NATO INNNOVATION CHALLENGE SCENARIO

12 October, Bucharest, Romania

Introduction

In today's complex and unpredictable environment, governments and organizations must be resilient in order to withstand shocks like natural disasters, failure of critical infrastructure, and military attacks.

The rise of hybrid warfare, combining multiple types of instruments, including not just conventional forces, but also disinformation, cyber-attacks and the use of proxy forces, has led to a new paradigm of vulnerability on the part of complex, relatively open societies. Among other trends, we find grey zone threats where adversaries deploy measures short of the threshold for armed response or which afford them significant deniability through problems related to attribution. These measures increasingly target civilian critical infrastructures, in domains such as energy, public administration, finance and banking, food distribution, water treatment or healthcare.

While creating resilience is a responsibility of individual institutions, it does not exist in a vacuum and requires coordination and commitment from a wide collection of interested and affected parties. This is especially true in the case of international and collective organizations such as NATO. Enhanced resilience strengthens NATO Alliance capabilities and is a critical component of humanitarian response, credible deterrence, and defence.

This was recognized and reinforced by the commitment made by the Allies in 2016 at the Warsaw Summit, through the agreement of the Seven Baseline Requirements for national resilience and the 2021 Strengthened Resilience Commitment. These requirements reflect the core functions of continuity of government, essential services to the population, and civil support to the military.

In some circumstances, military forces heavily depend on the civilian and commercial sectors for transport, communications, and even basic supplies such as food and water. At other times it is the civilian and commercial sectors which rely upon the military. Establishing, maintaining, and deploying resilient systems is key to both civil preparedness and military capacity.

This challenge addresses Resilience from a whole-of-society approach, combining the civilian, economic, commercial, and military factors. It emphasizes the importance of planned data collection, secure data sharing and effective data management during the crisis.

Scenario

Under a United Nations mandate, NATO conducts an operation to assist a partner nation to recover from an attack by a neighbouring power.

In this fictional scenario, NATO forces are deployed to assist the host nation rebuild infrastructure after a few months of conflict. The country is partitioned, a durable cease-fire is observed, but tensions between different factions threaten the reconstruction efforts and the facilitation of reconstruction (logistics, relief, etc.). NATO would be working to help the host nation recover from the damage caused by several months of war and is responsible for Planning Response activities.

NATO is supporting the host nation with supplies and equipment during a potential crisis situation. The majority of supply movement is based on civilian transport assets. As the security situation can deteriorate during the assistance operation, there is a need to develop a good understanding of the complete supply chain, as well as to ensure the effective management and security of sensitive data among military/governmental and civilian/private sector stakeholders.

Besides the infrastructure and logistical aspects, the data environment is much more complex than we usually expect. To get an accurate picture of the entire situation, different data sources and streams need to be collected and integrated. Among the mentioned stakeholders that can provide reliable data sources, publicly available datasets also play important role in giving us the insights into situational awareness at the ground. Data management and security should enable sharing and exploiting all available information in timely manner.

Challenge

The aim of this challenge is to receive innovative proposals on sub-topics related to **data management and security in the context of civil-military cooperation in support of reconstruction efforts, taking into account the relevant data streams**. Particularly, NATO is interested in having proposals addressing the following sub-topics:

1. **Ingesting data into common architectures for data management and/or data security**.
   This sub-topic focuses on proposing common architectures for data management and/or data security in support of civil-military cooperation, providing an overarching and interoperable information exchange system.
   During the support of a crisis, it is necessary to gather, analyse, and take action based upon data coming from a variety of sources. Some of these sources may be well established in advance and structured. Others will be situational, becoming important and available at the time of the crisis or action. This data may not be structured. We are looking for solutions which:

   a. Ingest and translate outside data into a common and interoperable architecture for management. Interoperability should be ensured in the three following dimensions: procedures, equipment and human aspects.

b. Ensuring that new data does not impact the security and operations of the management / analysis system.

2. **Integration with NATO Operations Logistics Chain Management.**
   This sub-topic addresses the integration between civil-military Host Nation and NATO Operations Logistics Chain Management systems. We are looking for a solution that:
   a. Collects, fuses and analyses data from disparate sources (logistics depots, maintenance facilities, medical facilities, fuel and energy, maintenance facilities, etc.)
   b. Identifies, locates and provides status of all logistics resources;
   c. Ensures the identification of weaknesses, chokepoints and vulnerabilities in the following areas: C2 (command and Control), authority and legislation, infrastructure, capabilities.
   d. Identifies potential future outcomes using predictive analytics techniques.

3. **Scalable data models to support the design of interactive dashboards and predictive analytics**. Integrated systems will generate massive amounts of data in a multi-domain security environment. In this context, it is essential to be able to design scalable data models displaying interactive dashboards, integrating predictive analytics, to provide commanders and national stakeholders (as appropriate) information awareness tools that facilitate decision making.

Solutions can include any combination of methodologies, concepts, techniques and technologies.
Solutions involving blockchain, augmented reality/virtual reality and artificial intelligence are particularly sought after.