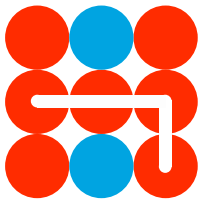
Strategic Analysis May 2018

Hybrid threats as a new 'wicked problem' for early warning

PATRICK CULLEN



Hybrid CoE

Hybrid threats as a new 'wicked problem' for early warning

Hybrid threats are designed to blur the distinction between peace and war, as well as complicate and fall below the target's detection and response thresholds. The wicked problems created by hybrid threats require new solutions for early warning. – writes Patrick Cullen, Senior Research Fellow at the Norwegian Institute of International Affairs (NUPI).

The evolving metaphors of early warning

For decades, practitioners and warning intelligence professionals have turned to metaphors to help simplify and communicate to a wider audience the different types of threats facing societies. During the Cold War this conversation often centred on the differences between "puzzles and mysteries". After the events of 9/11 radically altered our perceptions of the international threat landscape, the metaphorical conversation was altered as well. The term "wicked problems" entered the warning lexicon to describe a new set of dilemmas in warning intelligence. New and unfamiliar non-state actors like Al-Qaida, operating in an increasingly complex and uncertain globalized world, imposed new requirements for early warning. Today, after the annexation of Crimea, we may be witnessing a second inflection point for the metaphor of wicked problems.

Although hybrid threats cannot be conceptually reduced to the non-state terrorist threat that gave rise to the post-9/11 concept "wicked problems", for early warning, the two nevertheless contain many similarities. In this vein, Michael D. Reilly (2015) has gone as far as to call hybrid threats the Pentagon's new wicked problems. He argues that hybrid threats complicate the precise identification of what is most harmful or important, and that the true depth, complexity, and impact of these hazards lies un- or under-recognized until attempts to contend with hybrid threats are well underway.

Thus, today, hybrid threats represent a new evolution in the wicked-problem set facing the consumers and producers of early warning. Unlike previous wicked problems, hybrid threats are not wicked due to our unfamiliarity with a "new" non-state adversary. Nor are hybrid threats wicked because they operate in a highly complex international environment. Instead, hybrid threats are wicked problems by strategic design. This design is often carried out by state actors in an intentionally ambiguous fashion. This design also creatively exploits a whole range of tools that extend beyond the purely military realm to create negative effects within the targeted society. In doing so, **hybrid threats are designed to blur the distinction between peace and war, as well as complicate and fall below the target's detection and response thresholds. As a result, the wicked problems created by hybrid threats require new solutions for early warning**.

Puzzles, mysteries, and Cold War warning intelligence

During the Cold War, **puzzles – sometimes also called "secrets" – referred to information that existed as a "brute fact". In other words, puzzles referred to data that was in principle knowable through diligent intelligence-collection efforts**. Of course, what is knowable in principle is not always easily knowable in practice. Cold War puzzles were given this name precisely because they often refer to secret information that has intentionally been secured or concealed. Alternatively, **mysteries, unlike puzzles, refers to information that is strictly speaking unknowable. This is not because of real-world limitations imposed on collection efforts by an adversary defending its secrets, but because mysteries concern contingent events (such as a nuclear first strike) that may or may not occur at some point in the future**.

Since the nature of the type of knowledge attainable for puzzles and mysteries is different, collection strategies also differed. **Cold War puzzles were investigated with a heavy emphasis on data that could be collected from sensors pointed at adversary targets like army barracks or missile installations**. Ideally, this data would then be turned into binary yes/no answers to questions on indicator lists (e.g. are these missiles being fuelled?) used by warning officers to determine the actions of the enemy. **Mysteries, on the other hand, due to their contingent nature, necessarily involved a heavier emphasis on the role of analysis, risk and probability assessments**.

Despite these differences between puzzles and mysteries, the most likely and threatening dangers posed by the Soviet Union were widely understood and agreed upon. **Cold War warning intelligence collection and analysis had focused on information related to the Soviet's military sphere, and the vast majority of the indicators and indicator lists generated during this period dealt with various puzzles and mysteries tied to the adversary's armed forces or its military-related activities**. By a significant margin, Cold War warning intelligence collection was devoted to obtaining data on key military puzzles: the strengths, capabilities and activities of the armed forces of real and potential state adversaries. The collapse of the Soviet Union is a good example of how intelligence collection that is devoted to military puzzles does not always prepare for surprises.

9/11's wicked challenge to indications and warning intelligence

The terrorist events of 11 September 2001 came as a shock and a surprise. The attack provided a violent wake-up call for warning intelligence professionals and disrupted the thinking behind early warning indicators. The old and familiar intelligence puzzles and mysteries from the era of the Soviet Union duly became woefully outdated. **Threats which were well understood, military-centric, state-based, and relatively static had been replaced by a new threat environment characterized by elusive and evolving transnational threats and threat actors (e.g. terrorist networks) operating in a new milieu of globalization-driven structural complexity that had exponentially increased the level of uncertainty for the intelligence analyst**.

As a result, some members of the intelligence community began to argue that the indications and warning techniques

developed during the Cold War were no longer suitable for countering the novel threats created by non-state actors, and were incapable of anticipating or identifying the weak signals generated prior to these attacks. Other, slightly more optimistic observers, such as Gregory Treverton (2014), argued that the wicked problems generated by the post-9/11 environment had become so complex that the practical distinction between puzzles and mysteries was beginning to break down. Despite the differences in the epistemological status of the knowledge available to intelligence analysts when studying puzzles and mysteries, the empirical complexity of the new environment required more and more puzzles (and not only mysteries) to be expressed in probabilistic terms.

Today, state actors wielding considerably more power than terrorist organizations have demonstrated the ability and willingness to design hybrid threats that match non-kinetic means against the unprotected seams of liberal democratic societies. **By emphasizing elusiveness, ambiguity, operating outside of and below detection thresholds, and by using non-military tools to attack across all of society, hybrid threats** represent a new iteration of the complexity found in wicked problems.

Hybrid threats as a new wicked problem

Hybrid threats may be approached as a wicked problem for many reasons. As with all wicked problems, the true nature of the security problem may not always be immediately clear, and the nature of the problem is adaptively and reflexively embedded into our attempts to understand and resolve it. **Although the concept of hybrid threats is maturing, there are still multiple and different meanings of the term that complicate a consensus understanding of the problem. This problem alone can hinder effective early warning**. Hybrid threats also fulfill the wicked-problem criteria of an evolving threat. As Tom Ritchey (2007) has argued, wicked problems won't keep still, and new forms of wicked problems often emerge as a result of trying to understand and resolve a previous one. Moreover, **although hybrid threats share the same strategic characteristics, the diversity of ways in which individual hybrid threats match multiple instruments of power against the specific weaknesses of the society targeted can result in each individual hybrid threat campaign having a unique signature**. This makes early warning relating to hybrid threats significantly less predictable than the puzzles and mysteries of the Cold War, and arguably more complex than the wicked problems presented by the post-9/11 terrorist threat as well. The use of proxies, plausible deniability, and the strategic exploitation of ambiguity and uncertainty of who or what the adversary is may also create problems for analysts using a traditional and even current warning intelligence paradigm that is premised on knowledge of an easily identified adversary. The issue of the unknown adversary is especially problematic for warning intelligence officers attempting to attribute hybrid threat actions intentionally designed to complicate this process.

Today, the task of identifying future attacks is complicated by the sheer diversity of non-military instruments of power that need to be understood and monitored to provide adequate warning for hybrid threats. Warning intelligence must look for indications of activity that can turn into hybrid threats beyond the

traditional realm of military activity, extending into many different domains, with the political and economic being two obvious examples. This is not an easy process, and the relative weakness in diagnosticity for political and economic indicators that point in many possible threatening and non-threatening future directions at the same time is a significant problem that must be addressed.

One of the key insights from studies of hybrid threat early warning is that we are much less likely to correctly understand, or even see, the mysteries and puzzles of hybrid threats until the effects are already underway. Whereas Cold War puzzles and mysteries were by and large *known* unknowns (e.g. we knew what we did not know), hybrid threats are relatively likely to manifest as *unknown* unknowns (e.g. as threats we are not even aware we are unaware of). **This observation has already changed the practice of early warning, with some intelligence agencies experimenting with new methods and practices to develop a hybrid threat situational awareness**.

Part of this process involves new ways to "look at ourselves" in order to search for weak signals of unanticipated, ambiguous hybrid threat puzzles (i.e. brute facts that manifest as anomalies or patterns) that indicate a possible hybrid threat to our society. To the extent that these weak signals exist as brute facts, they are in principle detectable. Another part of this process of adapting warning intelligence to hybrid threats involves expanding the types of mysteries we are trying to understand. Thinking creatively and analytically about the possible coordinated use of the non-military (and not just military) tools in our adversaries' arsenals against our societies' weaknesses – and building analyses and indicators to counter these risks – is a case in point. **Today, adapting how we monitor not just ourselves, but also our adversaries, is crucial in order to respond to the wicked problem of hybrid threats**.

Author

Dr. **Patrick Cullen** is a Senior Researcher in the Security and Defence Group at the Norwegian Institute of International Affairs (NUPI). For the last four years he has acted as a Project Lead for the MCDC Counter-Hybrid Warfare project, a multinational defence programme headed by the United States Joint Forces Command. Dr Cullen is a regular speaker on hybrid warfare in national and multinational venues, including the United Nations Security Council, the European Defence Agency, and the European Centre of Excellence for Countering Hybrid Threats. Prior to his current position, Dr. Cullen worked on defence and intelligence projects at the political risk consultancy Eurasia Group in Washington D.C., and lectured on International Relations at the Barcelona Institute of International Affairs (IBEI). He holds a PhD in International Relations from the London School of Economics.

Literature:

Borg, Lars. "Improving Intelligence Analysis: Harnessing Intuition and Reducing Biases by Means of Structured Methodology." *The International Journal of Intelligence, Security, and Public Affairs*, 19:1, (2017): 2–22.

Cullen, Patrick, and Erik Reichborn. "Understanding Hybrid Warfare." MCDC Countering Hybrid Warfare Project, MCDC, January 2017, accessed May 25, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Cullen, Patrick, and Njord Wegge. "Adapting Early Warning in an Age of Hybrid Warfare," in *Intelligence Analysis in the Digital Age*, Stig Stenslie, Lars Haugom, Brigt H. Vaage (eds.), Førsteutkast til Fagbokforlaget, forthcoming 2018.

Grabo, Cynthia. *Handbook of Warning Intelligence*. Lanham: Rowman and Littlefield, 2015.

Hulnik, Arthur S. "Indications and Warning in Homeland Security: Seeking a New Paradigm." *International Journal of Intelligence and CounterIntelligence*, 18:4, 2005.

Omand, David. "Reflections on Secret Intelligence," Transcript of speech delivered to Gresham College, 20 October 2005.

Reilly, Michael D. "Hybrid Threat Center of Gravity Analysis: Cutting the Gordian Knot." National Defense University, 2015.

Ritchey, Tom. "Wicked Problems: Structuring Social Messes with Morphological Analysis." *Swedish Morphological Society*, 2007.

Treverton, Gregory. "Changing Threats, Evolving Methods," in *The Future of Intelligence: Challenges in the 21st Century*, Isabelle Duyvesteyn, Ben de Jong, Joop van Reijn (eds.), London: Routledge, 2014, 30–31.

United States Army Special Operations Command, "Perceiving Gray Zone Indications," White Paper, March 15, 2016.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978-952-7282-08-3

Hybrid CoE is an international hub for practitioners and experts, building member states' and institutions' capabilities and enhancing EU-NATO cooperation in countering hybrid threats located in Helsinki, Finland

Hybrid CoE