Assessment of Whole-of-Society Hybrid Conflict: Fusion of Activity Signals and Analyst Insight

Bas Keijser[1] **Thomas Powell** **Joris Westerveld** **Peter van Scheepstal**
TNO Defence, Safety & Security

Bas.Keijser@tno.nl

ABSTRACT

Analysis, assessment and decision-making in hybrid conflict is complicated for numerous reasons: signals of hybrid activities are multidimensional; combining information from multiple types of sources is necessary; and much of hybrid conflict is either covert or difficult to discern from normal state-to-state relations. Assessment of hybrid conflict needs to include strategic goals of adversary actors, societal vulnerabilities and context events exploited, activities performed across societal domains, and impact on the society targeted. In earlier work an analysis process was proposed based on these five elements of hybrid conflict. In this paper we build on this work and the wider intelligence literature to address the question of how to perform the assessment of hybrid conflict. Specifically, we outline a detailed assessment process that provides situational understanding for decision-makers to choose preventive and reactive responses to hybrid threats. The merit of the proposed process is in its integrated assessment of hybrid conflict combining both a targeted society perspective and an adversary actor perspective. Moreover, the presented assessment functions rely on the ongoing interaction between human-derived analytical insights – taking into account context, ambiguity, normality – and signals derived from incoming data – taking into account structuring and combining information from multiple sources. This integrated perspective goes beyond conventional analytical approaches. The assessment we present is well-suited to steer a combination of human and automated intelligence, and provides a blueprint for analytical methods and tooling to address the challenges of decision-making in hybrid conflict.

1.0 INTRODUCTION

Hybrid conflict is a type of conflict between states that mostly falls beneath the threshold of open war (see the definitions by e.g. EU, 2018, NATO, 2019 and at the Dutch level, NCTV, 2019). States in hybrid conflict use many measures of state power to influence other societies. These include diplomatic, informational, military, economic, financial, intelligence and law enforcement instruments. Case studies of hybrid conflict on a strategic level entail narrative and social media manipulation, tit-for-tat financial and economic sanctions, diplomatic threats, large-scale military exercises and many other whole-of-society interactions. Many types of hybrid threats are known from experiences in the previous years. For instance election influence in the United States, Chinese influencing through infrastructure investment, and Russian efforts in destabilising Ukraine.

Hybrid conflict poses varying challenges to decision-makers. This is because open military confrontation is mostly avoided and only activities below the legal threshold of armed conflict are applied. The cyber domain and information domain are the main domains in which influence activities directed at governments and societies take place. Due to the covert or obfuscated nature of many activities in hybrid conflict there is a major problem in attributing activities to state actors. Lastly, hybrid conflict is a creative orchestration of means and methods that creates novel situations that are inherently challenging to analyse. In this article, the assessment of hybrid conflict when confronted with the above challenges is investigated in more detail.

[1] Bas Keijser and Thomas Powell are co-first authors of this paper.

1.1 Challenges to analysis of hybrid conflict

The core analysis challenge for hybrid conflict analysts is to create a coherent picture of incomplete signals and activities of a hybrid threat actor. Monaghan, Cullen & Wegge (2019: 26) refer to this as hybrid warfare situational awareness. Building this situational awareness can be seen as laying a puzzle. Many pieces of the puzzle will be missing or are unrecognizable as a piece of the puzzle due to deception (Rietjens, 2020). Furthermore, some pieces of the puzzle will be gathered by other organisations within the government that are detached from an assessment cell that do not realise it is a relevant piece of a hybrid conflict puzzle.

A number of challenges to analysis and specifically intelligence analysis due to the nature of hybrid conflict have already been noted in the literature. Firstly, hybrid conflict is a society-on-society conflict, thus collection and analysis have many different, additional subjects (Treverton, 2021). The intervention space of hybrid conflict is multidimensional and very large (Bekkers, Meessen & Lassche, 2018: 7), geography matters less for influence activities, and the hybrid threat is persistent (Treverton, 2018). A basic knowledge and understanding across domains needs to be available to analysts of hybrid conflict, and they may need to build on domain knowledge from other experts too.

Secondly, hybrid threats emphasize "elusiveness, ambiguity, operating outside of and below detection thresholds, and […] using non-military tools to attack across all of society" (Cullen, 2018: 4). Thus, incoming signals may be incomplete because of the covert nature of activities by intelligence and proxy organisations for example (NCTV, 2019), but also because some activities on the face of it look beneficial to the society of interest, such as loan constructions with foreign state-owned enterprises.

Thirdly, time delays play an important role, effects of adversary actions manifest much later. Some activities exploit this time delay in the extreme to create vulnerabilities for later reference, which is called priming. Fourthly, the use of cyber and virtual means also causes an erosion of truth and credibility with policymakers and the public. Treverton (2018: 12) speaks of a "cacophony of narratives" in which analysts need to do their work. Lastly, numerous institutional challenges have been noted on data fusion and combination of perspectives in intelligence analysis (Treverton, 2018). The way in which hybrid conflict is analysed is not institutionalised yet. In summary, in terms of analysis and assessment, hybrid conflicts are a quintessentially wicked problem (Cullen, 2018).

To provide sound analysis of hybrid conflict, it is important to offer an integrated view of strategic goals, hybrid activities, societal effects and exploited vulnerabilities. Only when assessing these elements of hybrid conflict in concert, can its orchestrated nature truly be understood.

1.2 Importance of structured assessment for decision-making

To provide an integrated view on the state of a hybrid conflict to support decision-making, assessment needs a lot of attention. In line with NATO doctrine (AJP-2.1, 2016), we consider intelligence analysis as the process of reviewing data and information to provide significant facts and knowledge (p. 3-15; e.g., analysis functions in Table 1). Intelligence assessment involves interpretation of this data, information, facts and knowledge in a way that can inform decision-makers (p. 3-18; e.g., assessment functions in Table 3). Assessment of hybrid conflict has to combine data and information on strategic goals of the adversary actor, societal vulnerabilities exploited, activities performed by the hybrid actor across societal domains, and impact on the targeted society. Data and information on these topics are available in the form of both technical signals and human analyst expertise. Ways in which these are to be combined and interpreted are not apparent upfront.

It is beneficial to apply existing knowledge on the structure and modus operandi of hybrid conflict. This supports structuring insight into the state of hybrid conflict and thus supports analyst sensemaking. Although a novel challenge, any proposed assessment framework for hybrid conflict should adhere to existing intelligence analytical standards – to ensure a consistent standard of rigour, integrity, language and best

practice (e.g., DIVI, 2010; JDP-2, 2012). For instance the UK Professional Head of Intelligence Assessment common analytic standards state that assessment should be independent, clear, comprehensive, auditable, relevant, rigorous, objective and timely (UK PHIA, 2019). The nature of hybrid conflict demands extra attention to comprehensiveness (whole-of-society relevance), auditability (based on traceable evidence) and objectiveness (accounting for analyst bias). The incremental step-by-step process presented in this paper addresses all three of these challenging criteria in the hybrid context.

Once provided, assessment of hybrid conflict supports provisioning situational understanding to a decision-maker on the basis of which preventive and reactive responses need to be formulated. For this purpose, tailored assessments are necessary. Furthermore, the incremental nature of hybrid threats means it is necessary to iteratively gather data and information to advance and update assessment as the conflict progresses. In this way repeated assessment of hybrid conflict provides a basis of actionable insight for a decision-maker.

1.3 Contribution to practice and theory

The core question that is answered in this article is **'how should assessment of hybrid conflict be performed?'** We present a single, new way of assessing hybrid conflict. This assessment process has been designed reasoning from available analysis input describing elements of hybrid conflict and necessary output to provide decision-maker support, see also section 2.2.

The contribution of our work is two-fold. Firstly, the practical contribution is that the process of assessment can be used by analysts of hybrid conflict to support decision-makers that have a responsibility to formulate a policy response. Secondly, the theoretical contribution is that our work provides a complementary way of intelligence assessment to the method basis in the existing literature. More precisely, we contribute an assessment method that takes an integrated perspective of hybrid conflict from both a targeted society perspective and an adversary actor perspective. Furthermore, we provide a conceptual framework that enables the combination of analyst-driven and data-driven insights that is essential for producing comprehensive assessments. In addition, the presented structure of hybrid conflict using goals, operations, and vulnerabilities can be used to create smart algorithms and data analysis tools. Future work can use this structure to develop automated approaches for identifying, extracting and linking these important elements of hybrid conflict.

2.0 METHOD

2.1 Link to existing literatures

The challenges of intelligence analysis are well-known in the open literature (Lowenthal, 2016; Hutchins, Pirolli & Card, 2007). First of all, intelligence is frequently about human beings that act irrational or change their mind at the last moment (Lowenthal, 2016: 292). Furthermore, analysts have to work with fragments of the information they would like to have that are also possibly unreliable or imprecise (*ibid.*). Other factors that contribute to the challenge of the intelligence analysis task are time pressure, cognitive workload and the difficulty of human judgment (Hutchins, Pirolli & Card, 2007). Wide-ranging judgments are necessary on plausibility, trustfulness and weight of pieces of data, after which data needs to be combined to respond to an analysis question (*ibid.*). Many of these general challenges also arise when analysing hybrid conflict. However, because of the intricacies of hybrid conflict previous challenges form an even bigger problem and some new challenges also play a role. Intelligence challenges of hybrid conflict have not been extensively studied in literature, bar some analysis by Treverton (2018), Cullen (2018), Rietjens (2020) and various chapters in Weissmann et al. (2021). See the discussion above, under 1.1.

Hybrid conflict as an intelligence problem can primarily be seen as a complexity in the triad of puzzles,

mysteries, and complexities (Treverton, 2014). Menkveld (2021) notes that a complex intelligence problem aims at understanding "a network that is adaptive and exhibits aggregate properties that emerge from local interactions among its entities mutually constituting their own environment". It is a situation in which many actors – e.g. an adversary actor, proxies, criminal groups, a targeted society and its social structures – respond to each other and to the circumstances in which the conflict takes shape, without exactly "repeating any established patterns" (Treverton, 2014: 29). However, it must also be noted that some of the intelligence problems embedded in hybrid conflict actually entail puzzles and mysteries. The "who done it"-issue of attribution after a cyberattack simply is a puzzle, while predicting future hybrid operations constitutes a mystery.

Assessment of complex intelligence problems should focus on sensemaking and interaction between intelligence analyst and decision-makers about the drivers of conflict (Moore, 2011). Moore et al. (2021: 2) describes sensemaking as "the deliberate attempt to understand a situation and how it emerged" using inference to the best possible hypothesis. Its goals are "to achieve an explanation in terms of causes, which can include human intentions, beliefs and actions, and to derive courses of action from that understanding". The process is elaborately described by Pirolli & Card (2005: 4): external data sources are searched and filtered for relevant data, pre-structured information is read and evidence is extracted, the evidence is schematised, after which a case is built and a story is told that makes sense of the situation. Thus assessment is performed by an analyst applying database searches to combine his previous insight with available evidence. Next to applying database searches and using visualisation techniques (see e.g. Doppler Haider et al., 2019), many other ways of sensemaking through data analysis can be imagined, such as combining data analytics and machine learning techniques with analyst insight to study human terrain surveys (Powell & Eles, 2018).

Our work is an application and operationalisation of sensemaking to hybrid conflict. It implements elements of previously developed methods in various fields, including classical threat-based intelligence analysis (Vandepeer, 2011), strategic warning (Grabo, 2002; Wirtz, 2013), structured analytic techniques (Pherson & Heuer, 2020), a complex systems approach to conflict (Gallo, 2012), policy analysis (Enserink et al., 2010), and societal risk assessment (Pruyt & Wijnmalen, 2010). Our contribution is to connect the aforementioned methods and ways of looking at hybrid conflict. We go beyond conventional analytic approaches that either deliver assessment from a red-actor perspective or a blue-actor perspective, or either present quantitatively derived signals of ongoing hybrid activities or qualitative analyst insights. Instead, we provide an integrated way of assessing hybrid conflict that combines a red-actor and blue-actor perspective, using both quantitative and qualitative insights. The assessment provided can be used to support strategic decision-making when confronted with hybrid threats.

2.2 Design of the assessment process

We describe an assessment process designed from scratch. We used a design thinking approach (Owen, 2006), applying elements of problem decomposition and synthesis of available analysis methods to accommodate for support to decision-makers. In doing so the aim is to "bring tangible, fresh expressions of what can be" in the analysis of hybrid conflict (Owen, 2006: 17). The development process started by making an inventory of the available input in an analysis process of hybrid conflict, and by making an inventory of insights necessary for decision support. These were connected step-by-step to form an assessment process that provides an integral view of hybrid conflict.

In developing the assessment functions described in this work, we limited our scope to functions that provide situational understanding of a single hybrid campaign. We define a hybrid campaign as all of the activities performed by one actor directed at a single society of interest[2] (or a single international organisation

[2] In a comparable way a hybrid campaign directed at an international organisation composed of multiple countries can be analysed. Some changes to the vulnerability analysis are then appropriate.

composed of countries) which serves one or multiple strategic objectives of the hybrid actor. By initially limiting our scope to a single hybrid actor performing one hybrid campaign, we make our research question manageable whilst retaining a whole-of-society perspective. However, it is entirely possible to use the proposed process to assess multiple hybrid campaigns side-by-side. When assessing multiple hybrid campaigns, all of the assessment functions described below remain relevant. Further attention to attribution to alternative state actors, competing hypotheses about these actors, and relations between hybrid actors is then also necessary.

Various types of assessment are necessary for decision support, summarised by Monaghan, Cullen & Wegge (2019) as detect, deter and respond. More specifically, a key challenge is to warn for and interpret the first incoming signals of hybrid activities – this supports a decision-maker in understanding a conflict in its earliest stages and supports forecasting of plausible development directions of conflict. In parallel, risk assessment of hybrid threats should be supported. For this purpose an assessment of plausible hybrid operations that can target a society of interest should be produced. This assessment informs suitable deterrence measures. When the hybrid conflict has actually started in earnest, it is important to support the monitoring of the state of conflict. In this state a reflection of current and recent activities, possibly attributed to an actor should be available. Furthermore, the state of society and its vulnerabilities should be analysed. Lastly, decision support can indirectly focus on providing a decision-maker with priorities for preventive (reacting to observed vulnerabilities) and reactive measures (reacting to observed hybrid activities) in hybrid conflict.

Table 1 shows the five analysis functions that are available to provide input to the further assessment of hybrid conflict. These inputs draw on the elements outlined in section 2.1 from literatures on societal risk assessment and intelligence, strategic, and policy analysis (e.g., Vandepeer, 2011; Enserink et al., 2010; Grabo, 2002; Pherson & Heuer, 2020; Pruyt & Wijnmalen, 2010; Wirtz, 2013). To break down the assessment of hybrid conflict into several assessment functions a confrontation matrix of available analyses of hybrid conflict was used (see Table **2**). The confrontation represents the possible combinations of input analyses of hybrid conflict (described in Table 1) and the names shown are the resultant assessment functions, which are described in more detail in the next section. The derived assessment functions were analysed by designing assessment questions relevant for an analyst to support a decision-maker.

Table 1: Available inputs to assessment in terms of analysis of hybrid conflict

Analysis function	Description
Actor analysis	Analysis of adversary actor in terms of strategic goals, lines of operation, capabilities and recent activities
Vulnerability analysis	Analysis of targeted society in terms of societal functions, and vulnerabilities to hybrid operations
Context analysis	Analysis of upcoming events that can be exploited in the context of hybrid operations
Monitoring & detection of activities	Screening for hybrid activities targeted at a society of interest, using both known indicators and detection of new types of activities[3]
Monitoring & detection of effects	Screening for effects of hybrid activities in the society of interest, using both known indicators and detection of new types of effects

Table 2 – Confrontation of all available inputs, noted in Table 1, to find assessment functions. Context analysis is left out in this confrontation, it is later added to the assessment if relevant.

	Vulnerability analysis	Monitoring and	Monitoring and

[3] Frameworks for understanding the operational environment can help with managing the multitude of signals involved in monitoring and detection (M&D). For instance, M&D of activities may use DIMEFIL and M&D of effects may use PMESII.

		detection of activities	detection of effects
Actor analysis	Preparatory hybrid risk assessment	Strategic actor assessment	Holistic campaign assessment (*part*)
Vulnerability analysis		Holistic campaign assessment (*part*)	Societal effects assessment
Monitoring and detection of activities			Plausible connections assessment

3.0 DESCRIPTION OF ASSESSMENT FUNCTIONS

Five assessment functions for the analysis of hybrid conflict involving an adversary actor and a society of interest are identified, as shown in Figure 1 and described in much more detail in Table 4. Of these five, function 1 combines insights solely derived from preparatory analysis on the hybrid actor, vulnerability of the society of interest and context events relevant to hybrid operations. Function 2 combines insights solely from monitoring and detection of activities and effects. Functions 3 to 5 rely on the combination of preparatory analyst-driven input and information-driven input from monitoring and detection. In terms of sequence, function 1 should be conducted first since it relies on preparatory analysis – and this can even be done before monitoring and detection of possible hybrid activities has started. This qualitative preparatory work should be updated iteratively, depending on the latest events, the intensity of the hybrid campaign, and when a specific need to do so is identified (see the intelligence development sub-functions in Table 3). After this functions 2 to 5 can be realised in parallel and can be updated on an ongoing basis.

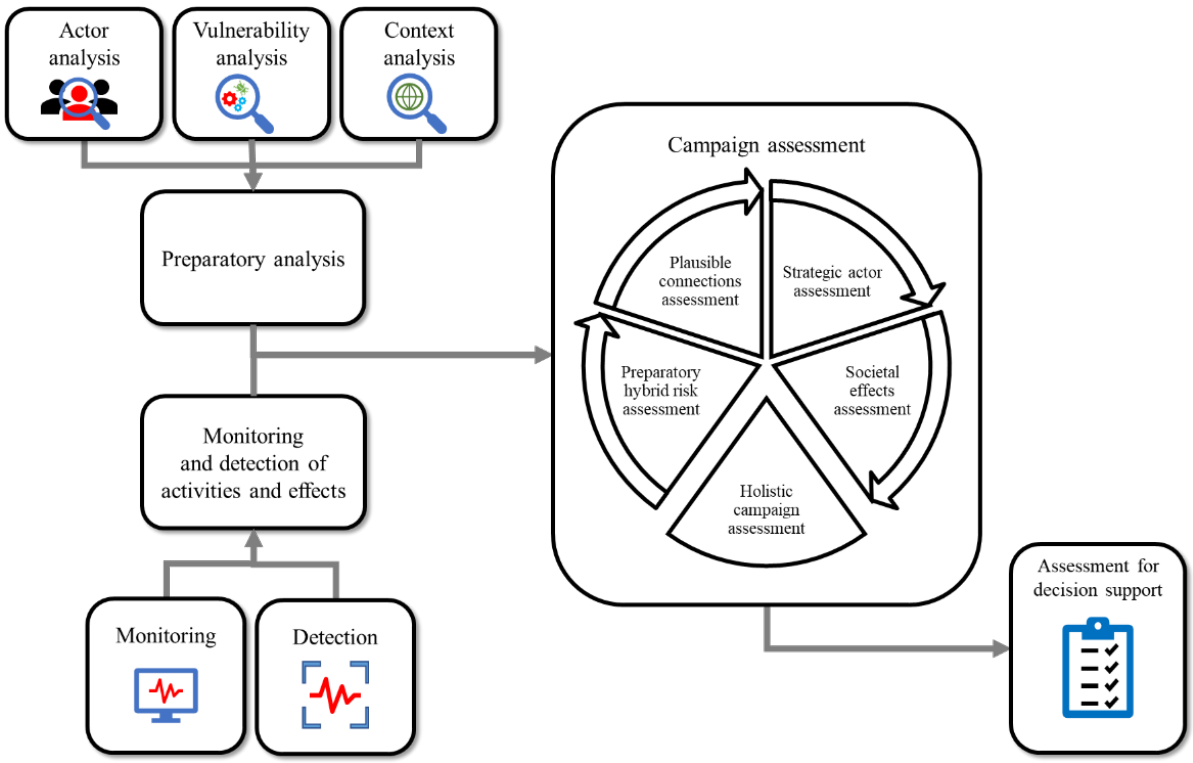

Figure 1 – Schematic overview of the campaign assessment functions and their inputs

The results of the five assessment functions shall likely be taken up in an analytical workspace. We do not

present such a workspace nor a dashboard for visualisation of the results here. Instead, the main result of each function is described in Table 3 and Table 4 along with the subfunctions for each assessment function, and the assessment questions that they address. These questions are often layered in nature. For instance, one function may focus on the descriptive question "What activities has an actor conducted to pursue their goals?" And a later function provides extra insight on the issue through a further descriptive question "What effects have been observed due to these activities?" Later, explanatory assessment questions can be used to find reasons for events to occur by referring to strategic actor goals or societal vulnerabilities – e.g., "Are these signals part of a deliberate campaign or simply opportunistic?". Predictive and prescriptive questions on expected further developments – "What may happen next?" – and mitigating measures –"What can we do about it?" – can be used to start actual decision support. In this way, the assessment functions complement and build upon one another to provide an integrated assessment of a hybrid campaign.

It is important to consider ways in which our proposed hybrid assessment process might be vulnerable to the challenge of analytical bias (UK PHIA, 2019). The framework of hybrid conflict applied in the assessment process mainly reasons from rational lines of operation representing coherent packages of activities directed at a strategic goal. This approach has the potential to fall foul of tunnel vision: hybrid activities are sometimes more opportunistic or surprising – which may be missed out in assessment if the analyst makes an assessment by trying to confirm the presence of well-known lines of operation only. There are two partial solutions included in our process to help address such bias: (1) iteratively check for necessary updates to the framework used and the preparatory analyses, as suggested in some of our assessment sub-functions; and (2) the ability to apply the process to multiple adversary actors and thereby construct competing hypotheses of a hybrid campaign. Other ways to mitigate bias could supplement the proposed process with other structured analytical techniques, such as analytical reasoning from contradictory evidence or critical thinking methods such as devil's advocacy (Pherson & Heuer, 2020).

Table 3 – Overview of assessment functions, sub-functions, and questions addressed per sub-function. The letters in front of assessment questions correspond to the letters in front of the assessment subfunctions.

Assessment function	Assessment subfunctions
Description of assessment questions	
1. Preparatory hybrid risk assessment Assessment of the risks a hybrid actor poses to a society's vulnerabilities, accounting for forthcoming context events.	a. Actor vulnerability confrontation b. Context forecasting
a. Can a specific vulnerability be targeted by a certain actor's goals and capabilities? How susceptible is the vulnerability to being targeted? What is the impact of the vulnerability being targeted? *b. Can an upcoming context event be exploited by an actor's goals or capabilities? Is an upcoming context event relevant to vulnerabilities?*	
2. Plausible connections assessment Assessment of the observed links between activities of a hybrid actor and effects in a society of interest, accounting for past context events.	a. Activities-effects assessment b. Intelligence gap detection c. Context assessment
a. Which activities caused the observed effects? What is the impact of observed activities on the society? *b. Are there observed effects for which the activity that caused it are unknown?* *c. Have observed activities targeted or used context events? Is an observed effect related to a context event? Can the current exploitation of a context event be related to a vulnerability? Does the current exploitation of a context event advance an actor's goals or capabilities?*	
3. Strategic actor assessment Assessment of the activities conducted by the hybrid actor to achieve its goals, including the applied capabilities, future expected activities and intelligence requirements.	a. Strategic status b. Activity forecasting c. Plausible attribution d. Intelligence development – Activity revision e. Intelligence development – Actor warning f. Actor analysis revision g. Actor-activities mapping

a. Do observed activities match with actor goals? How many observed activities are in line with the actor's goals? Which capabilities have been applied by the actor? *b. What observed activities can be expected in the future by an actor, reasoning from its current goals?* *c. Can observed activities be attributed to an actor?* *d. Which new activities are performed by the actor?* *e. Do new observed activities give rise to changing goals or novel capabilities?* *f. Does the preparatory analysis need to change due to new intelligence developments?* *g. Which locations are being targeted to achieve the hybrid actor's goals?*

Table 4 – Overview of assessment functions continued

4. Societal effects assessment Assessment of observed effects and their impact on societal vulnerabilities, including priorities for developing resilience, future expected effects and intelligence requirements.	a. Societal system status b. Effect forecasting c. Intelligence development – effect revision d. Intelligence development – vulnerability warning e. Vulnerability analysis revision f. Resilience radar g. Vulnerabilities-effects mapping
a. Does an observed effect impact a vulnerability or a societal function? *b. Does the presence of certain vulnerabilities make certain effects more likely in the near future?* *c. Which new effects in the society of interest have been observed?* *d. Are the new observed effects due to vulnerabilities not seen before?* *e. Does the preparatory analysis on vulnerabilities need to change due to new intelligence developments?* *f. Which vulnerabilities should be strengthened to mitigate against observed effects?* *g. At which locations have effects impacted a vulnerability?*	

5. Holistic campaign assessment Assessment of the hybrid campaign as a whole, combining a hybrid actor perspective and a society-of-interest perspective, and identifying focus areas to mitigate a hybrid campaign.	a. Effect actor assessment b. Vulnerability targeting assessment c. Holistic campaign overview d. Mitigation assessment e. Campaign mapping
a. Does an actor have the intent or goal(s) to inflict the observed effects? Does an actor have the capability to inflict the observed effects? *b. Is an observed activity targeting one of the identified vulnerabilities?* *c. Which actor goals lead to activities that affect a societal vulnerability? What does the goal-activity-effect-vulnerability 'chain' look like as a whole? Are there important nodes in this chain? What are prominent enablers of the above chain for the hybrid actor?* *d. How might the society of interest break this chain and disrupt the hybrid campaign?* *e. Where are events associated with goals-activities-effects-vulnerabilities located?*	

4.0 CASE STUDY

In this section we illustrate the assessment functions with a case study, relying on a fictional scenario that plays out in the context of the COVID-19 pandemic. Due to space restrictions, the case study is limited in scope to a single hybrid actor directed to a single strategic goal by leveraging a single vulnerability in a single society of interest. Nevertheless, the case study shows how the functions can be used to fuse incoming signals from multiple societal domains with analyst insight to provide a whole-of-society assessment of hybrid conflict.

It is October 2021, and in EU country A the relative shine of a summer in which a number of COVID-19 restrictions were lifted, has well and truly worn off. Despite redoubled attempts to bolster vaccination levels, the emergence of a new 'Gamma' COVID variant – extremely infectious but not lethal in most cases – is leading to what experts predict to be a latest wave of COVID infections. Public vaccination uptake and subsequent efficacy of vaccines in breaking the link between infection and serious illness are key determinants of whether another strict lockdown will be needed this autumn.

Based on the preparatory analysis (upper-left part of Figure 1), qualitative analyst insights of the case study result in the identification of societal vulnerabilities and hybrid actor goals as inputs into our assessment functions. A major vulnerability is the erosion of public trust in the country's public health institute, both in the vaccine programme and in their advice to the government regarding restrictive measures. This needs to be overcome to avoid a repeat or worsening of major riots as seen in early 2021. Such unrest would be a crucial contributor to loss of government control over the COVID-19 crisis. At the same time, this scenario plays into the strategic goals of hybrid actor X, who sees EU country A's situation – also mirrored in other European countries – as an opportunity to undermine unity both within and between EU member states. Preparatory analysis identifies that hybrid actor X will seek to increase social tensions within EU nations, and destabilise the political decision-making between EU nations.

The other major input to our assessment functions are incoming signals (lower-left part of Figure 1). This comprises two elements, namely information that is detected from intelligence collection about the activities

of an adversary hybrid actor, and information that arises due to monitoring of deleterious effects in the societal system in EU Country A. For our fictional case study, the following signals have been observed:

- Open source reports allege that a number of politicians and senior government officials of EU country A received payments from a known senior figure in the regime of actor X in return for espousing anti-vaccine views and other narratives favourable to actor X (activity 1, in the political domain).
- A major hack has been detected at the country A's public health institute, attributed to a hacking collective linked to actor X (activity 2, infrastructure domain and cyber domain). A breach was detected in the network security measures giving unrestricted access, including to vaccination records, for a period of three days (effect 1, infrastructure domain and cyber domain). Subsequently, vaccination information, including the names of thousands of citizens and apparently altered vaccination records, were leaked via an anonymous Twitter account (activity 3, information domain).
- According to public opinion polls, trust in EU country A's public health system dipped to its lowest point since the start of the COVID-19 pandemic (effect 2, social domain).

Drawing on these inputs from the preparatory analysis and incoming signals, we can illustrate the additional insights obtained by fusing them using our assessment functions.

Preparatory hybrid risk assessment: This assessment function does not use the above signals and relies solely on qualitative analysis of societal vulnerabilities and actor goals. The *Actor vulnerability confrontation* for this case study shows that the identified vulnerability of public trust in EU country A's public health institute can be exploited by actor X to achieve its goal of increasing social tensions within EU nations. *Context forecasting* shows a number of future context events that may be leveraged to target the vulnerability and further the state actor's goal. Namely, parliamentary elections in late 2021 in some EU countries, the religious holidays of Mawlid and Christmas, and World Immunisation Week in early 2022.

Plausible connections assessment: This assessment function examines the activity and effects signals, without reference to the preparatory analysis. The *Activities-effects assessment* shows the causal connection between activity 2 and effect 1. It also shows a link between activity 2 and subsequent activity 3. *Intelligence gap detection* shows plausible but not confirmed links between activity 1, activity 3 and effect 2. Confirming these activity-effect links is a potential focus for intelligence collection, especially focused on more sensitive measures of effects on public trust. The *Context assessment* shows that more activities and effects were observed during the summer months, the same period in which EU country A's government made an attempt to vaccinate more citizens and re-open society.

Strategic actor assessment: The strategic actor assessment provides detailed assessment regarding the activities and goals of hybrid actor X. The *Strategic status* shows that activities 1, 2 and 3 are part of a concerted focus on increasing social tensions within EU nations, whilst actor X has been less active in striving for other goals (e.g., control of diaspora in other countries). *Activity forecasting* shows that similar activities may be continued, most likely in the information and infrastructure domains focused on destabilising political decision-making between EU countries, with the EU vaccine passport a possible target. *Plausible attribution* shows that, in light of the other observed activities, activity 3, conducted by an anonymous actor, is likely to be attributable to actor X. *Intelligence development* can help shed more light on this, for instance by focusing on whether the Twitter account is employing an already-known or novel modus operandi. The locations of these activities as revealed by *Actor-activities mapping*, show a focus on informational and infrastructure activities targeting governmental institutions in the country's capital city, rather than, for instance, physical activities focusing on vaccine production centres or logistics hubs.

Societal effects assessment: The societal effects assessment provides a detailed assessment of effects in the

society of interest. The *Societal system status* shows that effect 1 and effect 2 have contributed to the erosion of public trust in the country's public health institute. Meanwhile, other vulnerabilities, such as the integrity of water management systems, remain unaffected in this case study. The *Resilience radar* shows that, in comparison with other vulnerabilities, this is a serious development, which could lead to the delay or disruption of strategic policy decisions, suggesting urgent mitigating efforts are necessary. *Effect forecasting* shows that, if this vulnerability were to worsen, one would expect to see deteriorating social cohesion, with certain groups being less willing to vaccinate and responding negatively when they are denied freedoms such as access to the service and entertainment industry. The *Intelligence development* functions show that a network breach of the severity of effect 1 is yet to be seen, this requires more intelligence collection to determine whether this is a novel vulnerability in the integrity of strategic cyber infrastructure. This supports *Vulnerability analysis revision*, which signals the need to update the preparatory analysis.

Holistic campaign assessment: This function provides a holistic perspective of the hybrid campaign. The *Effect-actor assessment* shows that the observed effects contribute to the goal of actor X to increase social tensions within EU nations. The *Vulnerability targeting assessment* shows that all activities target the erosion of public trust in EU country A's public health institute. These assessments can be seen in their broader context in the *Holistic campaign overview*. By visualising the goal-activity-effect-vulnerability 'chain', it is clear that single high-impact activities targeting government institutions such as activity 2, are complemented by ongoing low-impact activities in the political and information domains (activities 1 and 3). Indicators of public trust show that activity 2 caused a disproportionate impact on this vulnerability, suggesting that actor X's cyber capabilities are an important enabler in striving for their strategic goals. To interrupt this campaign, *Mitigation assessment* suggests the need for immediate efforts to protect strategic cyber infrastructure and longer-term efforts to restore public trust and strengthen social cohesion. *Campaign mapping* shows that while the activities and effects were observed in the capital city of country A, they contribute to a vulnerability of national reach and importance.

5.0 DISCUSSION AND CONCLUSION

5.1 Challenges to assessment of hybrid conflict

There are a number of challenges to the research approach we applied to the assessment of hybrid conflict in this paper. Firstly, our descriptions of hybrid conflict tend to reason from the situation of a single society targeted by a single actor, while this will in some cases be too simplistic. Most conflicts involve more actors. However, our models can be generalised to a multi-society, multi-actor situation by replicating the analysis of actors and vulnerabilities, and thus replicating multiple assessments. That said, a more complete assessment of strategic-level interactions over time between states is necessary, examples of which include the analysis of archetypical dynamics between state actors (e.g. Keijser et al., 2020), and the analysis of cross-domain deterrence mechanisms (e.g. Sweijs & Zilincik, 2021). Furthermore, an explanatory understanding of hybrid conflict needs to include analysis of internal dynamics as reasons for foreign policy decisions by adversary actors (e.g. see "other causes" in Brown, 2018: 71).

The assessment process presented provides a structured process through which to analyse available information and evidence on hybrid conflict. There are some challenges related to the quality of this type of structured assessment process. Analytical bias is one important challenge that we have already considered in section 3 (UK PHIA, 2019). Another methodological challenge is that the assessment process has to cope with the possibility of limited or non-representative evidence inherent to the analysis of hybrid conflict (also mentioned in section 1.1). A partial solution to this is to integrate anticipatory methods that can be used to discover formerly unknown-unknowns (Kerbel, 2019). This can also be done through anomaly detection with (big) data analysis.

In this article a design method was followed aiming at an assessment process that gathers available input

analyses and provides various types of decision support. This assessment process is one of many possible ways of assessing hybrid conflict. In using design thinking we inferred to the best possible process. Thus, although our process is based on a breadth of relevant literature, we did not compare the utility of multiple potential methods. Separately, the described assessment process is not exhaustive, in that it provides only the most relevant elements for a strategic-level assessment of hybrid conflict. An example of an intelligence challenge not fully covered is sensitive early warning of hybrid threats. Lastly, the assessment functions should be tested in the context of a more detailed case study than the one presented here, which was limited by lack of space in this article.

5.2 Conclusion and further research

In this article a novel, integrated process for assessment of hybrid conflict was presented. A whole-of-society perspective on hybrid conflict able to combine multi-dimensional insights into actor activities, capabilities and goals and societal vulnerabilities was provided. The presented assessment relies on the ongoing interaction between human-derived analytical insights – taking into account context, ambiguity, normality – and signals derived from incoming data, taking into account structuring and combining information from multiple sources. Furthermore, our view of assessment is well-suited to hybrid analytical approaches – including hybrid artificial intelligence tools – in which human and automated intelligence are combined and thus optimised. Considering the complexity and volume of the information, the strain on resources and limits to the absorption capacity of both analysts and decision-makers, automated approaches are a crucial tool in the analytical toolbox.

Further research efforts should be aimed at operationalising the assessment process and trying it out in practice. This research would need to analyse and accommodate user challenges as well as policy and organisational challenges. In some way, we assume a perfect policy situation of an assessment cell that is integrally responsible for the analysis of hybrid conflict and that has access to all necessary information sources. However in reality, analysis of hybrid conflict has in most countries not been institutionalised (as noted by Treverton, 2018). Furthermore, research and evaluation efforts should analyse the added value of this approach compared to current ways of analysing hybrid conflict.

Many types of follow-up studies can be done that focus on single types of assessment presented above, such as strategic actor assessment or studying societal effects of hybrid activities in more detail. One such follow-up study could use the assessment framework presented to conduct directed data collection and advanced analysis in order to, for instance, identify patterns in hybrid modus operandi or detect anomalies. Although challenges of black numbers and unknown unknowns remain, the research ideas outlined above would represent a major advancement of the analysis of hybrid conflict building both on data insights and analyst insights. We hope the assessment functions described in this paper can provide a blueprint for intelligent analytical tooling mitigating the challenges of decision-making in hybrid conflict.

REFERENCES

[1] Bekkers, F., Meessen, R. & Lassche, D. (2018). *Hybrid conflicts: The new normal?* The Hague: TNO & The Hague Centre for Strategic Studies. Available via https://repository.tudelft.nl/view/tno/uuid:c280883b-13af-4654-aa8a-9a8e7a0d2a99. Accessed on 11th of August, 2021.

[2] Brown, J. (2018). An alternative war: The development, impact, and legality of hybrid warfare conducted by the nation state. *Journal of Global Fault Lines*, 5(1-2): 58-82.

[3] Cullen, P. (2018). *Hybrid threats as a new 'wicked problem' for early warning*. Strategic Analysis, Number 8. Helsinki, Finland: The European Centre of Excellence for Countering Hybrid Threats. Available via https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/. Accessed on 11th of August, 2021.

[4] Defensie Inlichtingen en Veiligheid Instituut (2012). *Analysis Handbook: Theory and methodology in Intelligence analysis (title translated from Dutch).* DIVI publication HB 30-31.

[5] Doppler Haider, J., Gastecker, B., Pohl, M., Seidler, P., Kodagoda, N., & Wong, B. W. (2019). Sense-making strategies in explorative intelligence analysis of network evolutions. *Behaviour & Information Technology*, 38(2), 198-215.

[6] Enserink, B., Hermans, L. M., Kwakkel, J. H., Thissen, W. A. H., Koppenjan, J. F. M., & Bots, P. W. G. (2010). *Policy analysis of multi-actor systems*. The Hague: Lemma.

[7] European Union (2018). A Europe that protects: Countering hybrid threats. Brussels: EEAS. Available via eeas.europa.eu/sites/eeas/files/hybrid_threats_en_final.pdf. Accessed on 11th of August, 2021.

[8] Gallo, G. (2013). Conflict theory, complexity and systems approach. *Systems Research and Behavioral Science*. 30 (2013): 156-175.

[9] Grabo, C. M. (2002). *Anticipating surprise: Analysis for strategic warning*. Center for Strategic Intelligence Research, Joint Military Intelligence College.

[10] Hutchins, S.G., Pirolli, P.L. & Card, S.K. (2007). What makes intelligence analysis difficult?: A Cognitive Task Analysis. In: Hoffman, R.R. (ed.), *Expertise Out of Context: Proceedings of the Sixth International Conference on Naturalistic Decision Making*. New York: Psychology Press.

[11] Joint Doctrine Publication - 2 (2010). *Intelligence.* Netherlands Ministry of Defence, The Hague.

[12] Keijser, B., Veldhuis, G., Scheepstal, P. van (2020). Towards a dynamic theory of hybrid conflict: An exploration with system archetypes. *Proceedings of the 17th Operations Research & Analysis Conference.* STO-MP-SAS-OCS-ORA-2020. Paris: NATO STO.

[13] Kerbel, J. (2019). *Coming to terms with anticipatory intelligence*. War on the Rocks. Available at https://warontherocks.com/2019/08/coming-to-terms-with-anticipatory-intelligence/. Accessed on August 9th 2021.

[14] Lowenthal, M. (2016). Intelligence analysis. In Oleson, P.C. (ed.), *AFIO's Guide to the Study of Intelligence* (pp. 291-296). Falls Church, VA: Association of Former Intelligence Officers.

[15] Menkveld, C. (2021). Understanding the complexity of intelligence problems. *Intelligence and National Security*, Ahead-of-print, 1-21.

[16] Monaghan, S., Cullen, P., Wegge, N. (2019). *MCDC Countering hybrid warfare project: Countering hybrid warfare*. MCDC.

[17] Moore, D.T. (2011). *Sensemaking: A structure for an intelligence revolution.* Washington DC: National Defense Intelligence College.

[18] Moore, D.T., Moore, E., Cantey, S., Hoffman, R.R. (2021). Sensemaking for 21st century intelligence. *Journal of Intelligence History*, 20(1), 45-59.

[19] NATO (2016) *AJP-2.1 – Allied Joint Doctrine for Intelligence Procedures.* NATO Standardization Office (NSO).

[20] NATO (2019). *NATO's response to hybrid threats.* Available via https://www.nato.int/cps/en/natohq/topics_156338.htm. Accessed on August 11th, 2021.

[21] NCTV (2019). *Chimaera: An analysis of the 'hybrid threat' phenomenon*. The Hague: National Coordinator for Security and Terrorism. Available via https://english.nctv.nl/documents/publications/2019/09/05/analysis-of-the-%E2%80%98hybrid-threat%E2%80%99-phenomenon. Accessed on 11th of August, 2021.

[22] Owen, C. (2006). Design thinking: Notes on its nature and use. *Design Research Quarterly*, 2 (1), 16-27.

[23] Pherson, R.H., Heuer Jr., R. J. (2020). *Structured analytic techniques for intelligence analysis*. Los Angeles, CA, USA: CQ Press.

[24] Pirolli, P., Card, S.K. (2005). The sensemaking process and leverage points for analyst technology as identified through cognitive task analysis. *Proceedings of International Conference on Intelligence Analysis*. May 2005. McLean, VA, USA.

[25] Pohl, M., Haider, J., Pallaris, C., & Wong, B. W. (2015). Guidelines for sensemaking in intelligence analysis. *2015 European Intelligence and Security Informatics Conference* (p. 177). IEEE.

[26] Powell, T.E. & Eles, P.T. (2018) Afghan profiles: Finding structure in survey data to better understand the human terrain. *Proceedings of the NATO IST-160 Specialist meeting on Big Data and Artificial Intelligence for Military Decision Making*, STO-MP-IST-160. Paris: NATO STO.

[27] Pruyt E., Wijnmalen D. (2010) National risk assessment in The Netherlands. In: Ehrgott, M., Naujoks, B., Stewart, T., Wallenius, J. (Eds.), *Multiple criteria decision making for sustainable energy and transportation systems*. Berlin: Springer.

[28] Rietjens, S. (2020). *A warning system for hybrid threats – is it possible?* Hybrid CoE Strategic Analysis No. 22. Helsinki: The European Centre of Excellence for Countering Hybrid Threats. Available via https://www.hybridcoe.fi/publications/a-warning-system-for-hybrid-threats-is-it-possible/. Accessed on 11th of August, 2021.

[29] Sweijs T., Zilincik S. (2021) The essence of cross-domain deterrence. In: Osinga F., Sweijs T. (Eds.), *NL ARMS Netherlands Annual Review of Military Studies 2020*. The Hague: T.M.C. Asser Press.

[30] Treverton, G.F. (2014). The future of intelligence: Changing threats, evolving methods. In: Duyvesteyn, I., de Jong, B., van Reijn, J. (Eds.), *The Future of Intelligence: Challenges in the 21st Century* (pp. 27-38). London: Routledge.

[31] Treverton, G.F. (2018). *The intelligence challenges of hybrid threats: Focus on cyber and virtual realm*. Stockholm, Sweden: Swedish Defence University.

[32] Treverton, G.F. (2021). An American view: Hybrid threats and intelligence. In: Weissmann, M., Nilsson, N., Palmertz, B. & Thunholm, P. (Eds.), *Hybrid Warfare: Security and Assymetric Conflict in International Relations* (pp. 36-45). London: I.B. Tauris.

[33] UK Professional Head of Intelligence Assessment (2019). *Professional development framework for all-source intelligence assessment*. UK Cabinet Office publications.

[34] US Department of Defense (2021). *DoD intelligence and security professional certification*. Available via https://dodcertpmo.defense.gov/CDASA/. Accessed on 11th of August 2021.

[35] Vandepeer, C. (2011). *Rethinking threat: Intelligence analysis, intentions, capabilities and the challenge of non-state actors.* PhD thesis. Adelaide, Australia: University of Adelaide.

[36] Weissmann, M., Nilsson, N., Palmertz, B. & Thunholm, P. (Eds.), *Hybrid warfare: Security and asymmetric conflict in international relations*. London: I.B. Tauris.

[37] Wirtz, J.J. (2013). Indications and warning in an age of uncertainty. *International Journal of Intelligence and Counterintelligence*, 26(3): 550-562.