Early Warning and Hybrid Threats: A Whole of Government Approach

Dr Patrick Cullen

Bucharest 17 Oct 2019
Common elements of early-HW definitions

“Any adversary that *simultaneously* and *adaptively* employs a *fused* mix of *conventional* weapons, *irregular* tactics, *terrorism* and *criminal* behavior in the battlespace to obtain their political objectives.” (Frank Hoffman)

- HW uses a mix of conventional and irregular tactics and weapons + terrorism and criminal behavior
- HW uses this fused mix of elements to create synergies in which the sum of the whole is greater than its parts
- HW is innovative and adaptable and exploits the advantages of each kind of force according to the weaknesses in the enemy
Critique of early HW concepts

• Too focused on the following:
  • Non-state actors
  • Material over cognitive
  • Kinetics and violence (versus non-military/non-violence)
  • Tactical and operational (versus strategic logic of HW)
  • Defensive (versus offensive) uses of HW
Evolution of the HW concept

• New empirical reference points changes the meaning:
  • Russian actions in Ukraine, Chinese actions in South China Sea, Election hacking

• Conceptual debate expands
  • Both state and non-state actors
  • Offensive use
  • Hybrid Threats: focus on non-military and non-kinetic aspects of “war”
  • Persistent “below threshold” activities
  • Threats to homeland security in a US/NATO/EU context (and elsewhere)
From August 2014 to September 2015
(New York Times)
“Broad, complex, adaptive and highly integrated combination of actions with overt and covert, military, paramilitary and civilian, conventional and non-conventional means in pursuit of an objective.”

Key points:

• HW uses all instruments of power (MPECI) as tools of attack
• Expands the battlefield by targeting whole of society (PMESII)
• High degree of control leads to possibility of synchronization
• Exploitation of ambiguity
• Describe rather than define HW

• A generic concept and future oriented approach

• Applicable to both non-state and state actors (although capabilities, means and ways differ)

• The shape HW takes depends on context

• HW is often creative, ambiguous, non-military and non-kinetic, no longer primarily reliant on the enemy’s military capabilities
• Capability to synchronize different instruments of power tailored to vulnerabilities within the target system to achieve synergistic effects

• HW can create damaging effects and degrade or undermine the adversary while staying below detection and political and military response thresholds

• HW need not escalate in a linear progression of distinct phases

• HW can operate over varying very long time-scales
HW Synchronization and Horizontal Escalation

Figure 1 – Hybrid warfare escalation
Our description of HW

3 elements that combined make up HW:

“The synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve effects.”

Plus:

“Intentionally exploit creativity, ambiguity, non-linearity and the cognitive elements of warfare (...) tailored to remain below detection and response thresholds.”
C-HW Early Warning and Situtional Awareness

- Detection
- Assess yourself, not just your enemy
- Focus on unfamiliar ways and means (M(PECI))
- Monitor non-traditional targets (PMESII whole of society)
- Create a baseline of normal to help "see" negative changes to critical functions by HW events
  - Death by a 1000 ambiguous cuts
  - Pattern recognition, anomaly discovery, indicators
- Look for synergies and 1st and 2nd order effects
Visualizing the hybrid warfare case study
Visualization of real-time monitoring

- HW events change over time and create different stresses
Current Efforts at HW Warning Intelligence

• A Finnish approach
  ➢ “Discovery”: Looking for unknown unknowns
  ➢ A new approach to whole of government collection and analysis

• An Austrian Army approach
  ➢ “Monitoring”: Looking for known unknowns
  ➢ Adapting an old approach (CoG) methodology to C-HW early warning
Finnish Hybrid Threat Situational Awareness

• Institutionalized whole-of-government monitoring of national critical functions (hub and spoke approach)

• (the spokes): leveraging Ministry SMEs as early warning sensors
  ➢ Focus on anomaly detection, semi-structured surveys

• (the hub): dedicated HT Warning Intelligence team:
  ➢ Collection experimentation, pattern discovery; ‘event’ analysis, hybrid threat situational awareness
Austrian Army use of CoG for HW

- AUT Army experimentation with an old (Cold War) military planning method for new and wider (C-HT) applications

- Center of Gravity model:
  - military planning tool for anticipating possible enemy actions by linking the adversary’s assumed objectives, capabilities, requirements, and the potential effects of these actions on one’s own critical vulnerabilities
  - Warning Intelligence: Find the networks (the attackers to be disrupted, and your network to be defended), define and deploy sensors for early warning

- Applying a ready-made process to an expanded target set (PMESII) and non-military means (M(PECI)) of attack
  - Handing this tool to Ministries across the whole of government for them to apply
  - Working with experts outside the Armed Forces for non-military CoG analysis
  - Experimenting on how economic targets can be hit, or weaponized in an attack
• The Austrian Army is not using the CoG as a “discovery” tool for finding unknown-unknowns

• It is being used to find hybrid threats that are known-unknowns: CoG models anticipated adversary behavior, builds templates of hypothesized attack methods, and creates indicator lists

• The innovation of the AUT military is expanding the CoG method to limit surprise by expanding intelligence monitoring activity to include a wider set of potential targets, and non-military ways and means of attack
HW Warning Intelligence: Recommendations

• National continuous self-assessment and monitoring of critical functions and vulnerabilities across all (PMESII) sectors

• Enhance traditional threat assessment activity to include non-conventional (PECI) tools and capabilities (and) search for synchronization of these tools in tailored attacks

• Build a process that directs comprehensive cross-government efforts to understand, detect and respond to hybrid threats + engage in multinational coordination and cooperation

• Experiment with and adopt warning intelligence methodologies for known-unknown and unknown-unknown hybrid threats
• Questions?