Terrorism Experts Conference

&

Executive Level Defense Against Terrorism Seminar

(TEC 2020)

Combined COE-DAT Online Event

3-4 November 2020

Ankara, Turkey

Contents

TEC 2020 Team

Academic Advisor
Prof. Haldun YALÇINKAYA (TUR)

Seminar Director
Col. Pavlin RAYNOV (BGR AF)

Deputy Seminar Directors
Maj. Zekeriya TOSUN (TUR A)
Cpt. Gökhan CİN (TUR A)

CIS Specialist
Mrs. Selvi KAHRAMAN (TUR Civ.)

Seminar Assistant
Mrs. Aslıhan SEVİM (TUR Civ.)

Speakers Organizations
Mr. Stephen HARLEY, Freelance Consultant
Ms. Susan SIM, S Rajaratnam School of International Studies, Singapore
Dr. Zeynep SÜTALAN, Atılım University, Turkey
Dr. Afzal ASHRAF, The University of Nottingham, UK
Ms. Stephanie FOGGETT, The SOUFAN Center, US
Prof. Mustafa KIBAROĞLU ,MEF University, Turkey
Prof. Salih BIÇAKCI, Kadir Has University, Turkey
Prof. Ronald Sanford BEARSE, Massachusetts Maritime Academy, US
Col. Daniel Wayne STONE, Deputy Director COEDAT

Rapporteurs
Ms. Alice LÕHMUS (EST)
Ms. Elif Merve DUMANKAYA (TUR)

TEC 2020 Concept

COE-DAT is developing a Best Practices in Counter-Terrorism handbook project in coordination with TOBB-University in Ankara, Turkey, as well as other universities such at the US Army War College and Nottingham University, UK. COE DAT is attempting 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 2020 were planned to support the Handbook project. The initial chapters were the backbone and an opportunity to introduce, to review, and to collect outcomes for future development and improvements of the first draft of the Handbook. Because of the COVID pandemic, Terrorism Experts Conference and Executive Level Defence Against Terrorism Seminar were conducted on-line between 03-04 November 2020 as a combined activity on the topic of "The Military Role in Countering Terrorism". The duration of the working day was 4 hours between 14.00 and 18.00 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.

The initial chapters of the Handbook are:

a. Hard Power, Soft Power and Smart Power: Civilian-Military Challenges in CT
b. Critical Infrastructure Protection
c. Developing National Counter-Terrorism Policy
d. Gender, Terrorism and Counter Terrorism
e. Weapons of Mass Destruction and Counter-Terrorism
f. Cyber Security in the Domain of Counter-Terrorism
g. Media and Counter-Terrorism

The last briefing/presentation offered the participants the COE DAT point of view on the future role of the military/NATO in counter-terrorism.

Each area were presented by their authors. Approximately a week prior to the event a synopsis/position paper were posted on COE-DAT's website for participants to review ahead of the event.

Terrorism Experts Conference
&
Executive Level Defense Against Terrorism Seminar
(TEC 2020)
Combined COE-DAT Online Event Program

Time (Local GMT +3)	**DAY ONE (November, 3rd)**	
13.30 - 14.00	Communications Check	
14.00 - 14.05	Welcome Address	Director
14.05 - 14.10	Administration Briefing	TEC/Seminar Director
14.10 - 14.20	**Opening Remarks** by Keynote Speaker	RADM J. Tammen DCOS ACT
14.20 - 14.30	Break	
14.30 - 17.40	**PANEL 1** "*Social Aspects and Policy Development in Countering Terrorism*"	Academic Advisor
14.30 - 14.50	Hard Power, Soft Power and Smart Power: Civilian-Military Challenges in CT	Mr. Stephen Harley
14.50 - 15.10	Developing National Counter-Terrorism Policy	Ms. Susan Sim
15.10 - 15.30	Gender, Terrorism and Counter-Terrorism	Dr. Zeynep Sütalan
15.30 - 15.50	Cyber Security in the Domain of Counter-Terrorism	Assoc. Prof. Salih Bıçakcı
15.50 - 16.00	Break	
16.00 - 17.40	**Questions & Answers and Open Discussion**	Academic Advisor
17.40 - 17.50	Break	
17.50 - 18.00	"**Hot Wash-Up**" of Day 1 Discussions	
Time (Local GMT +3)	**Day TWO (November, 4th)**	
14.00- 17.30	**PANEL 2** "*Domains of Terrorist Threats and Best Practices in Countermeasures*"	Academic Advisor
14.00 - 14.20	Weapons of Mass Destruction and Counter-Terrorism	Prof. Dr. Mustafa Kibaroğlu
14.20 - 14.40	Media and Counter-Terrorism	Dr. Afzal Ashraf & Ms. Stephanie Fogget
14.40 - 15.00	Critical Infrastructure Protection	Prof. Dr. Ronald Sanford Bearse
15.00 - 15.20	COE-DAT Presentation "Potential Future Role of NATO in Counter-Terrorism"	Col. Daniel Wayne Stone
15.20 - 15.30	Break	
15.30 - 17.30	**Questions & Answers and Open Discussion**	Academic Advisor
17.30 - 17.40	Break	
17.40 - 17.50	"**Hot Wash-Up**" of Day 2 Discussions	Academic Advisor, Col. Daniel Wayne Stone
17.50 - 18.00	Closing Remarks	Director

Main Outcomes and Common Points of TEC 2020

- **Military power most likely will not be the deciding factor in CT**; military power **should be used to support** a whole of government and whole of society approach **to address the root causes of terrorism**.
- Importance of having a balanced approach to CT - **whole of society, whole of government.**
- **Cooperation, Communication, and Coordination.**
- **Militaries need to adopt to the changing nature of conflict and terrorism.**
- Terrorism and violence is a **choice.**
- Community engagement is easier accomplished in some countries and some contexts than others.
- **Diversity** is a better term to use than culture.
- **Acknowledging women's role and agency is important to develop an effective CT strategy.**
- **Militaries should be cautious to maintain their long-term reputations** and not be tempted by short-term politics.
- There is a **need for strong public-private partnership.**
- **Sharing intelligence** between institutions/private sector is important.
- NATO should ask from nations **what is it that they need, what are their goals, what is their capability needs** instead of telling them what they need.
- **Threats and terrorism can be constrained, not prevented.**
- **Context should be considered in any CT strategy** and focus on local based actions.
- **CT is a social science and a multinational problem** - it does not have a straightforward solution.
- The need to distinguish **where is the truth** in on-line messaging.
- WMD are a **low probability** of use**, but a high consequence scenario.**

Opening Remarks - Welcome Address

Dear Generals and Admirals,
Dear Distinguished speakers and participants,
Ladies and gentlemen,

Good morning, good afternoon, or good evening, wherever you are in the world.

Please allow me to introduce myself: I am Colonel Barbaros DAĞLI, the Director of Center of Excellence Defence Against Terrorism. I would like to give you a warm virtual welcome to our flagship event for 2020. This year we combined the Terrorism Experts Conference with the Executive Level Defence Against Terrorism Seminar. It is my honour and great pleasure to welcome you all.

I am very pleased with the great interest this activity has received. We have more than 180 participants from 45 countries, across 5 continents and ranging from academia, regional organizations, national war colleges, combatant commands, partner nations, to NATO headquarters. Truly an impressive cluster of knowledge and expertise.

Unlike previous years, this year we combined our two flagship activities due to the current pandemic situation. I believe that by bringing together the combination of academic, theoretical, and strategic/operational practitioners will foster dialogue that will contribute to this activity and increase all of our knowledge on the topic of terrorism.

NATO, like many other organizations, suffers from the problem of achieving a common understanding and consequently, the difficulty of developing common documents in the field of counter-terrorism. COE DAT is trying to fill this gap with its Best Practices in Counter-Terrorism handbook project in coordination with TOBB-University in Ankara, Turkey, as well as other universities such at the US Army War College and Nottingham University, UK. During this webinar, you will have the opportunity to become acquainted with the content of the chapters by the authors themselves. COE-DAT recognizes each author are experts in their field and we highly appreciate their knowledge and contribution to our project.

The Best Practices in Counter-Terrorism handbook does not aim to present an in depth theoretical foundation of the various manifestations of terrorism and countering-terrorism. Our aim is to present practices, approaches, and policies that have shown successful results in different countries and/or different environmental conditions. COE DAT and the authors do not claim that the offered practices, policies, and solutions are the best, most accurate, and applicable for all environments; COE-DAT submits that these can be used as a starting point in the development of effective counter-terrorism policies and efforts.

With the last presentation, you will be acquainted with the point of view of COE DAT. The deputy director, Col Stone, will try to emphasize the role of the military in countering terrorism, both nationally and internationally and offer some potential recommendations for militaries in counter-terrorism strategies.

During these two days, and specifically within the discussions, we have set ourselves one main goal, and that is not to make you agree with us, but rather to provoke you to share your opinions, attitudes, and views. Your comments will give us insights on new ideas, perspectives, strategies, and techniques to better confront terrorism, and importantly we will have an enhanced network of counter-terrorism friends and counterparts.

Ladies and gentlemen, distinguished participants,

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

Thanks to those who have already sent questions and comments.

We rely on your support.

Thank you. Wish you all successful and interesting work.

Barbaros DAĞLI
Colonel (TUR A)
Director COE-DAT

Keynote Address (Synopsis)

Rear Admiral John Tammen who is the Deputy Chief of Staff for Allied Command Transformation Strategic Plans and Policies and the Flag Officer / General Officer Champion for COE-DAT to Supreme Allied Command Transformation provided the keynote address.

Terrorism in all its forms and manifestations pose a direct threat to our populations, security, and economies.

Military power cannot win versus terrorism alone. Terrorist organizations are ever evolving and adapting to attack society, governments, operating in the cyber domain, inciting protests, and acting as shadow governments.

To address terrorism, governments and societies must address the root causes of terrorism through a Whole of Government and Whole of Society approach. Militaries can aid government and society in this effort.

This year's conference topic is "The Military Role on Countering Terrorism". It focuses on the findings that COE-DAT has gained during the on-going development of its "Best Practices in Counter-Terrorism" handbook project in coordination with TOBB University in Ankara, Turkey; as well as with the US Army War College; Nottingham University, UK; and many other academics from around the world. COE-DAT's focus is at the strategic and operational levels focusing on what militaries and NATO can do to support a Whole of Government and Whole of Society approach to counter terrorism (CT). COE-DAT is focusing on areas militaries can support Whole of Government and Whole of Society and will discuss:

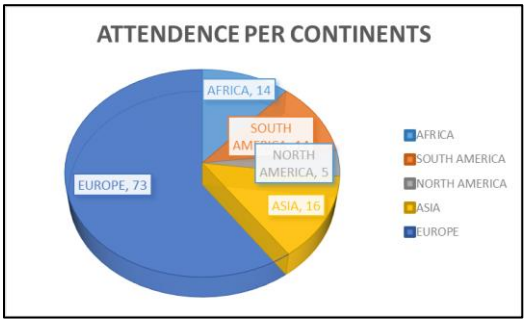
- *Hard Power, Soft Power leading to Smart Power: Civilian-Military Challenges in CT*
- *Critical Infrastructure Security and Resilience*
- *Developing National CT Policies*
- *Gender, and Terrorism and CT*
- *WMD and CT*
- *Cyber Security in the Domain of CT*
- *Media and CT*
- *COE-DAT will present what terrorism may look like over the next 10 to 20 years and potential future roles of NATO/militaries in CT*

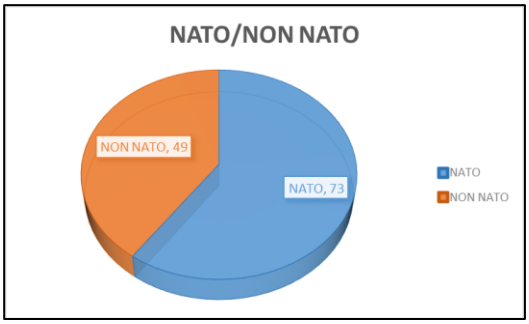
The presentations will focus on the accumulated best practices from around the world.

Military power alone cannot defeat terrorism, but together with government and society, militaries have a valuable supporting role to play in defeating terrorism and eliminating the causes.

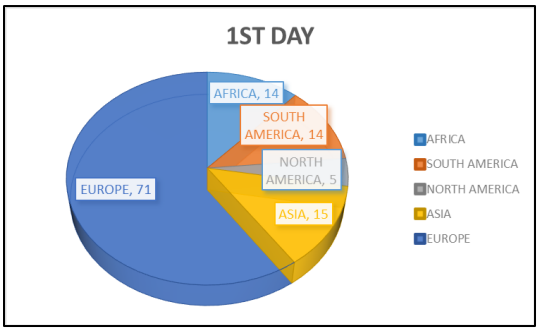
TEC 2020 Statistics

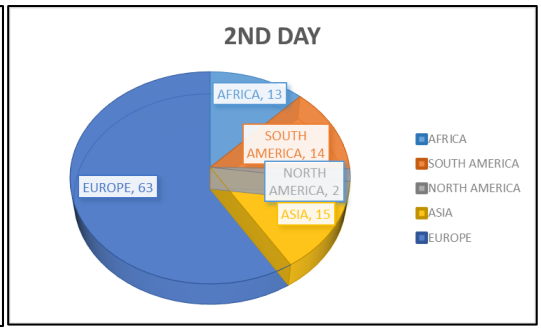
210 users were registered to join on-line the TEC 2020. 11 of them were members of COE DAT and 7 were briefers. **41 countries** from 5 continents were present at the TEC 2020. 7 participants join from MENA region and 1 from a country (Afghanistan) where NATO is carrying operation.





Totally **122 participants** attended the sessions. **104** were present both days, 119 (71 representatives from NATO nations and 48 from non-NATO countries) on 3rd Nov and 107 (60 representatives from NATO nations and 47 from non-NATO countries) on 4th Nov. 15 attendees joined only the first day and 3 appeared only at the second.





There were 14 participants from the academia, 12 executive level officers (OF-6 and above) and 4 civilians with equivalent higher level. 14 participants represented NATO entities.

54 questions were addressed to the lecturers totally. One participant (from Afghanistan) requested and was given the floor to express his comment on-line.

A new practice was initiated for TEC 2020. It was named "Forward Point" and the idea is a class of students, organized by the teacher to take part at a Conference/Seminar as one user from their university/college. The COE DAT fellow Col. Assoc.Prof. Petar Marinov, PhD arranged a Forward Point with 20 students in Rakovski National Defence College – Sofia, Bulgaria.

COE DAT considers the Forward Point as a good practice for the on-line events. It is an excellent example of combining the think-tank and the education functions. This format allows groping participants with similar level of knowledge and speaking mother language. The groups have independence to generate internal discussions and a big number of questions to the lecturers out of it.

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 lecturers and our panel moderator Prof. Dr. Haldun YALÇINKAYA 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 possible.

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 honour 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.

Barbaros DAĞLI
Colonel (TUR A)
Director COE-DAT

Annex A – Day 1, Panel 1: "Social Aspects and policy Developments in Countering Terrorism" Presentations, Questions, and Answers

Annex includes the following:

1. Hard Power, Soft Power, and Smart Power: Civilian-Military Challenges in CT
    a. Presentation
2. Developing National Counter-Terrorism Policy
    b. Presentation
3. Gender, Terrorism and Counter-Terrorism
    c. Presentation
4. Cyber Security in the Domain of Counter Terrorism
    d. Presentation
5. Day 1 Questions and Answers and open Discussion

Annex B – Day 2, Panel 2: "Domains of Terrorist Threats and Best Practices in Countermeasures" Presentations, Questions, and Answers

Annex includes the following:

6. Weapons of Mass Destruction and Counter-Terrorism
    a. Presentation
7. Media and Counter-Terrorism
    b. Presentation
8. Critical Infrastructure Protection
    c. Presentation
9. Potential Future Role of NATO in Counter-Terrorism
    d. Presentation
10. Day 2 Questions and Answers and Open Discussion

Annex A – Day 1, Panel 1: "Social Aspects and policy Developments in Countering Terrorism" Presentations, Questions, and Answers

Contents

Hard Power, Soft Power & Smart Power: Civilian-Military Challenges in CT

by Mr. Stephen Harley

Combining hard and soft power approaches to achieve strategic goals is not a new idea.

Julius Caesar, during the conquest of Gaul, achieved a decisive military victory over his rival, Vercengetorix, at the battle of Alesia in 52 BCE, the culmination of a back-and-forth campaign that saw Caesar side with one tribe against another, suffer setbacks and see allies turn against him but eventually triumph over the Gauls. As a result, Gaul was subsumed into the Roman Empire.

Caesar's victory in Gaul was not purely an exercise in 'hard' military power, nor for that matter 'hard' diplomacy (blackmail, coercion, manipulation, bribery). His decisive military victory, and his use of symbolic atrocity, such as the amputation of the hands of every fighting age male of the treacherous Ubi tribe or the eventual ritual strangulation of the leader of the vanquished Gauls, Vercengetorix, in Rome years afterwards, were undeniably '*hard*'. But Caesar was equally comfortable with the use of 'soft' approaches too, albeit not quite as '*soft*' as we might feel comfortable with today.

Caesar, for example, wrote the story of his campaign in Gaul, The Conquest of Gaul, close-run-things and all, in the third person: Caesar writing describes Caesar charging into the fray with his distinctive purple cloak flowing at times when decisive leadership was required. He also limited the vocabulary of his account to approximately 1300 words, to make the story (or Caesar's version of the story) more accessible beyond the erudite elite, and to make it more 'transmittable' for orators in public squares, the 'mass media' of the times. This limited-vocabulary account of the defeat of the Gauls was also used as a teaching text: the surviving Gauls were taught Latin using the story of their own recent ignominious defeat. That France still has military units called 'Legion' is indicative of how successful Caesar ultimately was. But would this far reaching achievement have been possible if Caesar had used purely hard power

approaches (as the Romans had done with a previous adversary, Carthage)? Is it not the softer elements of his approach (education, social and economic integration) that created the enduring effect and ultimately benefitted Rome more?

This research is about the applicability of the best examples of hard and soft power approaches to counter-terrorism, bridging the gap between the considerable body of literature on what constitutes the effective interaction of hard and soft power approaches to achieve foreign policy goals, and the potential role for integrated approaches in achieving the more specific objectives of counter-terrorism.

The study of the interaction of hard and soft power approaches (referred to when combined as 'smart power') is still a subject of academic discussion. However, much of the discourse is focussed on foreign policy or on the increasing importance of (but resistance to) soft power approaches. Little consideration has been given to implementing these concepts in counter-terrorism. As a result, there are few examples of the coordinated, consistent and effective implementation of hard and soft power approaches in unison in counter-terrorism.

The questions at the heart of this research are:

- What is meant by hard power and soft power (and smart power)?
- What does best practice mean in the integrated use of hard and soft power out-with the realm of counter-terrorism?

The research uses a Case Study based to answer the final question:

- What best practice examples can be drawn out of the integrated use of hard and soft power approaches to counter the terrorist group, al-Shabaab, in Somalia?

The research concluded that the integrated use of hard and soft power to achieve smart power remains the exception rather than the rule, primarily because of the continuing predominance of hard power proponents in positions of influence and in charge of large budgets. The lack of understanding of what soft power constitutes is slowly being addressed, but few nations actually audit their soft power potential in the same way they do their hard power.

However, some nations do understand the value of using hard and soft power approaches in interaction to achieve smart power and achieve national objectives. There is no reason why other countries cannot do this, as long as they have a system of values at their core that allows for the credible use of soft power. Nor is there any reason why international organizations such as NATO (along with the UN, the EU, the AU et al) cannot either, especially given the various grandiose charters that are at the core of each. In particular, military power can be adapted to soft power functions, but this a choice that some nations choose not to make. Other functionaries of government, such as diplomats and those involved in the law and business & trade seem to find it considerably easier to move between a hard and soft stance.

There are, though, some important conditions to be considered in the design of a smart power effort, especially if it is being applied in the realm of counter-terrorism.

Firstly, choose the 'face' of the campaign carefully. In an international environment, a degree of national and organisational self-awareness will be important: some countries may have a cultural affinity and can be overt in their engagement, others will be culturally discordant and their presence should be minimal or even covert. A former colonial power, for example, may not make the best 'lead' in an international campaign when there is perhaps a 'new' country that would be a more palatable option. In the case of Somalia, the African Union Mission includes troops from only one Muslim country: and that country, Djibouti, does not lead the mission. With the benefit of hindsight a better option may have been to recruit from Muslim African countries, or form the mission from out-with Africa (since many Somalis feel more affinity with the Gulf). This will be especially important if the terrorist group is strongly ethno-nationalist and/or religious (both are the case with al-Shabaab).

Secondly, coordination is essential. While this is hardly a revelation, coordinating with the stabilisation and humanitarian sectors might be very new for some but can yield results in an integrated, 'smart' counter-terrorism campaign.

Thirdly, in smart power, soft power leads. This may mean that the individual 'face' of a mission wears a suit, not a uniform. (Or perhaps even a t-shirt.) The 'face' may even be local, with attribution of activities always going to the local government or local actors. This requires national-level humility, and means the practice of sticking prominent flags and badges on everything and flooding the media with back-slapping

videos may have to be put aside until the terrorist threat is diminished (because every one of those flags and badges is potentially a magnet for a terrorist attack) - or possibly forever.

Fourthly, communication is vital and must take place before, during and after every activity, to shape, sustain and where necessary, react. Terror groups use both hard and soft power approaches (although we tend to focus on their hard power activities) and they also see the intrinsic value of communication. But their balance, by their own admission, is 10% operations/90% communication (so said Osama Bin Ladin) while the opposite appears to be the case with those fighting counter-terrorism. Communication must be built into all activities, not sit as a separate entity, and it must be credible (which will generally mean 'local').

Clearly there is much to be done to adapt existing organizational counter-terrorism structures to achieve the smart approach: but the examples of how to do it are certainly there - and are undoubtedly transferrable to the realm of counter-terrorism.

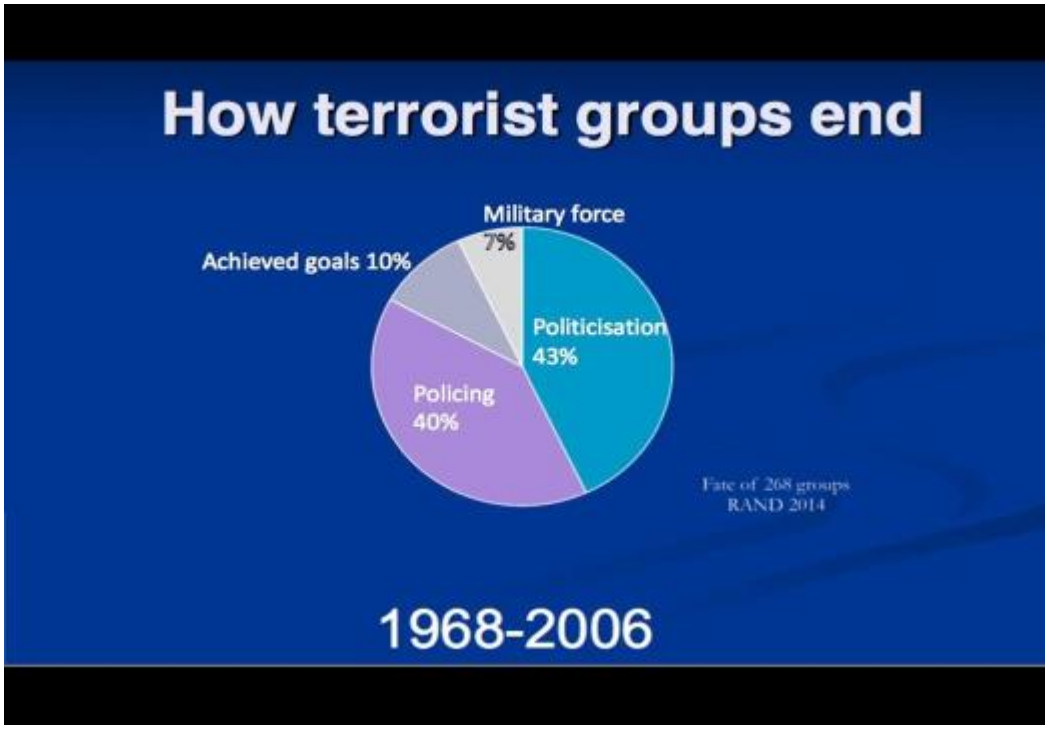
a. Presentation

Hard & Soft Power Approaches in Counter Terrorism

Overview

- **Historical Example:**
  - **Caesar's War in Gaul**
- Definitions:
  - Hard Power, Soft Power & Smart Power
- Case Study:
  - Countering al-Shabaab in Somalia
- Lessons Identified:
  - Smart Power in Counterterrorism


HISTORICAL EXAMPLE:
Julius Caesar & the Invasion of Gaul
Military Victory
Mass Amputation
'De Bellis Gallia'
Caesar's
GALLIC
WAR


How terrorist groups end
Military force
7%
Achieved goals 10%
Politicisation
43%
Policing
40%
Fate of 268 groups
RAND 2014
1968-2006

How Terrorist Groups End

- Methodology
  - *How did RAND define a Terrorist Group?*
  - *(How do you define a Terrorist Group?)*
  - *Have things changed since 2006?*
  - *Isn't RAND a US government sponsored think - tank?*
  - *Terrorist Groups often end for multiple reasons*

How Terrorist Groups End

- Alternative Endings:
  - Terrorist Groups often end for other reasons
    - *Become Criminal Gangs*
    - *Resource shortage (supporters)*
    - *Run out of steam (population & participants don't want to fight anymore)*
  - **Terrorist Groups often end for multiple reasons**

What is Hard Power?

- *Coercive*
- *Generally assumed to mean military power*
- *Can also mean the use of economic power*
- *Increasingly includes the use of legal and policing methods*

Military

Intelligence

Policing & Legal Measures

What is Soft Power?

- *Persuasive*
- *Generally means non-kinetic means*
- *Can include cultural, economic, informational and other means*

Communications

Education

Job Creation

Sport

What is Smart Power?

Hard Power	Soft Power
Military	Development/Aid including Infrastructure
Economic	Education
Diplomatic	Culture & the Arts
Legal	Sport
Policing	Tourism
	Religion/Philosophy
	Information

Operating in interaction...

Case Study:
Countering al-Shabaab in Somalia

Why did you join al-Shabaab?

CASE STUDY:
Countering al-Shabab

- *HARD POWER:*
  - *Military:*
    - *Strikes: Drone/Air/SF*
    - *Military Training*
  - *Law Enforcement:*
    - *Checkpoints, Forensics, Community Engagement, Military Court, Tips Hotline*
  - *Legal/Economic:*
    - *Sanctions, US Rewards for Justice*
    - *Anti-Terror Financing Initiatives*

CASE STUDY:
Countering al-Shabab

- *SOFT POWER:*
  - *Education/Culture/Religion:*
    - *Adult Learner courses*
    - *Redefining Somali History*
    - *Religious Education*
  - *Economic/Development Aid:*
    - *Job Skills*
    - *Micro-loans*
  - *Gender:*
    - *Countering Female Radicalisation*
  - *Negotiation:*
    - *High Level Defections programme*
    - *Low-level Defector Rehabilitation Centres*

Lessons Identified:
Hard Power + Soft Power = Smart Power

- **Choosing 'the Face' of the campaign**
- Co-ordinate, co-ordinate, co-ordinate
- Soft Power leads
- Communicate, communicate communicate

FINAL THOUGHT

'Which do you choose,
The hard or soft option?'
THE PET SHOP BOYS, 1984

Stephen Harley
CT/Strat Comms Consultant,
Somalia Area Specialist

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

Developing National Counter-Terrorism Policy

by Susan Sim

In the immediate aftermath of the 9/11 attacks on the United States in 2001, almost all countries put together ministerial-level steering committees and task forces to rapidly review and implement national policy initiatives to prevent and respond to future terrorist attacks. They did not start from scratch; 184 countries had by then already experienced at least one domestic or international terrorist incident at home (Rand Database), and most had in place anti-terrorism arrangements to manage what they perceived to be the threat level facing their populations. With the 9/11 attacks, transnational terrorist groups like al-Qaeda became an "extreme threat to international security" and defending against terrorism was elevated into a top policy priority for many nations.

The attacks also brought international organisations into uncharted territory as they sought to coordinate and harmonise the various national responses. The United Nations adopted a far- reaching resolution, UNSCR 1373 (2001), requiring all member states to deny terrorists safe haven and financial support and to cooperate in bringing them to justice. Subsequent Security

Council resolutions urged states to take preventive measures against terrorist use of the Internet to recruit and incite terrorist acts (Smith, 2011). These resolutions, driven by the shock of a continuing wave of terrorist attacks around the world, sought to patch the gaps in the international counter-terrorist framework consisting previously of 16 international treaties addressing issues such as the hijacking of planes, the taking of hostages, the financing of terrorism, the marking of explosives, and the threat of nuclear terrorism.

Over time, states began publishing their national counter-terrorism strategies, which generally invoked some permutation of ***Prevent, Detect, Deny, Protect, Pursue, Prepare*** and ***Respond***, i.e.

Prevent (individuals from turning to terrorism),

Protect (citizens and infrastructure by reducing vulnerability to attack),

Pursue (investigate terrorists and disrupt support networks) and

Respond (manage and minimize the consequences of an attack).

The language used in such national strategies is so similar across the world that some analysts fear a "cut and paste mentality" among policymakers who merely recycle language to "describe policy measures without critical interrogation of their meaning, relevance, or utility" (Feve and Dewes, 2019). This criticism, however, overlooks the fact that the so-called 3PR matrix does indeed have the advantage of allowing a more systematic manner of analysing national counter-terrorism strategies. The European Union introduced it as a framework in 2005 as a means of collecting empirical data, allowing it to give guidelines, to stress that government policies should have clearly defined 'aims' so that it is a conscious choice to mobilize specific 'resources' to counter the terrorist threat (Meijer, 2012).

As best practices go, that is what national counterterrorism policies should aim to do: conveying a greater sense of urgency and purpose while reassuring the public that their government is doing everything possible to protect them against terrorism. Indeed, since the so-called Islamic State of Iraq and Syria (ISIS) turned the idea of a caliphate from aspirational to reality and incited followers everywhere to mount attacks using everyday tools such as cars and knifes, the mantra quietly adopted in many nations to prepare citizens has been: "Not if an attack takes place, but when".

Then again, counterterrorism policy measures are often a reflection of the domestic political process. Governments have to get buy-in from citizens and secure funds from lawmakers. While policy may be triggered by a terrorist event that creates a groundswell of public demand for immediate pre-emptive action, political pressures may sometimes mitigate against more evidence-based counter-terrorism policy, while in some countries national leaders may make political decisions citing emergency conditions.

For the purposes of this presentation, "best practice" will thus refer to an approach or technique or activity that has been successfully implemented in at least one country, and shown to be effective and/or efficient in achieving a desired result, and is transferable elsewhere. It will also bear in mind that while most governments agree that systemic programme evaluations are important, almost no one does them although some work is now being done to evaluate programmes for preventing and countering violent radicalisation and extremism (Hofman and Sutherland, 2018), and that even the best

counterterrorism strategy as it appears on paper cannot guarantee successful outcomes since there are a range of external factors at play (Feve and Dews, 2019).

Using case studies drawn from the EU and other countries, this presentation will draw out best practices in building national resilience to terrorist activity, including the involvement of multiple stakeholders in designing and implementing programmes and policy measures. The EU, for instance, conducted its first ever assessment of the national anti-terrorist arrangements of its member states through a peer evaluation beginning 2003. It focused on the national responsibilities at government ministry, security and intelligence service and law enforcement agency level; identified national good practices with a significance for all or most other member states as best practices and offered as recommendations to close security gaps and enhance existing capacities from an operational and practical perspective, with each state free to implement them according to its national legal and political framework.

Responding to evolving trends precipitated by ISIS – lone-actor terrorism, foreign fighters, use of social media by terrorists – the EU has since revised its counter-terrorism strategy and urged member states to implement a raft of measures to prevent radicalisation and recruitment of European citizens by terrorist organisations. Although adaptable and robust national security policies should also be able to pivot to deal with new challenges such as far-right ethno-nationalist driven extremism, the longer term terrorist threat, however, is to institutional and societal resilience, as many countries have come to realise. Indeed the theme for this year's UN High-level Conference on Counter-Terrorism is "Building Institutional and Social Resilience to Terrorism". This presentation will thus also examine how a small city state like Singapore has been building a national counter-terrorism programme "to sensitise, train and mobilise the community to play a part to prevent and deal with a terrorist attack". Called SG Secure, the programme is about convincing people that every individual must assume some self-responsibility for protection against risk, for good relations between communities, and that everyone, including the private sector, must do its part to shore up societal and national resilience.

b. Presentation

BEST PRACTICES IN COUNTER-TERRORISM

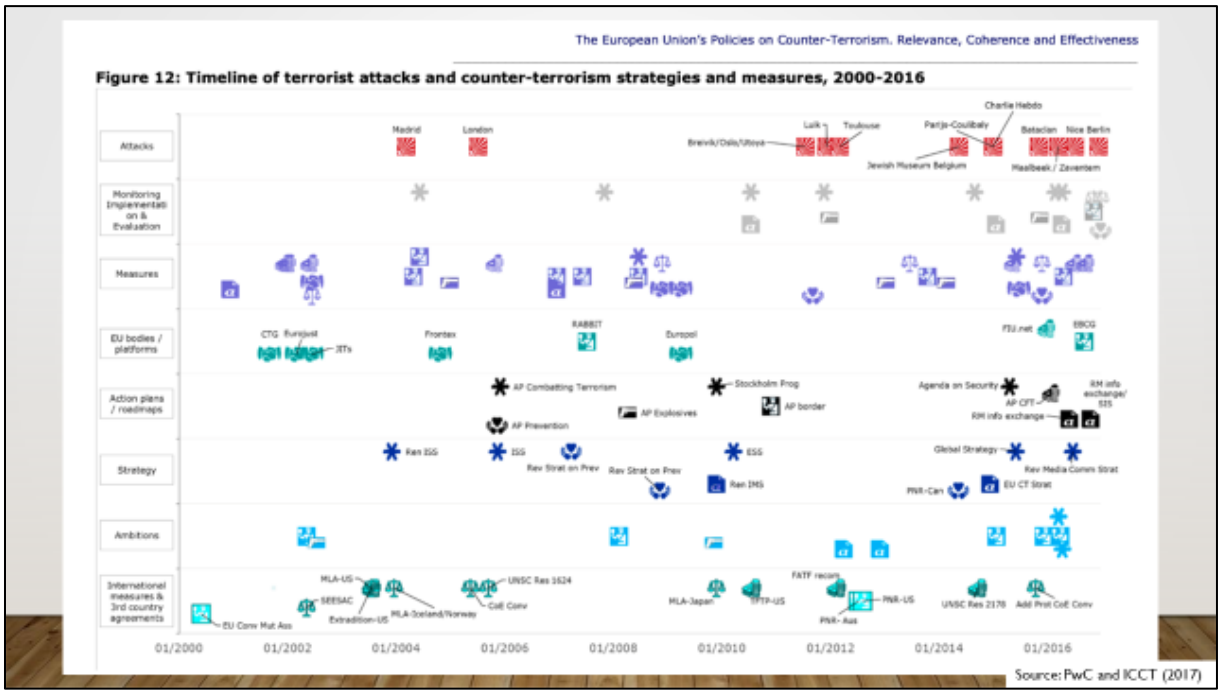
"Not if, but when"

Developing National Counter-Terrorism Policy in the Age of al-Qaeda and ISIS

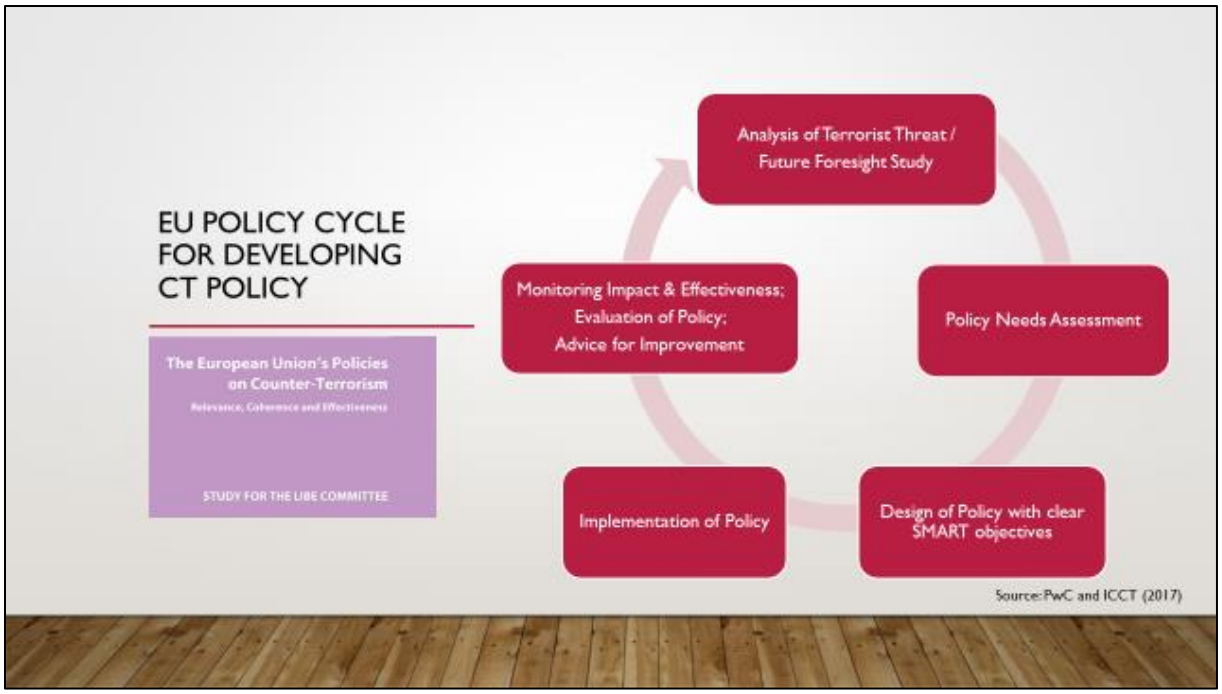
SUSAN SIM

Adjunct Senior Fellow, S Rajaratnam School For International Studies, Singapore

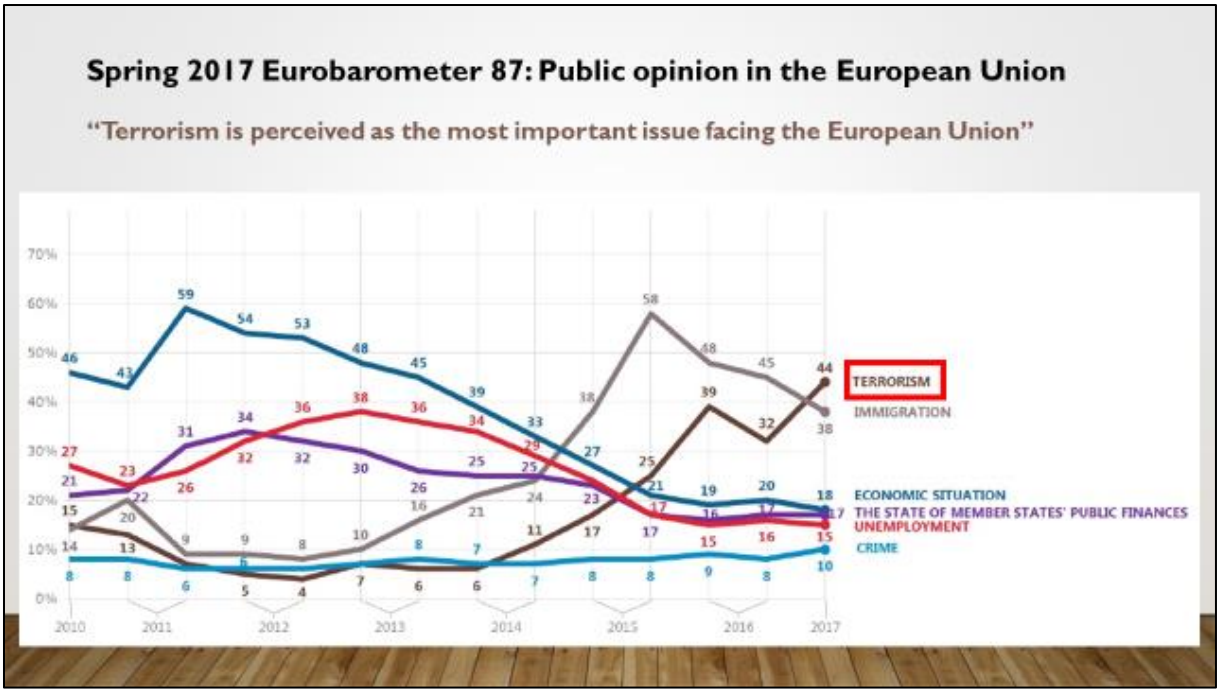
Vice-President For Asia, The Soufan Group




CT MORSE
Global Evaluation of the European Union Engagement on Counter-Terrorism
June 2010
The EU's counter-terrorism agenda has been to a large extent 'crisis-driven', and was heavily influenced by four major shock waves: (1) 9/11; (2) the Madrid and London bombings; (3) the Syrian civil war and rise of ISIS, the foreign (terrorist) fighters phenomenon, and the attacks on Charlie Hebdo, the Bataclan and Brussel/Zaventem; (4) the Nice and Berlin attacks and a series of small-scale attacks, featuring the rise of the lone actors and the weaponisation of ordinary life. Since these shocks were all related to Islamic terrorism, this has been the main EU counter-terrorism focus.


EU POLICY CYCLE FOR DEVELOPING CT POLICY
The European Union's Policies on Counter-Terrorism
Relevance, Coherence and Effectiveness
STUDY FOR THE LIBE COMMITTEE
Analysis of Terrorist Threat / Future Foresight Study
Policy Needs Assessment
Design of Policy with clear SMART objectives
Implementation of Policy
Monitoring Impact & Effectiveness; Evaluation of Policy; Advice for Improvement
Source: PwC and ICCT (2017)


DIRECTORATE-GENERAL FOR INTERNAL POLICIES
POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS
Constitutional Affairs
Justice, Freedom and Security
Gender Equality
Legal and Parliamentary Affairs
Petitions
The European Union's Policies on Counter-Terrorism
Relevance, Coherence and Effectiveness
STUDY FOR THE LIBE COMMITTEE
EN
"Governments, policy-makers, and politicians in most EU Member States feel the pressure of the population who call for adequate responses to these threats."


Spring 2017 Eurobarometer 87: Public opinion in the European Union
"Terrorism is perceived as the most important issue facing the European Union"
70%
60%
50%
40%
30%
20%
10%
0%
2010
2011
2012
2013
2014
2015
2016
2017
TERRORISM
IMMIGRATION
ECONOMIC SITUATION
THE STATE OF MEMBER STATES' PUBLIC FINANCES
UNEMPLOYMENT
CRIME

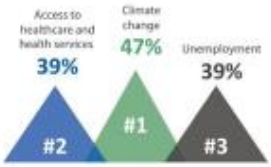
BIGGEST CHALLENGES FACED BY EUROPEAN CITIZENS

European Investment Bank Survey, September – October 2019

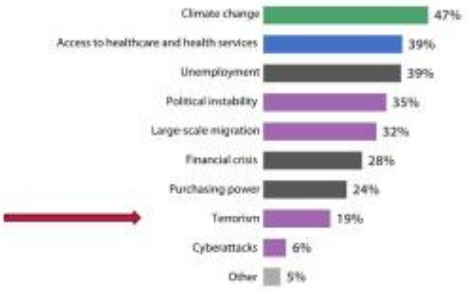
What are the three biggest challenges citizens in your country are currently facing?

European Union
28 088 respondents

Top 3 biggest challenges faced by EU citizens



All challenges



Spring 2020
Median across 14 countries surveyed

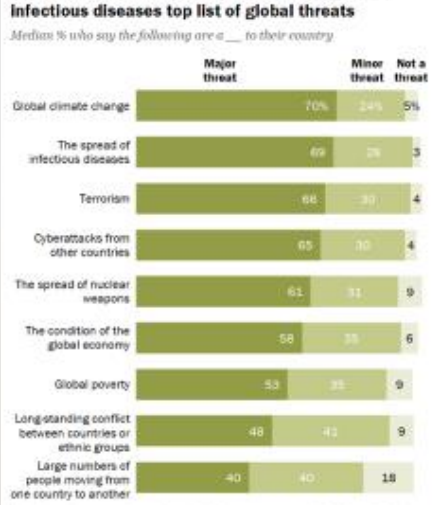
Belgium
Denmark
France
Germany
Italy
Netherlands
Spain
Sweden
United Kingdom

Canada
United States

Australia
Japan
South Korea

Across 14 countries polled, climate change and infectious diseases top list of global threats

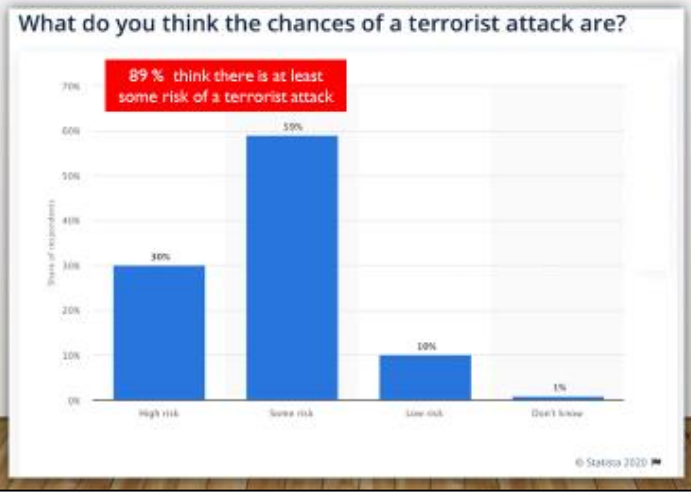
Median % who say the following are a ___ to their country



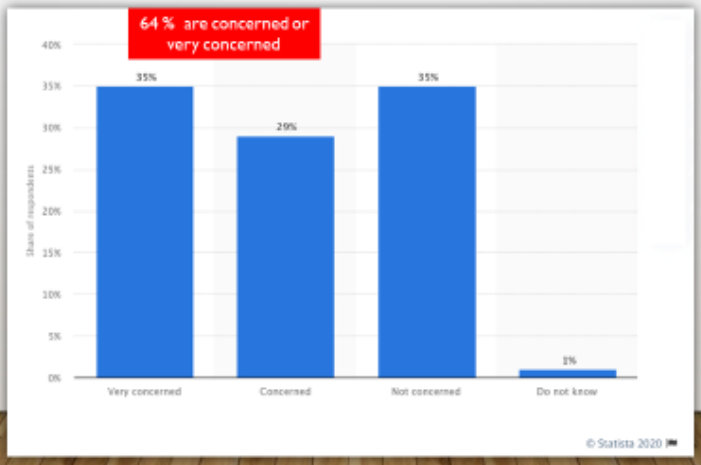
Note: Percentages are medians based on 14 countries surveyed. U.S., Canada, Belgium, Denmark, France, Germany, Italy, Netherlands, Spain, Sweden, UK, Australia, Japan and South Korea. Those who did not answer are not shown.
Source: Spring 2020 Global Attitudes Survey. Q13a-l.
"Despite Pandemic, Many Europeans Still See Climate Change as Greatest Threat to Their Countries"

PEW RESEARCH CENTER

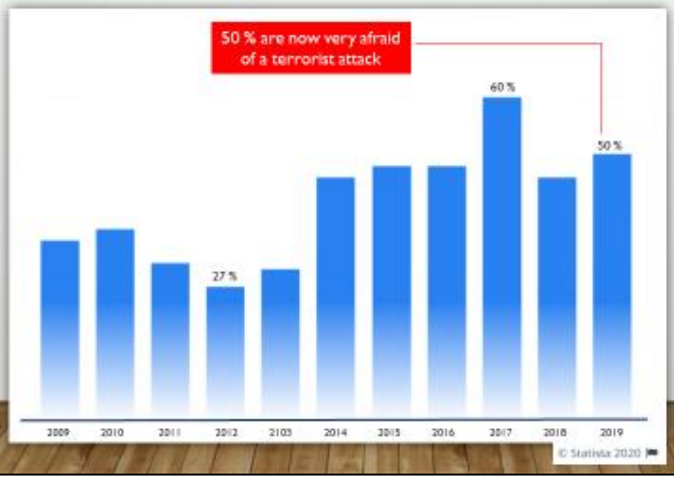
French public opinion on the possibility of a terrorist attack in **France** (October 2019)



How concerned are you about a terror attack occurring in **Norway** within the next five years (2020)



How afraid are Swedes of terrorism in **Sweden**? (2009-2019)



BASIC PREMISE OF NATIONAL COUNTER-TERRORISM POLICY-MAKING

- The public already fears it is a matter of **NOT IF** a terrorist attack happens, **BUT WHEN**
- National CT policy has to be about
  - preventing and mitigating an attack,
  - preparing the public to survive an attack and
  - the day after.
- And be seen to work

WHAT WORKS?

- **Best practice** refers to an approach or technique or activity or strategy
  - that has been successfully implemented in at least one country (i.e. field tested),
  - shown to be effective and/or efficient in achieving a desired result,
  - is far superior to other methods, and
  - is transferable elsewhere.
- What is best practice has to be **contextually mediated** – what is optimal for a specific society?
- **"Doing it right"**

NATIONAL COUNTER-TERRORISM STRATEGIES

- Most invoke some permutation of Prevent, Detect, Deny, Protect, Pursue, Prepare and Respond
- "Cut and paste mentality" among policymakers?

NATIONAL COUNTER-TERRORISM STRATEGIES

Singapore, 2004


The Fight Against Terror

SINGAPORE'S NATIONAL SECURITY STRATEGY

To deal effectively with the threat of transnational terrorism, Singapore has deployed a robust defence strategy built upon a well-organised network of government agencies, often working in partnership with commercial and private parties. This integrated, layered approach is structured around the Prevention, Protection and Response domains. By an effective combination of various measures, we can be confident of meeting major terror threats.

PREVENTION

Prevention represents the most critical layer of defence against terrorism. A successful strategy saves lives, preserves property, and avoids potential disruption to our economy and society. It entails an integration of effective diplomacy, good intelligence work, and strong border controls. Where we can, we must ensure that terror threats are eliminated before they materialise.

An Integrated Approach to National Security

THE EU'S 3PR MATRIX

European Union, 2005


THE EUROPEAN UNION
COUNTER-TERRORISM STRATEGY

The EU 's Counter-Terrorism Strategy covers four strands of work, fitting under its strategic commitment:

STRATEGIC COMMITMENT

To combat terrorism globally while respecting human rights, and make Europe safer, allowing its citizens to live in an area of freedom, security and justice

PREVENT	PROTECT	PURSUE	RESPOND
To prevent people turning to terrorism by tackling the factors or root causes which can lead to radicalisation and recruitment, in Europe and internationally	To protect citizens and infrastructure and reduce our vulnerability to attack, including through improved security of borders, transport and critical infrastructure	To pursue and investigate terrorists across our borders and globally; to impede planning, travel, and communications; to disrupt support networks; to cut off funding and access to attack materials, and bring terrorists to justice	To prepare ourselves, in the spirit of solidarity, to manage and minimise the consequences of a terrorist attack, by improving capabilities to deal with: the aftermath; the co-ordination of the response; and the the needs of victims

CONTEST

The United Kingdom's Strategy for Countering Terrorism

June 2018

NATIONAL COUNTER-TERRORISM STRATEGIES

United Kingdom, 2018

Fig. 2.1: CONTEST's Risk Reduction Model

Prevent	Pursue	Protect	Prepare
Safeguard people from becoming terrorists or supporting terrorism	Stop terrorist attacks happening in the UK and overseas	Stregthen our protection against a terrorist attack in the UK or overseas	Mitigate the impact of a terrorist incidents if it occurs

Primary outcome

Reduce intent	Reduce capability	Reduce vulnerability	Reduce impact

Address strategic factors

Extremism
Conflict and instability
Developments in technology

Overall effect

Reduce risk

Building Resilience Against Terrorism

CANADA'S COUNTER-TERRORISM STRATEGY

NATIONAL COUNTER-TERRORISM STRATEGIES

Canada, 2013

The Strategy

Prevent, Detect, Deny and Respond

This chapter describes how the Government is seeking to achieve the aim of countering domestic and international terrorism in order to protect Canada, Canadians and Canadian interests.

Building Resilience Against Terrorism has four mutually reinforcing elements:
Prevent individuals from engaging in terrorism;
Detect the activities of individuals and organizations who may pose a terrorist threat;
Deny terrorists the means and opportunity to carry out their activities; and
Respond proportionately, rapidly and in an organized manner to terrorist activities and mitigate their effects.

All four elements contribute to building a resilient Canada. The *Prevent* element fosters a Canada that is resistant to violent extremism. The *Detect* and *Deny* elements ensure Canada is able to identify terrorist activities early, and that it is a difficult target for would-be terrorists. The *Respond* element engenders a resilient society able to bounce back quickly when terrorist incidents do occur.

FRAMEWORK OF CANADA'S COUNTER-TERRORISM STRATEGY

AIM

To counter domestic and international terrorism in order to protect Canada, Canadians and Canadian interests.

PRINCIPLES

1. Building resilience
2. Terrorism is a crime and will be prosecuted
3. Adherence to the rule of law
4. Cooperation and partnerships
5. Proportionate and measured response
6. A flexible and forward-looking approach

BASIC PREMISE OF NATIONAL COUNTER-TERRORISM POLICY-MAKING

- The public already fears it is not a matter of IF a terrorist attack happens, but WHEN
- National CT policy has to be about
  - preventing and mitigating an attack,
  - preparing the public to survive an attack and
  - the day after.
- And be seen to work
- Effective CT policy influences
  - public confidence in government efforts to deal with terrorism and
  - the sense of insecurity from attacks

EU PEER EVALUATION OF NATIONAL CT ARRANGEMENTS OF MEMBER STATES

2003-2005

12. National good practices with a significance for all or most other Member States were identified as best practices and dealt with as recommendations in the interim report[8] and in this final report. They either reflect already existing situations in one or more Member States or have been developed on the basis of the experiences of the evaluation. This report aims to draw out of those evaluations those elements of good practice which might usefully be applied.

13. In general terms, recommendations have been identified from an operational and practical perspective. It is for each Member State to implement recommendations with regard to its national legal and political framework. Recommendations are to be considered in the national context taking into account political implications. Some recommendations aimed at closing security gaps and enhancing the existing counter terrorism capacity may require constitutional, legal or structural changes to current national arrangements.

Revised EU Strategy for Combating Radicalisation and Recruitment to Terrorism

2014

Key points:

- A balanced approach between security-related measures and efforts to tackle those factors that may create an environment conductive to radicalisation and recruitment to terrorism.
- Not just whole of government, but whole of society, and at all levels - local, regional, national, European and international level.

Good practices recommended include:

- Enhance government communications to also communicate what we stand for, our own norms and values: international law, human rights and the rule of law.
- Challenge the terrorist narrative, especially online
- Support and amplify counter-narratives emanating from those with local influence
- Train and equip first line practitioners like teachers, social and health care workers, religious leaders, community police officers, and prison and probation staff to provide them with a better understanding of radicalisation and recruitment to terrorism, and skills to discuss related issues
- Support individuals and civil society to build resilience
- Support disengagement initiatives
- Support further research into the trends and challenges of radicalisation and recruitment

BEST PRACTICE:

CLEAR COMMUNICATION

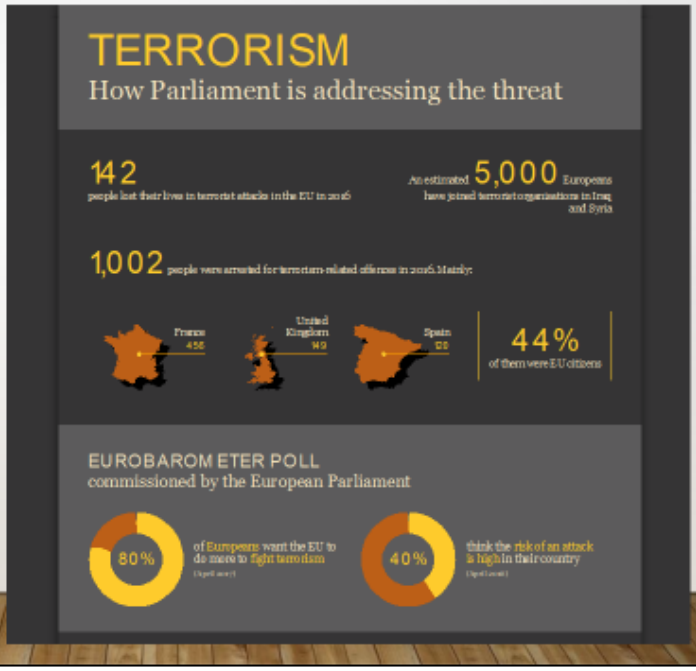
Provide threat assessment

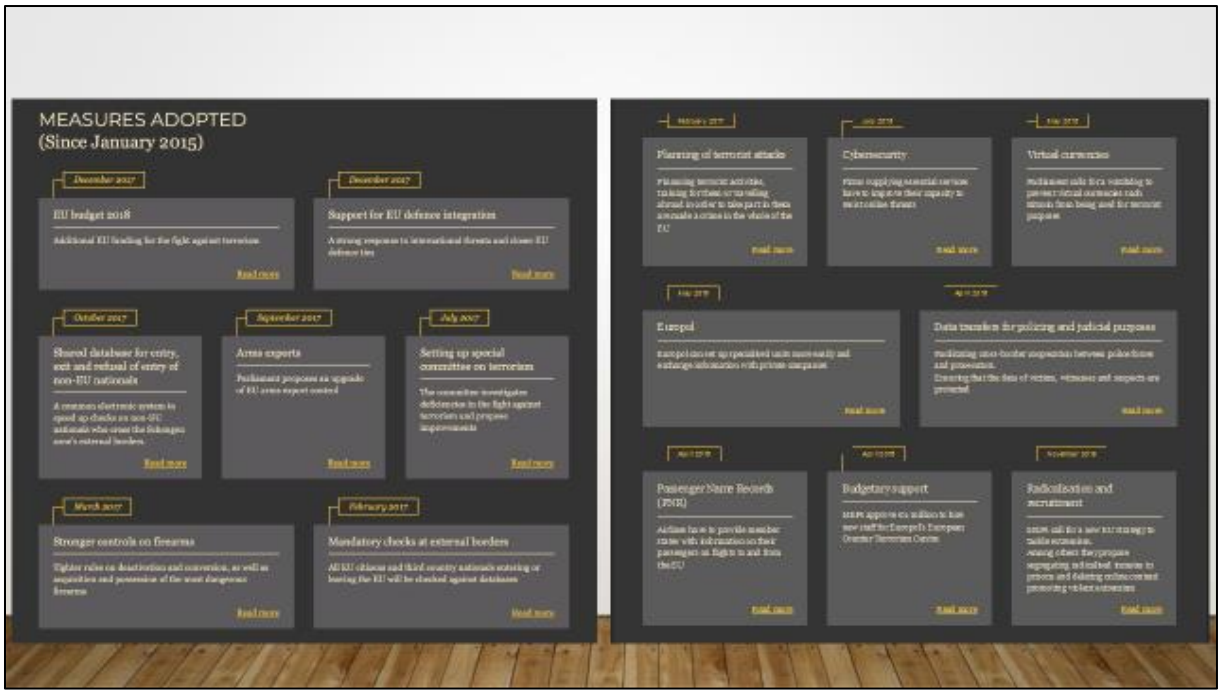
Explain measures

Stress societal values and norms

Make information accessible

https://www.europarl.europa.eu/infographic/europe-and-terrorism/index_en.html



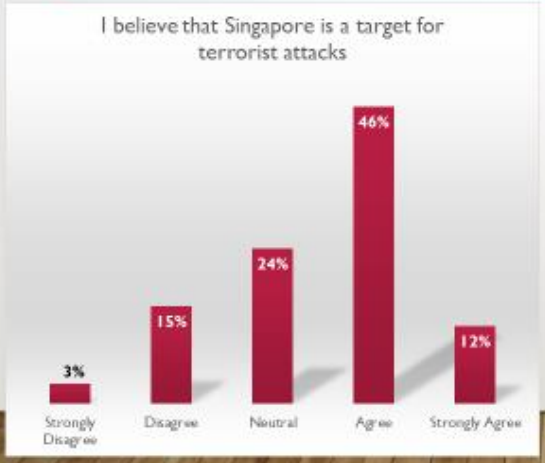


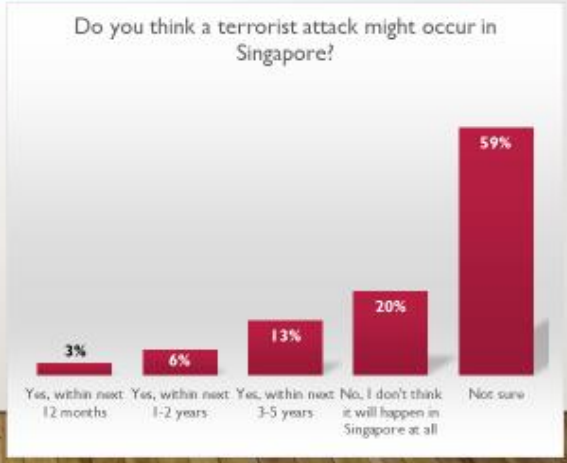
DOESN'T REMINDING PEOPLE OF THREATS MAGNIFY THEIR SENSE OF DANGER?

- Insecurity results from the sense that people cannot control their exposure to danger (Rothbaum, Weisz, and Snyder 1982; Witte 1992).
- Efficacious counterterrorism alleviates this problem by demonstrating that **governments are in control and can check the threat of violence**.
- Experiments have demonstrated that information about effective counterterrorism can reassure people about their security when the threat of terrorism is salient. People exposed to information about effective counterterrorism express greater confidence in the ability of governments to control terrorism and express less concern about the odds of future attacks (Hoffman, 2017).

SINGAPORE PUBLIC PERCEPTION SURVEY, 2018

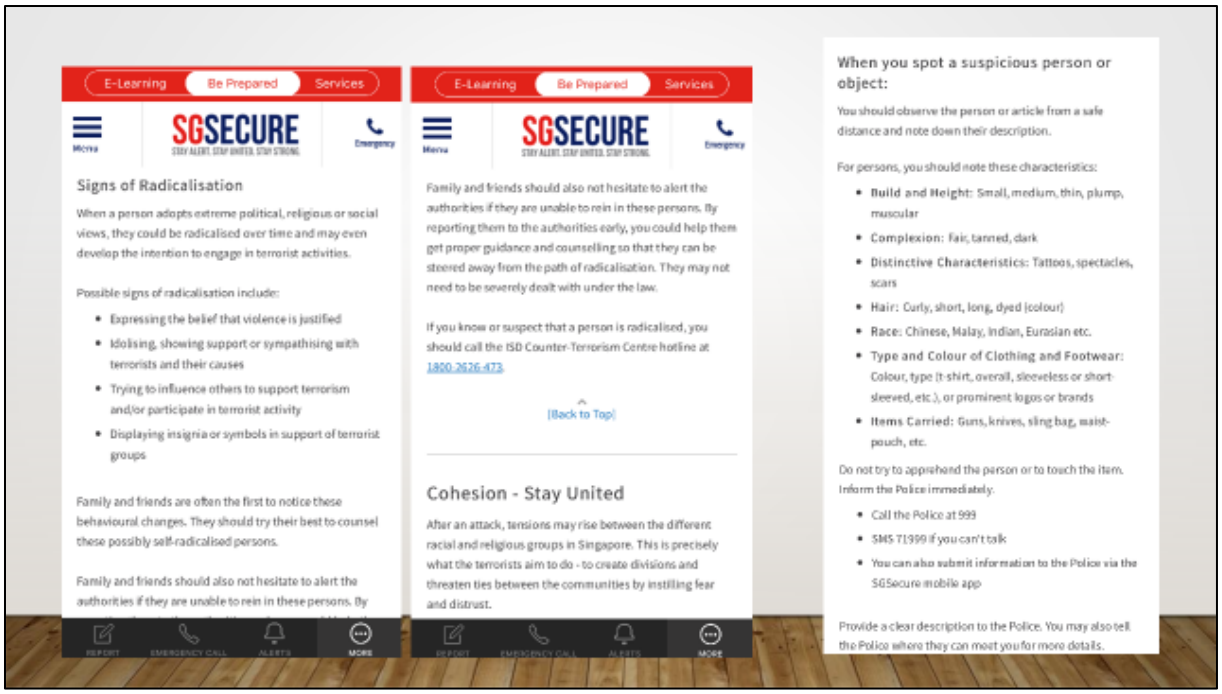
60% believe Singapore is a terrorist target but only 20% believe an attack is imminent



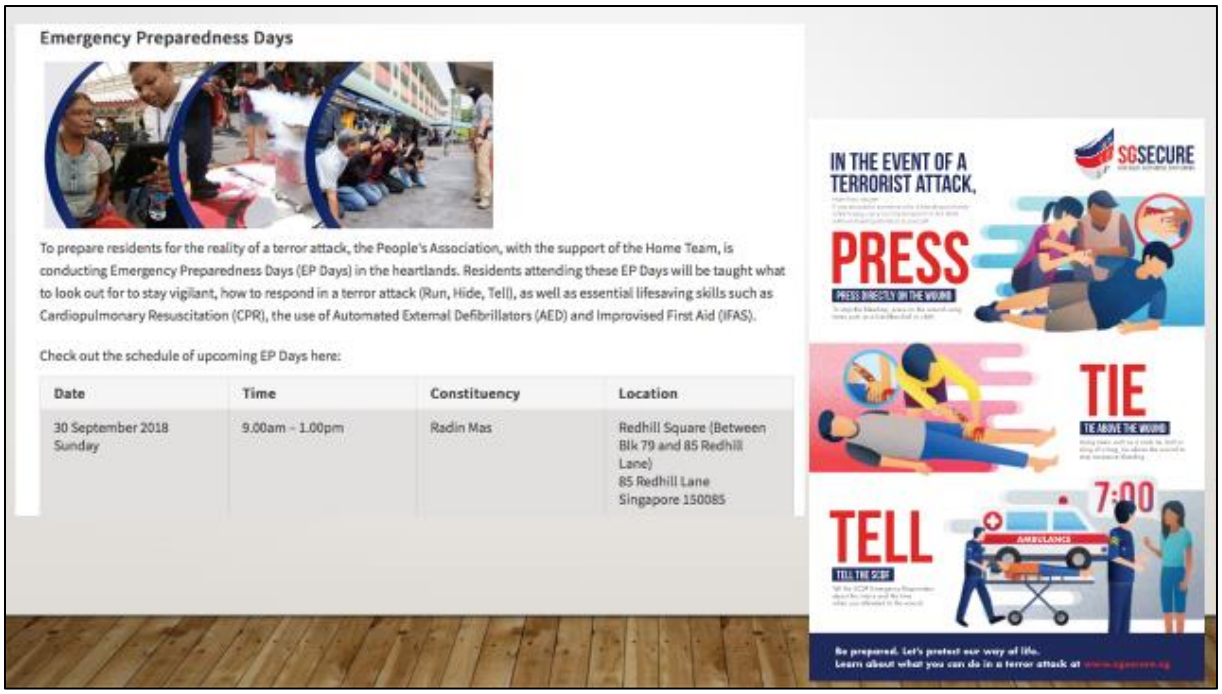


BUILDING A NATIONAL COUNTERTERRORISM MOVEMENT IN SINGAPORE

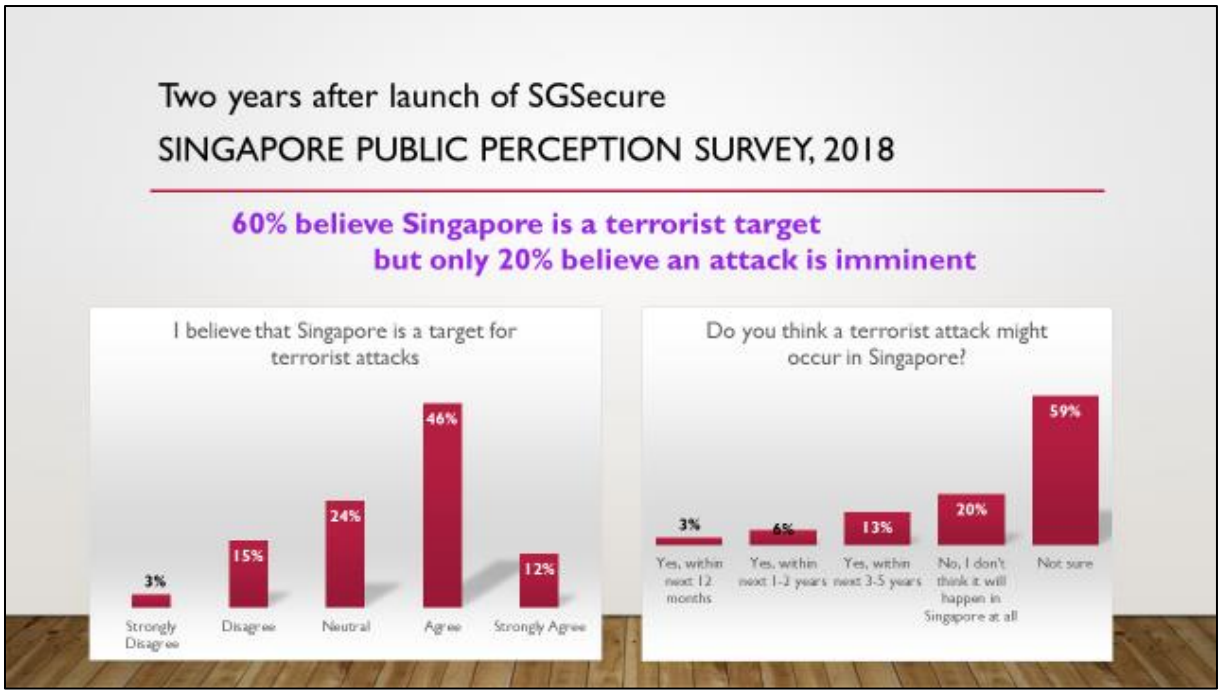

SGSECURE
RECEIVE ALERTS
Receive customised alerts on emergency incidents occuring at your chosen locations
MAKE REPORTS
Report incidents and suspicious behaviours/activities in 4 simple steps:
Take A Photo
Describe Incident
State Location
Submit Report
MAKE EMERGENCY CALLS
Make 999 calls or alert the Police via SMS
GET READY
Equip yourself with knowledge and skills through the e-learning module
BE PART OF THE SGSECURE MOVEMENT - DOWNLOAD THE SGSECURE APP TODAY!
Google Play
App Store


E-Learning
Be Prepared
Services
SGSECURE
Menu
Emergency
Signs of Radicalisation
When a person adopts extreme political, religious or social views, they could be radicalised over time and may even develop the intention to engage in terrorist activities.
Possible signs of radicalisation include:
Expressing the belief that violence is justified
Idolising, showing support or sympathising with terrorists and their causes
Trying to influence others to support terrorism and/or participate in terrorist activity
Displaying insignia or symbols in support of terrorist groups
Family and friends are often the first to notice these behavioural changes. They should try their best to counsel these possibly self-radicalised persons.
Family and friends should also not hesitate to alert the authorities if they are unable to rein in these persons. By
REPORT
EMERGENCY CALL
ALERTS
MORE
E-Learning
Be Prepared
Services
SGSECURE
Menu
Emergency
Family and friends should also not hesitate to alert the authorities if they are unable to rein in these persons. By reporting them to the authorities early, you could help them get proper guidance and counselling so that they can be steered away from the path of radicalisation. They may not need to be severely dealt with under the law.
If you know or suspect that a person is radicalised, you should call the ISD Counter-Terrorism Centre hotline at 1800 2626 473.
[Back to Top]
Cohesion - Stay United
After an attack, tensions may rise between the different racial and religious groups in Singapore. This is precisely what the terrorists aim to do - to create divisions and threaten ties between the communities by instilling fear and distrust.
REPORT
EMERGENCY CALL
ALERTS
MORE
When you spot a suspicious person or object:
You should observe the person or article from a safe distance and note down their description.
For persons, you should note these characteristics:
Build and Height: Small, medium, thin, plump, muscular
Complexion: Fair, tanned, dark
Distinctive Characteristics: Tattoos, spectacles, scars
Hair: Curly, short, long, dyed (colour)
Race: Chinese, Malay, Indian, Eurasian etc.
Type and Colour of Clothing and Footwear: Colour, type (t-shirt, overall, sleeveless or short sleeved, etc.), or prominent logos or brands
Items Carried: Guns, knives, sling bag, waist-pouch, etc.
Do not try to apprehend the person or to touch the item. Inform the Police immediately.
Call the Police at 999
SMS 71999 if you can't talk
You can also submit information to the Police via the SGSecure mobile app
Provide a clear description to the Police. You may also tell the Police where they can meet you for more details.


PREPARE A CONTINGENCY RESPONSE PLAN
PLANNING GUIDELINES FOR SPECIFIC TERROR ATTACK SCENARIOS
i. Armed Attacker Incident
ii. Suspicious Item Found
iii. Explosion
iv. Suspected Chemical Agent Release
DETER
DETECT
DELAY
DENY
OPERATIONS MEASURES
TECHNOLOGY MEASURES
PHYSICAL MEASURES


Emergency Preparedness Days
To prepare residents for the reality of a terror attack, the People's Association, with the support of the Home Team, is conducting Emergency Preparedness Days (EP Days) in the heartlands. Residents attending these EP Days will be taught what to look out for to stay vigilant, how to respond in a terror attack (Run, Hide, Tell), as well as essential lifesaving skills such as Cardiopulmonary Resuscitation (CPR), the use of Automated External Defibrillators (AED) and Improvised First Aid (IFAS).
Check out the schedule of upcoming EP Days here:
Date
Time
Constituency
Location
30 September 2018 Sunday
9.00am – 1.00pm
Radin Mas
Redhill Square (Between Blk 79 and 85 Redhill Lane)
85 Redhill Lane
Singapore 150085
IN THE EVENT OF A TERRORIST ATTACK,
SGSECURE
PRESS
PRESS DIRECTLY ON THE WOUND
TIE
TIE ABOVE THE WOUND
7:00
TELL
TELL THE SCDF
AMBULANCE
Be prepared. Let's protect our way of life.
Learn about what you can do in a terror attack at


SGSECURE
AFTER A TERRORIST ATTACK,
KEEP CALM
STAY INFORMED
BREAKING
DO NOT SPREAD RUMOURS
DO NOT SPECULATE
CARE FOR OTHERS
HELP OTHERS RETURN TO DAILY ACTIVITIES


Two years after launch of SGSecure
SINGAPORE PUBLIC PERCEPTION SURVEY, 2018
60% believe Singapore is a terrorist target
but only 20% believe an attack is imminent
I believe that Singapore is a target for terrorist attacks
3%
15%
24%
46%
12%
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree
Do you think a terrorist attack might occur in Singapore?
3%
6%
13%
20%
59%
Yes, within next 12 months
Yes, within next 1-2 years
Yes, within next 3-5 years
No, I don't think it will happen in Singapore at all
Not sure

SGSECURE Public Perception Survey 2018

97 %	agreed that all Singaporeans have a role to play in preventing and dealing with a terror attack
75 %	said they were generally alert and keep a lookout for suspicious behaviours or packages when in a public place
89 %	would also contact the relevant authorities, should they spot suspicious behaviour in public places
80 %	think they know how to respond at a scene of an explosion - that they must report, take cover, protect themselves. That's an increase from 50 % in 2015.
96 %	believed that all Singaporeans will stand united regardless of race or religion should an attack happen in Singapore
76 %	were willing to help other Singaporeans affected by a terrorist attack here

BEST PRACTICE:

CHALLENGING TERRORIST NARRATIVES

Role of Religious Leaders and Groups

- After arrest of AQ-linked terrorist network in Singapore in December 2001, a group of Islamic clerics came together to form the **Religious Rehabilitation Group (RRG)**
- They provide religious counselling to detainees to "unlock" their bai'ah (pledge) to amir (group leader) and address the beliefs that allow them to justify killing
  - Volunteer clerics vetted by RRG leaders and security screened;
  - Act in personal capacity, not for any group
  - Not paid by government, but given counselling skills
  - Now a crucial community partner in state's counter-radicalisation efforts, which also includes psychological counselling for terrorism suspects
- Another volunteer group known as the **Aftercare Group** looks after families and children


BEST PRACTICE:
ENGAGING THE COMMUNITY
Building societal resilience
"I would highlight as most important - community engagement - the quality of which determines not just societal support for state security action but makes the whole of society a latent embedded resource for early warning & intelligence as well as a staple factor for social resilience in adverse consequence management."
"The challenge is that in the age of al-Qaeda and ISIS, community engagement involves a dynamic composite of both Muslim and non-Muslim constituencies and their elites. Given legacy issues, it is not easy to do but needs to be done; perhaps easier in some societies than others."
Retired national security coordination leader in Singapore

Gender, Terrorism and Counter-Terrorism

by Dr. Zeynep Sütalan

Gender aspect of terrorism and counterterrorism (CT) are two of the least addressed areas in policy-making world if not in academia. The need to further address this issue stems from the fact that neglecting the different roles women play in terrorism creates security gaps due to the deficiencies in the terrorist threat assessment, and thus insufficient CT and countering violent extremism (CVE) programming. Therefore, in addition to and other than being victims of terrorism, women can consciously and deliberately decide to join terrorist organizations and can become supporters, facilitators, recruiters, perpetrators and propagandists of terrorism. Together with recognizing the agential power of women in terrorism, it is essential to admit that increasing and meaningful inclusion of women both in the design and implementation of CT and CVE programming is key to success. Recognizing women's agency in terrorism and counterterrorism is operationally effective. Equally important is the fact that, it is an international legal responsibility in line with the Women, Peace and Security (WPS) agenda of the United Nations (UN) and its link to the CT and CVE efforts constructed with the relevant UN Security Council Resolutions.[1]

The lack of gender-sensitive approach generally in security and particularly in the field of counterterrorism does not mean that there are not any substantial efforts to overcome the predominant gender-blindness. Though not immune from deficiencies, there are certain practices that we can identify as best practices in the field of CT and CVE. Therefore, in regard to the best practices in addressing the gender aspect of counterterrorism, this article utilizes three case studies: mother schools, female engagement teams and gender advisors. The idea is to highlight different roles women can play in regard to counterterrorism. With these case studies, three roles women can play in CT and CVE as preventers, counter-terrorists and change-makers are scrutinized in relation to three different levels of analysis which are local level, operational level and cultural-institutional level.

[1] United Nations Security Council Resolution (UNSCR) 1325 (2000) on Women, Peace and Security (WPS) that the international community admitted the differential impact of armed conflict on women, girls and children, and recognized the need to include women in building and maintaining peace and security. With UNSCR 2242 (2015) WPS agenda joined together with the CT and countering violent extremism (CVE) work.

a) Women as Preventers: Mother Schools

It is fair to evaluate women's role as preventers as 'the first line of defence'. Motherhood may be referred as the first recognized role of a women that can contribute to CT, more precisely CVE that leads to terrorism. In line with mothers' roles in the household and ability to recognize changes in the family members - for instance, changing behaviours of their children like leaning to violent manifestations, becoming more short-tempered and anxious, etc. Therefore, women as mothers have a unique potential to contribute in building resilience in the community.[2] According to Schlaffer "[…] they *(mothers of terrorists)* already speak the language of security. After many of these conversations with mothers across the globe, I realized that they are on the forefront of a new security paradigm. They need to be the building blocks for a bottom-up security approach."[3]

The model was developed in 2008 by the Women Without Borders and Sisters Against Violent Extremism (SAVE). Therefore, it is a civil society initiative, the value of which has been recognized widely by the international community. The pilot programming took place in India, Pakistan, Tajikistan, Indonesia, Nigeria and Zanzibar. The project was based on the assumption that the women in line with their innate maternal instinct and ability was to identify radicalization and willing to and able to fight against it. "The central components of the Mother Schools curriculum are building confidence and self-esteem, increasing knowledge and reflection of parent-child dynamics, and delivering specific training in countering radicalization."[4] In line with the increasing challenge of the foreign terrorist fighters, the program is being adopted to Europe, particularly in Austria, Belgium, Germany, United Kingdom, and Macedonia.

Despite the benefits, the assumption that the model is based upon or the similar assumptions in many different CVE contexts, criticized for overestimating women's role as primary influencers in their societies or preventers of radicalization. Though limited

[2] Edit Schlaffer and Ulrich Kropiunigg, "A New Security Architecture: Mothers Included!", Naureen Chowdhry Fink, Sara Zeiger, Rafia Bhulai (ed.), *A Man's World? Exploring The Roles of Women in Countering Terrorism and Violent Extremism*, (Hedayah and The Global Center on Cooperative Security, 2016), pp.54-75.

[3] Edit Schlaffer, "Mothers, the much needed, but missing ally for counterterrorism", 30.10.2016, https://en.unesco.org/news/edit-schlaffer-mothers-much-needed-missing-ally-counterterrorism

[4] Schlaffer and Kropiunigg, "A New Security Architecture", p.63.

in number comparative studies have revealed that the patriarchal structures display different characteristics in different contexts and thus differing roles for women. Therefore, "context matters" has to be born in mind. Besides, the possibility that the mothers of the (potential) terrorists may be supporters of terrorism or they themselves might be radicalizers or recruiters should always be included in CVE programming.

b) Women as Counter-terrorists: Female Engagement Teams

The women-focused strategy of Female Engagement Teams (FETs) evolved out of necessity for the US Marine Corps, first in Iraq then in Afghanistan, to search local women for hidden explosives and weapons. Later their roles as female operatives for body search was extended to gather intelligence and information via engaging with the women in the society. In order to get a chance to engage with women and develop friendship, FETs are tasked to provide mobile medical services for women and children in rural areas.[5] However, it should be noted that seeing the women in the targeted population as a 'source of intel' holds the risk of endangering the security of these women.

What necessitates to be underlined in regard to including women in the CT campaign as a female counterterrorist or a potential female heart to be won in the targeted population is all about 'operational effectiveness'. This is not about realizing feminist agenda or WPS work, empowering women and women's rights. The primary motivation behind was achieving force protection. In line with the ongoing presence of FETs in Afghanistan, there is a tendency to link the strategy of FETs with the WPS agenda in terms of increasing women's participation in conflict prevention, but as put forward by Laastad Dyvik, "FETs should not be read as a 'feminist awakening' within the 'soldier scholar' vanguard of counterinsurgency theory."[6]

The experience of FETs in Afghanistan has displayed that female soldiers have a deescalating effect since they are accepted by the Afghan men and women in their contact with women in the practice of body and house search. Female soldiers also enabled the access to population not only via women to women contact, but also via

[5] Keally McBride and Annick T. R. Wibben, "The Gendering of Counterinsurgency in Afghanistan", *Humanity*, Summer 2012, pp.199-215.

[6] Synne Laastad Dyvik, "Women as 'Practitioners' and 'Targets': Gender and Counterinsurgency in Afghanistan", *International Feminist Journal of Politics*, 2014, vol. 16, no.3, p.422.

being respected for being soldiers and being women. Their being viewed as 'third gender' enabled Afghan men to approach them as well. These advantages in terms of positive engagement with men and women in local population has served for intelligence gathering and thus force protection, but could also be utilized for more strategic purposes like increasing women recruitment into local security forces.[7]

FETs were criticized in terms of bartering operational effectiveness over advancing women's rights reflecting a tension between pragmatism and idealism. It also holds the risk of intrumentalising women and WPS for operational needs and requirements such as force multiplication as long as it is posited as a practice of meeting the requirements of the WPS agenda.

c) Women as Change-makers: Gender Advisors

One of NATO's fundamental efforts for implementing the WPS agenda turns out to be the Gender Advisors appointed to NATO headquarters and operations. Gender Advisors served the purpose of protecting women and women's rights in armed conflicts, guarantee women's involvement in in peace and security and to achieve gender equality in military. Based on the summaries of the national reports, it was identified that there are 697 Gender Advisors in national armed forces of NATO members.[8]

According to the Bi-Strategic Command Directive 40-1, which was adopted in 2009 and revised twice in 2012 and 2017, Gender Advisor's role is defined as providing advice on the implementation of the UNSCR 1325 and related resolutions "and the integration of gender perspective including, but not limited to, operations/missions, crisis/conflict analysis, concepts, doctrine, procedures and education and training"[9]. Within this framework, Gender Focal Points are created to support and facilitate the role

[7] Sippi Azarbaijani-Moghaddam, "Seeking out Their Afghan Sisters: Female Engagement Teams in Afghanistan", CMI Working Paper (Bergen:CHR Michelsen Institute, 2014).

[8] Although these numbers inform us about the situation, it is not a reflecting the full picture since not all NATO nations or partner nations are reporting. It can be said that there is a decrease in the number of nations reporting since the year 2016. Summary of the National Reports of NATO member and Partner Nations to the NATO Committee of Gender Perspectives, 2018, 65, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/7/pdf/200713-2018-Summary-NR-to-NCGP.pdf (Reached on 1 October 2020.)

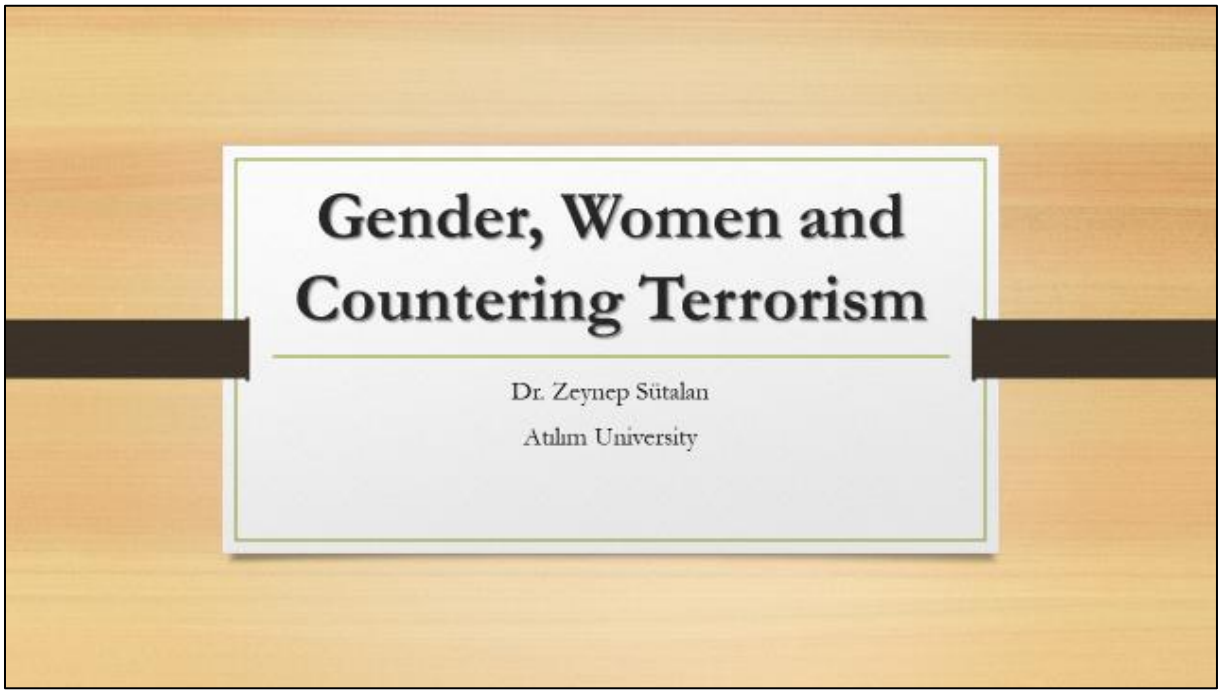
[9] Bi-Strategic Command Directive 040-001 (Public Version): Integrating UNSCR 1325 and gender Perspective into NATO Command Structure, 17 October 2017. https://www.act.nato.int/images/stories/structure/genderadvisor/nu0761.pdf

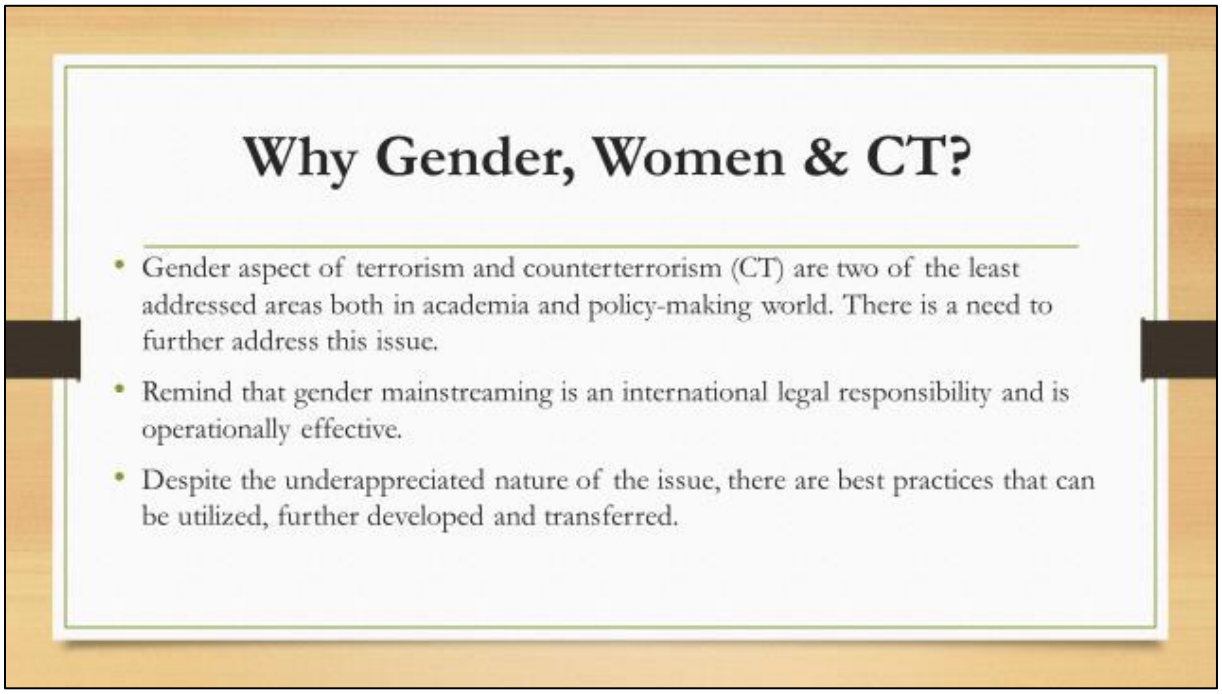
of Gender Advisors in staff functions. Since NATO aims at integrating gender perspective in planning, operations, missions, education and training as well as exercise and evaluation; and gender mainstreaming in all NATO policies and programmes in all areas and at all levels, the post of Gender Advisor has a critical role in the institutionalization of these efforts. However, despite the acknowledgement of the potential of Gender Advisors in terms of regendering military and society, there are several challenges they face, one of which is ironically the resistance from inside (the military) making their jobs twice harder for embedding gender diversity in the military. They do still suffer from lack of clarification of mandates, being burdened by additional responsibilities, difficulties in establishing their positions in the chain of command, insufficient pre-deployment training and lack of resources.

The research done by Megan Bastick and Claire Duncanson about the experiences of Gender Advisors in NATO and partner militaries based on the reflections of 21 Military Gender Advisors over a seven-year time period provides us with critical insight about the issue.[10] As they highlight: "[…] Military Gender Advisors can be agents of institutional change, given at least basic institutional support. They can, as they reported to us, change mindsets on an individual level, initiating conversations about equality and discrimination, challenging colleagues as to their attitudes."[11] Change in established gendered institutions with hyper-masculinity like military cannot happen overnight. Therefore, even 'small wins' and 'incremental changes' necessitates recognition and further support.

[10] Megan Bastick and Claire Duncanson, "Agents of Change? Gender Advisors in NATO Militaries", *International Peacekeeping*, 25:4, 554-577.
[11] Ibid, 573.

c. Presentation





Women, Peace and Security (WPS) & Countering Terrorism (CT)

- **UNSCR 1325 (2000)**
  - Women, girls and children are **affected** from armed **conflicts in a different way** (ex: being exposed to gender-based violence)
  - Women should be
    - **protected** from gender-based violence
    - **empowered** to prevent conflicts
    - **provided with equal role** in peace and security building

Women Peace and Security (WPS) and Countering Terrorism (CT)

- **UNSCR 2242 (2015)**
  - joined the WPS agenda together with the CT and P/CVE
- UNSC, UN CTC and CTED underline that gender sensitive approach to CT and CVE necessitates focus on:
  - "(i) women and girls as victims of terrorism,
  - (ii) women as perpetrators, facilitators, and supporters of terrorism, {agents of terrorism }
  - (iii) women as agents in preventing and countering terrorism and violent extremism,
  - (iv) the differential impact of counter-terrorism strategies on women and women's rights." (See https://www.un.org/sc/ctc/focus-areas/gender/).

Best Practices

Gender-sensitive Approach to Counter-terrorism

- **Women as Preventers: Mother Schools**
- **Women as Counter-terrorists: Female Engagement Teams (FETs)**
- **Women as Cultural Change-makers: Gender Advisors**

Mother Schools

- Civil society initiative
- Developed in 2008 by the Women Without Borders and Sisters Against Violent Extremism (SAVE)
- The project was based on the assumption that the women in line with their innate maternal instinct and ability was to identify radicalization and willing to and able to fight against it.
  - Background: Study on "Can Mothers Challenge Extremism?" (mothers living in Northern Ireland, Israel, Palestine, Egypt and Pakistan)
- Pilot programming took place in India, Pakistan, Tajikistan, Indonesia, Nigeria and Zanzibar.
- The curriculum is implemented through trusted community partners, and the modules in the curriculum are continually monitored and evaluated through weekly Skype sessions with the Women without Borders team.

Mother Schools

- These schools are viewed as the starting point for building resilience in these families and communities.
- **Identifying early warning signs of radicalization.**
  - **Endowing women with necessary skills** and information to recognize and react to the signs of radicalization and where to apply to.
- The model is being adopted to Europe (Austria, Belgium, England, Germany and Macedonia)- FTF Challenge

Are women primary "influencers" in their societies?

- **Criticisms**
  - Women's role as primary influencers and preventers of radicalization is overestimated.
  - Contextualizing women's role in their societies is essential.
- **Recommendation**
  - The possibility that the mothers of the (potential) terrorists may be supporters of terrorism or they themselves might be radicalizers or recruiters should always be included in CVE programming.

Women as Counter-terrorists
Female Engagement Teams (FETs)

- FETs evolved out of necessity for the US Marine Corps, first in Iraq then in Afghanistan
  - to search local women for hidden explosives and weapons
    - to train local forces on searching techniques
  - gather intelligence and information via engaging with the women in the society
    - Trust-building measures (distributing medical and school supplies, sitting and talking with local women, visiting schools and hospitals, providing access to clean water, leading community discussions on topics such as hygiene, childbirth or breastfeeding)

Women as Counter-terrorists
Female Engagement Teams (FETs)

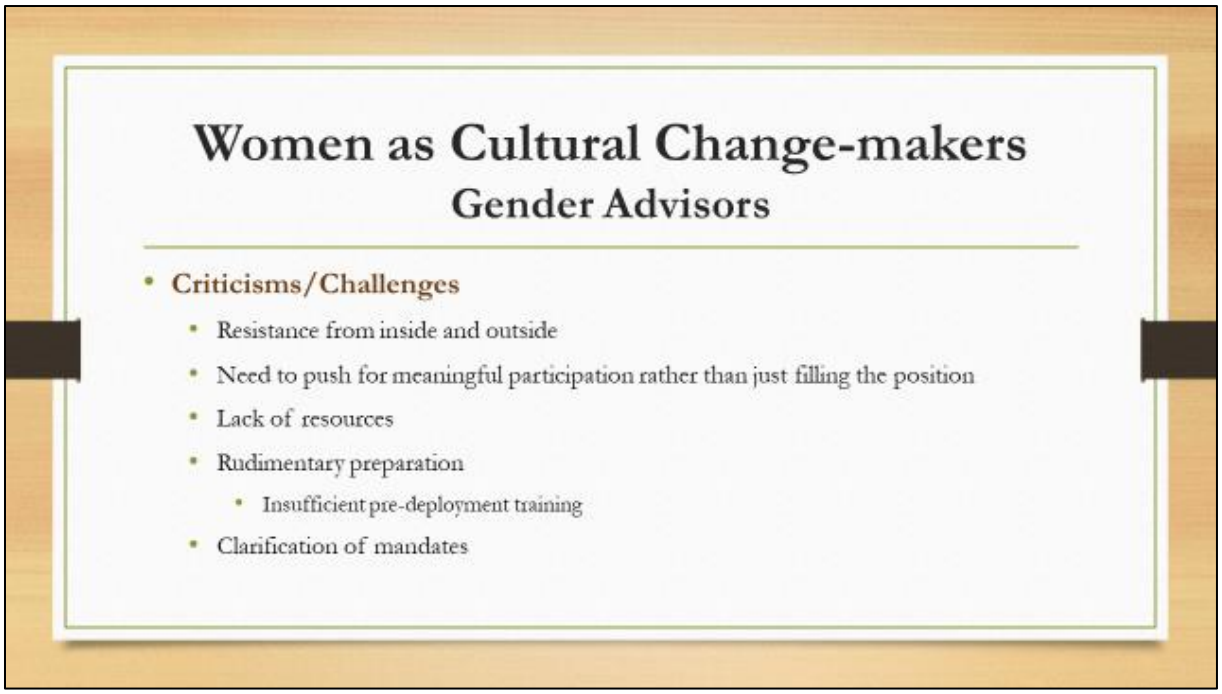
- US military
  - Lioness Team-2003), ~20 women soldiers, Iraq
  - FETs -2009, Afghanistan
- FETs- Britain, Sweden, Norway, Jordan
- **Benefits**
  - Intel-gathering
    - discovering caches of weapons, drugs, money.
    - identifying where the IEDs or mines placed
  - Force protection

Women in Operations: Female Engagement Teams (FETs)

- **Criticisms**
  - bartering operational effectiveness over advancing women's rights
    - pragmatism vs idealism
  - risk of instrumentalizing women and WPS for operational needs and requirements such as force multiplication
  - masculinizing and militarizing women

Women as Cultural Change-makers
Gender Advisors

- Actors for regendering military and regendering society
- Play an important role in operational effectiveness in terms of
  - embedding gender diversity in the military
  - revising policies and standards


Women as Cultural Change-makers
Gender Advisors
Criticisms/Challenges
Resistance from inside and outside
Need to push for meaningful participation rather than just filling the position
Lack of resources
Rudimentary preparation
Insufficient pre-deployment training
Clarification of mandates

Cyber Security in the Domain of Counter-Terrorism

by Assoc. Prof. A. Salih Bıçakcı

"The world is never going to be perfect, either on- or offline; so let's not set impossibly high standards for online."
Esther Dyson[12]

Terrorism and Cyber space have a particular relationship. Cyber space is presenting *sui generis* characteristics which affect related domains such as kinetic world that we interact in. Terrorism has a polymorphic and liquid characteristic. As Hoffman (2006) noted, it is arguably easier to define what makes as an act of terrorism in the history. But contemporary terrorists benefit from all advantages of technology to achieve their goals. This situation obfuscates demarcation between terrorism and cyber domains.

In the last decade, with the increase of digitalization, most of the services of private and state entities were carried to the cyber domain. The digitalization process also promoted the usage of new platforms and devices which advanced the connectivity of people and services to each other. The hyperconnectedness also produced new opportunities and capacities for individuals, corporations and states. This shift also connected the locality with the global space. So, a node in hyperconnected cyber space would easily affect the level of global security with an attack, news or activity. This presented a unique opportunity for terrorist groups as they could producie extensive impact with minor investment. Cyber space, in this sense, is presenting an amplifying effect on terrorist(s) attacks or actions.

While organizing this research, the main obstacle is to limit the best practices for all cyber space. The disinformation campaigns and use of cyber space for terrorist purposes are kept out of the scale of this research. Terrorist individuals and groups use cyber space either for planning, training, recruitment, cooperation, financing and reconnaissance. In all these actions, the cyber space is used as a medium to facilitate their goals. However, in cyber space there are hardware, software and policies which regulate the activities and functionalities up to its design purposes. These infrastructures make several services run for millions of people. Any service such as Twitter, Instagram or YouTube gives its programmed functionality for all users without knowing their

[12] Ross Anderson, *Security Engineering*, Wiley, 2008.

intensions. As much as the messages of the users do not contradict with the policies of the service provider, the platform would continue to serve to the user. The propaganda purposes of the terrorist individuals and organization as depicted in this example is not the concern of this research. If terrorists decide to hacks the platform or hack the individuals in the same platform to have chances to distribute their message under other names or personas, this would be in scope of this study. On 23 April 2013, The Associated Press' Twitter account has sent a message: "Two explosions in the White House and Barack Obama is injured." The message created a small catastrophe in the stock markets[13] and later understood that a group called Syrian Electronic Army had captured Twitter account of the Associated Press. The example demonstrates a majör case in which Twitter should push the Associated Press to use two-level authentication and force its users to change their passwords periodically. On the other hand, the Associated Press should be sensitive about the phishing attempts to protect its Reputation.[14]

There are also disruption and destruction attacks in which the perpetrators aim to stop the services or harm the target. In these types of attacks, terrorists target an asset in the cyber space to disrupt or destruct a service (or a computer-digital system) and the consequences of such an act would appear in the kinetic world. In this research, one will concentrate on these types attacks which terrorists target for assets in the cyber space. In these types of attacks, terrorist aim to intimidate or shock the audience by showing of their power and present the weakness of protectors of the society or structure. Any success would give remarkable message to the public or the audience. To harden the security of these services would quickly increase time or energy that the attacker should spend on a particular attack. In most cases, the attackers swiftly prefer to find a less hardened target to achieve their goal.

In risk management, the calculations for a particular system is built on two variables: threats and vulnerabilities. These two concepts are strongly associated in the cyber security. Vulnerabilities and threats have different meanings from the perspective of defenders or attackers. Threats are quickly changing and its levels are altering from

[13] Max Fisher, "Syrian hackers claim AP hack that tipped stock market by $136 billion. Is it terrorism?", *The Washington Post,* 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackersclaim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/ (Accessed on 23 September 2020)

[14] Geoffrey Ingersol, "Inside The Clever Hack That Fooled The AP And Caused The DOW To Drop 150 Points", *Business Insider*, 2013, https://www.businessinsider.com/inside-the-ingenious-hack-that-fooled-theap-and-caused-the-dow-to-drop-150-points-2013-11. (Accessed on 12 August 2020)

country to country. The asset (target) has no authority or control on threats. Since a cyber domain or system is made of several components, the owner of facility could not have authority on threats in several levels. Therefore, harnessing threats is not a preferable method to follow for the risk management. As clearly formulated by Ucedavelez, "for an attacker perspective, vulnerabilities are opportunities to attack an application to achieve specific goals such as stealing confidential information. A vulnerability such as weak encryption used to protect the data or weak authentication to access that data might facilitate a threat agent to access such as confidential data by brute forcing authentication and as well as by performing an attack against the weak encryption used by the application".[15] From the defender perspective managing and reducing the vulnerabilities is efficient way for minimizing the risks. Vulnerability is a common term to define the security exposures in a network, operating system or other software or application software component in the system, and also human error (intentionally or accidently) inside the organization.

Any vulnerability can potentially compromise the system or network if exploited. In this research, as a part of best practices in the defense against terrorism, one will focus merely on the vulnerabilities of computer systems. The computer systems in the cyber domain have various components such as hardware, software, data and connection layer (fiber optics, land lines, etc). There are major commonalities among the computer systems but each computer system has certain differences. In the computer systems, there are two sides: one is the attack surface and trust boundaries is the other one. Each computer system has different front-ends and appearance which forms the attack surfaces. The offender/attacker starts its mission by reaching to the convenient end. The large attack surfaces would extend the possibilities of an attack. To minimize the attack surface is generally difficult or not reasonable. The second category, trust boundaries, is representing inside of the systems which tries to define trusted zones in an infrastructure. Trust boundaries are the critical spaces from the point of a defender to reinforce andextend the zone which would assist the threat modelling. In the classical approach, to minimize the attack surface as much as possible, secure and extend trust boundaries as much as possible is the main rule. However, the experiences in cyber security field demonstrated that the human element is also critical and they also periodically have to be checked to sustain the security.

[15] Tony Ucedavelez – Marco Morana, *Risk Centric Threat Modelling*, Wiley, 2005, p. 635.

Protection and maintenance of cyber security for the running systems will reduce the surprise effect for possible terrorist attacks. In cyber security literature, there are several methodologies to secure the computer systems. In additional to differences of computers system structures, to compile best practices for securing cyber domain is terribly challenging task due to dynamic nature of the threat landscape. Even though the vendors are showing utmost care to protect their products, there is always possibility of the presence of zero-day exploits, bugs and backdoors. In addition to these problems, human capital who are using these Information and Communication Technology (ICT) based systems are also significant components of the systemic security. Human is forming the weakest link of the cyber security. All security measures have to be compatible with the rules of human-machinery interaction and most of the designs are not giving required attention to the issue. For example, the computer access systems working with human interfaces have to be protected with an access policy. In most cases, in order to secure the systems, the length of password has to be long to prolong the duration required to achieve a successful brute force attacks. However, the limitations of human cognitive system and business mindset for efficiency mainly prevents to use long and meaningless passwords.

Changing threat landscape, different computer system structures and human inadequacies or malign intentions could be secured against terrorist attacks via adopting a macro cyber security approach. In the cyber security literature, there are several cyber security maturity models[16] implemented in different sectors. Basically, a maturity model is an organized way to convey a path of experience, wisdom, perfection attributes, indicators or acculturation in a particular sector. The cyber security maturity model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline.[17] The cyber security maturity models also help to build a cyber security culture which would shape and focus behaviors and code of conducts of the human capital as well.

The major advantage of cyber security maturity models is understanding security as a process which has to repeat and renewal for responding swift advancement of

[16] For a comparison of cyber security maturity models, see; Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative Study of Cybersecurity Capability Maturity Models. Software Process Improvement and Capability Determination, 100–113. doi:10.1007/978-3-319-67383-7_8

[17] Cybersecurity Capability Maturity Model (C2M2) Program, https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sectorcybersecurity-0 (Accessed on 12 September 2020)

threats and vulnerabilities. The security of the computer systems is mostly comprehended by business owners as a task that has to be checked in to-do lists. However, the ICT systems are like living organism which needs continuous care and maintenance in accordance with the daily dynamics. Any changes in the organizational structure or design of the systems have to be handled with an utmost supervision and restructured up to the new settings. These ICT mechanisms also have specified working on specific working conditions and durations which requires a tailor-made change management strategy. The cyber security maturity models attempt to build a hierarchy and documented process which aim to minimize vulnerabilities and build a proactive stance against any attacks, sabotages or accidents. In this paper, the cyber security maturity model made-up from ten domains.

1- Risk Management

The first domain is to design the risk management systems and resilience planning. The risk management domain targets to build up, operate and maintain a cyber security risk management program for your enterprise. This program will identify, analyze and mitigate the cyber security risks up to your requirements. It will also understand risks for infrastructures and stakeholders. In the recent years, the cyber security sector have reached a consensus on that with given enough time and resources, every security technology is breakable; therefore from the very first day the responsibility of the institution is to learn to build a resilient ICT technology. After all disruptions, either human made or natural hazard, all systems swiftly should be capable to keep up their functionality and services. This should be the utmost goal of all the ICT systems from a defensive approach.

2- Asset, Change, and Configuration Management

The second domain is identification of the assets and change management. In most institutions, the boards, CSO, CRO or decision-makers have limited knowledge about their assets which would cripple their decision making process for better grasp of their risks. The risk perception is one of the major issues for the protection of the institution. It also determines the budget allocation of the institution for the security. The major goal of the asset, change, and configuration management is to manage the organization’s IT and OT assets, including both hardware and software, relevant to the risk to critical infrastructures and organizational objectives. In some of the business

oriented institutions, the security is understood as one time investment which could continue its functionality as it works. However, the ICT systems are working in a complex environment which demands compatibility and high level association. To keep up the ICT systems up to date, a change management strategy is required which includes investment, management and implementation steps. The outdated technologies would create further security problems in addition to the new ones. Up to the researches, nearly 1 million new malware threats released every day.[18] For example, if you are using Windows Server 2003 which has reached its end of support on July 2015, it means that you are either at greater risks of cyberattacks and exploitation by third parties or you are paying high prices to keep the server running.[19]

3- Identity and Access Management

Third step is identity and access management which are critical for the physical and cyber security of the institutions. As a follow up to Asset, Change, and Configuration Management, in this step creating and managing identities for granting access to cyber or physical assets of the organization are implemented. To control the access is key point between cyber security and HR departments. Several departments involve to this process in an organization. Most of the institutions have certain trust on their workers. The Fortinet report in 2019 demonstrates that there is a rising risk in all sectors for the insider threats9. Inside the company is understood as in the limits of trust boundary, thus, the focus to the staff is limited. It should be noted that all cyber incidents occur as a result of malign intentions but sometimes the lack of expertise or basic training would cause accidents which would cause unexpected results.

4- Threat and Vulnerability Management

Fourth step is focusing on threat and vulnerability management. This domain is one of the major components of the protection of the organization. Main goal is to establish and regulate main plans, procedures, checklist and implant necessary technologies to detect, identify, analyze, manage cyber security threats and

[18] Virginia Harrison and Jose Pagliery, "Nearly 1 million new malware threats released every day", *CNN*, 2015, https://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/index.html (Accessed on 11 July 2020)

[19] David Goldman, "Navy pays Microsoft $9 million a year for Windows XP", *CNN Business*, 2015, https://money.cnn.com/2015/06/26/technology/microsoft-windows-xp-navy-contract/ (Accessed on 23 June 2020)

vulnerabilities compatible with the strategy of the organization. In this part, institutions have to decide about their level of protection. It is not feasible to establish a protection regime against all threats. Some of threats are more urgent and more probable than others. Each organization has a different structure and range of software. To understand the possible risks in different operating systems and digital components, organizations would use risk (reporting) matrix (see Figure 1) to calculate possible threats and vulnerabilities for their structure. The visualization and probability calculation of the risks would help decision-makers on their judgement.[20]

IMPACT ⇨ LIKELIHOOD ⇩	Negligible	Minor	Moderate	Major	Catastrophic
Remote	Very Low Risk	Low Risk	Low Risk	High Risk	Very High Risk
Unlikely	Very Low Risk	Low Risk	Moderate Risk	High Risk	Very High Risk
Possible	Low Risk	Moderate Risk	Moderate Risk	High Risk	Very High Risk
Likely	Low Risk	Moderate Risk	High Risk	Very High Risk	Very High Risk
Certain	High Risk	High Risk	High Risk	Very High Risk	Very High Risk

Figure 1-Risk Matrix[21]

Risk reduction begins with collecting and analyzing vulnerability information of your organization which would clarify your threat actors and their intentions. There are certain studies in threat management to cluster the possible threats. Major security problems in cyber security are grouped as spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege.[22] There are also several methodologies, but MITRE ATT&CK is giving a detailed roadmap on how an attacker would proceed.[23]

[20] *Risk, issue and opportunity management guide for Defense acquisition* programs, 2017, Department of Defense – USA.
[21] Bukowski, L. (2019). Logistics decision-making based on the maturity assessment of imperfect knowledge, Engineering Management in Production and Services, 11(4), 65-79.
[22] Adam Shostack. "Threat Modeling."2014, Wiley.
[23] https://attack.mitre.org/matrices/enterprise/ (Accessed on 18 October 2020)

5- Situational Awareness

The main goal of this domain is to establish technologies to collect, analyze and warn the operators to obtain status and summary information regarding to the operational cyber security condition. The ultimate goal is to form a Common Operating Picture (COP) to be effective in decision making, rapid staff actions, and appropriate mission execution in complex and dynamic environment of the organization's cyber security setting. Bennet defines situational awareness as "the knowledge of where you are, where other friendly elements are, and the status, state, and location of the enemy14". He also categorized "the levels of situational awareness":

Level 1 situational awareness involves perceiving the critical factors in the environment.

Level 2 situational awareness is understanding what those factors mean, particularly when integrated together in relation to the decision maker's goals.

Level 3 situational awareness is the highest level, which is an understanding of what will happen with the system in the near future."[24]

In an organization, if COP suggests a need for heighted security, then visitors are screened more carefully, the Helpdesk conducts malware scans on misbehaving laptops, and human resources sends out reminders about phishing. Senior management reviews the COP and the cyber response teams should be prepared to extraordinary action such as shutting down the Web site, if necessary. At the highest state of alert, they change firewall rule sets to restrict nonessential protocols like video conferencing, delay all but emergency change requests, and put the cybersecurity incident response team on standby.[25]

6- Information Sharing and Communications

The cyber hygiene of an organization is relevant with its ecosphere. Since the organization is working in an interconnected and complex environment, to warn the relevant parties and learn the recent security development is critical for the protection. To establish and maintain relationships with internal and external entities, to collect and provide cybersecurity information would in most cases reduce risks and increase operational resilience of the organization. Information sharing practices will help

[24] Brian T. Bennett, *Understanding, assessing, and responding to terrorism : protecting critical infrastructure and Personnel*, Wiley, 2007, p. 292.
[25] Ibid.

organizations to get informed about the rising risks also intelligence regarding to their vulnerabilities. The information sharing practices also refine communication skills of the parties which might be relevant in case of emergency. To decide what to share and how to share would also reinforce the organizational communication skills and expedite the decision-making process.

7- Event and Incident Response, Continuity of Operations

This domain is highly connected with situational awareness. The monitoring capacities of the organization would continuously observe the operations when they detected an escalation in any level of operations, they will define the suspicious incident and quickly react to support the security of the organization. This domain has five major steps to follow:

1. Detect Cybersecurity Events
2. Escalate Cybersecurity Events and Declare Incidents
3. Respond to Incidents and Escalated Cybersecurity Events
4. Plan for Continuity
5. Management Activities

In some OT environment, the responding requires specification on a certain environment (eg. SCADA) in which case, the organization has the responsibility to find ways to build up required training and to cultivate necessary experience among its staff.

8- Supply Chain and External Dependencies Management

Today, the cyber security scene of an organization is highly connected with other organizations which particular functions and IT environment. This interdependence among infrastructures, operating partners, suppliers, service providers, and customers is increasing. Supply chain cyber security experts are extensively discussing how to mitigate and manage the third party risks. The organization should identify these thirdparty risks and form a management plan as well. When we realize that cyber security devices and other IT/OT hardware are mostly obtained by third-parties, we could understand the criticality of management of supply chain and external dependencies.

9- Workforce Management

In the cyber security chain, the utmost significant issue is workforce management. The maturity of cyber security program in an organization which is only possible by constructing a robust security culture. This domain aims to ensure the ongoing suitability and competence of personnel in all departments to have required level of awareness and proper training to sustain the security. Organizations might have high reliance on the technology, but the staff is critical when it comes to utilize cyber security equipment. The level of expertise and training of the staff would harden the protection level and expand trust boundaries.

10- Cybersecurity Program Management (CPM)

All domains are necessary to establish the cyber security maturity model but to build up cyber security program and its management is crucial as much as other steps. The CPM decides about appropriate policies and focuses on the execution of these rules including strategic planning. As C2M2 manual clearly noted, "A cybersecurity program is an integrated group of activities designed and managed to meet cybersecurity objectives for the organization and/or the function"17. The higher management of the organization has to be involved in the formation of CPM process (see Figure 2) and the policies has to be in line with the management policy. In case of a change in the highlevel management, the new management people should revise organization's CPM strategy up to the most recent management approach. The sophisticated CPM should regularly update its outlook on people and policy risks, operational and technology risks. The management also focus on introduction of these updates to its workforce and integration of them to its security culture. On the other hand, the CPM should have to be consistent with the framework of the state-level regulations and approaches.

The CMP cycle basically demonstrate that the management should be vigilant to follow the cycle to mature its strategy and cyber security outlook.

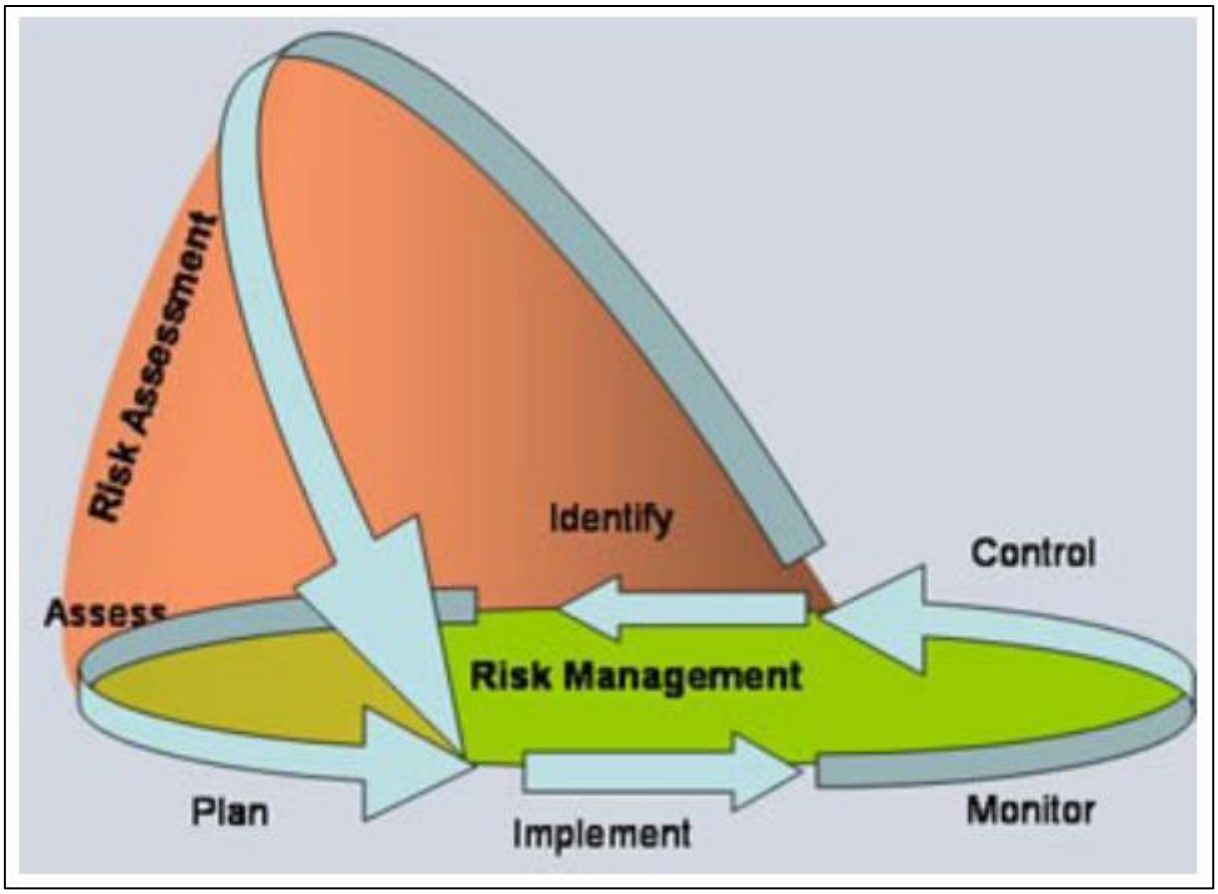


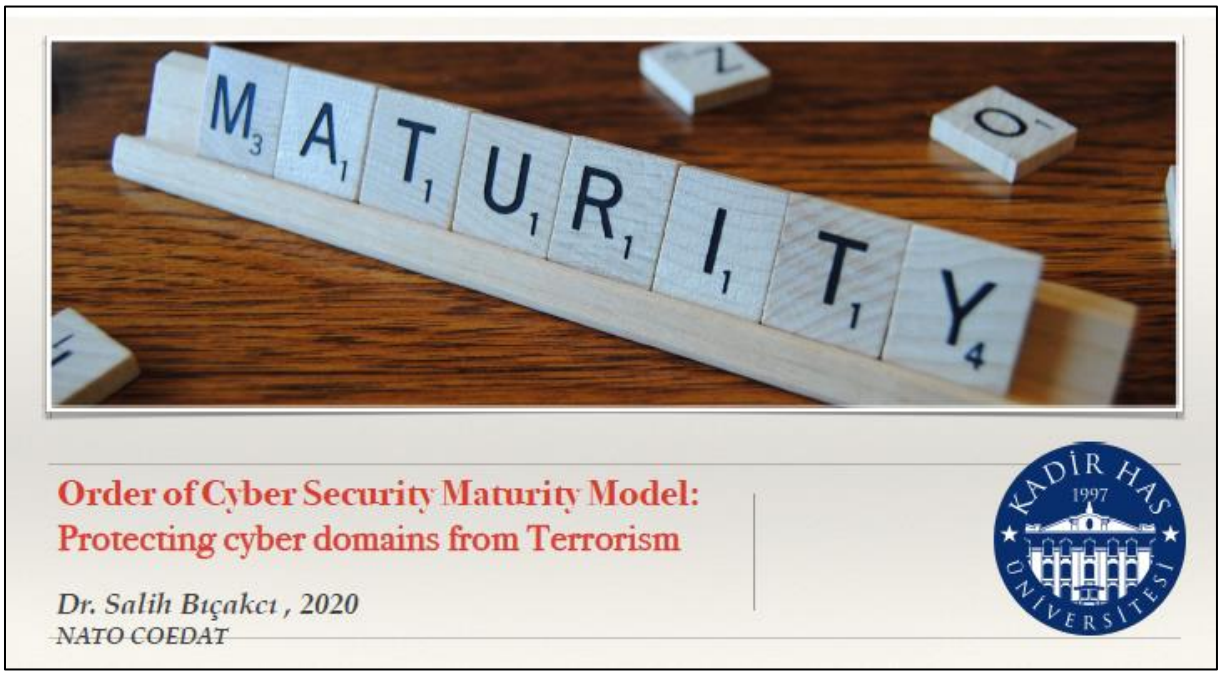
Figure 2-CPM cycle[26]

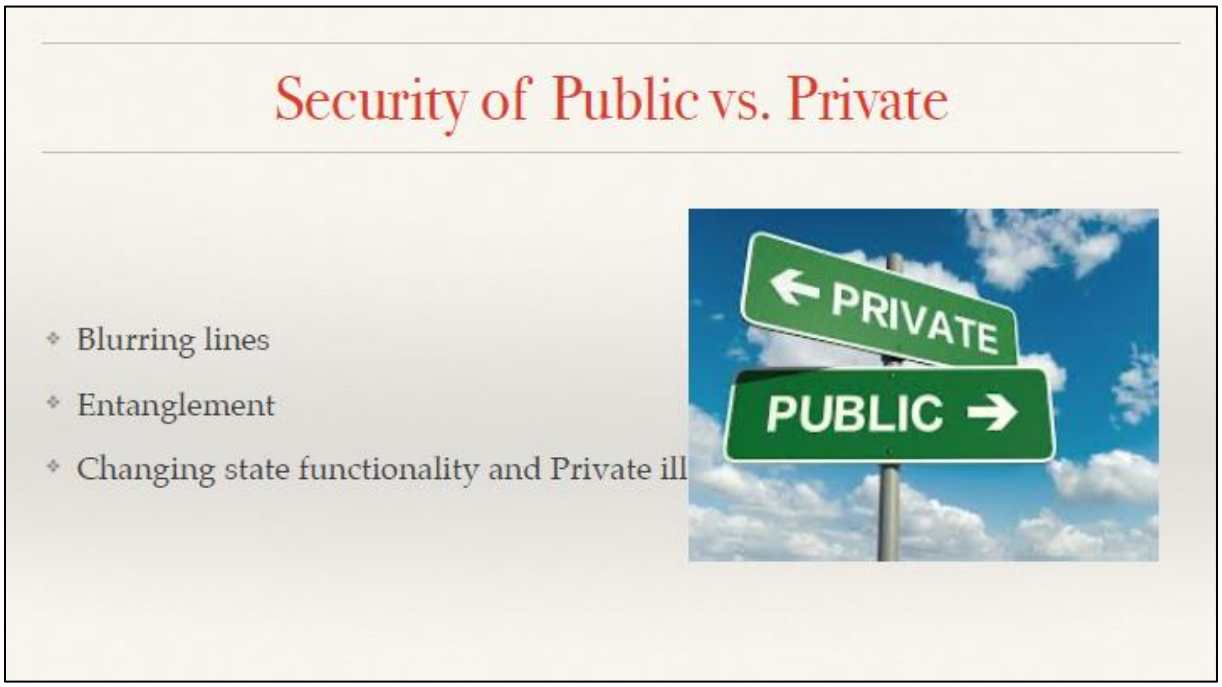
To conclude, this research intends to elaborate the cyber security maturity domains which would strengthen the computer system infrastructure against any terrorist attack. To list these domains is easier than to realize them. The realization of a such project requires total involvement of all parties to achieve this particular goal. All of the domains for cyber security maturity model talk with each other. A strict implementation of these strategies would also minimize use of cyber space for terrorist purposes. Any gap within a domain or disconnection among them would harm the overall process. Cyber security is not a solely information security question but multidimensional issue with the interaction of the multiple actors and multiple policies, laws and regulations. It is a shared responsibility and trust in a house, in an organization, in a corporation or in a public entity. The functionality is sustained by security and trust

[26] "Risk Management & Information Security Management Systems", *ENISA*, https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/riskmanagement-inventory/rm-isms (Accessed 15 August 2020)

for all relevant participants. Otherwise, the ICT infrastructure would be an easy target for the perpetrators.

d. Presentation





Capability scale

- a) Enabling – online activities that support the operations of terrorist groups, such as publicity and propaganda, recruitment, reconnaissance, clandestine communications between members, and disseminating manuals and know-how to incite and facilitate attacks by others.
- Disruptive – online activities that disrupt the information technology of opponents, including pro-active cyber breaches of networks; dissemination of malware; exfiltration of digital information; financial theft a;nd fraud; denial of service attacks; phishing and other information technology (IT) hacking activities.
- Destructive – cyber attacks that trigger physical damage or injury through spoofing operation technology (OT) and digital control systems; attacks on Supervisory Control and Data Acquisition (SCADA) systems; disabling control and safety systems

Enabling activity

Terror Group Website - Propaganda
Video and Social Media- Propaganda/Recruitment
Funding Operations Manual- Financing
Encrypted Communication- Coordination

Disruptive Activity

- Defacement of web sites
- DOS or DDOS -Service disruption
- Data Exfiltration Hack
- Cyber Financial Heist/Ransomware

Destructive Activity

- Sensor Spoofing
- Control Engineering Compromise
- Damaging and Disabling Infrastructure
- Limited destruction on Multiple targets

Risk Management and resilience planning

a. Balance between functionality and security
   i. Budget issue
   ii. Improvement of the security has to be planned.
b. Defining risks
c. Defining responsibilities and coordination
d. Establishing strategic communication
e. Training the staff and build a risk culture

Identification of asset, change and configuration management

- Does it have a value to the organization? Will it cost money to reacquire? Would there be legal, reputational or financial repercussions if it cannot be reproduced on request? Would it have an effect on operational efficiency if it could not be accessed easily? What would be the consequences of not having it?
- Is there risk associated with the asset? Risks include: loss, inaccuracy, tampering, and inappropriate disclosure.
- Does the organization understand the content of the asset is and what it is for? Does the asset include all the context necessary to understand and identify it?
- Does the asset have a manageable lifecycle? Were all the constituent parts created for a common purpose? Will they be disposed of in the same way and according to the same rules?

"I want you to find a bold and innovative way to do everything exactly the same way it's been done for 25 years."

Identity and access management

- Disgruntled employees who feel disrespected and are seeking revenge.
- Convincing a worker to cooperate by disguising their malign goals
- Role of HR services
- Stealing blueprints of an item or intellectual property to return it into financial issue
- Use institutional infrastructure to host their malign services or hide their communications
- Use IT infrastructure to communicate under radar.

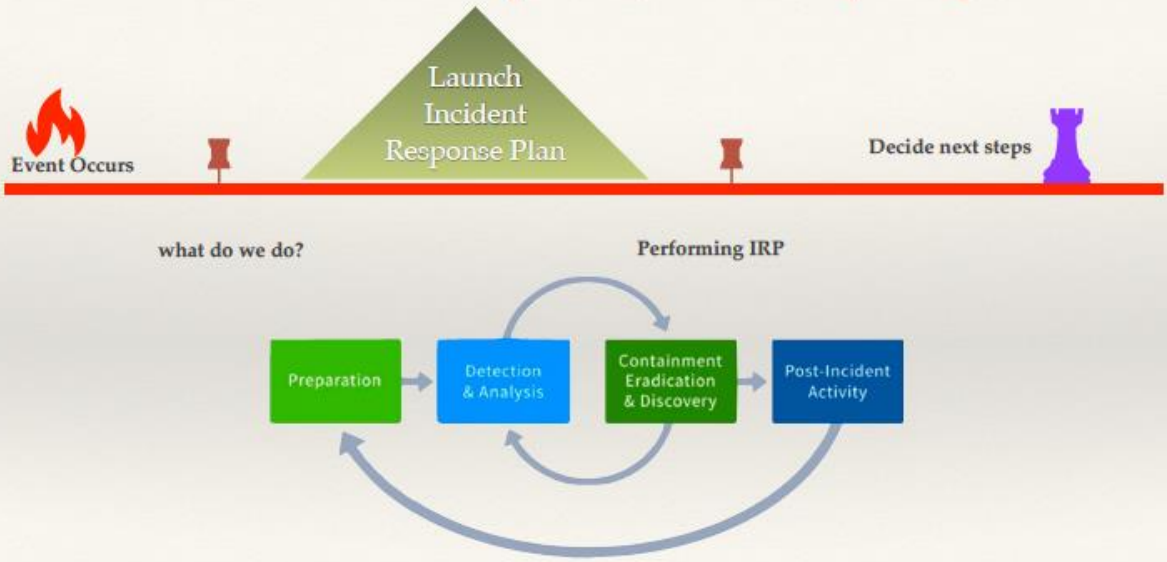
Threat and vulnerability management

- Human threat
- Clean desktop principle: Honda, Apple, etc.
- Supply system threat
- Environmental threat – esp. human caused ones.
- Safeguard your information system against fluctuations in
- electricity or electrical power outages and by ensuring that it is
- plugged into an Uninterruptible Power Supply (UPS).
- Ensure that backups are performed on a regular basis to
- safeguard your information against a catastrophic event such as
- a flood or fire.

Information sharing and communication

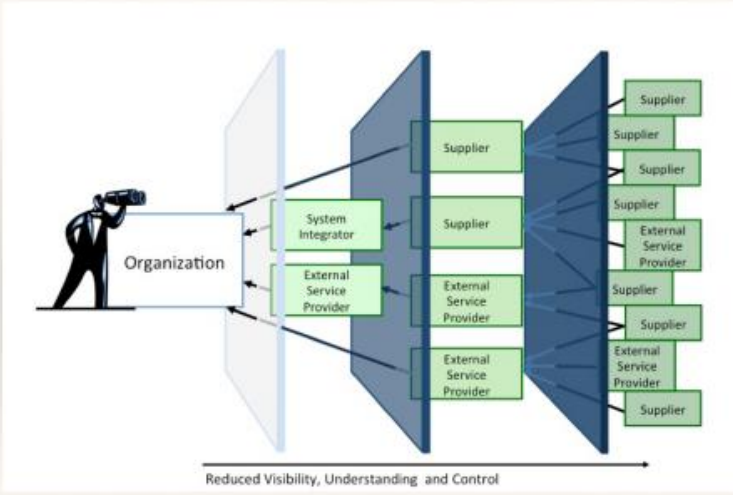
- Shared Situational Awareness.
- Enhanced Threat Understanding.
- Knowledge Maturation.
- Greater Defensive Agility.
- Improved Decision Making.
- Efficient Handling of Information Requests
- Rapid Notifications.

Event and Incident response, continuity of operations



Supply chain and external dependencies management

- Unsolicited computer maintenance and repair systems
- Outsourcing companies
- Controlling dependencies



Workforce management

Inconsistent Lexicon

While strides have been made, the language used to discuss cyber work and skill requirements is inconsistent. This hinders the nation's ability to assess capabilities, identify skill gap, and prepare the pipeline of future cyber talent.

Lack of Cybersecurity Professionals

A recent report by the *Partnership for Public Service* stated, "There is a nationwide shortage of highly qualified cybersecurity experts, and the government has fallen behind in the race for this talent.

Disjointed Professional Development

There is a lack of clearly defined roles and career paths for cyber work. Efforts to establish accreditation standards for cyber curricula and certifications have been inconsistent.

Cybersecurity Viewed as Separate Function

There is often a perception that cybersecurity is a stand alone function performed by specific cybersecurity professionals. As a result, cybersecurity is not recognized by many in the broader cyber workforce as being a part of their own daily work.

Cyber Security program management

- Change management
- Building cyber security culture with Management level coordination

Day 1 Questions and Answers and Open Discussion

Mr. Stephen Harley

Hard Power, Soft Power and Smart Power: Civilian-Military Challenges in CT

1) Regarding "we talk to terrorists every time", who do you mention as "we"?
LtCdr(N) Güzide Tirnava, MARSEC COE

According to Mr. Harley, the one talking to terrorists are 1) the ones **willing to do it** 2) the ones who are **most appropriate** to do it. In the case of Northern Ireland, it was the British government who was talking with the terrorists. However, the US has said that they do not think that they would have to be talking with al-Shabab. In this case, **third parties** are often used. Sometimes you do not realize you are talking to terrorists but there is always a debate. Norway and Switzerland use a lot of soft power in their approaches. Also, Turkey uses soft power in Somalia, mostly related to the links with the Islamic community. Overall, you can have "own people" talking to terrorists or use third parties.

2) What kind of soft power measures are being implemented to counter al-Shabab's female terrorists? *LTC Diana Morais, Portuguese MoD*

Mr. Harley emphasized that women do not have combat roles in al-Shabab. "White women" do not lead al-Shabab, i.e. Samantha Lewthwaite. However, there are women in the group who have a position of authority. Fighter wives are often in charge of running businesses, i.e. selling clothes, being in charge of construction companies or agricultural products. Al-Shabab is both part of the problem as it is part of the solution. It would not be good to apply hard power measures against them. Part of the solution is also using women as part of the negotiation, using their experience and reaching out to them - they are the ones growing and educating children. We need to think of children and the next generation - soft power is needed to address this.

Dr. Sütalan stressed **women's agency and role - women can be terrorists. If this is not acknowledged, it jeopardizes the countering strategy as well.** We need to recognize women's role in terrorism and have the necessary tools to act upon - women are also having roles as perpetrators. We need to identify these roles and take relevant legal measures, i.e. counter their businesses or take social measures, i.e. raising the next generation by providing

them with education. In the case of Boko Haram, studies have shown that **social conditions** also play a role, otherwise the only option that these woman are left with are joining terrorist organizations.

3) What if the terrorists are not ready to talk or rather communicate? *Ahmed Abdullahi, Nigerian Navy/Operations/Commander*

Mr. Harley agreed that sometimes, a terrorist organization does not want to talk for 20-30 years and in this case, **hard power can be used to undermine the organization and push the group into a position of willing to negotiate.** Some groups like Boko Haram and Daesh do not want to negotiate. Al-Shabab as a group does not want to talk or negotiate but some individuals in al-Shabab do. It is about **appropriateness and proportionality.**

4) Regarding the statistics about how 268 terrorist organizations ended, is there a declining trend about the effectiveness of the military means just because terrorists adapt faster than military forces in achieving their end states, acquiring high-tech weapons to utilize asymmetric ways? Was the degree of effectiveness of military means in 1968 higher, lower or same when compared to its effectiveness in 2006? Is there a significant trend in the change? *Col. Soner Özer, NAOC/Compat Plans Division/Division Head*

There are lots of potential questions about the RAND research and how they have approached the issue - the research stopped at 2006 and does not include Daesh, for instance. Mr. Harley emphasized the need to adopt. Terrorists groups are "flexible and survivable". Terrorist groups are now different from those of 2006 and 1968 - **we have to be constantly adapting**.

5) How can military instruments support soft power in CT? How can military be leveraged in CT as a stakeholder of smart power? *Lt.Col. Cenkan Sagir, SHAPE J5, Strategic Policy Officer (CT)*

This will be **further addressed in Mr. Harley's final chapter,** i.e. how some militaries are adapting, represent gender power and moving closer to a representative balance of 50% as well as put focus on **recruiting cyber and communication experts.** Norway and how they train their military staff is a good example of this while making military still relevant. **Military needs to adapt.**

6) What are the best practices on counter-narrative related actions undertaken in Somalia to combat terrorism against Al-Shabab? *Lt. Balajanov, State Security Service, Azerbaijan*

Mr. Harley highlighted that this will be further discussed in the final article. However, this is not the strongest part of hard and soft power in Somalia. This will be further addressed in Dr. Ashraf's and Ms. Fogget's article of the upcoming CT Handbook. You cannot transfer lessons learnt

from Afghanistan and Iraq to other societies - mass media and satellite based television is not as accessible. Afghanistan is a small, predominantly radio based network. We have forgotten a saying that "quantity has a quality all of its own". We can hire the most expensive advertising companies to make wonderful products but we might be better to get local people to produce something that is locally authentic and fits in with the local environment and do it in volume.

The United Nations spends ten million dollars a year on an information support team to support them and the African Union mission and the central government of Somalia. Al-Shabab appears to do it with two guys and two laptops and in terms of output, al-Shabab is thwarting the issue with a ratio of about 4:1 in terms of output. Do it local, do it cheap, do it quantity. **The best case would be to have a core narrative and a core ideology**, so you are coming from the front of the issue, not the back of it, i.e. by having a counter-narrative.

7) ***Comment: Soft power is a strategy of diplomacy - we use this style to avoid war and to show power without using it.*** *Col. Daher, General Directorate of State Security, Lebanon*

With regard to using soft power to avoid war, Mr. Harley commented it with the example of a "runny egg" - there are bits of the military which are going to have to extend into a soft power and some already are, i.e. diplomatic and economical sanctions. But there are also things that are very soft, job creation in economics is seen as soft power. We need to stop thinking of hard lines and start thinking of blurred lines.

8) According to hard-soft power balance, the best ratio is 90% soft power and 10% hard power. How can this be achieved, as now the ratio is the other way around? *Col. Marinov, Rakoski National Defense College, Bulgaria*

Mr. Harley commented that we are currently doing 90% of hard power and 10% short power - terrorists do 90% soft power and 10% hard power. How do we get to that stage - that is the whole point of this conference. This is where we can adopt our current tools, keep ourselves relevant and adjust to the changing environment. You cant go from 90% of hard

power to 10% as quickly. If we can get into 50/50, we would already be doing well - maybe we have to **adapt the individual institutions first**. You can look at the struggles that governments have through social media - no one seems to use Twitter and messaging the way terrorist groups do. These are the things we have to adjust with.

9) How do you assess an eventual outreach process for applying soft power techniques considering that the majority of the terrorist activities are carried out in hostile environments where external opinions/influence/presence can determine a violent response? *OF-2 Dragoș Gabriel MOLDOVAN, ROU, MoD*

Mr. Harley highlighted that one of the challenges is that we often apply soft power in soft places but stop short of applying it in hostile environments. Turkey is a good example of engaging soft power in Somalia and not applying combat power. If a country can do this in a country like Somalia, **this can be a model to follow for other countries.**

10) Which law is followed during these activities when they are in a foreign country? Do they follow the international law or the national implementation? Because terrorist groups have this evolution from a simple group into internationally organized professional groups. *Capt. (N) Tayfun SARGIN, Turkısh Coast Guard / Anti Smuggling and Org. Crime D. / Head of Dept.*

Mr. Harley also emphasized the need to **coordinate**. If you want to achieve objectives but cannot apply soft power in an environment, **get someone else do it.** In Somalia, this is the reason why the African Union has the military lead. For instance, USA is constrained in meeting terrorists and now, some of these terrorists in Somalia are part of the government, someone else does it for them - we just have to be adaptable and flexible. Do not tell your troops the mission objective but the end message you want people to get. We have talked about tactics and mission command for decades but are we actually applying it yet and be more serious about the application of tactics.

11) Who has the biggest interest in terrorist groups being financed? *Col. Petar MARINOV, Rakoski National Defence College / Land forces / Associate professor, Bulgarian armed forces*

According to Mr. Harley, by the very nature, terrorists need things that are illegal such as guns and fake IDs. “Terrorism is an expensive hobby” and you probably have to do something illegal. Groups like al-Shabab put a lot of emphasis on smuggling (fake drugs,

watches, printer cartridges). UNODC talks about the terrorist criminal nexus - the two groups are increasingly knitted together. Several terror groups have also become crime groups later on, i,e. IRA in Ireland.

Ms. Susan Sim

Developing National Counter-terrorism Policy

1) Would letting the society being part of the solution result in securitization of the society? Can the SG Secure model from Singapore be transferred to other cases? *Prof. Yalcinkaya, TOBB ETÜ*

Ms. Sim highlighted that she would not call the issue as "securitization". We have to look in terms of scale - Singapore is a small city state. It may be possible to apply the model on a city level but not on a national level, i.e. do it on a level of London. **Everything depends on context.** Every country has a different culture. Singapore is a multicultural country with different races and religions - the state must give space for different races and cultures. It is a process of give and take by accepting differences and celebrating commonalities.

2) Singapore is one of the leading country, having important academicians' works on terrorist rehabilitation. Based on the fact that the efficiency of the recidivism is not certain, what are the results of terrorist rehabilitation programs performed in Singapore? *Col. Engin AVCI, Gendarmeria and Coast Guard Academy / Research Centers / Deputy President*

According to Ms. Sim, there is a known 1 case of a person who has gone back to terrorist activities after going through a rehabilitation program. It is true that after a terrorist counseling program, a person can take on a lone wolf attack. It is a long term process that **needs political will** and understanding of different beliefs. It is important to achieve objectives without violence and to rehabilitate terrorists, so that they can go back to society. However, you can never be sure whether a terrorist that has undergone a rehabilitation program will go back to terrorist activities. But it is important to give people second chances and be there - this required political will.

***3) Every country has a diffe*rent cultural mix - when cultures have opposing views, how can we overcome it?** *Col. Marinov, Rakoski National Defence College, Bulgaria*

Ms. Sim pointed out that in multicultural societies, we have to understand each other's differences. Singapore is a secular state but there is space for different religions and cultures - this is a process. As such, every state should give space to these differences. There is a continuing alienation of migrant communities as well as lack of understanding and trust for governments and state. We should have a common education process and throughout communication in place. This is a hidden part of the best practice. **Terrorism is a choice -** no one gets pushed to terrorism. Only a minority of people leave their home on purpose to die in foreign countries. Policies can have a lot to do with it and being clear about our principles. Ms. Sim highlighted that we should talk about **diversity**, instead of using the term "cultural".

Prof. Bicakci agreed with Ms. Sim and added that humiliation of people leads them being eliminated from the system. Although terrorism is a choice, we create the environment for that choice. We let the presence of the terrorists on the Internet but we are not throughout following their activities.

Dr. Sütalan added that it is not the issue of culture or religion, but how you keep up with terrorism. There are different causes of terrorism at different levels - there are about 200 variables for individual radicalization. Certain societies are always having fertile ground for terrorism. However, we know that there are no direct studies between economy and terrorism but indeed, money does matter when terrorists are provided with it. Everything is **contextual** and does not depend in certain culture or religion. With regard to Mother Schools, patriarchy is everywhere and patriarchical societies themselves differ.

4) What is the difference between extremism and terrorism? Is the definition related to nations' perception? Why is terrorism seen more severe threat than extremism? *Col Burak Dedeoğlu, TR*

Ms. Sim stressed that a person can have extremist beliefs but if one does not act on them, it does not mean that a person is breaking any laws. Radicalization can evolve into extremism and later on develop into terrorism by getting one's hands dirty with blood. A terrorist attack is always a criminal offense as well.

5) What is the link between a national strategy and the civil emergency plan or counter terrorism policies? *Lt.Col. Hamidou SOUMAH, MoD / Land Forces / Chief of Operation Center*

Ms. Sim added that national security strategies are statements of national goals, values and ambitions that a nation upholds. CT policies are about measures to be used to achieve strategic goals but we tend to use these terms interchangeably. However, many countries tend to publish their national CT strategies but do not share their operation plans with everybody.

Dr. Zeynep Sütalan
Gender, Terrorism and Counter terrorism

1) ***Are there studies which could give a percent ratio for women necessary to be involved in CT effort?*** *Capt. (N) Mihai Danila, Defense Staff/Operations Directorite, Romania*

Dr. Sütalan pointed out that there are no precise recent studies but agreed that *numbers* do matter by giving and idea if women are represented or not. It is known that about 10% of women are represented in police forces while this is 20% in Europe. These numbers are quite low and the number of women in CT are even lower than that. NATO average for women representation in militaries is around 11%. Prof. Yalcinkaya added that in Turkey, there is a desire for women to be part of a solution, as seen by the mothers of PKK terrorists in Diyarbakir.

2) ***Are women a positive or a negative factor in terrorism?*** *Col. El Husseini, General Directorate of State Security/Regional Directorate/Head of Regional Officce, Lebanon*

Regarding the role of women, Dr. Sütalan emphasized that women can be part of the problem as well as be part of the solution. Women as terrorists serve as a negative role while women as part of counter-terrorism are seen as having a positive role.

3) What is the relevance of gender sensitivity in cyber domain in the frame of defense against terrorism? Is there any benefit expected from the gender perspective in deterring or preventing cyber terrorism or cyber support of terrorist organizations? *Col. Soner Özer, NAOC*

Dr. Sütalan pointed out that there is a difference whether we talk about cyber terrorism which requires technical expertise or terrorist use of the Internet which refers to online matters. However, **cyber domain needs a gender sensitive approach** as the behaviors of women and men differ. In the 2019 COE DAT`s Women and CT workshop, the OSCE colleagues pointed

out that **artificial intelligence has been developing with pure male biases.** There are different patterns between male and female behavior in a social context and this needs to be recognized.

Prof. Bicakci added that it depends whether we are talking about an offender or a defender. As defenders, there are brave female coders and hackers. Some IT guys may even give keys to important software and service places and thus, be blinded by the female's beauty. We need to be careful about the issue and take care of our computers. Also, there is a difference in thinking and understanding between men and women, also in their reactions.

4) What could be an example of women becoming victims of implementation of CT Strategies? *Col. Marinov, Rakoski National Defense College, Bulgaria*

According to Dr. Sütalan, in a gender based violence, i.e. rape and harassment, women can be victims of CT strategy. Also, while utilizing hard power and hit terrorists in an operational environment, women can take the side of their husbands and get deprived. There are differential impacts to this.

Throughout the discussion, Dr. Sütalan added that the WPS agenda also includes the issue of children and minors. The issue of children in armed conflict has a different agenda. Mothers can indeed help to spot early warnings whether their children are becoming radicalized. However, WPS and children in armed conflict have two different agendas. Regarding the question of how CT strategy measures can promote gender equality, Dr. Sütalan stressed that in CT operations, the practice or norm itself would promote gender equality. CT measures at the operational and tactical level could be utilized for increasing consciousness.

5) How can counter-terrorism measures promote, rather than hinder, gender equality? 2nd Lt. Tracy CHEIBAN, MoD / Army Intelligence / Analyst, Romania

Female Engagement Teams can be an example of this by having positive encounters with the society. This can also increase consciousness in a local population and have a role in promoting gender equality. This also depends on a context.

Prof. Salih Bicakci

Cyber Security in the Domain of Counter-terrorism

1) What would you recommend to do to prevent a cyber attack from occurring in the first place? *Mr. McNally Stephen, NATO Intelligence Fusion Centre, GBR*

Prof. Bicakci highlighted that terrorist groups and their actions differ from culture to culture and from geography to geography. We live in an age of hybridity by using both analogue and digital tools and means to execute our goals. While it is acknowledged that **risk management** is expensive, it is needed to prevent the cyber attack. Overall, terrorism is a political science and international relations problem. Economic model of the world is changing. If we could have a silver bullet for the issue, would be great, but the reality is different. Computer systems also differ from each other. Preventing cyber attacks is hard - we are living in an age of identity.

2) ***What is a good way or strategy to use cyber domain in an offensive manner to deter terrorist organizations (especially those based on ideology or politically oriented ones)?*** *Col. Soner ÖZER NAOC, Compat Plans Division, Division Head*

When we talk about terrorist use of the Internet, there are threats we can see and threats we cannot see. Indeed, we can try to take them "out of the Internet" but if you deter terrorism, they can go use the Darkweb, for instance. If networks close, radicalization still grows - this is something we cannot see and it has to be balanced. Everyone has different intentions. For instance, Daesh talks to unemployed people and can convince them to go to Syria. We need to take control and focus on de-radicalization. We need to focus on intelligence sharing and law enforcement and let them communicate because otherwise terrorists will use political violence.

3) All presentations and conferences focus on terrorism and how we can treat it to determine and block its capabilities but why don't we focus on the reasons of the presence of terrorism? Why do we have terrorism? *Col. Khaled EL HUSSEINI, General Directorate of State Security, Regional Directorate, Head of Regional Office, Lebanon*

Prof. Bicakci emphasized that the problem with terrorism differs from culture to culture. Terrorism has become international due to processes globally - there are differences in terrorism between third and fourth wave. Stopping terrorism will not be possible but constraining and

countering is. Countering terrorism is hard - you need to be working with law enforcement and also focus on the economic and political side, it has no easy solution.

4) ***How do radicalized ideas get to the IT & Cyber specialist, making them radicalized individuals? What should be the part of the contingency plan when planning the reaction to a terrorist attack? What is the ratio between the planning prior and the planning at the time if the attack?*** *Col. Petar MARINOV, Rakoski National Defence College / Land forces / Associate professor, Bulgarian Armed Forces*

Prof. Bicakci stressed that terrorists are not really different from us - they are often highly educated. Radicalization is a process and involves a misinformation and disinformation campaign in which truth is not easily distinguished. Therefore, human resources in companies play an important role to follow and assess people for critical positions. Everyone has lots of plans when a terrorist attack took place but are often not prepared for it. Fear has an important aspect - fear affects us biologically. You have to tell people what to do. People are often shocked, not knowing what to do and thus want to go for an easy solution. During the current COVID-19 period, people sit at home and are on the Internet more than before. The person who usually sits in the security operations room is now sitting in his living room - thus, not being as secure as in normal circumstances. We have to focus on action plans and be ready for back ups.

Regarding **how the COVID-19 has affected the *modus operandi* of terrorist groups,** Prof. Bicakci added that during the current pandemic, people are separated and there is more risk between parties - we have not been trained for such pandemic. There is less communication between people We need more expertise in hospitals, we act like we are having old problems but the current COVID-19 situation is something new. New problems may be cybercrime and ransomware, also attacks on hospitals.

Ms. Sim commented that she does not agree that terrorists are changing their tactics because of the current pandemic - we have seen latest attacks on Kabul, for instance. However, SARS was nothing what we are seeing now with COVID-19 - **better preparedness is needed.** Dr. Sütalan added that youth and people are indeed spending much more time online during the current COVID-19 period - we should be aware of this and act accordingly. Prof. Yalcinkaya added that the current pandemic would not prevent terrorist attacks on the field, as seen also in Vienna.

5) What is the strategy to eliminate terrorism from our society and to protect our mind from terrorists' mental control? *Col. Mounir DAHER, General Directorate of State Security / VIP Directorate / Head Of Section, Lebanon*

Prof. Bicakci further highlighted throughout the discussions that we are dealing with a network centric warfare - extension of hybrid warfare. It has to form consciousness among all leaders. There are new understanding requirements from the battleground as well as need for training exercises. Decision makers in CT should also pay attention to changing of teams and mentality in order to adopt to changing nature of conflict. Dr. Ashraf reiterated throughout the presentation that it is not possible to eliminate terrorism throughout, **but rather constrain.**

Annex B – Day 2, Panel 2: "Domains of Terrorist Threats and Best Practices in Countermeasures" Presentations, Questions, and Answers

Contents

Weapons of Mass Destruction and Counter-Terrorism

by Prof. Dr. Mustafa Kibaroğlu

Defining the Nature of the Threat

The threat of use of weapons of mass destruction (WMD) in terrorist attacks is real and credible, and the realization of the threat is a matter of when, not if. Thus, countering WMD terrorism must gain prominence among the security policies of the concerned authorities.

Countering WMD terrorism requires effective and extensive inter-agency cooperation both within the state apparatus as well as between the states. Yet, one of the biggest hurdles in front of achieving this objective is the lack of like-minded leadership among the top decision makers in the international political arena.

Those who believe that terrorism with WMD is an exaggeration, if not a hype, emphasize that despite much propagation to that effect by scholars and experts in the field, there has not been any major incident to date. Some even believe that scenarios involving terrorist use of WMD have been propagated purposefully by Western intelligence agencies in order to incite fear among the less developed countries so as to manipulate their foreign and security policies.

Under such circumstances, where top political leaderships around the world underrate the threats emanating from the possibility of WMD and the material used in their manufacture falling into the hands of terrorist networks, it is unlikely for the rest of the world to effectively counter WMD terrorism.

Multilateral Efforts for Countering WMD Terrorism

One sure way to eliminate the possibility, and thus the probability of terrorism particularly with nuclear and radiological weapons would be to eliminate the availability of all nuclear and radiological material so as to keep them away from the reach of the terrorist groups. But, this is hardly possible due to the existence of huge number of nuclear weapons, large stocks of fissile material coming from weapons dismantlement programs as a result of the disarmament agreements between the United States and Russia, and the and nuclear power and research reactors that exist in many states.

Hence, preventing unauthorized access of terrorist groups to nuclear and radiological material must be the primary goal of the governments. Thus, disrupting the terrorist networks that are involved in the illicit trafficking of nuclear and radiological material becomes extremely crucial. In order to achieve this objective, various measures at different levels must be taken, extending from the individual level to global level, and with a long-term as well as short-term vision.

In that sense, one particular best practice example in countering WMD terrorism is the "Nuclear Security Summit" series launched by the then US President Barack Obama back in March 2010 that brought together some 50 world leaders in Washington DC. Among the issues that were tackled during the Summit was securing the excessive amounts of Highly Enriched Uranium (HEU), which is the basic ingredient of nuclear explosives, coming out of the weapons dismantlement programs involving the United States and the former Soviet Union republics where nuclear weapons were either produced and/or deployed in large numbers during the Cold war era and in its immediate aftermath.

At the 2010 and 2012 Nuclear Security Summits the participating countries have endorsed the consensus view that, given the security risks, the use of HEU outside military technologies should be minimized to the extent that it is technically and economically feasible. Several countries took individual steps to minimize or eliminate civil HEU. The Summit meetings have also taken place in 2014 in The Hague, and the last one in 2016 back in Washington DC, both of which have sustained the spirit and the momentum created in the previous ones. But, would this be enough for effectively countering WMD terrorism?

The long-term objective must be the total dismantlement of all nuclear, chemical and biological weapons. For this to happen, among other things, it is necessary to create a conducive environment in order to build confidence among nations so that in the long term they won't need WMD to rely on for protecting their vital interest. Hence, strengthening the existing non-proliferation regimes in the field of nuclear, chemical and biological weapons, must be the minimum condition in the medium term for building confidence so as to pave the way to peace accords between the conflicting parties in the long term.

Existing WMD nonproliferation treaties and conventions are the Nuclear Non-Proliferation Treaty (NPT – 1968), the Biological Weapons Convention (BWC – 1972), and the Chemical Weapons Convention (CWC – 1993). In the short term, new elements must be added to these regimes by negotiating and then concluding a Fissile Material Cut-Off Treaty

(FMCT), as well as the entry into force of the Comprehensive Nuclear Test Ban Treaty (CTBT), a verification mechanism of the BWC, and the universalization of the CWC.

Even if the objective of banning the military applications of science and technology that are used in the manufacture of nuclear, chemical and biological weapons would be possible, a variety of peaceful applications of science and technology in these fields will continue to exist in the long-term as well. Thus, the objective must be to secure also the nuclear, chemical, and biological material that will be used in the peaceful applications of science and technology, and to keep them out of the reach of the terrorists

A very important step in that direction has been the United Nations Security Council (UNSC) Resolution 1540, adopted unanimously in April 2004, calls on all states to take cooperative action to prevent trafficking of WMD. For Resolution 1540 to be effective in preventing transnational terrorist organizations from acquiring weapons of mass destruction, states must fully and effectively implement the binding decisions of the UNSC. But, to what extent the member nations will respond to the calls of the Council remains to be seen.

There is also the Proliferation Security Initiative (PSI), which is put in operation by the United States in May 2003 with the cooperation of friendly countries. PSI is a global initiative aimed at stopping shipments of WMD, their delivery systems, and related materials worldwide as well as to create a more dynamic, creative and proactive approach to preventing proliferation to or from states and non-state actors of proliferation concern by using existing legal authorities, national and international.

The Cooperative Threat Reduction (CTR) Program, also known as the "Nunn-Lugar Program" after the two US Senators, namely Sam Nunn (D, GA) and Richard Lugar, (R, IN) who have initiated the bill at the US Congress in the wake of the Cold War also need to be mentioned within this framework as well. Because they have been as useful as international treaties and UN conventions. The purpose of the CTR programs has been to help the former Soviet republics to destroy weapons of mass destruction and the associated infrastructure in order to reduce the chances of the material used in their manufacture falling into the hands of terrorist groups or some states of concern. Nunn-Lugar has been one particular domain of intensive cooperation and collaboration between the United States and Russia that has not been negatively affected by the deterioration of the relations between the two states in the post-Cold War era.

The Nuclear Security Guidelines (INFCIRC/225) of the International Atomic Energy Agency (IAEA), first issued in the 1970s, also are of fundamental importance. Although not mandatory, these guidelines are adopted by most states and have been made a requirement through bilateral agreements. In the same vein, the IAEA's Illicit Trafficking Database Program (ITDP), involving the voluntary notification by government authorities of illicit trafficking incidents, provides a valuable source of information that helps the member states to better understand threats and vulnerabilities.

The Convention on the Physical Protection of Nuclear Material and Nuclear Facilities of 1987, with 161 states parties and 44 signatories as of June 2020, requires states to implement measures to prevent theft, diversion or sabotage of nuclear material while being transported internationally. A 2005 Amendment extends the scope of the Convention to nuclear material in domestic use and storage, and to protection of nuclear facilities from sabotage.

Similarly, the International Convention for the Suppression of Acts of Nuclear Terrorism, which was adopted in 2005 by the United Nations, with Russia and the United States being the first countries to sign, must be endorsed by more states in addition to the 115 states which have signed and ratified it.

An equally important task should be to prevent the unauthorized transfer of nuclear expertise through the movement of trained personnel, including those in retirement. The risk of such personnel being recruited by terrorist groups is not negligible. In addition to the efforts of states and the international organizations, non-governmental organizations, the private sector must be engaged especially in addressing the inherent security risks associated with exporting advanced technologies, equipment, and material. The World Nuclear Association, and the World Institute for Nuclear Security (WINS), which is founded in Vienna in 2008, are such institutions that aim to share information and experience among the industry nuclear security professionals, as well as to promote training.

Nuclear forensics, which involves the analysis of nuclear material recovered from either the capture of unused material or from the radioactive debris following a nuclear explosion so as to identify the sources of the material and the industrial processes used to obtain them, should be encouraged. The ability to identify and trace specific nuclear materials and techniques through legal prosecution would have a deterrent in respect of nuclear terrorism. Terrorists do not need to produce and detonate radiological or nuclear weapons to achieve their goals. Cyber

attacks by sophisticated terrorists on the command and control centers of nuclear-armed states is a significant threat.

Turkey's Policy and Practice in Countering WMD Terrorism

It goes without saying that finding ways to stem further proliferation of WMD is in Turkey's primary interest. Therefore, Turkey assists international efforts to strengthen the non-proliferation regimes as well as to counter the threat posed by the presence of non-state actors that are known to pursue WMD capability.

In line with its general stance against proliferation of WMD, Turkey has declared its support to the Proliferation Security Initiative (PSI) as soon as it was launched by the United States in May 2003. Turkey, while following other PSI activities, has itself hosted land, sea and air interdiction PSI exercises, first in May 2006 and in successive years with the participation of dozens of guest nations and continues to actively contribute to the PSI.

Pursuing an active policy against terrorism, Turkey joined, as initial partner state, the Global Initiative to Combat Nuclear Terrorism (GICNT). Ankara hosted the Initiative's second meeting in 2007.

Turkey has also welcomed the UN Security Council Resolution 1540, and with a view to fulfilling the provisions of international non-proliferation instruments and arrangements to which Turkey is party, an enhanced system of export controls is implemented. Turkey submitted its first report in November 2004 and has regularly updated its reports over the years. Last update has been made in August 2020. This living document requires updates as changes take place in legislation and international commitments. Due to delays caused by the coronavirus pandemic, all activities related to Comprehensive Review on the status of implementation of resolution 1540, including the open consultations, is postponed until 2021

Turkey has also taken a number of steps to counter illicit trafficking, such as acceding to the Nuclear Suppliers Group (NSG) in 1999. Accordingly, Turkey has undertaken the process of adjusting its national export control regime (i.e., laws and regulations) to that of the NSG countries. Currently, the Turkish export controls system is in line with the European Union's standards. Turkish national legislation, developed in the context of the country's safeguards agreement and other IAEA protocols, provides Turkish authorities with the legal basis to control the materials and equipment covered by the list of the NSG.

Concomitantly with its application to the NSG, Turkey has undertaken the same stance toward the Zangger Committee and became a member soon after its application in 1999. This has been considered by Turkish security authorities as almost an automatic outcome of the formal accession to the NSG.

Turkey also joined the Australia Group in 1999. Since, it has taken steps to include the items of the list, which indeed differ by one or two items from the other universal export control lists.

Turkey became a member of the Missile Technology Control Regime (MTCR) in April 1997. Since, Turkish delegations have been active in participating the meetings of member states as well as promoting new ideas with a view to rendering the controls much more effective. In this context, the Turkish security elite believe that it is essential to demonstrate to the actual and potential proliferators that the MTCR is a solid block of like-minded nations which are unified with the determination to fight against proliferation.

Turkish law enforcement authorities cooperate with international agencies such as INTERPOL to promote national and regional interagency to counter nuclear smuggling. Turkey is also a participant of the U.S. State Department's Export Control and Related Border Security Program (EXBS) and provides radiation interdiction training and equipment to Turkish law enforcement agencies.

Turkish authorities maintain that the success of the above-mentioned export control regimes will depend on the continuous and coordinated exercise of vigilance and restraint in the transfers especially to the regions of concern. Similarly, the collective capability of the regime to foresee developments and to be proactive in devising measures to reverse threatening proliferation trends is also crucial for successful implementation of export control regimes.

For its part, Turkey has devised and implements an export control system, which is based on continuous inter-agency coordination and consultation, which involves the Exporters' Unions, Under-Secretariat of Foreign Trade, Under-Secretariat of Customs and the Ministry of Foreign Affairs, Ministry of Defense, and the Ministry of Economy. By the interaction of these agencies within a mutually reinforcing multi-layered system of licensing, registration and control, Turkey could effectively track the movement of listed items in and out of the country.

The export of sensitive and dual-use materials covered by international instruments and export regimes is controlled by virtue of a two-tier mechanism that involves separate processes

of licensing by the Ministry of National Defense for military equipment, arms and ammunition and the Nuclear Regulatory Authority for dual use items described in the NSG control list; and registration by the Ministry of Economy.

For military equipment, arms and ammunition, the first tier is regulated by the Law Number 5201 dated July 03, 2004, which replaced original Law Number 3763 of 1940 regarding "The Control of Private Industrial Enterprises Producing War Weapons, Vehicles, Equipment and Ammunition". This law requires licenses to be obtained from the Ministry of National Defense for the export of all weapons and ammunition. The Ministry of National Defense issues every year a list of all weapons, ammunition, explosive materials and their parts, which are subject to licensing. Items listed in the NSG list, are regulated by the "Regulation on Export Licensing of Materials, Equipment and Related Technologies Employed in the Nuclear Field" published in the *Official Gazette* on February 15, 2000, No: 23965, and updated in 2007 (*Official Gazette* No. 26642 on September 19, 2007).

As to the second tier, it is the duty of the Ministry of Economy to take all monitoring, control, arrangement and orientation measures regarding exports and to draft the general export policy of Turkey. In fulfilling its duties, the Ministry of Economy avails itself of the 13 exporters' unions located around the country. Istanbul Metals and Minerals Exporters' Union (IMMIB), like other exporters' unions, is responsible for the implementation of the general export policy, under the auspices of the Ministry of Economy. All exporters are required to be a member of an exporters' union in order to be able to export any good or material.

Sensitive goods, technologies and dual-use materials are registered by IMMIB, which denotes this registration on the customs declaration. This mechanism enables a centralized monitoring of the export of sensitive goods, technologies and dual-use materials on the basis of exporting company, product, quantity and value. IMMIB determines whether or not the good to be exported is subject to export controls. If so, then this export is submitted to the procedure described above, where permissions from relevant institutions are sought.

Conclusion

Non-proliferation and counter proliferation efforts spent in the international arena have much in common. They both aim at saving the world from the scourge of catastrophic consequences of possible uses of WMD by states or non-state actors. But, they also differ in

many ways, mainly due to the dissatisfaction of some members with the effectiveness of the treaties or conventions in terms of achieving the objectives set out in the articles. This paper touched upon the multilateral efforts for countering WMD terrorism and also presented Turkey's policies and practices in these respects, all of which will be further elaborated in the final and longer version of the chapter.

a. Presentation

WEAPONS OF MASS DESTRUCTION (WMD)

NUCLEAR WEAPONS

Explosive devices that release huge amounts of energy and radiation achieved by splitting the fissile material (HEU and/or Plutonium) resulting in a self-sustained chain reaction

CHEMICAL WEAPONS

Toxic chemical substances, such as choking, blister, blood, and nerve agents that cause incapacitation, injury or death of the target population including humans, animals, and plants

BIOLOGICAL WEAPONS

Infectious diseases caused by micro-organisms, such as viruses, bacteria and fungi that cause incapacitation or death of the target population including humans, animals, and plants

THREAT OF TERRORISM WITH WMD: HYPE OR REALITY?

Threat emerges as a combination of intentions and capabilities

Intentions exist in states even if not declared

Non-states have already declared their intentions

Advancements in science and technology help states and non-states to develop and/or acquire capabilities

The THREAT of use of WMD by terrorists is NOT a HYPE, it is REAL and it is believed by many experts to be a matter of "WHEN NOT IF"

Countering WMD Terrorism

THE THREAT POSED BY WMD TERRORISM IS REAL, *BECAUSE …*

Chemical, Biological, Radiological, Nuclear (CBRN) weapons and/or material used in their manufacture are accessible

The profile of terrorist organizations change, and they are able to recruit "scientists" and "experts" to exploit emerging opportunities

Religious or mystic beliefs boost recruits, and deterrence has limited, if any, effect to prevent such terrorist groups from resorting to WMD

Terrorist organizations do not need sophisticated weapons systems, as "crude" or "dirty" weapons, such as Radiological Dispersal Devices (RDD), may be sufficient for them to achieve their goals

Countering WMD Terrorism

THE THREAT POSED BY WMD TERRORISM IS REAL, *BECAUSE …*

Means and methods of attack may require simple machinery or techniques. Dispersing a chemical or biological agent can be carried out by agricultural sprayers, ventilators, civilian aircraft

Effects of biological agents are delayed giving enough time to terrorist to hide away without a trace

Metropoles and other residential areas are vulnerable to terrorist attacks due to low level of security checks. Industrial facilities, critical infrastructure, harbors, airports may be the primary targets

Contingencies that involve the use of WMD in terrorist attacks are "LOW PROBABILTY vs HIGH CONSEQUENCE" scenarios

DIFFICULTIES IN TAKING MEASURES AGAINST WMD TERRORISM

One sure way to eliminate the possibility of terrorism with WMD would be to eliminate the availability of all nuclear, chemical, and biological material that can pass into the hands of terrorist groups. But, this is not possible due to the existence of:

..WMD stockpiles in a number of states

..Material coming from dismantlement of weapons

..Nuclear power and research reactors

..Dual-use chemical and biological facilities

..Nuclear, chemical, biological research laboratories

DIFFICULTIES IN TAKING MEASURES AGAINST WMD TERRORISM

Even if the long term objective of banning the military applications of science and technology that are used in the manufacture of nuclear, chemical and biological weapons, various forms of peaceful applications of science and technology in each of these fields will continue exist in the foreseeable future

Thus, the immediate and the short term objective must be to secure the nuclear, chemical, and biological material that will be used in peaceful applications of science and technology, as well as to keep them out of the reach of terrorist organizations

In order to achieve this objective, various measures must be put in place extending from the individual state level to global level, and with a long term as well as medium and short term vision

MULTILATERAL MEASURES TO COUNTER WMD TERRORISM

COOPERATIVE THREAT REDUCTION PROGRAM

The Cooperative Threat Reduction (CTR) program, also known as "Nunn-Lugar" after the two US Senators who have initiated the program in 1991, is a pioneering example in regard to countering WMD terrorism

The purpose of the CTR programs has been to help the former Soviet republics to secure and dismantle the weapons of mass destruction and the associated infrastructure in order to reduce the chances of the material used in their manufacture falling into the hands of terrorist groups or some states of concern

United States and Russia have established institutional "government to government" and "lab to lab" links for effective cooperation and collaboration between the concerned parties

MULTILATERAL MEASURES TO COUNTER WMD TERRORISM

PROLIFERATION SECURITY INITIATIVE

The proliferation Security Initiative (PSI) is a global initiative aimed at interdicting shipments of WMD, their delivery systems, and related materials worldwide

Announced in May 2003 by the US President George W. Bush, PSI originates in the US National Strategy to Combat Weapons of Mass Destruction, issued in December 2002, which recognizes the need for more robust tools to defeat the proliferation of WMD around the world

The goal of PSI is to create a more dynamic, creative and proactive approach to preventing proliferation to or from states and non-state actors of proliferation concern by using existing legal authorities, both national and international

MULTILATERAL MEASURES TO COUNTER WMD TERRORISM

PROLIFERATION SECURITY INITIATIVE

21 states have formed the Operational Experts Group* (OEG) with a view to having an essential role in ensuring the effectiveness of the PSI by:

...leveraging related counter proliferation efforts;

...contributing customs, law enforcement, military and other security experts and assets to interdiction exercises;

...hosting PSI meetings, workshops, and exercises with other PSI-endorsing states; and

...working with specific partner states to improve their capacity to combat the proliferation of WMDs**

**OEG countries: Argentina, Australia, Canada, Denmark, France, Germany, Greece, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Poland, Portugal, Russia, Singapore, Spain, Turkey, United Kingdom, United States*

***https://www.psi-online.info/*

MULTILATERAL MEASURES TO COUNTER WMD TERRORISM

UNITED NATIONS SECURITY COUNCIL RESOLUTION 1540

The UNSC Res 1540, adopted unanimously on 28 April 2004, calls on all states to take cooperative action to prevent trafficking of WMD: It

8. Calls upon all States:

a.. To promote the universal adoption and full implementation, and, where necessary, strengthening of multilateral treaties to which they are parties, whose aim is to prevent the proliferation of nuclear, biological or chemical weapons

b.. To adopt national rules and regulations, where it has not

c.. To renew and fulfill their commitment to multilateral cooperation, in particular within the framework of the IAEA, the OPCW and the BTWC, as important means of pursuing and achieving their common objectives in the area of non-proliferation and promoting international cooperation for peaceful purposes

MULTILATERAL MEASURES TO COUNTER WMD TERRORISM

UNITED NATIONS SECURITY COUNCIL RESOLUTION 1540

9. Calls upon all States to promote dialogue and cooperation on nonproliferation so as to address the threat posed by proliferation of nuclear, chemical, or biological weapons, and their means of delivery

10. Further to counter that threat, calls upon all States, in accordance with their national legal authorities and legislation and consistent with international law, to take cooperative action to prevent illicit trafficking in NBC weapons, their means of delivery, and related materials

For the Resolution 1540 to be effective in preventing transnational terrorist organizations from acquiring WMD, states must fully and effectively implement the binding decisions of the UN Security Council

MULTILATERAL MEASURES TO COUNTER WMD TERRORISM

NUCLEAR SECURITY SUMMITS

One particular initiative in countering WMD terrorism is the "Nuclear Security Summit" series launched by the US President Barack Obama who brought together some 50 world leaders in Washington DC in March 2010

Among the issues that were tackled during the first Summit was securing the excessive amounts of Highly Enriched Uranium (HEU) coming out of the weapons dismantlement programs, involving the United States and the former Soviet Union republics, where nuclear weapons were either produced and/or deployed in large numbers during the Cold war era and in its immediate aftermath

MULTILATERAL MEASURES TO COUNTER WMD TERRORISM

NUCLEAR SECURITY SUMMITS

At the 2010 and 2012 Nuclear Security Summits the participating countries have endorsed the consensus view that, given the security risks, the use of HEU outside military technologies should be minimized to the extent that it is technically and economically feasible

Several countries took individual steps to minimize or eliminate their civil HEU stocks at their disposal

The Summit meetings have also taken place in 2014 in The Hague, and the last one in 2016 again in Washington DC, both of which have sustained the spirit and the momentum created in the previous ones

INSTITUTIONAL MEASURES TO COUNTER WMD TERRORISM

THE ROLE OF INTERNATIONAL INSTITUTIONS

The role that some international institutions, such as the International Atomic Energy Agency (IAEA), and the Organization for the Prohibition of Chemical Weapons (OPCW) do play is quite significant

The IAEA's Nuclear Security Guidelines (INFCIRC/225), first issued in the 1970s, are of fundamental importance

Although not mandatory, these guidelines are adopted by most states and have been made a requirement through bilateral agreements

INSTITUTIONAL MEASURES TO COUNTER WMD TERRORISM

THE ROLE OF INTERNATIONAL INSTITUTIONS

The IAEA's Illicit Trafficking Database Program (ITDP), involving the voluntary notification by government authorities of illicit trafficking incidents, provides a valuable source of information that helps the member states to better understand threats and vulnerabilities

As of January 2019, the ITDB contained a total of 3497 confirmed incidents of which there are 285 incidents that involved a confirmed act of trafficking or malicious use (Group I), 965 incidents for which there is insufficient information to determine if it is related to trafficking or malicious use (Group II) and 2247 incidents that are not related to trafficking or malicious use (Group III).*

****IAEA Incident and Trafficking Database Incidents of nuclear and other radioactive material out of regulatory control 2019 Fact Sheet***

INSTITUTIONAL MEASURES TO COUNTER WMD TERRORISM

THE ROLE OF INTERNATIONAL INSTITUTIONS

The Convention on the Physical Protection of Nuclear Material and Nuclear Facilities (CPPNM) of 1987, with 159 parties and 44 signatories, obligates parties to make specific arrangements and meet defined standards of physical protection for international shipments of nuclear material for peaceful purposes (plutonium, uranium 235, uranium 233 and irradiated fuel), according to Annexes I and II and IAEA INFCIRC/225,as well as to implement measures to prevent theft, diversion or sabotage of nuclear material while being transported internationally

A 2005 Amendment extends the scope of the Convention to nuclear material in domestic use and storage, and to protection of nuclear facilities from sabotage

INSTITUTIONAL MEASURES TO COUNTER WMD TERRORISM

THE ROLE OF NONGOVERNMENTAL ORGANIZATIONS

In addition to the efforts of states and international organizations, non-governmental organizations and the private sector must be engaged especially in addressing the inherent security risks associated with exporting advanced technologies, equipment, and material

The World Nuclear Association, and the World Institute for Nuclear Security (WINS), which is founded in Vienna in 2008, are such institutions that aim to share information and experience among the industry nuclear security professionals, as well as to promote training

INSTITUTIONAL MEASURES TO COUNTER WMD TERRORISM

THE ROLE OF NONGOVERNMENTAL ORGANIZATIONS

Nuclear forensics, which involves the analysis of nuclear material recovered from either the capture of unused material or from the radioactive debris following a nuclear explosion so as to identify the sources of the material and the industrial processes used to obtain them, should be another area that should be encouraged

The ability to identify and trace specific nuclear materials and techniques through legal prosecution would have a strong deterrent function in respect of nuclear terrorism

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

CONTOURS OF TURKEY'S POLICY TO COUNTER WMD TERRORISM

Turkey assists international efforts to strengthen the non-proliferation regimes as well as to counter the threat posed by the presence of non-state actors that are known to pursue WMD capability

Turkey has declared its support to the PSI as soon as it was launched by the United States in May 2003. Turkey, while following other PSI activities, has itself hosted land, sea and air interdiction PSI exercises in May 2006

Pursuing an active policy against terrorism, Turkey joined, as initial partner state, the Global Initiative to Combat Nuclear Terrorism (GICNT). Ankara hosted the Initiative's second meeting in 2007

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

CONTOURS OF TURKEY'S POLICY TO COUNTER WMD TERRORISM

Turkey has welcomed the UN Security Council Resolution 1540, and submitted its first report in November 2004

Turkey has regularly updated its reports over the years and the last update has been made in August 2020

This living document requires updates as changes take place in legislation and international commitments. But, due to delays caused by the coronavirus pandemic, all activities related to Comprehensive Review on the status of implementation of resolution 1540, including the open consultations, is postponed until 2021

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

CONTOURS OF TURKEY'S POLICY TO COUNTER WMD TERRORISM

Turkey has also taken a number of steps to counter illicit trafficking, such as acceding to the Nuclear Suppliers Group (NSG) in 1999

Accordingly, Turkey has undertaken the process of adjusting its national export control regime (i.e., laws and regulations) to that of the NSG countries

Currently, the Turkish export controls system is in line with the European Union's standards

Turkish national legislation, developed in the context of the country's safeguards agreement and other IAEA protocols, provides the legal basis to control the materials and equipment covered by the list of the NSG

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

CONTOURS OF TURKEY'S POLICY TO COUNTER WMD TERRORISM

As almost an automatic outcome of its accession to the NSG, Turkey has undertaken the same stance toward the Zangger Committee and became a member soon after its application in 1999

With the same logic, Turkey joined the Australia Group in 1999, and it has taken steps to include the items of the list, which indeed differ by one or two items from the other universal export control lists.

Turkey also became a member of the Missile Technology Control Regime (MTCR) in April 1997 and has been actively participating in the meetings of member states with a view to promoting new ideas so as to render the controls much more effective

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

TURKEY'S EXPORT CONTROL MECHANISM

Turkish law enforcement authorities cooperate with international agencies such as INTERPOL to promote national and regional interagency to counter nuclear smuggling

Turkey is also a participant of the U.S. State Department's Export Control and Related Border Security Program (EXBS) and provides radiation interdiction training and equipment to Turkish law enforcement agencies

Turkish authorities maintain that the success of the above-mentioned export control regimes will depend on the continuous and coordinated exercise of vigilance and restraint in the transfers especially to the regions of concern

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

TURKEY'S EXPORT CONTROL MECHANISM

Turkey has devised and implements an export control system based on continuous inter-agency coordination and consultation among the Ministry of Foreign Affairs, Ministry of National Defense, Ministry of Economy, Ministry of Trade, Ministry of Agriculture and Forestry, National Intelligence Agency, Nuclear Regulatory Authority, and the Exporters Unions

By the interaction of these agencies within a mutually reinforcing multi-layered system of licensing, registration and control, Turkey could effectively track the movement of listed items in and out of the country

The export of sensitive and dual-use materials is controlled by a two-tier mechanism that involves separate processes of licensing by the MND for military equipment, arms and ammunition and the NRA for dual use items described in the NSG control list; and registration by the Ministry of Economy

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

TURKEY'S EXPORT CONTROL MECHANISM

For military equipment, arms and ammunition, the first tier is regulated by the Law Number 5201 dated July 03, 2004, which replaced original Law Number 3763 of 1940 regarding "The Control of Private Industrial Enterprises Producing War Weapons, Vehicles, Equipment and Ammunition". This law requires licenses to be obtained from the Ministry of National Defense for the export of all weapons and ammunition

The Ministry of National Defense issues every year a list of all weapons, ammunition, explosive materials and their parts, which are subject to licensing. Items listed in the NSG list, are regulated by the "Regulation on Export Licensing of Materials, Equipment and Related Technologies Employed in the Nuclear Field" published in the Official Gazette on February 15, 2000, No: 23965, and updated in 2007 (Official Gazette No. 26642 on September 19, 2007)

Countering WMD Terrorism

TURKEY'S COUNTERMEASURES

TURKEY'S EXPORT CONTROL MECHANISM

As to the second tier, it is the duty of the Ministry of Economy to take all monitoring, control, arrangement and orientation measures regarding exports and to draft the general export policy of Turkey

In fulfilling its duties, the Ministry of Economy avails itself of the exporters unions located around the country

Istanbul Metals and Minerals Exporters Union (IMMIB), like other exporters' unions, is responsible for the implementation of the general export policy, under the auspices of the Ministry of Economy

All exporters are required to be a member of an exporters union in order to be able to export any good or material

TURKEY'S COUNTERMEASURES

TURKEY'S EXPORT CONTROL MECHANISM

Sensitive goods, technologies and dual-use materials are registered by IMMIB, which denotes this registration on the customs declaration

This mechanism enables a centralized monitoring of the export of sensitive goods, technologies and dual-use materials on the basis of exporting company, product, quantity and value

IMMIB determines whether or not the good to be exported is subject to export controls. If so, then this export is submitted to the procedure described above, where permissions from relevant institutions are sought

Thank you for your attention ☺

Media and Counter-Terrorism

by Dr. Afzal Ashraf and Stephanie Fogget

Our study has indicated that there are few examples of good practise in terms of Counter terrorism (CT) and the media, certainly in a military context. Those that exist, appeared to be successful in a limited sense in terms of time and the targeted audience. Those practises also suffer from blowback in terms of creating a misleading context within which CT operations can take place and also in terms of contaminating the long term reputation of the military with the failures or errors of short term political leadership. Good practise, by definition, can only continue to be effective if the conditions within which that practise is developed remains unchanged. The nature of the terrorist threat is evolving and so CT operations are also adapting. The nature of mass media is changing dramatically as is the relationship that various consumers of mass media have with it. Given these and other evolutions, it is unsurprising that few examples of best practise can be identified. However, this study does offer some best principles which could be applied to future CT media strategies to improve their effectiveness. These come from both a military and a civilian context and are chosen for their possible adaption to the counter terrorism scenario.

We accepted the definition of best practice as "a technique, an activity, a strategy, a methodology or approach that has been shown, through application and evaluation, to be effective/and or efficient in achieving a desired result." The few such examples that existed were evaluated by looking at what the history of terrorism can teach us about our attitudes and assumptions about terrorism. We also looked at how terrorists take advantage of contemporary channels including TV, radio and traditional press and media. The relationship between conventional mass communications and online, especially social media, communications was explored to determine the increasingly interdependent nature of these two mediums. This approach allowed us to develop an understanding of the principles, which rarely change, and of the practice, which must adapt to a continually evolving threat and context.

A historical approach reveals that international terrorism and attempts to counter it both military and political go back over a century. There is a propensity for analysts to be mesmerised by the medium at the expense of the message. The majority of CT analysis in the military context is rightly focussed on identifying *who* poses a threat and *what* that threat is so that it can be effectively countered. In the media or communication context that

analysis should aim to understand *why* the threat exists and *how* it should be stopped. All terrorism is designed to convey a message and knowing what that message is provides a basis for countering not just the message but the underlying rationale of the terrorists.

In the context of CT related conflict, it may be helpful to think in terms of one of Clausewitz' trinities: Peoples passion, Political rationality and military judgement. All of these are mediated through communication, usually through the media. The overall responsibility for the conflict rests with political power with the military responsible only for military judgement. In recent conflicts involving CT, the division of responsibility has not been clear and the military has tended to present or support political decision-making as well as speaking directly to the people of nations involved in the conflict. It would be appropriate for the military to communicate only those matters that affected military judgement, both in terms of Military aspects of the CT threat and its responses to them.

One of the major challenges in CT operations is responding to allegations of or to the actuality of collateral damage or military mistakes. Failure to do so effectively can result in an advantage for terrorists. For example, the Kunduz incident, where a large number of civilians were killed by an air strike was responded to by the Taliban setting up an 'inquiry' which resulted in a report indicating an objective, critical and emotive approach impressing both at the national and, to some extent, at the international level. Other incidents involving civilian casualties have also tended to be responded to slowly, after detailed investigations have taken place. By that time any admission of failure or compensation is ineffective because the terrorists and others fill the information gap with allegations of deliberate targeting and cover ups. To avoid such situations, some generals have responded by adopting an active, sympathetic and affective approach involving immediate condolences to the families of the victims and assurances of best endeavour to avoid similar mistakes. This approach also adopts the mantra "first with the news" (as long as accuracy is not compromised) and "first with the truth." However, these good practises have not necessarily been maintained by other leaders.

At the domestic level, the US government has successfully misrepresented al Qaeda's strategic narrative, causing considerable frustration to that terrorist organization. However, it has not been as successful in countering al Qaeda's (AQ) narrative in non-western parts of the world. Indeed, the very act of CT in the form of the War on Terror has legitimised AQ's narrative in many parts of the world. Furthermore, the very effectiveness of this misrepresentation of AQ's narrative as an existential and non-negotiable threat to

Western interests has indoctrinated many involved in military ops, constraining their ability to think more accurately and widely about the range of choices and operational courses of action in support of their communication strategy. It is important, therefore, to have a mechanism whereby militaries involved in CT do not become victims of the propaganda of their own side.

In major CT related operations there is sometimes pressure to construct messages and actions to aid political objectives. For example, during the Iraq war the US government needed to present the growing insurgency to publics as being a foreign fighter phenomenon rather than an organic uprising. A media strategy was devised, involving military commanders, to paint Abu Masab Al Zarqawi as a major insurgent leader when in fact he led a relatively small group at the time. The long term impact of this was that it greatly benefited him and AQ in terms of profile and it presented the Coalition with a greater CT challenge in the long term.

The contemporary media landscape has witnessed dramatic changes. There is a complex fusion and interplay between mass media, social media and communication applications on the Internet. There are no distinct boundaries between them and it is almost impossible to devise distinct or separate strategies for mass media and social media. Overall, there has been a shift from one way communication to two way communication. There has been a change from slightly delayed editorially mediated content to unfiltered and immediate access to information. Most significantly, there has been self-imposed segregation in both mass media and social media with groups of people gravitating towards sources of information that reinforce, rather than challenge their worldview, beliefs and prejudices. This situation creates echo chambers and serves to isolate and inoculate groups from counter messages.

These changes have represented both a challenge and an opportunity. Evidence indicates that terrorists have been able to adapt and exploit these opportunities. Despite considerable resources and much effort by way of initiatives, states and militaries have yet to demonstrate sustainable successes in the exploitation of this new media environment in the CT context. Many media strategies are based on unproven hypothesis such as counter narrative initiatives. There is also a problem with the measurement of effect with such activities meaning that there is little reliable data to suggest that success has been or could be delivered.

The available literature is rich on the matter of *how* terrorists use traditional and new media, including for propaganda, radicalization, recruitment, fundraising, communications, and operations. Less apparent is evidence to explain *how* their use and exploitation of media leads to violent action and *what* serves as an effective government response.

The following are some non-military examples of communications principles or practices that might be adapted for a military context:

1. **Lessons and evidence on what actually works from public health campaigns:** "There is a substantial and growing literature around the role media producers can play in promoting social cohesion, encouraging more inclusive participation in public discussion, and increasing knowledge."[1]

2. **Public-private partnerships & critical infrastructure model:** "There are clear benefits in taking lessons learnt from longstanding efforts on terror financing into account when developing a response to the online terrorist threat." View the online space more in line with critical infrastructure and develop partnerships and policies related to counter-terrorism similar to financial sector, cyber defence, etc.

3. **The importance of community/local in many successful security-related campaigns:** "Adopt a multi-stakeholder approach between Governments, the ICT industry and civil society organizations in preventing and countering violent extremism and terrorism online"[2]

4. **Learning from market research and 'Madison Avenue' advertisers:** "While social media is still relatively new (Twitter launched in 2006), many of the best practices for using it are based on well understood marketing approaches. … social media campaign must be part of a broader marketing strategy, whether to sell more

[1] Baruch et al., 'Evaluation in an Emerging Field'.
[2] The Global Counterterrorism Forum (GCTF), 'Policy Toolkit: The GCTF Zurich-London Recommendations on Preventing and Countering Violent Extremism and Terrorism Online'.

shoes of a particular brand or to convince at-risk populations not to engage in violent extremist behaviour."[3]

Conclusions

We recommend that the principle of Politics has Primacy should be applied to CT media strategies so that they are subordinate to and aligned with the CT political narrative. There should be a clear distinction of responsibility and transparency of ownership between the narrative relating to political rationale and those targeting the people's passions from those that relate purely to military judgement. The military should avoid straying outside its area of responsibility.

Commander's Intent should also be expressed in terms of the "Message I want to Send is…" That way, media becomes a strategic objective rather than a Line of Ops. As with other aspects, media ops should involve seamless coordination between tactical, operational, strategic and grand strategic levels of command. In a coalition situation, sideways alignment between nations is equally important.

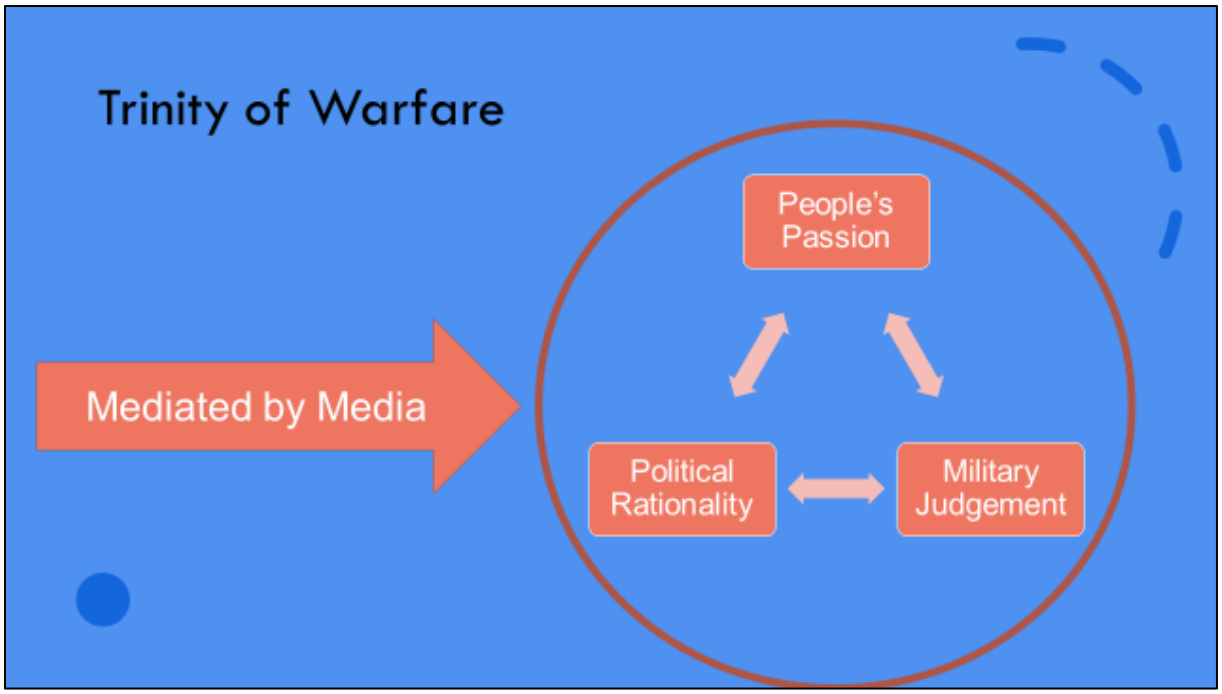
Effective messaging can change behaviour, which can be difficult to reverse afterwards. It is therefore important to avoid being tempted by short term gain when it could lead to long term pain. This point is linked to the need to clearly differentiate between military and political messaging and areas of responsibility. In democracies when political power demonstrates failure, its reputation declines and it is usually replaced. The military is mostly an enduring institution whose reputation remains with it. Reputation is key in determining a military's coercion and deterrence capability and should not be contaminated by political failure. Militaries should defend their reputation during CT operations by making it clear, through the media, what the military is responsible for and what the political power is responsible for.

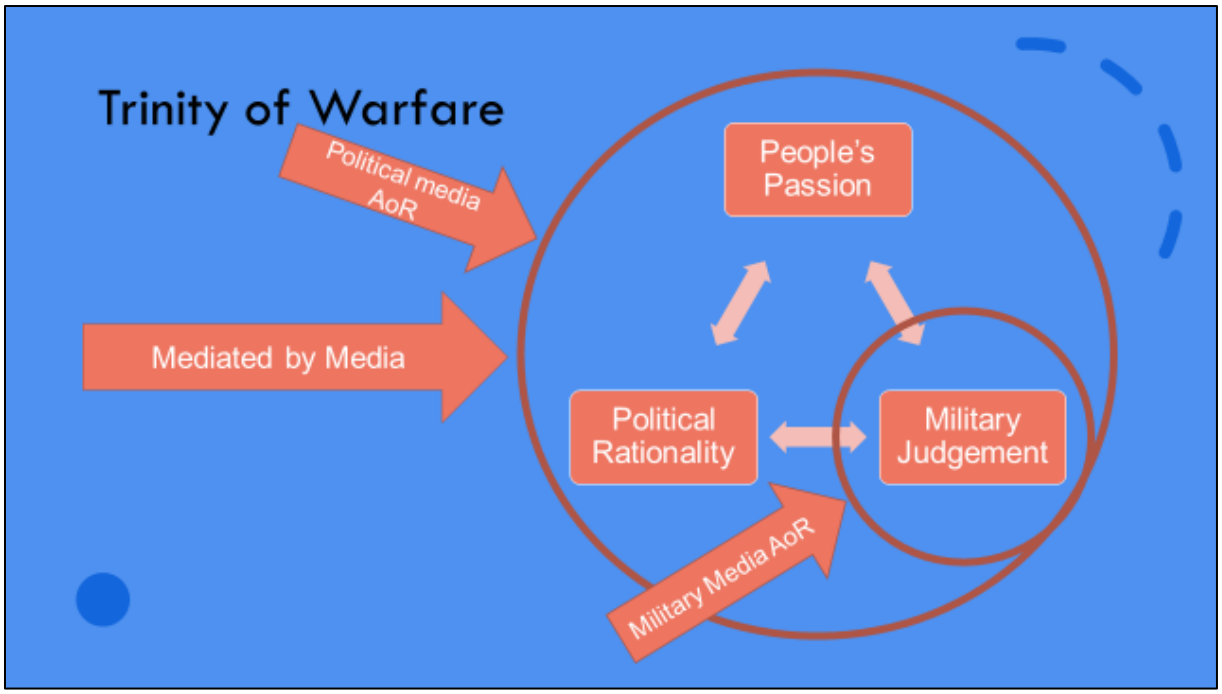
It is important for militaries' message effectiveness for them to gain the reputation for being "First with the News" and "First with the Truth." NATO CT commanders should understand the principles and practices, outlined in this study, that have been successfully used by both militaries and commercial organizations so that they can effectively adapt them to a particular ops environment.

[3] Helmus and Bodine-Baron, 'Empowering ISIS Opponents on Twitter'.

b. Presentation


Context – Best Practice or Best Principles
More examples of Poor Practice than Good Practice
All examples of Good Practice have Blowback
Lessons: Go for Bespoke Practice
By Adopting Best Principles


Trinity of Warfare
Mediated by Media
People's Passion
Political Rationality
Military Judgement



History Relevance

- **New** Analysts: Mesmerised by **Medium** not **Message**
- Incompletely understood as:
  - Internet and social media,
  - Al Qaeda and ISIS ideology or,
  - Religion
- Historical approach:
  - Exposes continuities & discontinuities
  - Understand and challenge own Assumptions about Threats

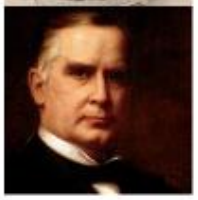
Deed or Discourse?

- Pisacane's "propaganda of the deed"
- A Smokescreen
- Pisacane's statement was Propaganda Supporting Revolutionary Terrorism
- Deeds are for Discourse (message)

Global Terrorism is not New Anarchist Assassinations








- French President Carnot in 1894 — 1894
- Austrian Empress Elisabeth 1898 — 1898
- President William McKinley 1901 — 1901
- 1897 — Spanish Prime Minister Cánovas 1897
- 1900 — Italian King Umberto I 1900
- 1914 — Archduke Franz Ferdinand 1914

International CT is not New

Pan-European conference – Rome 1898

- Int Terrorism Dangers recognised through laws passed by:
- France, Spain, Italy, Germany, Switzerland and several other countries …
- Aimed at controlling anarchist:
  - Propaganda
  - Use of explosives
  - Travel and Extradition

Taliban Media Response to Kunduz

- Appointed Fact-Finding Committee
- Report Covers
  - How Incident Occurred
  - All Killed were Civilians
  - White Phosphorous Used
  - Details of 79 Victims – Final toll unknown
- *"And when it is said to them: 'Make not mischief on the earth,' they say: 'We are only peace Makers." "Verily! They are the ones who make mischief, but they perceive it not." [Qur'an 2:11-12]*

Objective, Critical and Emotive

Traditional Reaction

- IED Incident 3 Mar 07 Nangahar province
- Marine Spec Ops Reaction: 12 Civilians dead
- Afghan Spec Ops Cmdr, Maj Gen Francis Kearney Apologizes but:
- Marine Gen James Conway:
  - *"I would just as soon that no one - in any chain of command - apologize or talk about 'terrible, terrible mistakes' or those types of wrong doings,"*
  - *"Presumption of innocence every service member enjoys."*

Parochial, Unsympathetic and Passive

The New Approach

- Gen McChrystal: "*We are extremely saddened by the tragic loss of innocent lives. I have made it clear to our forces that we are here to protect the Afghan people, and inadvertently killing or injuring civilians undermines their trust and confidence in our mission. We will redouble our efforts to regain that trust.*"

Active, Sympathetic and Effective

Vice-Admiral William McRaven apologizing to Haji Sharabuddin

Successful Counter Narrative?

"You ransack our lands, stealing our treasures and oil, simply because of the pressure you exert via your international influence and military threats." Bin Ladin's 'Letter to the American People' 26 Oct 02

"They hate our freedoms--our freedom of religion, our freedom of speech, our freedom to vote and assemble and disagree with each other." President Bush Sep 01

From Mass Media to Terrorist Social and other Media Messaging

Contemporary Media Landscape

- Terrorist and extremist groups use media environment for a range of reasons: propaganda, radicalization, recruitment, incitement to terrorism (lone wolf & inspired attacks); financing; training; planning; communicating; operations; cyberattacks.
- Traditional media designed as one-way communication to deliver carefully crafted message to an audience; social media designed as two-way communication to deliver messages and to initiate conversation with audience.
- Traditional media designed to be less immediate with trained editors determining what their audiences would see before publication or broadcast; new media designed to be immediate with terrorist groups and extremist individuals determining what their audiences will see, when they will see it and how they will see it.
- Rise and evolution of new media shifts calculus on how best to manage evolving media and terrorism question.

Communications Response to Terrorism?

- With rise of new media and social media, terrorist groups have less need to go through traditional media to have messages disseminated.
- "It is just plain embarrassing that al-Qaeda is better at communicating its message on the Internet than America…How has one man in a cave managed to out-communicate the world's greatest communications society?" – Former Secretary of Defense Robert M. Gates, 2007
- "Both foreign and domestic terrorist organizations use sophisticated messaging to promote their brand of violent extremist ideology…The US is presented with the challenge of countering that messaging." 2016 report U.S.'s Office of the Director of National Intelligence
- Significant focus today on leveraging tech, media and communication strategies, tools and programs in counter-terrorism, especially in counter-narrative work.
- Despite push in this direction, there is presently limited evidence that terrorist violence can be countered in this way.
- "Communications-based responses to violent extremism and terrorism online, especially those conducted by civil society, remain in their relative infancy." GCTF:

Counter Narrative & Messaging

- **Discussion on counter-narratives and counter-messaging in response to terrorism is in infancy**
- **Similar to challenge faced by CVE - sub focus on 'counter-messaging' or 'counter-narratives' is equally underdeveloped**
- **Lack of evidence that violent extremism can be countered by an alternative set of communications**
- **Communications campaigns can result in major blowback if they fail or are perceived to stigmatize certain communities**
- **Security and military actors should proceed with caution as the impact on public trust and credibility in their existing 'brand' can be compromised.**

Best Principles

- Politics has Primacy (Responsibility
- Coalition Coordination
- Avoid Short Term Gain at Expense of Long Term Pain
- Seamless Coordination between Tactical, Operational, Strategic and Grand Strategic
- Commander's Intent: What Messages do You want to Send?
  - Not a Line of Op but a Mission Objective
- First with the News
- First with the Truth
- Defend Military Reputation

Critical Infrastructure Protection

by Prof. Dr. Ronald Sanford Bearse & Dr. Carol Vervain Evans

In 2017, UN Security Council Resolution 2341 was adopted as the first ever global instrument entirely devoted to the protection of critical infrastructure against terrorist attacks. Its provisions reflected renewed willingness on the part of the international community to elaborate and upgrade mechanisms needed to minimize risks to critical infrastructure caused by terrorist attacks and to adequately respond to and recover from such attacks.

Critical infrastructure can be broadly defined as the systems, assets, facilities and networks that provide essential services so vital to a nation that their incapacity or destruction would have a debilitating impact on national security, economic security, prosperity, and public health and safety.

Terrorists have increasingly shown interest in attacking critical infrastructure and recent attacks have exposed the intrinsic vulnerabilities of several critical infrastructures in a variety of sectors such as energy, transportation, water and communications.

From an operating perspective, critical infrastructure is increasingly interdependent and vulnerable due to the nature of thier physical environments, functionality, supply chains, and cyber interconnections. One coordinated terrorist attack on a single point of failure could lead to the disruption or destruction of critical infrastructure causing cascading effects across multiple sectors both nationally and regionally.

Since its inception NATO has sought to protect its critical infrastructure against a variety of threats. NATO is committed to developing or further improving Member State and partner nation strategies for reducing risks to critical infrastructure from terrorist attacks by raising awareness of the relevant risks, taking preparedness measures, promoting better interoperability in security and consequence management, conducting joint training, education and exercises.

Member States have also committed to exploring ways to establish or strengthen national, regional and international partnerships with stakeholders, both public and private, as appropriate, to share information and experience in order to prevent, protect, mitigate,

investigate, respond to and recover from the effects of terrorist attacks on critical infrastructure.

NATO and other international organizations, such as the European Union and United Nations, are working with international, regional and subregional organizations to identify and share good/best practices and measures to manage the risk of terrorist attacks on critical infrastructure. They are also committed to fostering targeted capacity development, information sharing, training and exercises, technical assistance, and technology transfer to protect critical infrastructure from terrorist attacks.

NATO has taken a more vigorous approach to protecting critical infrastructure under its civil emergency protection and counterterrorism policies.

NATO civil preparedness is primarily concerned with aspects of national planning that affect the ability to contribute to Allied efforts in continuity of government, continuity of essential services to the population and civil support to military operations. These three critical civilian functions have been translated into seven baseline resilience requirements. Together with a package of resilience guidelines, assessments and a tailored toolbox, their objective is to support nations in building greater security and resilience and provide benchmarks against which to assess the state of civil preparedness. The seven baseline requirements for NATO civil preparedness are:

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

NATO's work on civil preparedness with Allies and partner nations includes "left of bang" requirements (building situational awareness and readiness prior to potential incidents or attacks), as well as "right of bang" requirements (managing the consequences of incidents and attacks).

In addition to civil emergency protection activities which contribute the protection of Alliance and partner nation critical infrastructure, NATO's Center of Excellence Defence

Against Terrorism (COEDAT) has also been playing a role in protecting critical infrastructure against terrorist attacks.

Since 2013, nearly 500 students have attended COEDAT's Critical Infrastructure Protection Against Terrorist Attacks (CIPATA) Course to raise awareness of the growing threat to critical infrastructure, share valuable lessons learned, present case studies and practical tools, and discuss major trends, issues, concerns impacting the development of critical infrastructure protection policies, plans and procedures. The CIPATA course is being modified to deliver better content in the form of case studies and practical tools to better serve NATO's long-term interests in this area.

Taught by top-notch practitioners from around the world, the course provides a unique educational platform that:

- Exposes students to the essential elements of modern national CIP/CISR policy and planning
- Discusses how CIP/CISR supports national and economic security, as well as economic prosperity
- Focuses on all critical infrastructure sectors, particularly energy and transportation
- Increases student knowledge and understanding of current and emerging issues, concerns and challenges in developing and implementing national CIP/CISR policy and plans
- Identifies the roles and responsibilities of government, the private sector, non-government organizations, international organizations and others in protecting critical infrastructure
- Emphasizes the need for clear and unambiguous methods for defining risk terms and risk methodologies for use in protecting critical infrastructure
- Provides students with concepts, methods and tools which can be used to improve the security and resilience of critical infrastructures in their countries
- Explains the essential need for public-private partnerships and information sharing mechanisms for protecting critical infrastructure; and
- Provides an immersive practicum that enables students to apply what they learned during the course in an exercise simulating terrorist threats and attacks against critical infrastructure.

In addition to offering the CIPATA course, COEDAT signed a Memorandum of Agreement with the US Army War College last year to explore ways in which both entities can help each other in the area of CIP/CISR. Initial projects include writing a book on CISR focused on lifeline infrastructure sectors; developing an online listing of CISR reference materials; developing a COEDAT course on CISR for senior officials; and exploring new opportunities to more directly assist Alliance and partner nations in developing CIP/CISR policies, plans and procedures.

NATO has made appreciable progress in protecting critical infrastructure, but the process is complex and a continuing challenge - requiring multiple streams of work performed by a wide variety of public and private sector stakeholders. The major steams of work include:

- Identifying and Determining the Criticality of National Infrastructure
- Determining the Terrorist Threat to and Risk to specific Critical Infrastructures
- Determining Critical Infrastructure Vulnerabilities
- Mapping Critical Infrastructure Dependencies and Interdependencies
- Using Applicable Risk Management Approaches or Methods
- Developing and Implementing National Critical Infrastructure Protection Policy
- Establishing Mechanisms for Sharing Information with Owners and Operators of Critical Infrastructure
- Managing the Response to a Credible Terrorist Threat or Attack Against Critical Infrastructure
- Establishing and Implementing Mechanisms for Sharing Information and Intelligence to Support Critical Infrastructure Protection Planning and Operations
- Interdiction and Disruption of Threats to Critical Infrastructure
- Developing and Implementing Continuity of Operations/Disaster Recovery Plans for Critical Infrastructure
- Providing Physical and Cyber Protective Measures
- Ensuring the Integrity, Security Continuity of Critical Infrastructure Supply Chains
- Minimizing Critical System Recovery Times

- Adopting the Principal Concepts of Critical Infrastructure Security and Resilience

Therefore, when thinking initially about "best practices" in the critical infrastructure protection domain, one probably envisions a list of ***what*** a nation, ministry, agency or specific sector or industry has done in one or more of these workstreams that is demonstrably effective in achieving a critical infrastructure protection goal or objective.

In this regard there are several recently published compendiums/reports of best/good practices in protecting critical infrastructure against terrorist attacks and other threats; three of which are:

- The 2018 Report by the United Nation's Counter-Terrorism Implementation Task Force's Working Group on the Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security titled: *The Protection of Critical Infrastructure Against Terrorist Attacks: A Compendium of Good Practice.* This report addresses prevention, preparedness, mitigation, investigation, response, recovery and provides valuable reference material on the development of strategies for reducing risks to critical infrastructure from terrorist attacks.

- The 2019 report by the United States Department of Homeland Security titled: *A Guide to Critical Infrastructure Security and Resilience.* This report contains basic information of U.S. lessons learned over the last 15 years, which may be helpful to other countries, particularly those countries that are considering developing or refining their own voluntary and regulatory-based infrastructure protection/security and resilience programs.

- The 2019 book published under the NATO Science for Peace and Security series titled, *Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection.* This book presents edited contributions from the NATO Advanced Training Course on Critical Infrastructure Protection - Best Practices and Innovative Methods of Protection, which was held in Agadir, Morocco, from 6 to 12 May 2018. This course brought together specialists

from Member States and partner nations working in the area of protecting critical infrastructure to share their knowledge and expertise.

We (the authors) believe it is more important to identify ***how*** (the manner in which) nations, ministries, agencies, and specific sectors can best foster the communication, cooperation, collaboration, coordination and concentration required to build sustain a viable, risk-based critical infrastructure protection posture – one that is flexible and adaptable to changing conditions (both foreseeable and unexpected), enables rapid recovery from disruption, and reduces the risk to critical infrastructure and the risk of loss due to a disruption by minimizing their vulnerability. Focusing on the **"*how*"** will help harmonize work streams, produce economies of scale, and more effectively allocate financial and human resources.

Goal of Paper

The goal of this paper is to: (1) define the nexus that exists between the critical infrastructure protection and counterterrorism communities; (2) define best practices for fostering the communication, cooperation, collaboration, coordination and concentration required to effectively perform critical infrastructure protection work streams; (3) describe the challenges associated with implementing best practices, and the consequences of failing to overcome them; and (4) provide recommendations to strengthen NATO's ability to help Alliance and partner nations apply best practices (and valuable and costly lessons learned) in developing and implementing infrastructure security and resilience policies, plans and procedures.

Keywords

Critical Infrastructure Protection, Critical Infrastructure Security and Resilience, Lifeline Infrastructure, Critical Infrastructure Reliability, Terrorism, Infrastructure Security, Best Practices, Counterterrorism, NATO, NATO Partner Nations, Public-Private Partnerships, Intelligence and Information Sharing, Risk Analysis, Risk Assessment, and Risk Management

References

John D. Moteff, Critical Infrastructure Protection: Background, Policy and Implementation, 2014, http://www.fas.org/sgp/crs/homesec/RL30153.pdf

The Infrastructure Security Partnership, Understanding Resilience: Disaster Resilience Begins with You, July 30, 2013, http://www.tisp.org/index.cfm?cdid=13180

The 2012 Critical Infrastructure Symposium: Lessons Learned from Past Attacks on America's Infrastructure, Raymond H. Bennett, Ph.D., P.E., Baker Engineering and Risk Consultants Inc., 2011 http://tisp.org/index.cfm?pid=12831

U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience, pp. 10-12, Appendix B, 2013, http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508.pdf

Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies, 2004, http://www.ce.cmu.edu/~hsm/im2004/readings/CII-Rinaldi.pdf

Michel Van Eeten, Albert Nieuwenhuijs, Eric Luiijf, Marieke Klaver, and Edite Cruz, "The State and the Threat of Cascading Failure across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports," Public Administration, 89(2), 2011, 381–400, http://onlinelibrary.wiley.com/doi/10.1111/j.1467-9299.2011.01926.x/abstract

NATO Parliamentary Assembly, The Protection of Critical Infrastructures, 2007, http://www.nato-pa.int/default.asp?SHORTCUT=1165

Council of the European Union, Council Directive 2008/114/EC: Identification and Designation of European Critical Infrastructure and the Assessment of the Need to Improve their Protection, http://www.euractiv.com/en/security/critical-infrastructure/article-140597

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, On Critical Information Infrastructure Protection: Achievements and Next Steps: Towards Global Cyber-Security, March 2011, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

National Strategy for Global Supply Chain Security, January 2012, http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf

U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience. Washington, DC, 2013. See Executive Summary; Risk, 15-20, 23-25. http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf

French, Geoffrey S. "Intelligence Analysis for Strategic Risk Assessments." In Critical Infrastructure Protection: Elements of Risk. Arlington, VA: George Mason University, 2007. http://cip.gmu.edu/wp-content/uploads/2014/03/ElementsofRiskMonograph.pdf

French, Geoffrey S. and David Gootzit. "Defining and Assessing Vulnerability of Infrastructure to Terrorist Attack." in Vulnerability, Uncertainty, and Risk: Analysis, Modeling, and Management: Proceedings of the ICVRAM 2011 and ISUMA 2011 Conferences (2011): 782-89. http://cedb.asce.org/cgi/WWWdisplay.cgi?274192

Ross Anderson and Shailendra Fuloria, Security Economics and Critical National Infrastructure, http://www.cl.cam.ac.uk/~rja14/Papers/econ-cni09.pdf

The Infrastructure Security Partnership, The Infrastructure Security Partnership, Infrastructure Resilience, and Interdependencies, (March 2010), http://www.tisp.org/index.cfm?cdid=11972

Arjen Boin, Mark Rhinard, and Magnus Ekengren, "Institutionalizing Homeland Security Cooperation in Europe: Counter-Terrorism and Critical Infrastructure Protection Compared," International Studies Association (March 26, 2008), http://citation.allacademic.com//meta/p_mla_apa_research_citation/2/5/0/8/6/pages250863/p250863-1.php

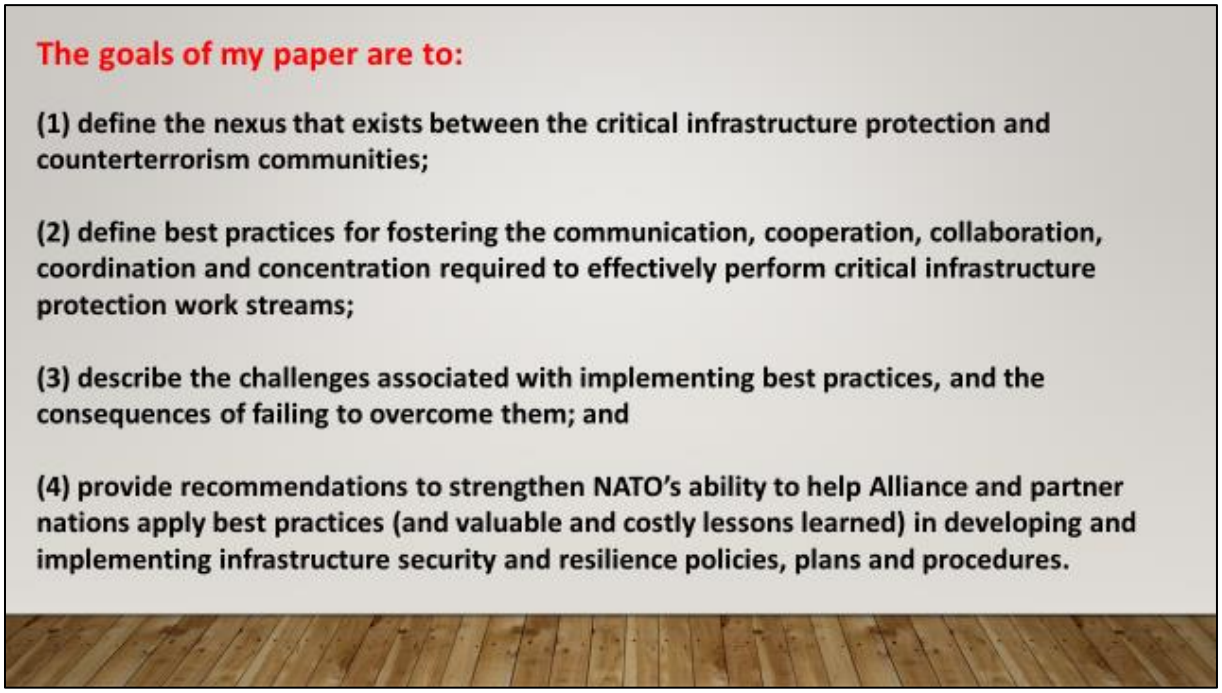
Bach, C. et al. (2013), "Adding value to critical infrastructure research and disaster risk management: the resilience concept", http://journals.openedition.org/sapiens 6.1, https://journals.openedition.org/sapiens/1626

Critical Five (2014), Forging a Common Understanding for Critical Infrastructure Shared Narrative, https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

OECD and EU JRC (2018), System Thinking for Critical Infrastructure Resilience and Security - OECD/ JRC Workshop - OECD, http://www.oecd.org/gov/risk/workshop-oecd-jrc-system-thinking-for-critical-infrastructure-resilience-and-security.htm

Verner, D., F. Petit and K. Kihaek (2017), "Incorporating Prioritization in Critical Infrastructure Security and Resilience Programs - HOMELAND SECURITY AFFAIRS", Homeland Security Affairs, Vol. 13, https://www.hsaj.org/articles/14091

c. Presentation



BACKGROUND

- What is Critical Infrastructure (CI) and why is it important?
- A few questions for the audience
- Increased Interest in attacking CI
- UN Security Council Resolution 2341

NATO DEFINITION OF CRITICAL INFRASTRUCTURE

Those facilities, services and information systems which are so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economy, public health and safety and the effective functioning of the government."

A FEW QUESTIONS FOR THE AUDIENCE

- Has your country identified its "critical infrastructure"?
- Does your country have a National Critical Infrastructure Protection Policy or Strategy?
- Which Ministry, Department, Office of Agency in your national government is responsible for coordinating critical infrastructure protection efforts?
- Who in your national government works with private sector owners and operators to protect critical infrastructure against terrorist attack?
- What kind of information and/or intelligence does your national government share with private sector owners and operators of critical infrastructure?
- Who in your country assesses the risk to critical infrastructure?
- Is the protection of critical infrastructure in your country a national security priority?

INCREASED TERRORIST INTEREST IN ATTACKING CRITICAL INFRASTRUCTURE

- Terrorism is a direct threat to the citizens of NATO countries and to international stability and prosperity
- Terrorists have increasingly shown interest in attacking critical infrastructure - attacks have exposed vulnerabilities of CI
- Consequences of a coordinated terrorist attack on a single point of failure

RECENT NATO CRITICAL INFRASTRUCTURE PROTECTION (CIP) EFFORTS

- NATO Collective Defense and Collective Security
- CIP under NATO civil emergency planning (CEP) and counterterrorism (CT) policies.

THE SEVEN BASELINE REQUIREMENTS FOR NATO CIVIL EMERGENCY PLANNING

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

RECENT COEDAT CRITICAL INFRASTRUCTURE PROTECTION (CIP) EFFORTS

- COEDAT Activities
  - 5-Day CIPATA Course
  - 2-Day Executive Seminar on CISR
  - Memorandum of Agreement with the US Army War College
    - Book on CISR, On-line Reference Library,

COEDAT'S CRITICAL INFRASTRUCTURE PROTECTION AGAINST TERRORIST ATTACKS COURSE CONTENT

- Essential elements of national CIP/CISR policy and planning
- Case Studies, and stakeholder roles and responsibilities government, military, industry, NGO, regional/international organizations
- Threat/Vulnerability/Risk analysis, Risk Assessment and Risk Managemnt tools/methods, and public-private partnerships, dependenciy/interdependency analysis, information sharing
- Cross sector and international communication, cooperation, collaboration, coordination and concentration (5C's), and current/emerging issues, concerns and challenges in developing national CIP/CISR policy and plans, and a day-long Immersive Student Practicum

CIP IS VERY COMPLEX AND A MAJOR CONTINUING CHALLENGE REQUIRING MULTIPLE STREAMS OF WORK PERFORMED BY A WIDE VARIETY OF PUBLIC AND PRIVATE SECTOR STAKEHOLDERS

- Identifying CI
- Mapping CI dependencies/interdependencies
- Determiine the Terroist threat against CIs
- Developing/Implementing National CIP Policy and Plans
- Information/Intelligence Sharing with CI Owners and Operators
- Interdiction and Disruption of Threats
- CI Continuity of Operations/Disaster Recovery Plans
- Defiining/Implementing Protective Measures
- Ensuring Integrity, Security Continuity of CI Supply Chains
- Minimizing Critical System Recovery Times
- Adopting the Principal Concepts of Critical Infrastructure Security and Resilience

RECENT PUBLICATIONS ON BEST/GOOD PRACTICES ON PROTECTING CRITICAL INFRASTRUCTURE AGAINST TERRORIST ATTACKS

- The 2018 Report by the United Nation's Counter-Terrorism Implementation Task Force titled: ***The Protection of Critical Infrastructure Against Terrorist Attacks: A Compendium of Good Practice.***
- The 2019 report by the United States Department of Homeland Security titled: ***A Guide to Critical Infrastructure Security and Resilience.***
- The 2019 book published under the NATO Science for Peace and Security series titled, ***Critical Infrastructure Protection: Best Practices and Innovative Methods of Protection.***

Potential Future Role of NATO in Counter-Terrorism

by Col. Daniel Wayne Stone

I Introduction

1. NATO's Counter-Terrorism objectives are to project stability and support cooperative security.[4] This is closely linked to NATO's three essential core tasks - collective defense, crisis management and cooperative security. Military power alone will not be able to deter, defend against, nor defeat terrorism; military and Hard Power are not the primary instruments of power to be used in the fight against terrorism; soft power is the best method to address root causes of terrorism through Whole of Government (WoG) and Whole of Society (WoS). NATO must engage to a much greater extent with Allies, Partner Nations, Nations of Interest, the International Community, Non-Governmental Organizations, and civil society to set conditions inside of nations to address the grievances and root causes of terrorism through the application of diplomacy and Soft Power by, with, and through partner nations (PNs) and nations of interest (NoI).
2. **What is the terrorist threat to NATO?** It is the destabilization of nations and regions on NATO's borders and potentially inside NATO nations themselves.
3. *The future role of NATO should be proactive by using all political and military means and capabilities of the organization, in order to create conditions within a country or in a certain region which help to handle terrorism related problems locally through a combination of Soft and Hard Power by the nations themselves. This helps to avoid deployment of NATO forces in major CT operations.*[5]

[4] MC 0472/1 MILITARY COMMITTEE CONCEPT FOR COUNTER - TERRORISM

[5] This statement is in line with MC 0472/1 MILITARY COMMITTEE CONCEPT FOR COUNTER – TERRORISM:

"NATO has unique assets and capabilities to support partner CT capacity building. NATO agreed areas where the Alliance can provide added value in training and advising partners on CT are based on partner's requirements identified by NATO and requests of assistance to NATO. Reinforcing NATO's ability to conduct CT capacity building and improving the provision of CT education and training to Partners in the agreed areas supports NATO's CT objectives to project stability and support cooperative security."

II Terrorism Changes in the Next 20 Years

4. Over the next 20 years, terrorist organizations will continue to develop and modify the ways in which terrorist activities are conducted. Areas of concern for COE-DAT are:

a. Cyber:

i. Terrorist organizations will continue to try and turn a terrorist into a cyber professional (they will continue to struggle in this area), but the greater danger is the radicalization of cyber professionals.

ii. Terrorist organizations will use cyber-attacks against critical infrastructure, cities, and businesses to raise funds[6] [7] [8] [9].

iii. Terrorist organizations will develop capabilities to attack critical infrastructure in an attempt to cause physical harm by releasing flood waters, de-railing trains, and shutting down power grids to name a few[10] [11].

b. Merging of Terrorist groups with Criminal Syndicates: [12]

i. Links between terrorists and criminals will continue to expand.

ii. Narcotics and terrorist will work closer to move, protect, and sell drugs. This will provide funding for terrorists, gain access to illicit entry routes into nations.

---

[6] Robert Muggah and Marc Goodman, "Cities are easy prey for cybercriminals. Here's how they can fight back," World Economic Forum, 30 September 2019, Our cities are under cyberattack. Here's why - and what to do about it | World Economic Forum, last accessed 1 July 2020.

[7] Alan Blinder and Nicole Perlroth, "A Cyberattack Hobbles Atlanta, and Security Experts Shudder," *New York Times*, 27 March 2018, https://www.nytimes.com/2018/03/27/us/cyberattack-atlanta-ransomware.html, last accessed 23 October 2020.

[8] Alan Blinder and Nicole Perlroth, "Hard Choices for Cities Under Cyberattack: Whether to Pay Ransom," *New York Times*, 29 March 2018, https://www.nytimes.com/2018/03/29/us/atlanta-cyberattack-ransom.html, last accessed 23 October 2020.

[9] William Turton, "Companies Facilitating Ransomware Payments Could Face Penalties," *Bloomberg*, 2 October 2020, https://www.bloomberg.com/news/articles/2020-10-01/companies-facilitating-ransomware-payments-could-face-penalties?sref=EJ3iffSv, last accessed 23 October 2020.

[10] Arie Egozi, "Cyber Strike By Foreign Force Caused Iran Explosion: Israeli Experts," *Breaking Defense*, 2 July 2020, https://breakingdefense.com/2020/07/cyber-strike-by-foreign-force-causes-iran-explosion-israeli-experts/,

[11] Kevin Collier, "Major hospital system hit with cyberattack, potentially largest in U.S. history," NBC News, 28 September 2020, https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254, last accessed 23 October 2020.

[12] Webinar, "The Sahel Region Border Challenges," Border Security Report, 30 September 2020, https://www.bigmarker.com/border-security-report/The-Sahel-Region?bmid=2f5baeb7b7f8, last accessed 30 September 2020.

iii. Linkage between organized crime and corruption both enables and provides funding to terrorist organizations. [13]

c. WMD:

i. Terrorist will continue to try and acquire WMD.

ii. Although obtaining a nuclear bomb will continue to be a priority for terrorist organizations, this will continue to be an aspiration.

iii. More realistic is the development of a "dirty" bomb made out of radiological material from hospitals and research facilities.

iv. Biological attacks will become normal. COVID-19 has shown the power of a virus and many terrorist organizations are seeking ways to actively weaponize COVID-19. In the future efforts by terrorist organizations into the development of weaponized biological elements will increase. Potential risk areas are centers of disease research, anthrax, ricin, and exotic tropical diseases. Contamination of water sources or aerosol sprays from light aircraft or from city buildings are possibilities. [14] [15] [16] [17] [18]

d. Social Unrest: [19]

i. Terrorist organizations will try to infiltrate and support social unrest inside of nations. Terrorist will try and use these social movements as cover to conduct attacks and create greater confusion inside of nations and stoke social grievances.

ii. It is also assessed that adversary nations of NATO will support social movements inside of NATO nations to sow discord. A potential tactic will

---

[13] Kayla Izenman abd Tom Keatinge, "Exploring Connections: Corruption, Terrorism and Terrorist Financing," RUSI, 2 April 2020, https://rusi.org/publication/occasional-papers/exploring-connections-corruption-terrorism-and-terrorist-financing, last accessed 7 October 2020.

[14] Hannah Allam, "'A Perfect Storm': Extremists Look for Way's to Exploit Coronavirus Pandemic," National Public Radio, 16 April 2020, https://www.npr.org/2020/04/16/835343965/-a-perfect-storm-extremists-look-for-ways-to-exploit-coronavirus-pandemic.

[15] Joce Sterman and Alex Brauer, "Experts say domestic terrorists could see coronavirus as a window of opportunity," Sinclair Broadcast Group, 6 April 2020, https://fox11online.com/news/spotlight-on-america/experts-say-domestic-terrorists-could-see-coronavirus-as-window-of-opportunity.

[16] Bridget Johnson, "How Terrorists Are Trying to Make Coronavirus More Friend Than Foe," *Homeland Security Today*, 14 April 2020, https://www.hstoday.us/subject-matter-areas/counterterrorism/how-terrorists-are-trying-to-make-coronavirus-more-friend-than-foe/.

[17] Natasha Bertrand, Daniel Lippman, and Lara Seligman, "Officials probe the threat of a coronavirus bioweapon," *Politico*, 23 April 2020, Officials probe the threat of a coronavirus bioweapon - POLITICO.

[18] COE-DAT's study on "NATO in the COVID-19 Environment and the Threat of Terrorism," 28 August 2020, pp 4 & 11-12.

[19] COE-DAT's study on "Africa: A Hybrid Battleground,".14 August 2020.

to be to support, fund, train, and arm opposing social factions to cause unrest and violence and distract government and security forces[20] [21] [22].

e. Rise of populism and the back-sliding of democratic orders to authoritarianism will continue. Adversarial nations will exploit this trend and pursue hybrid warfare strategies that focus on non-military methods to stoke tensions and sow discord inside of NATO nations.

f. Continued rise of irregular warfare as the new norm. Adversarial nations will increase the use of private military corporations and support terrorist groups and groups opposed to national governments as ways to disrupt NATO nations, PNs, and NoI. This will provide official deniability of actions just short of war. [23] [24] [25] [26] [27]

g. Economic pressures from shrinking economies, slow recovery from COVID-19 pandemic, and shortfalls in developing nations will contribute to continued inequalities inside nations and make them vulnerable to terrorist ideologies.

h. Migrations of persons from areas of violence into NATO, PN, and NoI will cause a backlash by other terrorist organizations that oppose the mass migration of persons. Religiously motivated terrorist organizations will inspire Right-Wing terrorist organization who will inspire Left-Wing and Antifa organizations to commit terrorist acts.[28]

i. Authoritarian regimes and authoritarian leaning governments will justify the arrest of journalists, dissenters, and opposition parties by falsely accusing them of

---

[20] Oleksandr Danylyuk, "Protests, a pandemic and evidence of a hybrid war," *C4ISRNET*, 5 June 2020, Protests, a pandemic and evidence of a hybrid war, last accessed 1 July 2020.
[21] Podcast, "The Changing Landscape of Domestic Terrorism, With Bruce Hoffman, Council on Foreign Relations, 16 June 2020, https://www.cfr.org/podcasts/changing-landscape-domestic-terrorism-bruce-hoffman.
[22] COE-DAT's study on "The Role of Irregular Forces in Russia's Hybrid Warfare," 30 June 2020, pp 8 &12.
[23] Jeff Goodson, "Irregular Warfare in a new era of great-power competition," Modern War Institute, 20 May 2020, https://mwi.usma.edu/irregular-warfare-new-era-great-power-competition/ , Last accessed 1 July 2020.
[24] Paul Stronski, "Implausible Deniability: Russia's Private Military Companies," Carnegie Endowment for International Peace, 2 June 2020, Implausible Deniability: Russia's Private Military Companies - Carnegie Endowment for International Peace, last accessed 1 July 2020.
[25] Patrick Tucker, "Mozambique Is Emerging As The Next Islamic Extremist Hotspot," *Defense One*, 6 July 2020, https://www.defenseone.com/threats/2020/07/mozambique-emerging-next-islamic-extremist-hotspot/166638/.
[26] COE-DAT's study on "Africa: A Hybrid Battleground,".14 August 2020.
[27] COE-DAT's study on "The Role of Irregular Forces in Russia's Hybrid Warfare," 30 June 2020, pp 6 &14-15.
[28] Amelia Wynne, "Fears Italy's coronavirus crisis could trigger surge in far-right extremism as stricken nation faces worst recession since Second World War," *Daily Mail Online*, 18 April 2020, https://www.dailymail.co.uk/news/article-8232267/Fears-Italys-coronavirus-crisis-trigger-surge-far-right-extremism.html.

"supporting" or "defending" terrorism to suppress dissent.[29] [30] This will weaken international response to these governments as the "specter" of terrorism is a threat to all nations.

III What should NATO's approach to countering terrorism be?

5. NATO's ultimate goal should not be to conduct combat operations and missions to deter and defeat terrorism (and non-state actors), but rather NATO should institute a policy of support to Allies, Partner Nations (PNs), and Nations of Interest (NoI). NATO would be better served by implementing policies, procedures, and methods to support Allies, PNs, NoI, and the IC in Soft Power activities to address the root causes and grievances of terrorism which will more effectively interrupt terrorist operations that direct military force. This policy would have NATO use all elements of its power to support, coach, train, and advise Allies, PNs, and NoI in their fight against terrorism.

6. Although CT is a national responsibility,

- **a.** NATO can use its political and military power all across the spectrum from support to the international community (IC), support to Allies, support to partner nations (PN), support to nations of interest (NoI), through operations and missions of NATO forces, as a last resort.
- **b.** NATO should support the IC's counter terrorism efforts. NATO should continue to support the UN's efforts in areas in which the Alliance can provide relevant military assistance that is non-duplicative of other sources of support.
- **c.** NATO should use its political leverage to support a Whole of Government (WoG) and Whole of Society (WoS) approach to combatting terrorism by addressing the root causes people join terrorist organizations. The WoG and WoS approach should be promoted to IC at large, Non- Government Organizations (NGOs), regional associations, individual PNs, and NoI. NATO should encourage nations and organizations to address the root causes of terrorism (such as inequality, rule of law, good governance, delivery of essential services (if a nation does not provide these

[29] "Russian Journalist To Appeal Ruling By Russian Court In Controversial Case," *Radio Free Europe Radio Liberty*, 6 July 2020, https://www.rferl.org/a/russia-journalist-svetlana-prokopyev-verdict/30709068.html.
[30] https://www.amnesty.org/en/latest/news/2020/05/egypt-end-relentless-attacks-on-journalists-and-other-media-workers/

services terrorist organizations will), and strengthening of democratic institutions as a few examples).[31] [32]

d. NATO should encourage nations to apply Soft and Hard power to combat terrorism. Education and Training both at NATO facilities and in country teams should focus highlight the interplay of Soft and hard Power. The role of the military in CT should be highlighted but caveated by the fact that CT is primarily a non-military activity; addressing the root causes is far more important that military or hard power. [33]

e. NATO should develop teams of experts that in coordination with individual national requests to conduct assessments of national CT capabilities and develop defined requirements with the host nation based on required capability and capacity. The end result of these assessments would be a national list of validated requirements certified by NATO that the nation could then use to seek out donor nations to assist in obtaining (similar to the NATO/Jordan Border Security workshops that defined Jordan's requirements, validated by NATO, and many donor nations provided support based on NATO's validation).[34] [35] [36] [37]

f. NATO can advocate for reform within nations and make NATO support contingent on visible actions taken by nations to address the systemic root causes of terrorism.

g. Resilience is one of NATO's seven key competencies.

i. As NATO Secretary General Jens Stoltenberg stressed at the Global Security 2020 Bratislava forum, "resilience is in NATO's DNA (as) Article Three of the

---

[31] COE-DAT's study on "Africa: A Hybrid Battleground," 14 August 2020.

[32] Webinar, "The Sahel Region Border Challenges," Border Security Report, 30 September 2020, https://www.bigmarker.com/border-security-report/The-Sahel-Region?bmid=2f5baeb7b7f8, last accessed 30 September 2020.

[33] Raphael Obonyo, "African youth and the growth of violent extremism," United Nations, 23 December 2019, https://www.un.org/africarenewal/magazine/december-2019-march-2020/african-youth-and-growth-violent-extremism, last accessed 14 September 2020.

[34] "Esper signs 10-year US military cooperation deal with Morocco," *Military Times*, 4 October 2020, https://www.militarytimes.com/news/your-military/2020/10/04/esper-signs-10-year-us-military-cooperation-deal-with-morocco/?utm_source=Sailthru&utm_medium=email&utm_campaign=EBB%2010%2C05.20&utm_term=Editorial%20-%20Military%20-%20Early%20Bird%20Brief, last accessed 5 October 2020.

[35] Jim Garamone, "U.S., Tunisia Sign Road Map for Defense Cooperation," *DOD News*, 1 October 2020, https://www.defense.gov/Explore/News/Article/Article/2368982/us-tunisia-sign-road-map-for-defense-cooperation/, last accessed on 5 October 2020.

[36] Kevin Bilms, "The Defense Department Just Published A Summary of the National Defense Strategy's Irregular Warfare Annex. Here's Why It's So Significant," *Modern War Institute*, 2 October 2020, https://mwi.usma.edu/the-defense-department-just-published-a-summary-of-the-national-defense-strategys-irregular-warfare-annex-heres-why-its-so-significant/, last accessed 5 October 2020.

[37] COE-DAT's study on "Africa: A Hybrid Battleground," 14 August 2020.

Washington Treaty places a duty on Allies to become more resilient".[38] NATO should reconsider its strategic objectives in a new concept to provide appropriate answers on the field of critical infrastructure security and resilience. Recent events such as the drone attacks against Saudi oil refinery and the outbreak of Coronavirus pointed out how the critical infrastructure, such as energy supply or global transportation chains, are vulnerable. When there are disruptions to the services critical infrastructure provide, there is the potential for costly direct economic impacts, such as the cost of repairing damage to physical structures, and indirect economic impacts to society.[39] [40]

ii. NATO should be prepared to counter subversive actions and unrests based on ethnic, national, religious, or other lines of division. To tackle these threats, NATO members must enhance their resilience in the fields of finance and economy, with particular attention paid to diversification of the supply of energy resources and to combatting corruption. They must also strengthen the resilience of the society against manipulation.[41] [42] [43] [44]

h. NATO should develop CISR requirements teams to help identify Critical Infrastructure (CI) and provide advice on how to develop redundancy and resilience for to Allies, PNs, and NoI.

i. NATO should develop Red Teams to identify new threats and wargame possible solutions. NATO should gather science fiction writers, future thinkers, tech companies, and think tanks to speculate on potential future threats

---

[38] Jens Stoltenberg, Keynote Speech at the Global Security 2020 Bratislava Forum, 7 October 2020, https://www.nato.int/cps/en/natohq/opinions_178605.htm, last accessed 26 October 2020.
[39] COE-DAT's Lessons Learned workshop on "Strengthening the Security and Resilience of NATO and Partner Nation Critical Infrastructure Against Terrorist Attacks," posted on JALLC portal.
[40] Key finding of the "Crisis Management In Terrorism" seminar organized by COE-DAT.
[41] COE-DAT's study on "The Role of Irregular Forces in Russia's Hybrid Warfare," 30 June 2020.

[42] Kevin Bilms, "The Defense Department Just Published A Summary of the National Defense Strategy's Irregular Warfare Annex. Here's Why It's So Significant," *Modern War Institute*, 2 October 2020, https://mwi.usma.edu/the-defense-department-just-published-a-summary-of-the-national-defense-strategys-irregular-warfare-annex-heres-why-its-so-significant/, last accessed 5 October 2020.
[43] COE-DAT's study on "The Role of Irregular Forces in Russia's Hybrid Warfare," 30 June 2020, p 18.
[44] Kayla Izenman abd Tom Keatinge, "Exploring Connections: Corruption, Terrorism and Terrorist Financing," RUSI, 2 April 2020, https://rusi.org/publication/occasional-papers/exploring-connections-corruption-terrorism-and-terrorist-financing, last accessed 7 October 2020.

j. NATO should promote critical thinking as a tool in combatting terrorism. Strengthening populations ability to see through the falsehoods in terrorist narratives can reduce the likelihood a person will join a terrorism organization.

k. NATO should continue to pursue emerging technologies such as "Big Data", "Advanced Analytics", and "Artificial Intelligence" as potential methods to improve counter-terrorism analysis. Emphasis should be on NATO nations sharing data from these technologies in order to provide "real-time" information and assessments. [45] [46] [47]

l. NATO must advocate for anti-corruption as a precursor for NATO support to PNs and NoI.

7. NATO should support the CT Action Plan and through each of the six core areas:

a. Awareness and Analysis:

- Support the UN, Allies, PNs, NoI, regional actors, NGOs with intelligence sharing where possible.

b. Preparations, Resilience, and Response:

- NATO support to Allies with niche military capabilities and training when requested. Enlarge PN and NoI attendance to NATO E&T that support defined CT objectives
- NATO develop CISR requirements teams to aid Allies, PNs, and NoI development of capability shortfalls that NATO can ultimately validate

c. Capabilities:

- NATO continue to support identified military capabilities that lend themselves to CT and support to NATO SoF.
- NATO support Allies upon request.

d. Capacity Building and Partnerships:

- Expand support to PNs and NoI in the 14+1 areas

[45] NATO Emerging and Disruptive Science and Technology presentation.
[46] Cohen, Raphael S., Nathan Chandler, Shira Efron, Bryan Frederick, Eugeniu Han, Kurt Klein, Forrest E. Morgan, Ashley L. Rhoades, Howard J. Shatz, and Yuliya Shokh, "The Future of Warfare in 2030," Rand Corporation, 2020, https://www.rand.org/pubs/research_reports/RR2849z1.html, last accessed May 2020.
[47] Cohen, Raphael S., Nathan Chandler, Shira Efron, Bryan Frederick, Eugeniu Han, Kurt Klein, Forrest E. Morgan, Ashley L. Rhoades, Howard J. Shatz, and Yuliya Shokh, "Peering into the Crystal Ball: Holistically Assessing the Future of Warfare," Rand Corporation, 2020, https://www.rand.org/pubs/research_briefs/RB10073.html, last accessed May 2020.

- In terms of CT, NATO should recognize PN CT requirements as NATO requirements in the development of CT E&T. It is far better for NATO to support PNs and NoI in their CT fight than for NATO forces to drawn into the CT fight.
- Develop NATO requirements teams to develop roadmaps for PNs and NoI development of credible CT capacity. End goal is a set of validated requirements that define the needs of a PN or NoI in CT that donor nations can provide support to.

e. Operations and Missions:

- When the Alliance collectively decides a threat is a collective one and authorizes military force to take direct action. Specific authorities should be granted to:
  - Train,
  - Train and advise,
  - Train, advise, and assist,
  - Intelligence and enabler support, and /or
  - Direct combat operations,
  - Nation build as required to set conditions to address root causes of terrorism.

f. Strategic Communications:

- NATO message support to IC, Allies, PNs, and NoI in CT
- NATO message the role of Soft and hard Power in CT
- NATO champion efforts to address root causes of terrorism
- NATO should advocate for nations to work with media outlets to minimize news publicity of terrorist activities that act to promote terrorist agendas. This can minimize propaganda of the deed and limit inadvertent propagation of terrorist messaging. Freedom of the press must be guaranteed throughout this process and promoted by NATO.
- NATO support internet freedom and caution about the risks of mass digital surveillance
- NATO should continue to develop a narrative clearly describing why the common values of NATO nations is important and what democratic values are and why they are important.[48]
- NATO should encourage nation to develop narratives of the values nations hold and provide a counterpoint to terrorist propaganda

[48] COE-DAT's study on "Africa: A Hybrid Battleground,".14 August 2020.

- NATO should encourage critical thinking in societies to combat terrorist ideologies

d. Presentation

Centre of Excellence Defence Against Terrorism (COE DAT)

Future Role of the Military / NATO In Counter-Terrorism

Overall Classification:
NATO UNCLASSIFIED

1/10

Disclaimer

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

UNCLASSIFIED

2/10

Overview

- Terrorism Changes in the Next 20 Years
- The Role of the Military / NATO in CT Now
- Potential Roles for the Military / NATO

UNCLASSIFIED

3/10

Ground Rule

- **Challenge Our:**
  - **Ideas**
  - **Conclusions**
  - **Recommendations**

UNCLASSIFIED

4/10

To set the stage for our discussion, we first will address the Terrorist threat to NATO which is the destabilization of nations and regions on NATO's borders and potentially inside NATO nations themselves.

Over the next 20 years, terrorist organizations will continue to develop and modify the ways in which terrorist activities are conducted. Areas of concern for COE-DAT are:

Cyber:

- Terrorist organizations will continue to try and turn a terrorist into a cyber professional (they will continue to struggle in this area), but the greater danger is the radicalization of cyber professionals.
- Terrorist organizations will use cyber-attacks against critical infrastructure, cities, and businesses to raise funds .
- Terrorist organizations will develop capabilities to attack critical infrastructure in an attempt to cause physical harm by releasing flood waters, de-railing trains, and shutting down power grids to name a few .

Merging of Terrorist groups with Criminal Syndicates:

- Links between terrorists and criminals will continue to expand.
- Narcotics and terrorist will work closer to move, protect, and sell drugs. This will provide funding for terrorists, gain access to illicit entry routes into nations.

- Linkage between organized crime and corruption both enables and provides funding to terrorist organizations.

WMD:

- Terrorist will continue to try and acquire WMD.
- Although obtaining a nuclear bomb will continue to be a priority for terrorist organizations, this will continue to be an aspiration.
- More realistic is the development of a "dirty" bomb made out of radiological material from hospitals and research facilities.
- Biological attacks will become normal. COVID-19 has shown the power of a virus and many terrorist organizations are seeking ways to actively weaponize COVID-19. In the future efforts by terrorist organizations into the development of weaponized biological elements will increase. Potential risk areas are centers of disease research, anthrax, ricin, and exotic tropical diseases. Contamination of water sources or aerosol sprays from light aircraft or from city buildings are possibilities.

Social Unrest:

- Terrorist organizations will try to infiltrate and support social unrest inside of nations. Terrorist will try and use these social movements as cover to conduct attacks and create greater confusion inside of nations and stoke social grievances.
- It is also assessed that adversary nations of NATO will support social movements inside of NATO nations to sow discord. A potential tactic will to be to support, fund, train, and arm opposing social factions to cause unrest and violence and distract government and security forces .

Rise of populism and the back-sliding of democratic orders to authoritarianism will continue. Adversarial nations will exploit this trend and pursue hybrid warfare strategies that focus on non-military methods to stoke tensions and sow discord inside of NATO nations.

Continued rise of irregular warfare as the new norm. Adversarial nations will increase the use of private military corporations and support terrorist groups and groups opposed to national governments as ways to disrupt NATO nations, PNs, and NoI. This will provide official deniability of actions just short of war.

Economic pressures from shrinking economies, slow recovery from COVID-19 pandemic, and shortfalls in developing nations will contribute to continued inequalities inside nations and make them vulnerable to terrorist ideologies.

Migrations of persons from areas of violence into NATO, PN, and NoI will cause a backlash by other terrorist organizations that oppose the mass migration of persons. Religiously motivated terrorist organizations will inspire Right-Wing terrorist organization who will inspire Left-Wing and Antifa organizations to commit terrorist acts.

The end result is the possibility that continued or worsening situations will destabilize nations and regions on NATO's borders that may drive NATO into an operational mission to counter-terrorism.

In order to counter the threat of terrorism and support NATO allies and partner nations, NATO has developed a CT Policy, Military Concept for CT, and annual Counter-Terrorism Action Plans.

The political nature of terrorism means that militaries will always be in a supporting role. Military capabilities can be used to advance non-military objectives, but:

Military power is unlikely to the decisive. A Rand study looking at how terrorist organizations end concluded that:

- Militaries win 7% of the time,
- Police and legal actions win 40% of the time,
- Terrorists win 10% of the time, and
- Terrorists join the political process 43% of the time.
- From RAND corporation study 1968-2006 done in 2014 of 268 terror groups endings.

Militaries are best used in collaboration with other instruments of power to enable activities and fill gaps with military capabilities.

NATO's Military Concept for CT objectives are: to project stability and support allies and partner nations through cooperative security.

This is closely linked to NATO's three essential core tasks - collective defense, crisis management and cooperative security. Military power alone will not be able to deter, defend against, nor defeat terrorism.

To accomplish this, NATO developed in 2012 a CT Policy where it identified some key principles and main focus areas for its CT strategy. In 2014, 2017, 2018, and 2019 NATO developed detailed action plans to support interaction with partner countries and organizations.

Compliance with International Law. NATO will continue to act in accordance with International Law, the principles of the UN Charter and the Universal Declaration of Human Rights. The UN Global Counter-Terrorism Strategy, International Conventions and Protocols against terrorism and relevant UN Resolutions provide the framework for all national and multilateral efforts to combat terrorism, including those conducted by the Alliance.

Support to Allies. Although individual NATO members have primary responsibility for the protection of their own populations and territories against terrorism, cooperation within NATO can enhance Allies' national efforts to prevent, mitigate, respond to, and recover from acts of terrorism. NATO, upon request, may support these efforts.

Non-Duplication and Complementarity. NATO seeks to avoid unnecessary duplication of the existing efforts of individual nations or International Organizations as it develops its own contribution to CT in a manner that complements those efforts.

AWARENESS *is an essential enabler for the planning, preparation and execution of all CT activities.* NATO's military contributions include providing terrorism-related information, intelligence and assessments regarding Terrorism in order to enhance NATO's overall Situational Awareness and sharing relevant CT-related information with key outside actors, where appropriate and when it is militarily relevant.

CAPABILITIES derives from NATO's expertise in countering asymmetric threats that lend themselves to counter terrorism. This enables NATO to support partner nations with niche military capabilities and training with METs, in-residence course attendance at NATO schools, or specifically designed Advanced Training Courses is areas such as CBRN, C-IED, CIP, Crisis Management, Cyber defense, Terrorist Use of the internet, Attacking the Network, Military Border Security, and Small Arms and Light Weapons to name a few.

ENGAGEMENT. Through engagement and strategic communication, we help build a common understanding of the CT concepts and NATO's potential military contribution to CT as part of a broader international effort. Optimal application of CT measures requires

internal, interagency and international collaboration to ensure that overall effects are complementary, mutually supportive and synchronized.

These are good starting points but more can be done to support partners address the underlying root causes of terrorism.

NATO's ultimate goal is to avoid combat operations and missions to deter and defeat terrorism by supporting Allies and Partner Nations (PNs). The implementation of policies, procedures, and methods to support Allies and PNs in Soft Power activities to address the root causes and grievances of terrorism would have NATO use all elements of its power to support, coach, train, and advise Allies and PNs in their fight against terrorism.

The future role of NATO should be proactive by using all political and military means and capabilities of the organization, in order to create conditions within a country or in a certain region which help to handle terrorism related problems locally through a combination of Soft and Hard Power by the nations themselves.

Military forces can be used to shape conditions to enable a political resolution. The struggle is over the population and solutions need to be people focused.

Militaries are very good at "Find, Fix, and Finish" using attack the network models. To support Smart Power initiatives, governments can utilize the organizational and discipline of military forces to Attack the Network to understand terrorist organizations in the "Find and

Fix" phases. It is in the "Finish" phase that instead of a kinetic action that other instruments of Soft/Smart power could be used such as diplomatic, financial, public diplomacy, info operations, legal actions and son on.

Military and Hard Power are not the primary instruments of power to be used in the fight against terrorism.

Soft power is the best method to address root causes of terrorism through Whole of Government (WoG) and Whole of Society (WoS). NATO envisions engaging to a much greater extent with Allies, Partner Nations, the International Community, Non-Governmental Organizations, and civil society to set conditions inside of nations to address the grievances and root causes of terrorism through the application of diplomacy and Soft Power by, with, and through Partner Nations.

- There is much debate about the causes of terrorism and if there is any direct correlation of underlying preconditions leading directly to terrorism.
- Lack of good governance structures are a significant contribution to terrorism. In areas of poor or weak governance, the preconditions of terrorism exist; all that is needed is a catalyst.
- Preconditions such as: inability of a government to provide basic services/infrastructure, ethnic and religious tensions, political violence, political grievances, poverty, economic collapse, urbanization, migration, population growth, bulge in youth population, increasing population density, unemployment, social changes, perception of inequality, corruption, repression, sense of humiliation, clash of cultures, violence or conflict, negative effects of globalization, lack of opportunities, ungoverned spaces, advances in technology, and hybrid threats from outside actors to name a few.
- Before someone goes from being radical to becoming a terrorist a triggering event generally must occur. 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.
- The lack of good governance in combination with some or all of the factors mentioned earlier leads to fragile or failed states which are perfect breeding grounds for terrorist organizations.

- The promotion of good governance, utilizing a whole of government approach, is vital to fighting terrorism to address the conditions conducive to the spread of terrorism. NATO policy and increasing cooperative activity enable engagement between Allies, partner nations, and other international institutions. Good governance is supported through a comprehensive defence and security capacity building program.

Potential ways NATO military can support partner nations develop capacity to deter and counter terrorism include:

Develop roadmaps to enhance Partner Nations CT capacity in coordination with NATO HQ . The end result of the roadmap is a set of NATO validated requirements that donor nations could use to aid in the Partner Nation's capability development. Example is the Jordan CT roadmap and Border Security workshop with NATO IS ESCD, COE-DAT, UN OCCT, and other that validated Jordan's Military Border Security CT requirements for donor nations to assist with.

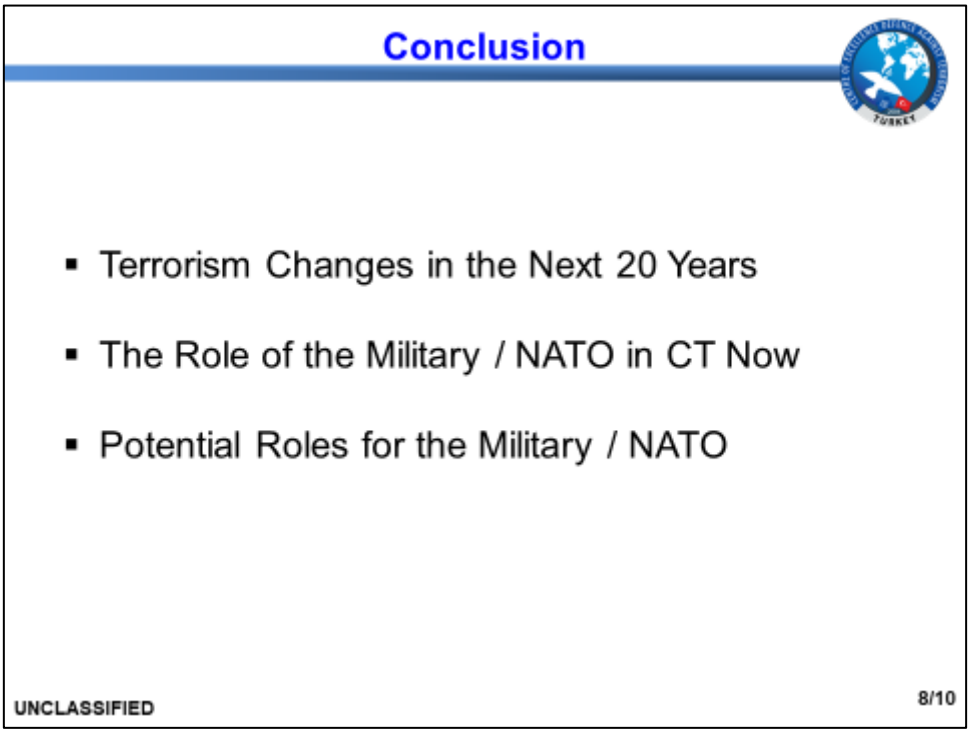
NATO can advocate for reform within nations and make NATO support contingent on visible actions taken by nations to address the systemic root causes of terrorism. NATO must advocate for anti-corruption as a precursor for NATO support to PNs and NoI

The development of Critical Infrastructure Security and Resilience requirements teams. These teams could assist Partner Nations to develop national strategies for CISR and to aid in the identification of capability shortfalls. NATO could validate these requirements for donor nations to assist in obtaining capabilities to fill gaps.

STRATCOM, advocate to Partner Nations to work with media outlets to minimize publicity of terrorist activities in order to take away publicity and the unintentional broadcasting of terrorist messages to the population. NATO message support to IC, Allies, PNs, and NoI in CT.

- NATO should continue to develop a narrative clearly describing why the common values of NATO nations is important and what democratic values are and why they are important.
- NATO should encourage nation to develop narratives of the values nations hold and provide a counterpoint to terrorist propaganda

NATO should promote critical thinking as a tool in combatting terrorism. Strengthening populations ability to see through the falsehoods in terrorist narratives can reduce the likelihood a person will join a terrorism organization.



Centre of Excellence Defence Against Terrorism

www.coedat.nato.int

UNCLASSIFIED 10/10

Day 2 Questions and Answers and Open Discussion

Prof.Mustafa Kibaroğlu

Weapons of Mass Destruction and Counter-terrorism

1) Is there a possibility of terrorist hijacking large oil tankers (Crude oil carrying ships for instance) in the near future and using it to cause destruction similar to hijacking of airplanes on Sep 11? If yes, what counter measures can you suggest? *Commodore Ahmed Abdullahi, Nigerian Navy/Operations/Commander*

Prof. Dr. Mustafa Kibaroğlu highlighted the strong possibility of terrorist hijacking large oil tankers. The record of the history shows that piracy incidents are not rare. In order to overcome the problem, NATO and some foreign countries have come together to cooperate on the issue by forming a naval force to combat hijacking, but it depends on the intention. With 9/11 we have seen something very novel and while many people did not think about such a possibility at that time, the consequences were high. Terrorists do not have moral values, they are not bound to legal treaties and conventions - it depends on their chances to carry out possible attacks.

2) How much do you think coronavirus can inspire terrorists to try to recruit scientists to spread a similar disease in the future and not only WMD? *Maj. Hadi CHEHAITLY Lebanese Army/Directorate of Intelligence – Analysis*

According to Prof. Dr. Kibaroğlu stressed that "inspiration has no limits". We have the Aum Shinrikyo case - who somehow managed to convince and hire some scientists and microbiologists to cooperate with the organization. In early 2000s, Ebola case was another problem - the terrorists were trying to have access to dead bodies with whom they could work in the laboratories and examine them in order to use them in their future attacks.

Intention also plays a key role here. People with technical skills may possess evil intentions and they are very well aware that creating and developing diseases can be used as a strategic tool against their enemies. COVID-19 may have inspired terrorists with scientific skills and knowledge with evil intentions - they can possibly be thinking of developing diseases that can resist any medications. The Biological and Toxin Weapons Convention (BTWC) needs

a verification mechanism because there are two labs for biosafety levels. However, this is where the problem starts - once the disease spreads, there is no control. No sober minded person would like to spread a virus deliberately because you cannot control the spread of virus or constrain the effects of a biological agent. As a result, governments and international community **must constrain the terrorist organizations or evil minded people's access to that technology and know-how.** Overall, it is a **low probability but high consequences scenario.**

3) Do you see an opportunity for creating more initiatives such as "lab to lab" between other states members of NATO? *Col. Petar MARINOV, Rakoski National Defence College / Land forces / Associate professor*

If there happens to be a necessity to protect some facilities or material for the members of NATO and former members of the Warsaw Pact, the United States and other advanced countries would help to secure those critical elements. According to a PhD thesis in Bilkent University that Prof. Kibaroglu supervised, there are new examples of lab-to-lab initiatives. But still, states' willingness to cooperate and collaborate with each other has an utmost priority. As long as states do not consent to come into a mutual platform, it is hard to have a common understanding. It **all comes down to sovereignty and willingness of a country, unless a country wants to cooperate firstly.** Either there needs to be some universal pressure from the international community like in the case of Iraq and Syria or cooperation like South Africa.

5) What are the chances for a given terrorist group/organization to reach out to a means of nuclear weapons (radiation isotopes) and chemicals materials? *Col. Petar MARINOV, Rakoski National Defence College / Land forces / Associate professor*

This issue was taken seriously by two senators and the Cooperative Threat Reduction was initiated in order to make all the installations where nuclear elements were involved. More than two decades and a huge amount of money was allocated to this project to dismantle thousands of nuclear warheads as well as keep some scientific knowledge in proper places and keep safe against third parties.

6) ***What are your views on one of the tools to counter WMD that is certainly de-armament and non-proliferation efforts currently seems to be on the verge of collapsing given the demise of the INF treaty and disagreement on START talks?*** *Mr. Oğuz EZİK*

Prof. Dr. Kibaroğlu reminded that states have a lot to do with their own capability to prevent terrorists organizations from having access to these nuclear materials and knowledge. We need a **combined and collaborated effort. Therefore, this CT Handbook plays a role -** one country cannot do enough on its own. This is a global threat and no one can be safe from this threat - cooperation is the key. Terrorists may find very "creative" ways and means to disseminate chemical agents or have access to some material that if they detonate radiological weapon with a conventional explosive, they can pollute the environment just like if an oil tanker would do if crashed as in the first question. We are losing a momentum, it is not like 1970s, 1980s or 1990s - the INF Treaty is not just history, unless by February 2021 United States and Russia agree to at least for new talks and behold arms control. However, this may all collapse and every state may turn to themselves in terms of policies. However, this may play into the hands of "states of concern" or violent non-state actors.

7) There are a lot of multilateral measures to counter WMD Terrorism, but Governments have to make more efforts to fight terrorism. What are possible strategies to prevent WMD attacks? *Col. Haitem NASSIRI Royal Armed Forces / 5t bureau / HQ / RAF*

Governments must take active as well as passive measures. For instance, preparing the society against possible biological agents that can be used in a terrorist attack or by a country of concern. This has many difficulties because you cannot vaccinate the entire society against all possible viruses or you cannot provide everyone with proper masks to protect people against these agents. So again, it comes down to **cooperation and collaboration. Governments must acknowledge that this threat is real -** this is not an exaggeration. They have to mobilize their own governmental mechanisms within their control and sovereignty and **cooperate to the extent as possible on government to government level and share intelligence.**

Intelligence is the most precious asset. Governments or states often do not share intelligence within their own institutions, let alone among states. We should not wait until something catastrophic happens to take action and cooperate. Unless governments agree to share intelligence, individual governments have limits in achieving fight against terrorism - government cooperation is about everything. Nuclear Security Summit is an example of this in which the purpose was to introduce the leadership of what we are talking about and that this is

not a scholarly exercise or a scenario of a remote possibility, but if and when it happens, the consequences will be catastrophic and people will regret of now cooperating before.

Dr. Ashraf Afzal, Ms. Stephanie Foggett

Media and Counter-terrorism

1) "What is your assessment of the viability of online counter-radicalization programs by governments especially where there are recurring problems of credibility?" *Maj. General Gbolahan OYEFESOBI (NGA), Defence Intelligence Agency/Deputy Chief of Defence Intelligence*

There is no objective measure of success - that is the problem we face. The London Bridge attacker couple of years ago was an individual already gone through the de-radicalization program. It was not an online program but was conducted face-to-face. In addition, the terrorist attack in Vienna carried out recently is believed to have gone under same programs.

If the matter is de-radicalization here, these cases clearly indicate that radicals and their radical thoughts do not change. As long as the reality around them does not evolve into a different environment, the terrorists do not change, either. Therefore, it is not adequate to only change the narratives. In terms of counter-radicalization, a great amount of financial support has been allocated on countering religious narratives. However, as terrorists keep creating "counter-counter narratives", these efforts of online counter-radicalization seem to have failed. Counter-radicalization programs only work with those people who are not susceptible.

1) ***"How can social media be used to prevent violent extremism being disseminated by terrorist groups on the same platform?"*** *Col. Haitem NASSIRI (MAR), Royal Armed Forces/5t Bureau/HQ/RAF*

Mr. Ashraf highlighted there has not been much success in this field. Even though several social media companies have tried to prevent these actions, these attempts have been

constrained. The attack in New Zealand proved that their abilities are constraint. The New Zealand mosque attacker broadcasted the attack live and recognized the constraints put on social media - about 200 people watched that attack live. Within 12 minutes, this was reported to the social media company. But still, nearly 4000 people had watched the attack as well as been uploaded by right wing channels until the video was removed by Facebook. Within 24 hours, Facebook alone had to block 1.4 million attempts to upload that program. This clearly shows the scale of the problem.

We have to accept that this is a battle space - we have to block messages as much as we can to constrain it. As a result, it could be stated that these social media platforms, at least in a foreseeable future, cannot be controlled. Based on our historical evidence of Al Qaeda, where the world's top intelligence services working together could not stop Al Qaeda to put its messages out and that was before social media came along. **We must accept that this is a place where we can constrain, but not stop.**

2) **"*Can an effective counter-terrorism communication strategy provide deterrence against terror organizations? Can we use STRATCOM as a deterrence tool*?"** Lt. Col. Cenkan SAĞIR (TUR), SHAPE J5 / Strategic Policy Officer (CT)

Dr. Ashraf pointed out that there has been no strong evidence that using STRATCOM or any other form of communication in which a terrorist group has been deterred. However, there have been tactical measures that have prevented attempts of attacks, i.e. preventing hijacking of airplanes on a strategic level. These are quite significant because once terrorist organizations are convinced that this method is not going to work, they stop trying. In terms of generic deterrence and to stop terrorists from furthering their cause to other means, Dr. Ashraf was not aware of any successful application of STRATCOM to achieve that.

3) ***"How can possibly be achieved a balance between the ratio 'a freedom to speech and minimizing the effect of the one of aim of the terrorist acts - producing a culture of fear'?*** *Col. Petar MARINOV, Rakoski National Defence College / Land forces / Associate professor*

Dr. Ashraf added that democracies have to remember that whatever they do in counterterrorism, they most not compromise their own values - this is an outcome of a life

research of Prof. Paul Wilkinson. Prime Minister Thatcher once tried cutting off the IRA of speaking their words and that did not work. **Debate is necessary** in society but we should not compromise freedom of speech but the balance of the debate is paramount. There is an imbalance of presentation between right wing terrorism and Islamist terrorism. There is up to three to five times more coverage given to Islamist terrorism than on right wing terrorism. Very rarely, right wing terrorism is actually identified as terrorism. What we see here is a disproportionate way of dealing with news. If we can suppress the fear of right wing terrorism, then surely we can do something similar to suppress the fear of Islamist terrorism.

It is important that the world leaders do not manipulate the media and the presentation of terrorism of political purposes. President Trump has declared that terrorism has been underreported but what he really meant was that it was not the right wing terrorism but Islamist terrorism. Recently, president Macron has started to do it mainly because of his electoral prospects given his main rival Le Penne and by suggesting that Islamist terrorism targets 80% of its own population and not Europeans.

5)"I am wondering whether the best principles (for media) mentioned during the presentation would still be the best in addressing, for example." *Lt. Elvin BALAJANOV (AZE), State Security Service / Counter Terrorism Department / Specialist*

Communications or media do not address the threat directly - they engage with the causes and the rationality of a threat. Dr. Ashraf emphasized that we must be very careful to prepare for the possibility of a WMD type of attacks but we must be very careful not to advertise and widely debate those issues. It is best to avoid such discussion through media coms of what we do not want terrorists to get hold of. The current tendency of fragmentation in those organizations may urge the individuals who have expertise on biology, chemistry and physics to take an action. In this regard, one of the best things in terms of media communication is to avoid to discuss things in public such as things that we do not prefer the terrorists to think about.

6)"*In his very interesting assessment, Dr. Ashraf told that narratives would only convince people who are not prone to be terrorist. But what about using the codes and values of the terrorist themselves, to discredit and debunk them? For instance showing them as cowards attacking weak people, women, to break their image of courageous knights."* *Col. Edouard ROUCHER (FRA), French Army - DRHAT / Deputy Head of Office*

It has been tried; however, the reflection/counter-narrative from the terrorists side was "*If you think we are cowards just because you believe we attack the weak ones, what have you done, Westerns?*" In an interview, the Secretary of State, Madeline Albright was asked why did you kill five hundred million children in Iraq through sanctions. Albright replied that although it was indeed a sensitive matter, they thought it was worth it. For instance, bin Laden's counter-narratives describe the West in a pejorative meaning due to killings and murders. That narrative of killing innocent women and children can be also found in religious teachings. Dr. Ashraf believes that the counter narratives have to come with some form of reality and thats where our weakness lies. He suggested that those narratives are successful for those who possess narrow perspectives. On the other hand, the counter-narratives do not actually pave the way for de-radicalization for people who already involved attacks and murdered innocent people.

Prof. Ronald S. Bearse

Critical Infrastructure Protection

1) ***Do you think terrorism has an indirect influence on long term relations between the nations?*** *Col. Mounir DAHER, LBN, General Directorate of State Security/VIP Directorate/Head Of Section*

Actually, it does not. However, it helps towards diplomacy. The answer of the question is that it depends on the situation and the level of trust that exist among the states. History matters, that is, even under the circumstances of war or peace. Having a dialogue is important.

Open discussion

Why does terrorism always grow in poor and incoherent societies? Do you think it is a strategy to spread their beliefs? *Col. Mounir DAHER, General Directorate of State Security / VIP Directorate / Head Of Section*

Dr. Bearse stressed that history has shown that **it does not matter whether terrorists come from rich or poor societies - terrorism is in every society.** What we have learned from the debriefing and people coming out of the battlefield area is to understand the dynamics of such terrorist groups, we do see them coming out of poorer societies. There is also terrorism in USA and it is not a poor society - terrorism does not only happen in less advanced societies. Terrorism has been around forever, it will continue, it is a way to prosecute and have your voice heard in societies that have been suppressed.

How can we interrupt the terrorist groups vain attempt to instrumentalize international A-list issues and matters, issues strongly vehicled by media all over the world, as a point in case, just yesterday the dubbed commander of Al-Shabab in Somalia threatened to take revenge from the French authorities due to the recent declarations against Islam. That is to say, how can we avoid paving the way for terrorists to ride the tide of events to widen their sympathizers? *Col. Haitem NASSIRI, Royal Armed Forces / 5t bureau / HQ / RAF*

Mr. Harley added that al-Shabab like many terrorists groups say more than its prayers - it has a very strong regional focus. Al-Shabab is not focused on attacking Western countries like France but rather Ethiopia, Djibouti and North Kenya. They are exploiting the need to fulfill the 24/7 news cycle with "stuff". But, they get a media inflation for saying something like that.

Prof. Yalcinkaya added that when comparing bin Laden's and al-Baghdadi's narratives, bin Laden's narrative was against non-muslims but al-Baghdadi's narratives was a peaceful invitation to join the group and preferred the use the term Deash, having negative connotations in their mind.

Col. Stone

Potential Future Role of NATO in Counter - Terrorism

1) ***Across the presentations we have seen proposals addressing examples of best practice across a range of areas, from the negotiation of international treaties on securing radiological materials to military media ops at the operational level. To give useful feedback on the development of the handbook it would be interesting to know who the anticipated users will be?*** *Mr. McNally STEPHEN, NATO Intelligence Fusion Centre / CT Intelligence Analyst*

*Combined answer below.

2) ***NATO launched Counter-Terrorism Reference Curriculum (CTRC) in 2020. It supports interested Allies and partner countries in enhancing their capacities to develop national skills and improve counter-terrorism strategies. Drawing on historical examples, the CTRC provides an overview of terrorist ideologies, motivations and methods, as well as contemporary counter-terrorism practices and potential future projections. COE DAT's project, CT Best Practices Handbook, will also serve in the same area. Will the Best Practices Handbook be complement project to CT Reference Curriculum? Or will the handbook be more unique product, which aims to serve mostly in academic area?*** *Lt.Col. Cenkan SAĞIR, SHAPE J5 / Strategic Policy Officer (CT)*

Regarding the **possible audience of the CT Handbook** and whether it is a complimentary product to the already published NATO **CT Curriculum,** Col. Stone highlighted that when the Handbook project started, the focus was on looking at the questions of what can we really get out there that would be beneficial? We tried to hit at the strategic and operational level to get the senior military officials and governmental officials to think about a different way of using military power and counterterrorism. It is faulty logic to believe that only high end activity gets rid of terrorism and to break that, it is part of what this book is all about. The Handbook is also designed for the operational country team planners, for people who do country teams. When we look at NATO and allied nations, they have country teams that look at campaign planning and this will be a useful tool for them as they look at what military power can do that and if this is the wrong tool, what tools are available on how can the military elements try to influence the non-military side of it?

These best practices are not all of the answers but have worked in some nations. **Context is very important -** some practices may work in one country, but may not work in the other as the context is not right. We are looking at strategic level leaders but ideally we are looking at

planners. The ultimate one it is the young officers who will grow up to be leaders of the future because these ideas will start shaping their ideology as they go forward.

Col. Stone added that the NATO CT Curriculum serves as an introductory course with broad ideas about terrorism and CT. The CT Handbook is more of a compendium of good practices and will look into very specific areas that we are interested in.

Regarding accumulating knowledge for the CT Handbook, Prof. Bicakci stressed that the age is changing, the generation is changing, the infrastructure in which we are functioning is changing - we have to care about all facilities. We are dealing with hybrid warfare. Terrorists are using all possibilities and ways to paralyse the system. We have to form consciousness of all readers. A new understanding is required to understand the battleground battle and the new generation battle. Even with new computer games, Daesh has been manipulating to use such games for training purposes and recruitment. This consciousness would help to understand them and for the leaders to understand the battleground. With this handbook, we will present a pool in which changing of these best practices will be presented.

With regard to **NATO's CT policies,** Col Stone added that for NATO, CT is the responsibility of an individual country but NATO also looks at the collective Alliance, the realization is looking through the Middle East and Northern Africa that they have the threat and we need to support other nations in fight against terrorism. NATO should focus on nations that are around NATO and help them secure themselves against terrorism because this would enhance NATO's security as well as themselves. NATO has come to a realization and is asking what is it that these nations need and helping to define where NATO can fit in? How can NATO help in terms of support? What is the need and requirement?

3) About CISR, do you think that NATO's cooperation is enough with other Governments especially in African countries? In which kind of platform is it effective? *Col. Nicodeme NDIONE, Armed Forces / Zone Militarie No7*

Col. Stone stressed that no, NATO is not doing enough but trying to find ways to do more. The COE DAT has focused on CIP courses and resilience and CISR teams to go to nations to look at what they have, what their policies are in terms of critical infrastructure and what is that they need and desire. This request can be given to NATO through country teams to push forward. If there is a demand signal, it helps NATO to fulfill it. Dr. Bearse added that the expertise teaching the CIP course in COE DAT has realized that those who have been involved

have learned the lessons in a hard way before the system has grown and identify what these nations need and build awareness that has now turned into requests from these nations - we are capable of doing it.

4) How far the tendency of supporting and influencing the institutional reforms in different state members by NATO, can reach? How far the tendency of supporting and influencing the institutional reforms in different state members by NATO, can reach? *Col. Petar MARINOV Rakoski National Defence College / Land forces / Associate professor*

Col. Stone pointed out that there is not much what NATO can directly do - there are limited things that NATO can do with regard to CT. What can NATO do in terms of influencing institutions and NATO nations? NATO can work with nations and **use its influencing force** of how nations are operating and change their institutional culture. In the security sector reform and defense institution building area there is capacity for that. These are the things that will take a long time - to change institutional process is not easy.

The COE DAT has focused on successful mobile training teams to interact with junior officials and provide them with institutional areas of CT as well as with useful tools. The longer there is connectivity between NATO and nations, the more there is bleeding over what we believe is common - that is what will create the institutional change. These junior officers will be the future leaders of these nations.

A nation's attack is up for the country's police and armed forces to directly respond, there is not much that NATO can do, unless NATO is requested to provide help. It is critical that NATO is talking to its Alliance and sharing information where applicable to make sure we are passing information to each other. This is why this event is also important for us because this is where we can talk to nations and learn about terrorism to get a better idea of it. If we can understand perspectives and issues of other countries, it is easier for nations to support each other. NATO talks to our partners to make sure we pass information to each other. **We have to communicate to understand the threat.**

5) Apart from the Hand book on CT, is there any plan to develop and publish a NATO STANAG for CT? We host the Commanders Counter Maraufing Terrorist Attack course in our school here and has been discussed with the international students whose backgounds include Military and Law Enforcement Thank youApart from the Hand book on CT, is there any plan to develop and publish a NATO STANAG for CT? We host the Commanders Counter Maraufing Terrorist Attack course in our school here and has been discussed with

the international students whose backgounds include Military and Law Enforcement? *Col. Nicodeme, NDIONE Armed Forces / Zone Militarie No7*

Col. Stone commented that from a practical standpoint it would be relatively unmanageable in a sense that a STANAG is a very set procedure whereas what we see in terrorism is rapidly changing. How NATO is handling this is setting out policies that came out in 2012 and more importantly, from 2014 onwards there is a yearly CT Action Plan and year by year evaluating success on a strategic and operational level. On a tactical level, i.e.e stability policing COE, civil-military COE all have a hand on working on a tactical and practical level.

***

How do you see the role of technical assistance and capacity building to be one of the major points in the cyber space? *Mr.Mirwais QADERI, National Directorate of Security / Counter Terrorism /First Deputy of CT Department*

Mr. Qaderi further touched upon CT issues of Afghanistan and the lack of capacity and capability to counter terrorists' narrative in Afghanistan. Dr. Bearse suggested that outside NATO, it is wise to think about talking to people on CENTCOM in order to talk to people who work in the State Department and have the experience of protecting domestic databases and not focus so much on the military side. NATO and the Estonian CCD COE have the capabilities to strengthen Afghanistan's expertise.

Dr. Bicakci added that to build up cyber capacity is a good effort and it needs **diligent and a long planned strategy.** The Estonian NATO CCD COE has done a lot of great work in this and has manuals how to best reach these capacities and goals for a country. For instance, there has to be cyber security capability in the military and MFA in sense of cyber diplomacy, focus should also be on intelligence and critical infrastructure protection. Dr. Bicakci suggested focusing on national security strategies regarding cybersecurity capacity building. NATO is also forming connections with global telecommunicating companies like Global Internet Forum to Counter Terrorism.

You also need to actively focus on **cyber intelligence and the human capital.** However, the problem is that the public sector pays less than private sector. Another issue is that different bodies have different types of cyber intelligence. Military and law enforcement have their own intelligence sources but you should build a common body to build this confidence. Also, you should have a body under the MFA who could talk to international companies, otherwise, you should learn their terms yourself - it is all about strategic

communication. Overall, the COE DAT would be a great place to start for having advice, also Estonian CCD COE. For CIP, Lithuania NATO ENSEC COE would be a good source for energy.

Overall, Prof. Yalcinkaya stressed that our main goal of this workshop was not to come up with the solution to eliminate all terrorism in the world but to accumulate the information knowledge and transfer this to a written document. Participants agreed that social context in which we discuss terrorism and CT issues is important. Prof. Bicakci added that it is not easy to give a quick practical solution to the military because of the nature of the problem. Terrorism is a geographical, human, time, context and a multinational problem.