CHIEFS OF TRANSFORMATION CONFERENCE: SYNDICATE SESSION 3
"Hybrid/Counter-Terrorism Connected to Resilience"

Premise:

"Alliance ability to conduct and sustain operations by preparing for, absorbing, recovering and adapting to the surprise or strategic shock [of Hybrid Attack and/or Terror] through harmonized and resilient structures, systems and processes enabled by the persistent collaboration across public, military and private stakeholders."
—Collaborative Resilience Capstone Concept (CoRe) Vision

The enormous complexity of NATO's security environment includes Allies, Partners, governmental and non-governmental organizations (GO/NGO), commercial entities and the public. NATO is defining its role in Resilience through the Civil Emergency Planning Committee (CEPC) policy, and aligning Counter-Terrorism (CT) and Counter-Hybrid Warfare (CHW) concepts, and action plans. NATO needs to collaborate to prepare, deter, and defend to be resilient against strategic shock, but *how* we work together is the challenge, especially when faced with a diverse community of interest (CoI), classification and national sensitivities. To frame this Resilience discussion we will use NATO's role in CT/CHW. At the core is information sharing.

Information sharing not only provides us the ability to learn from our combined experiences, but is critical for improved decision-making. Information and its derived intelligence is based on aligning civilian-military (CIV-MIL) cooperation. Information reinforces political control, provides indications and warnings, and CIV-MIL options earlier in the current-operations-to-crisis transition. This is vital political and military time to shape events, outcomes, and anticipates CT/CHW opportunities. Armed thus, CIV-MIL leaders provide the CT/CHW resources with the means and permissions to conduct operations (kinetic/non-kinetic), actions (key leader and staff engagements), and investments (OAIs). Key to this program's success is NATO's human capital.

The SOF adage, "people are more important than hardware", resonates in the Resilience enterprise. The Resilience CoI requires CT and CHW experts to provide sound CIV-MIL advice and to conduct CT/CHW OAIs to meet the NATO strategic ends.

Aim: The success of Resilience/ CT/CHW OAIs is structure; a comprehensive approach which includes:

1. Resilience/CT/CHW Situational Awareness for decision makers;
2. A CIV-MIL information collecting and sharing architecture;
3. A CT/CHW human capital plan to include Education and Training;
4. Interoperability (Standards, Agreements, Assessments, Resources, Exercises)

Why the concern over Resilience, Counter-Terror, and Hybrid Warfare: Working closely with NATO HQ, ACT will align the Resilience/CT/CHW concepts and action plans with emerging CEPC policy. Cross-functional action teams will incorporate the findings from the Chiefs of Transformation Conference to refine these processes. The strategic documents will in turn create a clearer picture of *what* NATO needs to do and *how* NATO supports Resilience/CT/CHW information collecting/sharing, investing in human capital and setting the standards for interoperability not only within the Alliance, but with our Partners, and including governmental and non-governmental organizations, commercial entities and the public.

How this Syndicate Session approached these challenges:

This session was facilitated by Dr. Robert Weaver and moderated by Dr. David Kilcullen, a critically acclaimed expert in this subject. Through elicitation and response, the audience was actively involved in sharing best practices, lessons learned and proposing solutions to the questions posed, below.

Questions we answered:

- What CT/CHW data does NATO need to collect/share to improve Resilience?
  - Military to Military
  - Civilian (to include private sector) to Military
  - Military to Civilian (to include private sector)
- What are the biggest challenges/opportunities with regard to information sharing?
- How does NATO Create Trust, Transparency, and Shared Awareness with the Private Sector?
- Resilience is more than civil preparedness: what process(es) does your nation use to assess national CT/CHW military-civil-private sector vulnerabilities? Do you have best practices and lessons learned to share?

Information Sharing Architecture

- How should the Alliance information sharing framework look?
- What innovative technologies should the Alliance / nations use to information share?
- How does NATO incorporate civilian and private sector into its information sharing architecture?

Human Capital

- What changes should NATO make to CT/CHW/Resilience human capital systems today, in 10yrs?
- Resilience is whole-of-government focused, how does a nation prepare its civil and private sector human capital in the face of CT/CHW?

Interoperability

- How do NATO nations increase:
  - Authorities (permission to train/operate with mil-civ-private sector);
  - Access (for leader/staff exchange to conduct engagements/assessments to include SME from mil-civ-private sector);
  - Resources (trained personnel, equipment, logistics, mobility, contracts); and,
  - Appropriations (funding)?
- What scenarios need to be created for exercises to address potential Resilience vulnerabilities; what best practices can NATO adopt from non-NATO exercises (national, regional, bi-lateral).
- What civil-military-private sector agreements does your nation/organization have in place to maintain resilience in the face of CT/CHW? How did you put them in place (contract, legislation, other)? What best practices, lessons can you share with the group?

Syndicate Discussion Main Points:

- Resilience is a whole of government function that is typically not led by the military. NATO planning/structure must be cognizant of that and the impacts of local culture on resilience planning/operations.
- Hybrid, resilience and counter terrorism priority information requirements (PIR) are not effectively shared and Nations do not have common agreement on actions PIRs should prompt.
- Hybrid, resilience and counter terrorism strategic communications are critical to gain and maintain public support for individual, community and national response programs including human capital.
- Utilize synthetic environment to certify military requirements along the 7 Baselines. Taking SJO and MJO force composition to simulate force movements.
- Critical thinking helps to create reliable information and a culture of trust.

Syndicate Actionable Items:

- To facilitate information sharing Nations (NATO) needs:
    - ACT to develop a synthetic information environment; able to be used by whole of DIMEFIL (PMESII) to early detect imminent threats/risks using a deviation from baseline process and assist whole of government./ whole of society in a proactive and reactive response.
    - A system of linked fusion centres across regions or nations.
    - Regional forums for discussions among Nations and other stakeholders on information sharing.
- Create minimum guidelines against each of the 7 baseline resiliency requirements for Civil Preparedness listed in the Warsaw Agreement.
- NATO must establish a common language and definitions for resilience and hybrid.
- There are three areas where NATO ACT can play a role in counter terrorism (CT), counter hybrid warfare (CHW) and resiliency:
    - Identify best practices for military integration/partnerships with civilan/private sector agencies/organizations that have a resilience/CHW role. i.e. law enforcement, industry, etc…
    - Identify best practices for military involvement in education of the public and elected leaders on CT/CHW awareness and response.
    - Provide a forum for human capital discussions on how to bring CHW skills into the military through non-traditional ways.

Syndicate Closing Plenary Slides