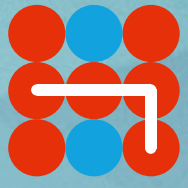
RESEARCH AND ANALYSIS

Hybrid CoE Strategic Analysis 22

JUNE 2020

A warning system for hybrid threats – is it possible?

SEBASTIAAN RIETJENS



Hybrid CoE

Hybrid CoE Strategic Analysis is typically a short paper (around 2,000 words) written by academic and research community experts. Strategic Analyses are based on long-term research experience, or on current or completed research projects. The idea behind the Strategic Analysis papers is to enhance understanding of different phenomena in the realm of hybrid threats. They do not present direct recommendations but aim to explain processes and identify gaps in knowledge and understanding, as well as highlight trends and future challenges. Each Strategic Analysis paper includes a literature list for further reading. Topics are related to Hybrid CoE's work in all of its main functions: training and exercises, communities of interest (hybrid influencing; strategy and defence; and vulnerabilities and resilience) as well as research and analysis.

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

ISBN 978-952-7282-61-8
ISSN 2670-2282

June 2020

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

A warning system for hybrid threats – is it possible?

> *"While many policymakers like to refer to 'connecting the dots' to derive accurate pictures of forthcoming events, this picture is highly inaccurate and unhelpful. In the case of hybrid threats, the dots are missing because they fall below the threshold, they look different due to deception or disinformation, or are impossible to understand due to some kind of encryption,"* writes Sebastiaan Rietjens, Professor of Intelligence & Security at the Netherlands Defence Academy.

Introduction

A warning system is a crucial ingredient in countering hybrid threats. Informing the decision-makers of affected countries as well as the population at large enables them to take appropriate measures. However, as Patrick Cullen (2018) convincingly argued in his Strategic Analysis, hybrid threats are wicked problems. They are ambiguous and fuzzy and lack proven knowledge and fixed standards to adequately address them. This makes devising a warning system for such threats intrinsically difficult and challenging.

Before hybrid threats materialize, they often send out only weak signals that are hard to detect and cannot easily be linked to any known trend or phenomenon (Kuosa, 2014). Moreover, these weak signals reside in a massive amount of irrelevant or misleading information, often referred to as noise (Gentry & Gordon, 2019). Furthermore, as Cullen argues, "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". He therefore concludes that hybrid threats require new solutions for warning. Treverton et al. (2018, p. 91) reach a similar conclusion when they state that warning for hybrid threats is "tricky but not impossible", and Nyheim (2015, p. 16) also stresses the need to adapt warning methods to the "emerged reality of hybrid conflicts".

This Strategic Analysis addresses this call for attention and explores how the warning process, including communicating these warnings in a timely manner, should be adapted to the context of hybrid threats. In doing so, the analysis draws upon insights from the strategic warning and early warning literature as well as the literature on complexity theory. Overall, it builds on Cullen's strategic analysis by focusing on the "how" of warning.

To this end, the paper discusses four phases in the warning process: (1) the direction of the warning efforts, (2) collecting the information, (3) analyzing the threats, and (4) communicating the warning analyses.

Direction

In line with the traditional view on warning, policymakers or military commanders provide direction for the warning process by stating their needs. They often refer to these as information requirements. According to former US Secretary of Defense Donald Rumsfeld, this implies finding the "known unknowns – things we knew we didn't know". **In the case of hybrid threats, such initial requirements are, however, debatable and often impossible to define. Now, *warners* and decision-makers alike find themselves in a position of not knowing what they don't know, Rumsfeld's *unknown unknowns*.** Compounding this problem is the multitude of participating actors in the warning process, and at the same time the lack of ownership of this process. **While traditional threats had one specific (intelligence) organization that provided guidance to direct the warning process, this is less so in hybrid conflicts. Here, there are**

constantly changing (networks of) actors that bring relevant resources to the table. This raises questions in terms of funding, coordination and human resources and calls for an alternative way of dealing with the direction of the warning process.

Drawing on the complexity literature, we know that the issue of self-organization is particularly relevant for organizations facing wicked problems (see e.g. Brown and Eisenhardt, 1997). This is because the accumulation of individual agents' frequent, locally initiated, and small improvisational interventions integral to self-organization can greatly enhance the adaptive capacity of complex systems. The actors explore these new paths and processes in interaction with each other, with or without minimal external control mechanisms. Morgan (2006) has introduced several design principles that help in the development of self-organization. How these principles are acted upon can vary according to the organization or network in question.

The first principle of self-organization according to Morgan (2006) is "the importance of redundancy". Organizations need to invest in slack information processing capabilities and skill-sets to decrease responsive dependency on the actions of a single local actor. Currently, intelligence organizations publicly claim that strategic warning is of the utmost importance. However, in practice, many see it merely as a ticked box and let most resources flow to other departments that "follow the 'hot' topics of the day" (Gordon & Gentry, 2019).

The second principle is to obey Ashby's law of "requisite variety", which means that the internal diversity must match the variety and complexity of its environment. In the case of hybrid threats, this implies that warning organizations should display a level of diversity that matches that of their adversaries. The many different stovepipes in the warning network as well as the lack of non-Western knowledge and insights inhibit this principle from being effectively implemented.

Principle three is labelled "minimum specs", which implies that the leadership must only define the essentials and offer enough freedom for distributed action. In particular, the oversight and ethics committees in many Western countries restrict intelligence agencies in their modus operandi, for example in collecting and sharing information. Meanwhile, private organizations such as Bellingcat are less bound by regulations, and their network of volunteers makes them rather flexible in tackling upcoming crises. The investigation into the downing of flight MH17 illustrates this well. By adopting unorthodox methods, such as penetrating Russian social media networks, Bellingcat was able to uncover numerous facts and identify people that were involved in the downing.

The fourth and final principle is "learning to learn". This principle emphasizes that in order to self-organize, members must possess a mindset of double-loop learning, but must also be granted the freedom to challenge existing norms, rules, and procedures. The closed and secretive culture as well as the bureaucratic organization of many intelligence communities and militaries clearly prohibit such learning and distance them from other sectors.

Collecting the information

Indicators are at the heart of the warning data collection process, providing a systematic framework for monitoring the situation and creating an alert. They are important in order to reduce "a complex situation to manageable concrete features and to assign useful issues against which to observe any transformations" (Odote, 2016, p. 83). Warning academics identify several requirements for indicators, the most prominent being predictive, diagnostic, unambiguous and collectible (see e.g. Gentry & Gordon, 2019; Treverton, 2009). While the indicators that were used during the Cold War largely met these requirements, this is often not the case for indicators that signal hybrid threats. Here, a great diversity of instruments, both military and non-military, as well as threat actors need to be understood and monitored to provide adequate warning (Cullen, 2018).

This challenge is enormous and demands bridging the gap between deductive and inductive methods (Bryman, 2012, p. 24) that use qualitative as well as quantitative data. When applying deductive methods, indicators are formulated upfront and based on general ideas or insights. This requires profound and established knowledge of a topic. Intrusion detection systems are a good example since their design is based on

general knowledge about how to protect computer networks.

Besides defining indicators that are based on established knowledge, it is important to apply inductive methods that start with observations and move backwards to generalizations. In light of the explosion of big data and advances in machine learning, warning organizations increasingly have models at their disposal that yield threat predictions (Sweijs, 2019).

However, since many of these models are largely a black box and provide correlations as opposed to explanations, they inform efforts to address the threats to a limited extent only. Hence, there is a need to apply deductive and inductive methods in parallel.

In addition, there is a growing consensus that warning methods need to integrate quantitative as well as qualitative data. Most warning methods seem to prefer quantitative data. Provided that these data are reliable, valid, timely, and adequately analyzed, these methods are indispensable. Simple metrics may render long discussions superfluous. **Meanwhile, many of the warning challenges demand interpretation, sense-making, and qualitative interpretation to provide depth as well as context- and actor-sensitivity. Events with the greatest impact usually happen unexpectedly, and can rarely be derived from numerical series.**

Overall, applying mixed method approaches that effectively combine quantitative inputs and sophisticated models with sound qualitative interpretation seem to be the most promising.

Analysis

While many policymakers like to refer to 'connecting the dots' to derive accurate pictures of forthcoming events, this picture is highly inaccurate and unhelpful (Gentry & Gordon, 2019). In the case of hybrid threats, the dots are missing because they fall below the threshold, they look different due to deception or disinformation, or are impossible to understand due to some kind of encryption. In an effort to meet these challenges, analysts apply a variety of methods. Well-known examples include the Delphi method, horizon scanning or trend analyses. In addition to these warning methods, analysts have started to borrow sophisticated methods from other domains as wide and varied as weather prediction, ecology, business management, and consumer behaviour forecasting (see e.g. Marr, 2016; Alley et al., 2019).

Moreover, *warners* may be able to avail themselves of more precisely tailored and targeted approaches that allow for a finer understanding. **Part of this revolution is the ability to take local knowledge or the views of people on the ground into account, so that one can bridge the gap between what analysts with their computer models and their internet searches concoct in capitals and what is happening on the ground. This requires first and foremost building better interfaces with local communities and people on the ground, whether through NGOs, embassies, or different means (Nyheim, 2015).** The emphasis may need to shift from only looking for formal knowledge among professionals and experts to being prepared to 'de-professionalize' the trade and be open to 'everyday knowledge'.[1]

Of specific significance to hybrid threats is incorrect and misleading information, delivered either intentionally (disinformation) or unintentionally (misinformation). There are many recent cases displaying these dynamics including but not limited to the murder attempt on Sergei and Julia Skripal in Salisbury in March 2018, the 2016 US elections, the use of chemical weapons in Syria by the Assad regime, or the aftermath of the downing of Malaysia Airlines flight MH17. Recognizing this type of information is crucial for analysts as well as extremely challenging (see e.g. Rietjens, 2019). Treverton (2018, p. 16) adds that during the analysis process the main challenge is coping with all the information and misinformation that is out there. Analysts are scattered throughout many different organizations and often have a substantial and varied amount of information at their disposal. **The concept of information overload is a well-known phenomenon and not unique to the warning process of hybrid threats. Information management scholars such as Rutkowski &**

1 This paragraph is taken from an internal document at the Netherlands Defence Academy that the author has drafted together with his colleagues Georg Frerks and Tim Sweijs.

Saunders (2019) have addressed this issue in great detail. This kind of literature is unfortunately not well known in warning communities, but could be very helpful in addressing this issue.

Communication and dissemination

The idea of warning is that it enables a timely response so that harm is prevented or at least reduced by appropriate action. Effectively communicating the warning to decision- makers or the population at large is therefore of great importance. From a warner's perspective, key communication requirements include source credibility, message content, and mode of communication (Meyer and Otto 2016, p. 198).

The extent to which the warning message finally influences actual decision-making and triggers a response depends on many other factors. An OECD study has flagged 28 of these factors and categorized them into personal, institutional and political factors, depicted in Figure 1. Although these factors were identified in the context of violent conflict, each of them seems to apply to the context of hybrid threats as well.

Although hybrid threats are considered to be wicked problems, a warning system does not seem to be impossible. It is just not functioning in a traditional sense. To better match reality, the warning process needs to be redesigned and *warners* and policymakers alike have to be aware of the pitfalls and difficulties that are inherent in this process.

Personal	**Institutional**	**Political**
Time and decision-making pressure	Institutional and departmental mandate	National/institutional interest and priorities
Competing priorities	Budget availability	Alliances and special relationships
Personal interest and experience	Turf considerations	Enmities and competition
Knowledge and understanding of situation	Risk-taking/risk-averse culture	Party and constituency politics
Training and analytical skills	Personnel turnover and institutional memory	Media coverage and CNN effects
Decision-making ability	Decision-making procedures	Advocacy pressure
Risk-taking profile	Available mechanisms and instruments	Political cost-benefit calculations
Personal relationships	Accountability considerations	Political consensus
Personal cost-benefit calculations and accountability	Security of staff memory	Politicization of information
Available information and analysis		

FIGURE 1. Factors that influence decision-making on responses to violent conflict (OECD, 2009)

Author

Sebastiaan Rietjens is Professor of Intelligence & Security at the Netherlands Defence Academy. He has conducted extensive fieldwork on military exercises and operations (Afghanistan, Mali, Greece) and has published widely in international books and journals, including *Human Relations*, *Armed Forces & Society*, *International Journal of Public Administration* and *International Journal of Intelligence and CounterIntelligence*. His main research focus is on intelligence within the military domain, intelligence cooperation, the future of intelligence organizations, and information warfare. Sebastiaan is a member of the editorial board of *Armed Forces & Society* and *International Journal of Intelligence and CounterIntelligence*, a board member of the Netherlands Intelligence Studies Association, and co-director of the NATO-funded project "Resilient Civilians in Hybrid and Population-Centric Warfare".

Literature

Alley, R., Emanuel, K. & Zhang, F. (2019). Advances in Weather Prediction. *Science*, Vol. 363, Issue 6425, 342–44.

Brown, S.L., & Eisenhardt, K.M. (1997). The Art of Continuous Change: Linking Complexity Theory and Time-Paced Evolution in Relentlessly Shifting Organizations. *Administrative Science Quarterly*, Vol. 42, No. 1, 1–34.

Bryman, A. (2012). *Social Research Methods* (4th ed.). Oxford: Oxford University Press.

Cullen, P. (2018). *Hybrid threats as a new 'wicked problem' for early warning*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats.

Gentry, J.A. & Gordon, J.S. (2019). *Strategic Warning Intelligence: History, Challenges, and Prospects*. Washington: Georgetown University Press.

Kuosa, T. (2014). *Towards Strategic Intelligence – Foresight, Intelligence, and Policy-Making*. Helsinki: Dynamic Futures.

Marr, B. (2016). *Big Data in Practice*. Hoboken: John Wiley and Sons Ltd.

Meyer, C.O. and Otto, F. (2016). How to warn: 'Outside-in warnings' of Western governments about violent conflict and mass atrocities. *Media, War & Conflict*, Vol. 9, no. 2, 198–216.

Morgan, G. (2006). *Images of Organization*. Thousand Oaks: Sage Publications.

Nyheim, D. (2015). *Early warning and response to violent conflict. Time for a rethink?* London: Saferworld.

Odote, P.O. (2016). *Role of early warning systems in conflict prevention in Africa: Case study of the Ilemi Triangle*. PhD Thesis. Nairobi: University of Nairobi.

OECD (2009). *Preventing Violence, War, and State Collapse: The Future of Conflict Early Warning and Response*. Paris: OECD/DAC.

Rietjens, S.J.H. (2019). Unraveling Disinformation: The Case of Malaysia Airlines Flight MH17. *The International Journal of Intelligence, Security, and Public Affairs*, Vol. 21, No. 3, 195–218.

Rutkowski, A-F. & Saunders, C. (2019). *Emotional and Cognitive Overload: The Dark Side of Information Technology*. Oxon: Routledge.

Staber, U. & Sydow, J. (2002). Organizational adaptive capacity: a structuration perspective. *Journal of Management Inquiry*, Vol. 11, No. 4, 408–424.

Sweijs, T. (2019). *The Promises and Pitfalls of Early Warning*. Speech on the Warning Symposium of the Dutch Ministry of Defence. March 28, 2019, Amsterdam.

Treverton, G.F. (2009). *Intelligence for an Age of Terror*. New York: Cambridge University Press.

Treverton, G.F. (2018). *The Intelligence Challenges of Hybrid Threats. Focus on Cyber and Virtual Realm*. Stockholm: Swedish Defence University & Center for Asymmetric Threat Studies.

Treverton, G.F., Thvedt, A., Chen, A.R., Lee, K. & McCue, M. (2018). *Addressing Hybrid Threats*. Stockholm: Swedish Defence University, Center for Asymmetric Threat Studies and The European Centre of Excellence for Countering Hybrid Threats.


Hybrid CoE