Countering Hybrid Threats: What Can CIMIC Do?

Chris Kremidas-Courtney
Senior Fellow, Friends of Europe
Lecturer, Geneva Center for Security Policy
Hybrid SME/Faculty, Institute for Security Governance

Hybrid Threats

- **Hybrid Threats: a challenge to nations, institutions, and private entities through a wide range of overt and covert activities targeted at their vulnerabilities.**
- **A way to achieve aggressive political aims “on the cheap.”**
- **Hybrid Threats vs Hybrid Warfare: avoid temptation to militarize a phenomenon that is actually much broader and more complex.**
- **A threat to both public and private entities, with the private sector often being the first targets of a hybrid campaign.**
- **Threat to public safety and security in the stricken nation.**

Hybrid Threats: Nothing New?

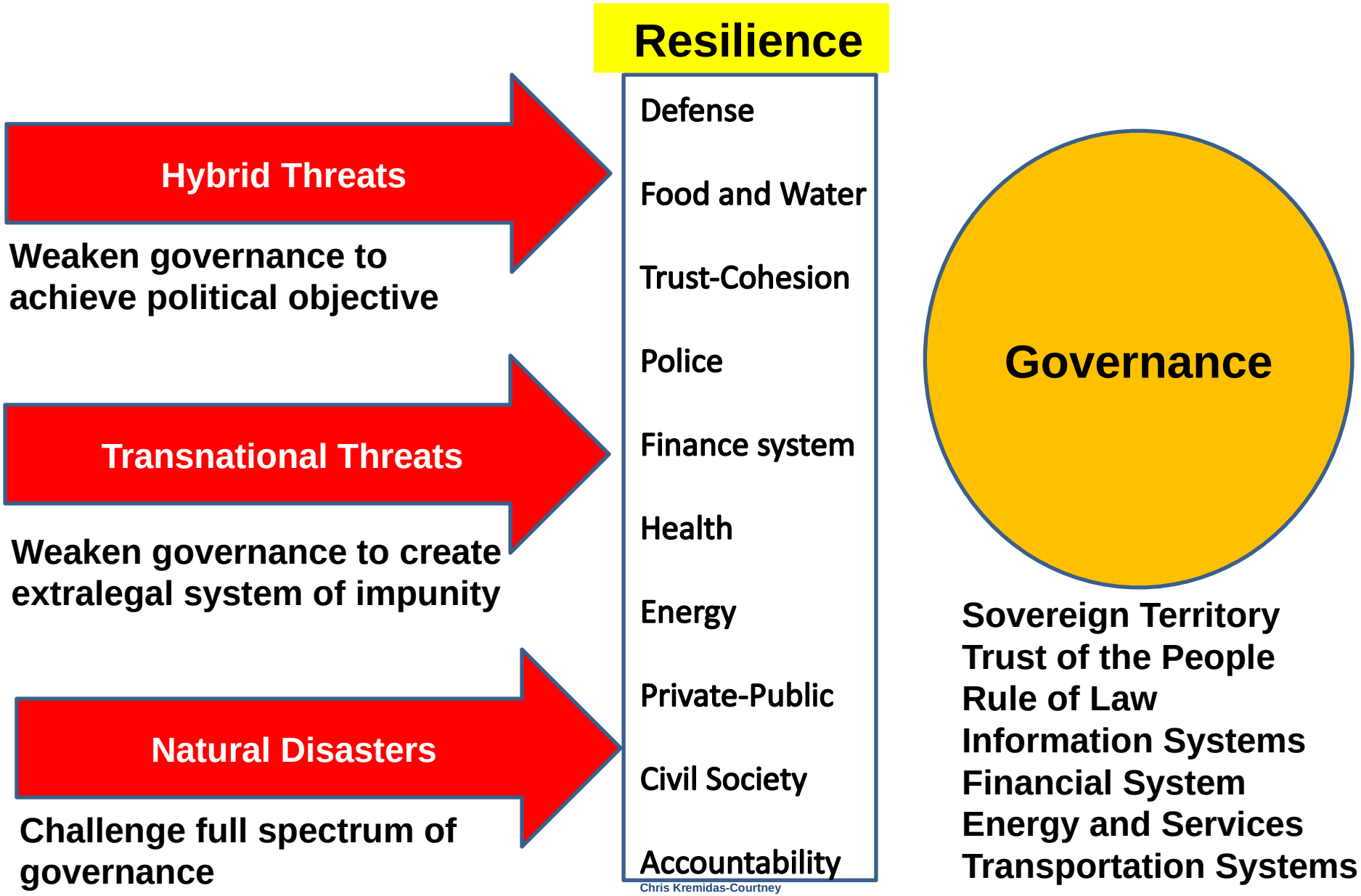
What makes hybrid threats different?

- **The new vulnerabilities presented by a globalized world interconnected by:**

  - Instant global communications
  - Systems of finance
  - Global commerce

- **The weaponization of globalization.**

Resilience as Deterrence



Chris Kremidas-Courtney

How to Deter Hybrid Threats?

- **Most theories of deterrence are based principally on the use (or threat) of military force**
- **Hybrid is a way to achieve political objectives “on the cheap.”**
- **What political aim? Destabilize another country; coerce, intimidate, conquer, etc.**
- **How to deter? <u>Raise the price</u> by hardening the “target” or being able to attribute and respond decisively, or both.**

Countering Hybrid Threats: Four Steps (Non-sequential)

- **Detect:** detecting a hostile state action (HSA) in time to react and minimize any potential damage.
- **Attribute:** attributing a HSA to a specific actor and to differentiate it from an accident, system failure, or human error.
- **Respond:** to change security posture and/or retaliate against the actor to which the HSA is attributed (in accordance with existing just war ethics).
- **Recover:** restoring functionality to the systems, capabilities, or societal coherence attacked through the HSA.

Hybrid Threats: Key Challenges

- **Disinformation: The response dilemma**
- **Attribution: Expert level – political level**
- **Consensus: Inter-ministerial and International**
- **Public and Private: Initial targets are private**

Hybrid Threats:
Solving Authority and Capability Gaps

- **Non-MOD ministries most often have the authorities to act – but lack some capabilities needed in crisis**
- **MOD often have the capabilities needed in a hybrid crisis – but lack the authorities**
- **National legal and policy frameworks to support inter-ministerial support and information sharing**
- **Tabletop exercises to identify gaps and vulnerabilities in legal and policy frameworks and test cooperative mechanisms**
- **No government can pay for the same capabilities twice**

Strengthening Governance to Counter Hybrid Threats

- **Resilient, credible, and capable governance; Resilience as deterrence**
- **Deeper cooperation among public, private, and international organizations**
- **High-trust societies are much more difficult for hybrid actors to target with disinformation campaigns.**
- **A whole-of-government approach**
- **A whole-of-society approach**
- **A comprehensive approach**

Whole of Government (WOG)

- **Agencies and ministries from national to local level work together and share information.**

- **Valuable for its ability to enable the authorities and capabilities of various ministries, agencies, and local governments**

- **Supported and supporting relationships (MOD seldom the lead)**

Whole of Society (WOS)

- WOG plus engagement with the private sector, civil society, and academia.
- Valuable for its ability to provide unique capabilities and information sources in addition to building support among the population for the effort
- People support what they help to create

Comprehensive Approach (CA)

- A way to achieve a common understanding and approach among all (interested) actors of the International Community.

- Requires actors to work together with a shared sense of responsibility and openness, taking into account and respecting each other's strengths, mandates,roles, and decision-making autonomy.

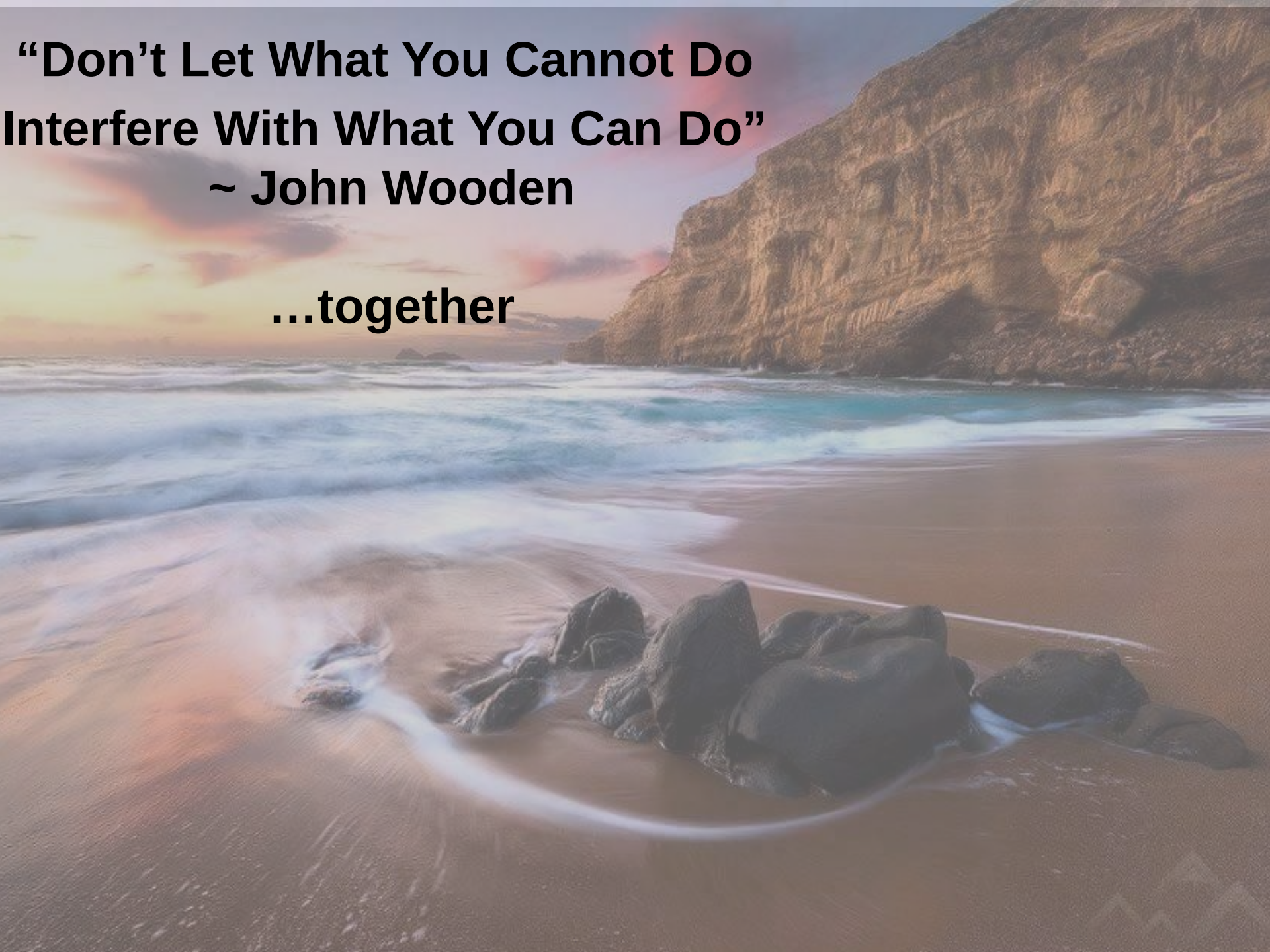
- In other words, the Comprehensive Approach is not hierarchical but rather a collaborative effort among equals.

Hybrid Threats: Key Lessons Learned

- **You can’t surge a relationship**
- **Attribution is the sovereign decision of the host nation (to include public messaging, etc)**
- **Once a crisis begins, the resiliency you’ve built already is what you’ll have to work with**
- **No government can pay for the same capabilities twice – solved via legal and policy reforms**
- **Supported and supporting relationships across ministries**

Hybrid Threats: What CIMIC Can Do?

- **Key role in Military Support to Civil Authorities**
- **Key role in building resilience**
- **Assisting with detection and attribution**
- **Assisting with response and recovery**
- **Assisting with strategic messaging**


“Don’t Let What You Cannot Do
Interfere With What You Can Do”
~ John Wooden
…together