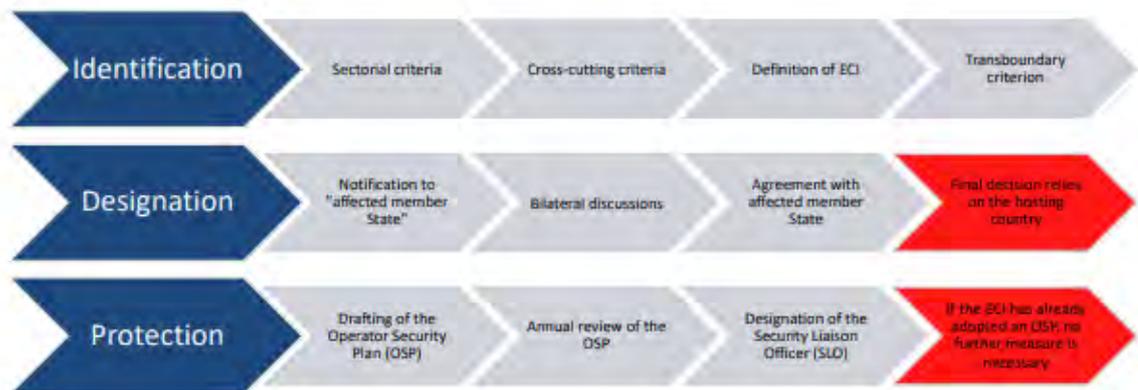
The European Programme on Critical Infrastructure Protection

7



The Directive on European Critical Infrastructures 114/08/EC

8



A model for assessing a Country's CIP-related maturity

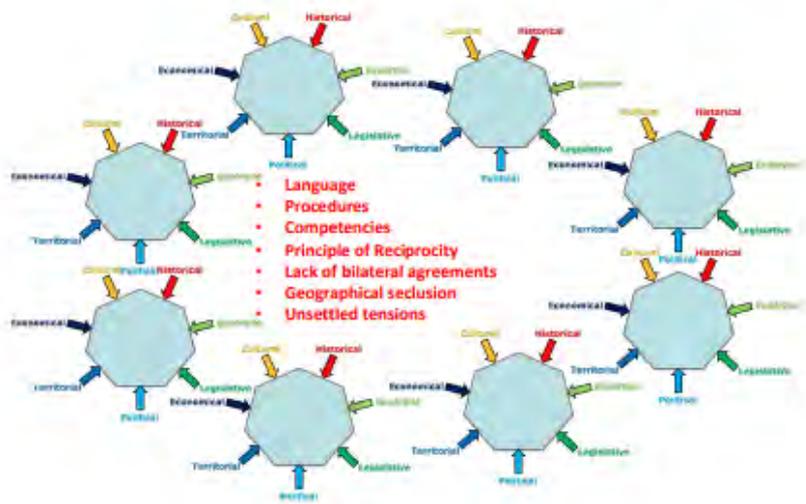
9



Small text at the bottom left of slide 9, likely a copyright notice.

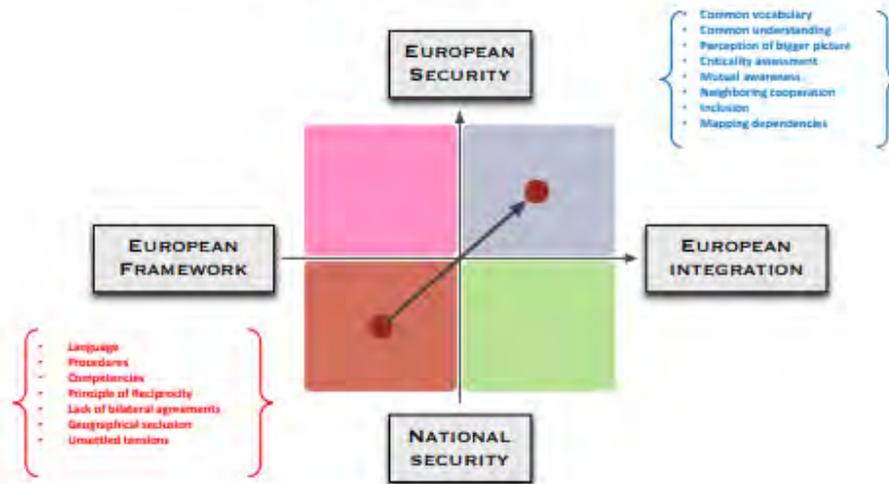
Cooperation around common strategies (Limits found at the beginning of the Journey)

10



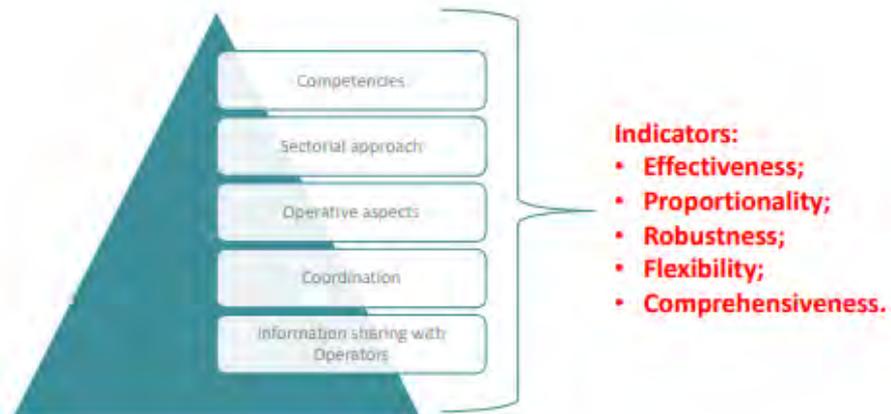
The EPCIP 17 yrs. later...

11



Assessing Member States' CIP State of Play: the "Security Pyramid"

12



How to “maintain” our common achievements?

15

Things to keep in mind...



Consolidation

Every new policy should be perceived as an **upgrade** that **consolidates** the achievements of the past.



Exercise

Every scenario, crisis, policy, measure, solidarity mechanism needs to be tested.



Training

Education, training and certification in quality (the experts of the future) are essential for growth.



Inclusion

Reinvesting time and efforts on the “external dimension” of the EUCIP.



Sharing

Improve and exploit the network of trust and information sharing.

THANKS FOR YOUR ATTENTION!

DAY II – Session 2: Questions and Open Discussion

Mr. David HARELL

1. Which could be the best practices to protect airports against mini-drone attacks?

We are all focused on the impacts, functions, and effectiveness on drones nowadays. We even saw drones displayed at the opening of the Tokyo Olympics. However, as security experts, we have think about what if drones codified with artificial intelligence are used with an intention of committing terrorist acts. Even a small apparatus on the drone can cause catastrophic devastation. As a result, sending a group of drones towards an aircraft is a frightening issue. Certainly, this case is already in our minds.

Going back to his presentation, Mr. Harell reminds, terrorist also seek to utilize new technological innovations to conduct their attacks. Drone technology is also really appealing to those groups. What can we do in this regard? We have to focus more on the legislation side. We need a more proper regulatory processes as well as licensing. Anybody should not be allowed to control, fly, and use drones. On the other hand, we can take kinetic measures to deal with that threat. For instance, we have some other weapons that are able to target the drone and eliminate any kind of threat. In order to bring it down, first you have to detect it. Another solution to this threat could be jammers. They detect the frequency of drones. The problem is jammers jams other things, as well potentially the equipment of an airport. Therefore, they have a double-sided effect. Modern approach to this problem is based on cyber capabilities. If you are able to detect the drone, then you are able to control it and bring it down. As a result, you have to possess all type of equipment that provide you with a protective bubble over the airport. Furthermore, neutralizing the drone attack is not efficient. You have to find the person who is controlling the drone.

2. 9/11 attacks were carried out by terrorists who had taken private pilot flight courses resulting in airport security practices being continuously revisited and updated. Now that it is harder for terrorists to infiltrate airport security in and around airports, for a terrorist network familiar with instrument flight, new technology like drones built as IED (like mortar shells installed) and open-source

knowledge like airport approach charts, real-time traffic tracking, and real-time radio broadcast over the internet pose drastic threat to incoming aircraft even for highly-protected HOSG VIP jets with various countermeasures for SAM missiles. Technology has not been able to solve bird strikes, yet terrorist use of explosive manmade birds as flying mines throughout the critical approach phase stands as real threat for all of us. Now airport security should extend to the cone from final approach fix to runway thresholds where autopilots control aircraft precisely depending on the charts directions (coordinate and altitude) regardless of visual conditions. Therefore, are there any studies or developments to fill that security gap that may lead to next generation 9/11?

A new technology should be developed in ICCW industry and organizations like ICAO, FAA and EASA to add drone detection to collision avoidance systems built in aircrafts and drone monitoring radars dedicated for approach cone area to warn aircrafts “on final approach” in thousands of airports worldwide.

Mr. Harell states that he is quite sure that there are some companies out there working on such issues. They understand that this is a problematic and expectedly it needs a solution in terms of cyber security. We have not seen terrorist use of swarm technology so far. However, this does not mean that we are not going to face that threat one day.

3. Are there lessons aviation security can learn from other regulated sectors? Does AVSEC regularly engage with such sectors?

In the security world, there are many lessons that can be learned across the board in all domains. The same processes, same ideas, same understanding of what is going around or the possible solutions make a great deal of cumulative knowledge in that sense. From a strategic point of view, countries that have different security and anti-terrorism agencies all under the same roof have a greater chance of integrating their experiences and lessons learned. This process of information, intelligence, and experience sharing between agencies does matter in terms of building a more comprehensive and extensive strategy against adversaries' malicious intentions.

- 1. Energy usage in 19th and 20th depended on carbon-based energy. Futurists foresee that 21st century will be the century of Hydrogen based energy in the future. Do you think so?**

One issue regarding the question is that even though we are moving more towards electrification, there are some processes that are particularly industrial. For example, heavy trucks do not lend themselves to electrification. Hydrogen is a way of making energy mobile. There is an energy input required to create the hydrogen then you move it around when the hydrogen recombines and releases the energy.

At this point, it is really hard to say that how much of the discussion about hydrogen is going to unfold. Also, there are also concerns about the limit of the technology to benefit from hydrogen. Dr. Sabonis-Helf personally believes that there is going to be a number of different energy resources and hydrogen is likely to be picked by the industry and transportation sectors that will not easily lend themselves to electrification.

- 2. What are the implications of North Stream 2 (NS2) to Ukraine resiliency?**

Dr. Sabonis-Helf reminds us to bear in mind that Russia wanted to take the guarantee of Europe in 2014 that they would respect existing contract to use Ukraine as a transit state until the contract expired. However, when it expired, they would not allow any more gas to transit through Ukraine to the European continent. Europe and the US cooperated in slowing down all the other pipelines so that Russia was compelled to sign another four-year agreement. Russia now has done that. On the other hand, Dr. Sabonis-Helf argues that the prospects of Russia continuing to transfer gas through the Ukraine after 2024 are very poor. Although it will represent an economic loss to Ukraine, relying on an adversary state is illogical. Interruptions in energy are happening in the transit states rather than the supplier or the receiver state. As a result, Dr. Sabonis-Helf thinks that the strategy is about delaying and she believes that Germany has great reasons in not involving in NS2. She also argues that the NS2 does compete with Turk Stream. Both of these compete with Ukraine. However, Ukraine's future in gas is actually in storage. That is because it has the largest underground storage of natural gas in Europe

as well as being one of the largest ones in the world. During COVID-19 pandemic, Ukraine stored the surplus gas in its storage tanks and acted as a price balancer. That is a more-likely role for Ukraine, it is going to be a storage state.

3. What are the repercussions to small countries in the Balkans from Russians LNG proactiveness and EU Green Deal?

The reality here is that the EU is already worried about stranded assets. Under the European energy law, nations that were transits and wanted to be hubs had to demonstrate that they had the capability to bring the gas at least from three different sources. Many nations have built LNG facilities and they chose not to use them. Because the LNG is much more expensive. Therefore, it becomes really national to use it as storage. There are number of states hoping to get into the business/being another hub for Europe; however, given the nature of the debate, Europe fears there are already too much infrastructure and the assets are going to be stranded. It is really hard to imagine anyone at this point getting an infrastructure investment. This is bad news for the Balkans, Turkmenistan, and Azerbaijan. But in terms of the prospects for the future, we should keep an eye on the Balkans.

4. How do you evaluate the poor cyber control of Ukrainian Government in regard to the hacking group? Is it not counterproductive or provocative when dealing with smart threat forces?

Dr. Sabonis-Helf states that she is also really concerned regarding that issue. The Ukrainian government has discovered that when they tried to take on the cyber alliance, the alliance started doing white-hat attacks on the Ukrainian government. As soon as they saw that the government is not very well capable of tackling this attack, they released the vulnerabilities of the government to the media. This situation put really hard pressure on the government. If, in fact, Ukraine is going to have close ties with NATO and if, in fact, there are going to be security benefits for Ukraine, having a non-

state entity that is not under the control of the government that makes its own decisions when provocative attacks are appropriate, is quite terrifying.

Mr. Alessandro LAZARI

- 1. Do you think that energy dependency, especially for European case on RF, might also create a risk for CISR? If yes, how should EU mitigate this risk?**

We are going through hard times in terms of natural resources. On the issue of electricity and gas transmission and distribution, the EU has spent a lot and supported some platforms such as European Network of Transmission System Operators for Electricity. They are making sure these transmission systems are resilient. However, at the same time, the EU holds multiple mitigator roles to ensure that diversification is being implemented. Transatlantic Pipeline and Trans-Anatolian Pipeline can be raised as examples. Italy is becoming a major hub. These are not only European achievements, but they are also national achievements. The reason is that every country develops a national strategy and makes sure that it has sufficient resources in order to meet the energy demand. To maintain the solidarity in terms of the energy issues, every member country should be highly resilient.