Proceedings of the 2018 Winter Simulation Conference
M. Rabe, A.A. Juan, N. Mustafee, A. Skoogh, S. Jain, and B. Johansson, eds.

HYBRID CONFLICT MODELING

Mariusz Balaban

U.S. Army
NTC
Fort Irwin, 92310, USA

Paweł Mielniczek

University of Warsaw
Krakowskie Przedmieście 26/28
Warsaw, 00-927, POLAND

ABSTRACT

Although representations of many elements of hybrid conflict can be identified in the literature, its more holistic view needs more research. The use of Modeling and Simulation (M&S) to represent past and emerging hybrid conflicts can aid in better understanding of their factors and deceptive mechanisms leading to the accumulative effects. Gained understanding could help in preventing, mitigating, and winning hybrid conflicts. Because hybrid conflict is not an entirely new phenomenon this paper offers a few historical examples followed by an attempt to clarify relevant to hybrid conflicts terms. Causal loop diagram (CLD) is used to represent theoretical model of hybrid conflict, while Dynamic Bayesian Network (DBN) demonstrates its implementation. The final section discusses a coordinated defense approach against hybrid threats and needs for a better hybrid conflict representation.

1 INTRODUCTION

According to Thiele (2015) ‘gray is the new color of war’. Although in the past irregular warfare have been often used due to the weakness of the actor with no sufficient means to engage using conventional warfare, future brings challenges where hybrid warfare is used not only by weak states and none-state entities but also by powerful and capable states. The following introduction presents a historic perspective on hybrid warfare, relevant to hybrid conflict terms, and found in the literature relevant modeling work.

1.1 Historic Perspective on Hybrid Warfare

One of common denominators for hybrid as opposed to traditional warfare is a blurring distinction between military and civilian (Jacobs and Lasconjarias 2015). Sari (2016) puts it even more explicitly, saying there is ‘a tendency toward blurring the lines between the states of war and peace’. It can be observed that although on a different scale, virtually all of the elements occurring in hybrid warfare have some analogies in conflicts which occurred before the UN Charter was adopted (UN 1945).

First, among early non-state actors having certain military power, one may list the medieval Hanseatic League and Nizari Ismailis (Assassins). Second, irregular forces and non-conventional methods of warfare are long-known in history, having been employed by insurgents, guerrillas and underground states fighting for independence as well as by special forces carrying out sabotage operations. The story of the Trojan Horse best illustrates that deception is nothing new. Third, terror is also old as this world, with torture, mass killings and repression being a method of subjugating occupied territories throughout the centuries. So do the attempts to assassinate important persons, e.g., Napoleon III in 1858 when a bomb caused multiple victims among the crowd. Although on a scale incomparable to modern times, likewise there are relatively old examples of terrorism, such as the Fenian dynamite campaign carried out by the Irish republican organization in 1881-85. Also, suicide attacks were employed long before 9/11, for instance by Japanese Kamikazes in 1944-45. Fourth, as an example of support for insurgents, we may indicate role of the Russian Empire, United Kingdom and France in the Greek War of Independence (1821-1829). Another example is the Targowica Confederation, where the anti-governmental

978-1-5386-6572-5/18/$31.00 ©2018 IEEE

confederation established by Polish and Lithuanian magnates in 1792 was inspired by the high-level Russian leaders and preceded the Polish-Russian War and the Second Partition of Poland. Fifth, precursor elements of cyber warfare were known before 1945, as for instance in 1932 Polish Cipher Bureau broke German Enigma machines used to protect classified information. Even at that time, it was hard to overestimate such advantage over the enemy. Sixth, the Ribbentrop-Molotov pact of 1939 is an example of 'diplomatic negotiations mollifying regional actors', as without this substantial contribution, the USSR would have been far less likely to remain neutral towards the expansion of the Nazi Germany. Seventh, the Second World War's airborne leaflet propaganda is an example of an information operation aimed at the homeland audience. Next, taking advantage of law occurred for instance when the USSR invaded Poland on September 17, 1939, despite a non-aggression pact of 1932, which was one of the reasons why Poland decided to reject Hitler's ultimatum and defend against German aggression. Eighth, similarly to U.S. policy towards Nicaragua in the 1980s or Russian occupation of Crimea since 2014, keeping armed forces on permanent exercise and using a threat of use of force was employed by Nazi Germany towards Czechoslovakia, Austria and Poland before the Second World War.

To sum up, hybrid warfare reflects a wide range of activities that state and non-state actors undertake in order to gain political, military, economic, social, information, infrastructure, physical environment, and time (PMESII-PT) advantages. It is not surprising that both now and throughout history political and military leaders looked for the best ways to achieve their goals and considered the pros and cons of every action, including these perceived as dishonorable. This truism was known long before the adoption of the UN Charter and post-Second World War development of international law. It should be noticed that hybrid warfare covers a wide range of threats, each being addressed by different institution. Among others: a) acts of regular warfare are addressed by regular forces, b) threat of use of force is addressed not only by boosting own military capacities, but also by diplomatic means, such as seeking alliances and guarantees, c) covert support for insurgents or terrorists is addressed by special forces, special agents and police, d) negative propaganda is addressed by national media to create counter-narratives, cyber-security specialists, in case propaganda is disseminated as a result of cyber-attacks, and even courts, in cases propaganda entails attacks on reputation, e) cyber-threats may be addressed by cyber-security forces, if they are available, or by cyber-security specialists, which usually would not be coordinated at a national level, f) espionage threats are addressed by counter-intelligence, and g) chemical or biological threats are addressed by special forces, special agents and police experts who eliminate chemical and biological threats or mitigate their effects.

In their work on the notion of hybrid warfare in international law, Karski and Mielniczek (2018) wrote: 'As argued, it is technically possible to wage hybrid warfare without an armed attack triggering the right of self-defense. This does not mean that the states being subject to such actions are defenseless, but rather that such dangers require the so-called 'flexible responsiveness'. In case one method merely constitutes a breach of non-intervention principle, it is possible to employ reprisals. Moreover, even if there are doubts as to whether certain actions reach the threshold of coercion, the retaliatory measures can be justified as retorsions. Especially in case of states too weak as to employ reprisals or retorsions effectively deterring the perpetrator, the idea would be to call allies to apply collective retorsions or reprisals'.

1.2 Relevant Terms

Hybrid threats, hybrid warfare, hybrid conflict, and hybrid war, are terms often used when describing the ongoing conflicts in the Middle East and Ukraine, but their meanings are not always consistent. U.S. Army defined hybrid threat as diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects (DA 2010). Newson (2014) defined hybrid warfare as a combination of conventional, irregular, and asymmetric means, including the persistent manipulation of political and ideological conflict, which can include the combination of special operations and conventional military forces, intelligence agents, political provocateurs, media representatives, economic intimidation, cyber-attacks, proxies and surrogates, para-militaries, terrorist, and criminal elements. He suggested that hybrid warfare places a premium on unconventional warfare activities conducted to enable a resistance movement to coerce, disrupt, or overthrow a government.

Thiele (2015) identified hybrid warfare as combining four instruments of power, i.e., diplomatic, informational, military, and economic (DIME). On the other hand, Cirimpei (2016) considered PMESII battlespace operational variables to assess country's vulnerabilities to a potential hybrid threat. Vaczi (2016) used levels of intensity of threats and intentions of actors involved to distinguish between hybrid threat, hybrid conflict, and hybrid war. Pawlak (2015) identified transition from a hybrid conflict to a hybrid war as a situation where hybrid threat evolves and intensifies to overt use of conventional force. Figure 1 shows dependencies between proposed definitions of several key terms central to this work.

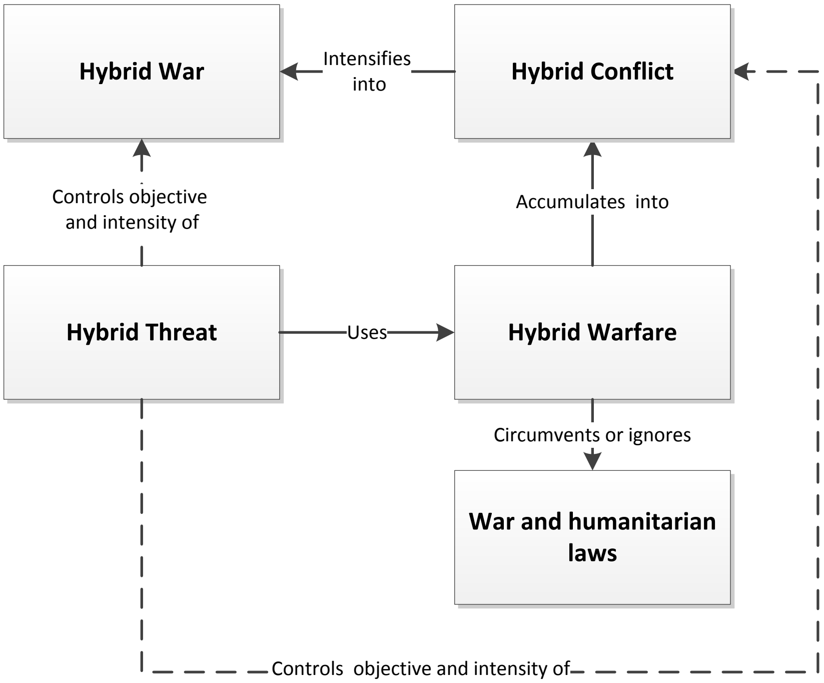

Figure 1: Dependencies between relevant terms.

The problem of defining terms related to hybrid warfare may have originated from their very broad scope and it is likely that the proposed below definitions will continue to evolve for their different purposes.

Definition 1 Hybrid warfare (HW) is a combination of at least two elements out of four main categories of power 1) Politico-diplomatic, additionally including legal and intelligence 2) military, additionally including paramilitary and irregular forces, 3) socio-economic, additionally including criminal elements and civilian measures, and 4) information and infrastructure (PDMSEII) all unified to achieve mutually benefiting effects.

Definition 2 Hybrid threat (HT) is an actor or a network of actors willing to engage in hostile, usually covert, activities employing HW. HT may be controlled or influenced by a nation-state, proto-state, or a non-state actor such as large organizations, which often attempts to either circumvent or ignore international laws.

Definition 3 Hybrid conflict (HC) is a state of conflict, which has not yet reached a state of conventional war, between two or more actors (nation-state, proto-state, or a non-state) aiming to achieve their political and/or strategic objectives via multiplicative effects of HW, coordinated by one or multiple HTs at tactical, operational, strategic, and political levels of conflict.

Definition 4 Hybrid war is a combination of a HC and overt use of conventional forces.

For instance, Hassan as-Sabbah, a leader of Nizari Ismailis is an example of HT (definition 2). He used a combination of asymmetric and psychological warfare (definition 1) to draw his opponents into a submission. A good example for definitions 3 and 4 is HC between Ukraine and Russia, which escalated into a hybrid war.

1.3 Relevant Modeling Work

Many elements relevant to HC representation can be found in the literature. Sokolowski and Banks (2007) used System Dynamics (SD) to develop insurgency model. The same authors provided a research approach that identified SD, Agent Based Modeling (ABM), Social Network Modeling (SCN), and Game Theory (GT) as methods that can be used to represent global events and demonstrated case studies of Columbian insurgency, Solidarity movement and collapse of Soviet Communism, Vietnam War, and Cuban missile crises (Sokolowski and Banks 2009).

Lieberman (2012) presented a methodology for modeling Complex Adaptive Social Systems (CASS) using ABM method. CASS could be used as a proxy generator of information about the inaccessible societies. For instance, population's approval rates of a war and satisfaction with a government would be of interest because some countries do not provide these data, which could be very helpful to staff and military commanders during a HC. The use of Dynamic Bayesian Network (DBN) by Lieberman (2012) is an interesting direction to capture a change of agent's perspectives, for example, after each step, values of prior probabilities and likelihood function probabilities are updated to accommodate for new information spurred by an event. As a side note, DBN can also be used to represent an aggregated system behavior.

Kott and Corpac (2007) pointed out that multitude of models and methods is required in order to span the environment defined by DIME and PMESII dimensions, where each model may represent its portion of the domain at the adequate level of fidelity. Because of cascading effects between interacting models unanticipated results can provide new insights and assist leaders and staff in better understanding of underlying causes of conflict by visualizing the drivers of instability, centers of power, leader's dilemmas, campaign planning, and interconnections between PMESII environment. Balaban (2015a) proposed a concept of M&S based collaborative foresight support system for conducting a simulation-based analysis of the lifecycle cost-effectiveness of various programs within Defense Acquisition System (DAS) represented in terms of force readiness against current and anticipated threats.

Pioch et al. (2009) proposed extension of the Commander's Model Integration and Simulation Toolkit (CMIST) to support advanced intent modeling allowing for the representation of more proactive agents capable of simulating a simplified model of the already simulated world, projecting the future state of the simulated world, including, for instance, adversary behavior. Kott and Ownby (2015) coined the term adversarial reasoning as computational solutions to determining the states, intents and actions of one's adversary, in an environment where one strives to effectively counter the adversary's actions. This may include belief and intent recognition, opponent's strategy prediction, plan recognition, deception discovery, deception planning, and strategy generation. Ground et al. (2016) discussed the use of Course of Action Development and Evaluation Tool (CADET), used for planning of US Army ground operations taking accounts for adversarial activity. Harder et al. (2017) proposed conceptual framework for an automated battle planning system in combat simulations.

Lowe and Pitinanondha (2015) presented SEBA framework for conceptualization of HC. It considers three domains, i.e., physical, information, and cognitive, in which entity may perform seven functions, i.e., sensing, understanding, decision-making, effects, information mobility, physical mobility, and logistics and support. Cayirci et al. (2016) developed a conceptual model for hybrid environments (CMHE) in which willingness of the targeted community must pass a certain threshold in order for that community to approve tackling with the offender. The difference between the threshold and the willingness defines the capacity of the offender who aims to increase the threshold and decrease the willingness, which is the opposite to defendant's objectives. The proposed coherent mathematical formulas describing relations between main factors allowed to conduct theoretical experiments via Monte Carlo Simulation that provided interesting insights into dynamics of HC.

The use of M&S to represent past and emerging HCs could help in better understanding of HC causes and deceptive actions leading to desirable PMESII effects, which can help in preventing, mitigating, and winning HCs. Although many separate elements of HC were captured and represented using M&S methods its holistic representation requires more work.

2 RESEARCH APPROACH

When conceptualizing a system that depends on multiple levels, i.e., political, strategic, operational and tactical it is important to find factors that allow to bind these levels into a holistic picture. In order to generate a high-level conceptual view of the main factors, their hypothesized causalities, and system's main feedback loops the authors decided to use causal loop diagram (CLD). SD, DBN, Discrete Event Simulation (DES), and ABM are popular M&S methods that can be used to convert high-level concepts into a low-level conceptual model and then into a simulation model (Balaban 2015b). DES and ABM are very useful for representing individual entities, which is beyond the scope at this stage of the research. Both, DBN or SD were considered because they can be used to represent system at aggregate level. DBN was selected because it helped to better represent uncertainty with limited data. The research approach involves development of a conceptual model, followed by its implementation using DBN and a demonstration of its use. A brief introduction of the two methods used in this work is presented next.

2.1 Causal Loop Diagram

CLD should capture the most important components or phenomena and their relations as links indicating directions of influence. Symbols "+" or "- placed on the links specify positive or negative relationships between factors. Positive relationship means that a variable pointed by an arrow follows the direction of change from a variable where the link originates. In a negative relationship the direction of change between the two variables is opposite. Links can form positive feedback loops that drive the change or negative feedback loops that stabilize the system. If a total number of negative links is odd the feedback loop is negative, otherwise it is positive.

2.2 Dynamic Bayesian Network as an Extension of Bayesian Network

DBN is an extended Bayesian Network (BN) with a temporal dimension where every time t = 1, 2, . . . , T represents one time-instant, or time-slice (Hulst 2006). In DBN each time-slice is a part of the model representing specific time-instance connected to another time-slice this way creating kth order transitions between time-slices. If the time-arc starts from the zero time-slice and affects node at nth time-slice, then, the arc is of the nth order.

3 REPRESENTATION OF HYBRID CONFLICT

This section reports on efforts to represent a HC. The purpose of this modeling effort is to propose a high-level theoretical model of HC and demonstrate feasibility of its implementation using DBN based on a sample case study found in the literature.

3.1 Conceptual Model

Based on its definition HC includes at least two sides, a HT called also an attacker, and its target. Figure 2 shows a proposed theoretical CLD of the HC. The *intensity of hybrid attacks* is controlled by *attacker hostile objectives* and under those objectives increases with the expanded *attacker hybrid warfare capabilities*. The increase of *intensity of hybrid attacks* effects in a higher *damage to target* and increases *intensity of countermeasures*. The *strictness of war laws* defines the line between the HC and hybrid war.

It positively affects a *perceived danger of conventional war*. The *perceived danger of conventional war* increases with a growing *intensity of hybrid attacks* and with a growing *intensity of countermeasures*, but additionally generates feedback links decreasing both of its causal factors.

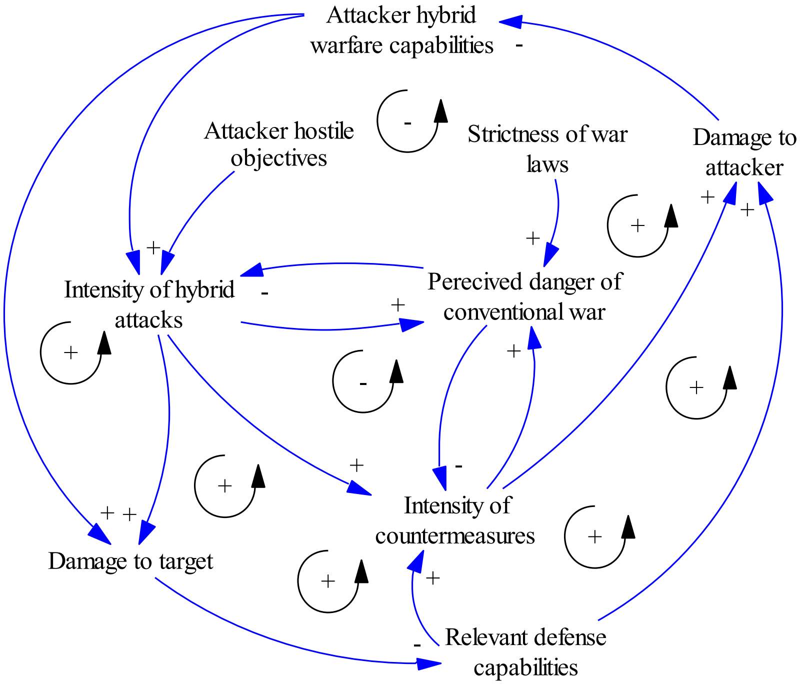
Attacker hybrid warfare capabilities
-
Attacker hostile objectives
-
Strictness of war laws
Damage to attacker
+
+
+
+
+
Intensity of hybrid attacks
-
Perecived danger of conventional war
+
+
+
-
+
+
+
Intensity of countermeasures
-
+ +
Damage to target
+
+
+
+
-
Relevant defense capabilities

Figure 2: Concept of HC.

The *damage to target* has a negative effect on its *relevant defense capabilities*, which has a positive relation with *intensity of countermeasures*. Both, *intensity of countermeasures* and *relevant defense capabilities* have positive relation with *damage to attacker*. Finally, the higher the *damage to attacker* the lower the *attacker hybrid warfare capabilities*, which has a positive relation with *damage to target*. With only nine factors at a very-high level this conceptual model has eight dynamic loops: six reinforcing and two balancing. Not surprisingly, this indicates high dynamic complexity of the system.

3.2 Model Implementation

Figure 3 shows implemented model of HC using DBN. The model allows for temporal reasoning by including a number of time-slices that represent HC phases. Rácz (2015) proposed three phases of HC: 1) preparatory phase that included strategic, political and operational preparation dimensions, 2) attack phase with exploding the tensions, ousting the central power from the targeted region, and establishing alternative political power and 3) stabilization phase, that focused on political stabilization of the outcome, separation of the captured territory from the target country, and lasting limitation of the strategic freedom of movement of the attacked country. Lowe and Pitinanondha (2015) used these phases in their example of SEBA framework. Karber (2015) proposed four levels of HW intensity: 1) political subversion, 2) proxy sanctum, 3) intervention, and 4) coercive deterrence. The first three levels from (Karber 2015) are used in the node *intensity of hybrid attacks*. Levels one and two align with the HC definition, while the third level with the hybrid war. The open use of force threatening political independence or territorial integrity of a state is prohibited by Art. 2(4) of the UN Charter (UN 1945), which can explain the deceptive behavior on the part of HT trying to circumvent UN. *Attacker hostile objectives* node considers these two objectives of HT. Threat against territorial integrity places a strong influence on intervention phase in the *intensity of hybrid attacks* node as compared to threating against political independence, which resorts to influencing political subversion and proxy sanctum phases. *Attacker hybrid warfare capabilities* are based on definition of HW. These four categories modulate *intensity of hybrid attacks*. Subsequently, *attacker hybrid warfare capabilities* along with *intensity of hybrid attacks* determine severity of *damage to target*, which are mapped along the same four PDMSEII categories, this time representing *damage to target*. *Damage to target* lowers *relevant defense capabilities* of the target.

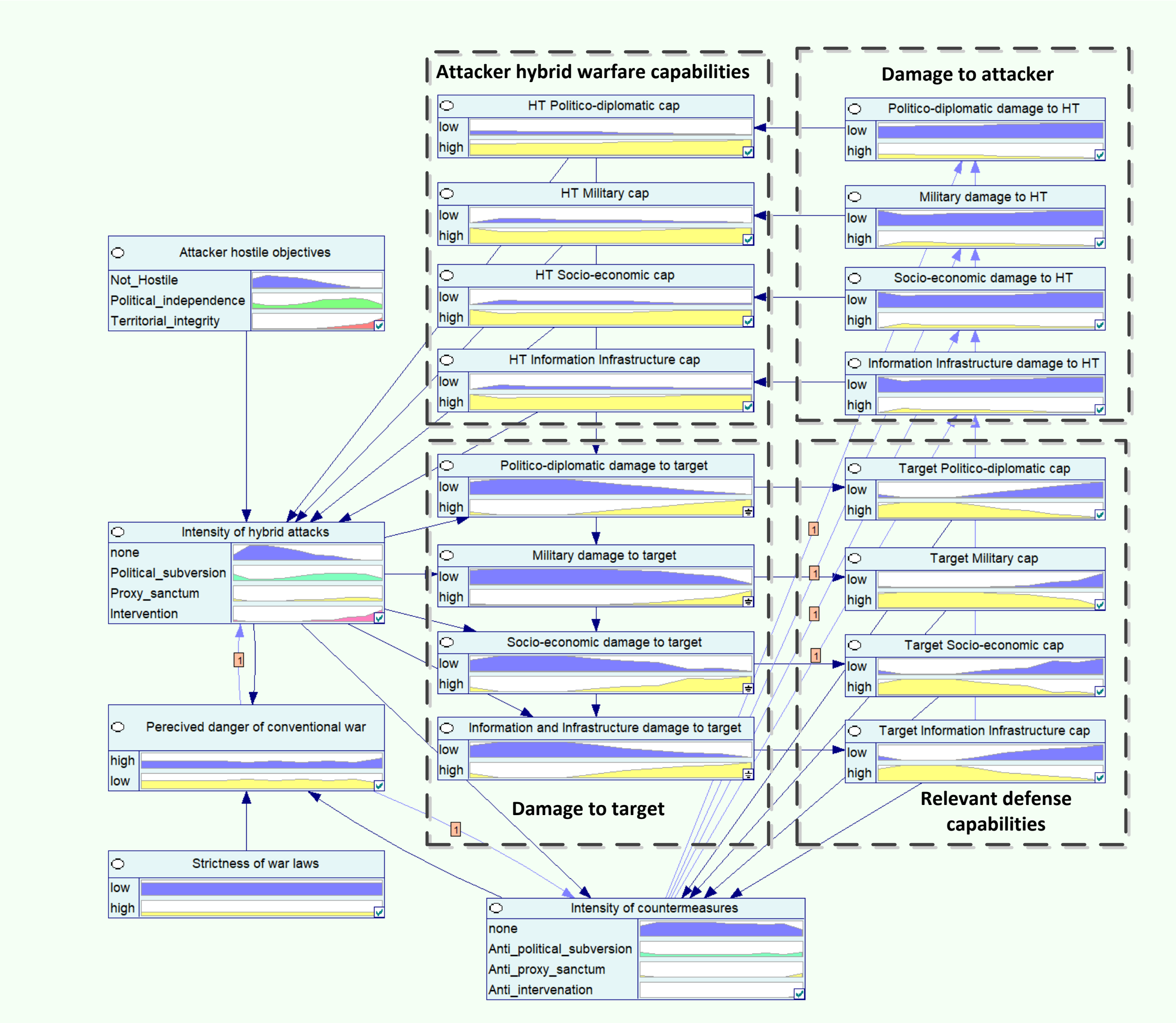
Attacker hybrid warfare capabilities
HT Politico-diplomatic cap
low
high
HT Military cap
low
high
HT Socio-economic cap
low
high
HT Information Infrastructure cap
low
high
Damage to attacker
Politico-diplomatic damage to HT
low
high
Military damage to HT
low
high
Socio-economic damage to HT
low
high
Information Infrastructure damage to HT
low
high
Attacker hostile objectives
Not_Hostile
Political_independence
Territorial_integrity
Intensity of hybrid attacks
none
Political_subversion
Proxy_sanctum
Intervention
Politico-diplomatic damage to target
low
high
Military damage to target
low
high
Socio-economic damage to target
low
high
Information and Infrastructure damage to target
low
high
Damage to target
Target Politico-diplomatic cap
low
high
Target Military cap
low
high
Target Socio-economic cap
low
high
Target Information Infrastructure cap
low
high
Relevant defense capabilities
Perecived danger of conventional war
high
low
Strictness of war laws
low
high
Intensity of countermeasures
none
Anti_political_subversion
Anti_proxy_sanctum
Anti_intervenation
1

Figure 3: HC model implemented using DBN.

Conditional probability tables (CPT)s that define *intensity of countermeasures* should be based on a defense strategy against HT. For instance, if attacker uses political subversion then its target may want to counter this subversion and, probably even more importantly, take actions to prevent escalation of *intensity of hybrid attacks* into proxy sanctum level by employing appropriate, anti-proxy sanctum, *relevant defense capabilities* that will in turn *lower attacker hybrid warfare capabilities*. If attacker or defender considers to escalate beyond HC defined by Art. 2(4) of the UN Charter (UN 1945) they should *perceive danger of conventional war*. Given a sufficient evidence of ‘bending’ or violating UN laws both attacker and defender risk, at least in principle, punishments by international community. Unfortunately, current war laws are not very strict and precise, inducing minimal negative feedback effects on *intensity of hybrid attacks* and *intensity of countermeasures*. The non-intervention principle enshrined in Art. 2(7) of the UN Charter leaves a large window of using HW as lawful, which encourages development of even more sophisticated HW. This, in a long-run, is a risky proposition.

Figure 3 shows two types of arcs between nodes: normal BN arcs and 1st order DBN transitions. The 1st order transitions include transitions from *intensity of countermeasures* to *damage to attacker's* PDMSEII variables, transitions from *relevant defense capabilities* to *damage to attacker's* PDMSEII variables, and from the *perceived danger of conventional war* to both *intensity of hybrid attacks* and *intensity of countermeasures.* This approach to implement delays of countermeasures was used for this demonstration, but more complex schema should likely be devised. For instance, higher order transition arcs, e.g., 2, 3, 4,… would allow to represent effects spanning multiple phases. All CPTs are assumed by the authors based on the estimations of the attacker and target. The model can be used in many ways, where selected nodes can be provided with additional input evidences based on new information or potential scenarios that decision-maker would want to infer about. The model demonstration below is only an example.

3.3 Model Demonstration

This section demonstrates an example of using the model based on the case study of HC presented by Rácz (2015). Table 1 shows probabilities of virtual evidences (VE) set in PDMSEII *damage to target* nodes for P(high) along the nine phases of this HC. The values of the virtual evidences were estimated by the authors based on (Rácz 2015) considering how the situation escalated during each phase.

Table 1: Input evidences for damage to target nodes.

Phase	Phase name and description (Rácz 2015)	Virtual evidence P(high)			
		PD	M	SE	II
1	**Strategic preparation** – established networks of loyal media and NGOs, established diplomatic and media positions, explored vulnerabilities in administration and economy	0.1	0.05	0.1	0.1
2	**Political preparation** - influenced dissatisfaction with the central authorities using media, information, bribed politicians, separatist, fueled ethnic, social, and religious tensions	0.2	0.05	0.2	0.2
3	**Operational preparation** – coordinated political pressure and disinformation, mobilized officials, officers, local criminal groups, mobilized armed forces of the attacker	0.4	0.1	0.4	0.4
4	**Exploding the tensions** – anti-government protests, sabotage attacks, first captured buildings, strong disinformation campaign by media, threat of conventional attack	0.6	0.4	0.6	0.6
5	**Ousting the central power from the targeted region** – continued capturing building and information infrastructure, blocked local media, disabled local armed forces, diplomatic pressure	0.7	0.5	0.6	0.8
6	**Establishing alternative political power** – phase 5 amplified plus declared alternative political center, media monopoly strengthened legitimacy of the new political bodies	0.8	0.6	0.6	0.8
7	**Political stabilization of the outcome** – organized referendum for independence with strong diplomatic and media support, 'new state' asked for help from the attacker	0.8	0.7	0.9	0.8
8	**Separation of the captured territory from the target country** – a) annexed captured territory (Crimea); b) military presence fighting central government, weaken political, economic and military	0.9	0.8	0.8	0.8
9	**Lasting limitation of the strategic freedom of movement of the attacked country** – loss of territory (economy, population, infrastructure), political destabilization, lack of full territorial control	0.95	0.95	0.95	0.95

Figure 4 demonstrates inferred probabilities of two factors at each phase: *intensity of hybrid attacks* and *attacker hostile objectives*. The *intensity of hybrid attacks* during phases one through three shows little symptoms of political subversion and minimal possibility of proxy sanctum or intervention, which aligns well with the statement: "…it is practically impossible to determine whether traditional Russian influence-gaining measures may be serving as preparation for a hybrid attack, before the offensive actually starts" (Rácz 2015, 59). Situation changes in phases four through six where "…open, organized, armed violence starts to occur…. unmarked units using high-tech Russian uniforms, weapons, vehicles and equipment appeared and started to set up barricades and checkpoints, blocking the gates of the Ukrainian military and police barracks" (Rácz 2015, 60).

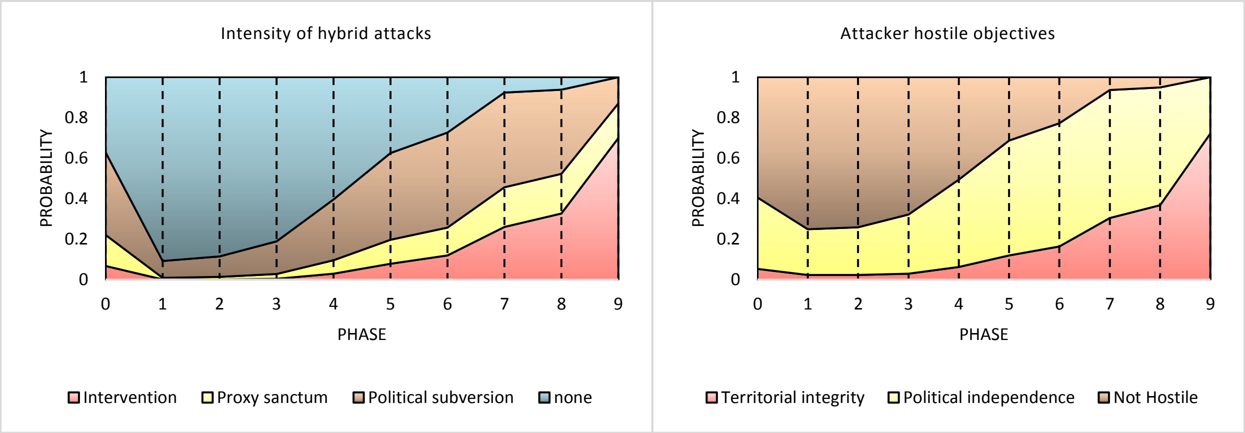

Figure 4: Inferred attacker hostile objectives and intensity of hybrid attacks.

During these phases *attacker hostile objectives* become apparent with the increased threats to target's political and territorial independence, which shifts towards threating territorial integrity during phases seven, eight, and nine, while *intensity of hybrid attacks* starts shifting towards intervention. Two outcomes, at the end of phase nine, can be observed in two cases of conflict in Ukraine: annexation of captured territory (Crimea) or transformation of the conflict into a limited conventional interstate war (Donbass) effecting in the denial of any control to the central government (Rácz 2015). Clearly, presented case only demonstrates a credible enactment of the past events and does not examine model's predictive power. A more systemic implementation of the factors and evidences should be considered in the future work in line with what is proposed in Section 4.

4 DISCUSSION

HTs require a comprehensive diagnosis. For instance, it would be pointless only to find and detain terrorists, if they re-appeared in even higher numbers, due to totally uncontrolled propaganda and incentives for joining them. It has already been years since businesses started using Big Data that allow to deliver personalized content and advertisements. The politicians already employ Big Data to help them in winning elections by identifying what voters want to hear. Now, it is time to think that Big Data, artificial intelligence (AI) and machine learning (ML) could be used for attacking societies (Helbing et al. 2017). Thus, there is a clear need to develop a sophisticated system countering those threats.

4.1 Threat Management and Coordination Unit

As HCs can occur simultaneously on different battlefields, e.g., military operations, diplomatic moves, information warfare, cyber warfare, economic moves, and terrorist attacks and on different scope, i.e., local, regional, national, and international, it is clear that the only institutions wielding enough power to respond, are the federal governments. However, the governments' deciding capabilities for PMESII-PT variables are limited to only most important cases.

As the number and variety of HTs is likely going to grow, at one point no person or even an office would be able to effectively coordinate response to all of them – especially if some threats are posed by automated means and quickly changing. Thus, there is a growing need to develop and implement an automated threat management system, which not only gathers and classifies reports on threats, but also suggests responses and provides an overview of how each case progresses.

Thiele (2015) advocated prevention against HTs, with early indicators needed to enable more agile responses. In order to countermeasure HTs a defense unit should be able to consider all PMESII-PT operational variables of the battlespace. Thus, from the pragmatic point of view there is a clear need for a hybrid defense coordination unit (HDCU), most likely established as an international entity.

Such unit would collect all reports on HTs and would have access to all classified information necessary to connect the dots. All the personnel within national institutions that normally collect information and/or address some of HTs, would be required to report threats that may have hybrid nature directly to the HDCU.

It would be helpful to establish a report form, with a checklist asking about levels of HTs based on established scales. An effective coordination of hybrid response would likely require collecting thousands of reports from all over a country or multiple countries. There would be a big difference between collecting and analyzing these reports individually, and using digital repository that automatically attributes reports to certain categories, or even particular cases. Categorizing and attributing threats to cases could involve a web-based solution to input and send reports, followed by a use of automatic or semi-automatic solution employing a combination of symbolic artificial intelligence (AI) and machine learning (ML) allowing to find patterns and fusion the data, making analysis more efficient and effective.

After initial gathering and analysis of information, a need for more information may be identified by an analyst or the AI/ML algorithms. The request would be forwarded to specific institutions via the same web-based solution, turning a formal inquiry into a duty to insert a response directly to the web-based forms, or contact the unit by different means, for instance within 24 hours after the unit requested the information. The formal framework should provide a step-by-step procedures, with appropriate templates allowing to alarm relevant institutions and suggest their response. The informational duty would cover providing information concerning action or explaining inaction contrary to the suggestions made by the HDCU. All archived, closed or frozen HT cases would still be useful in terms of connecting them with new reports and new acts of HW. Navigating through previous cases could be extremely useful for agents looking for answers about how similar issues were addressed in the past.

Quick recognition of HTs to forecast their effects is required to employ proportional, appropriate, and effective countermeasures. Quick and effective gathering of intelligence based on early indicators is critical but not sufficient. HT analysis can be compared to conducting criminal investigation, with the difference that to understand HT one must simulate a particular situation into the future to observe its effects. Because connecting dots in order to recognize objectives of HTs requires high cognitive skills, an M&S approach for supporting creative reasoning within coordination unit should be considered.

4.2 Needs for Hybrid Conflict Representation

Because one must think like a HT to understand its objectives, potential phases of conflict, actions, and decisions (Davis Jr 2015) military commanders, civilian leaders and staff need M&S tools to refine and test various ideas on how to deter and counter HTs. Modeling part of M&S as a cognitive activity can be especially useful. Representations of phenomena and processes related to cyber warfare that raise to the level of use of force such as regime change and coercive political interference, such as elections interference, would be helpful when developing policies and other measures which could prevent such attempts.

Non-conventional methods of warfare are lawful as long as they are not prohibited or do not infringe principles of international humanitarian law. Because the window of interpretation may be large the legality of warfare used may need to be analyzed. The main difference between traditional legal investigation and HW investigation would pertain to taking into account both past evidences and estimation of accumulated future effects as a result of HW influences. This would require making an estimated forecast to support case of potential illegality of the used warfare. Although using models to generate legal cases is still in its infancy (Fenton et al. 2013), arguably, it would be possible to represent not only past evidences leading to a verdict, but also forecasted state of a system (Balaban and Mielniczek 2017) to support HC arguments. For instance, a simulation model could be used to estimate effectiveness of proposed by the UN Security Council measures, e.g., embargos, demonstrations, and blockades. Similarly, a simulation model could be used to estimate adequate and effective collective self-defense measures against HT for armed force operations by air, sea, or land that should be employed to achieve desired effects.

More work on both theoretical and descriptive simulation models of HC is needed to allow for their higher predictive and prescriptive powers to estimate adequate and effective preventive and retaliatory countermeasures against HTs. Time required to develop required scenarios is prohibitive and new technological approaches are required to face this challenge. The M&S environment should allow for representation of complex HC at multiple levels of conflict: political, strategic, operational and tactical not limited to common principles of warfare and common hierarchy of combat models. A combination of multi-method (Balaban 2015b) and multi-resolution (Petty et al. 2012; Rabelo et al. 2015; Zeigler 2017) M&S is likely needed to achieve this vision.

ACKNOWLEDGMENTS

U.S. Department of Defense Distribution Statement: Approved for public release; distribution is unlimited. The views expressed in this document are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

REFERENCES

Balaban, M. A. 2015a. *The Support of the Acquisition Defense Governance Using Constructive M&S*. The 2015 ITEA Test Technology Review (TTR), at Huntsville, AL

Balaban, M. A. 2015b. *"Toward a Theory of Multi-Method Modeling and Simulation Approach"*. Ph.D. thesis, Modeling, Simulation & Visualization Engineering, ProQuest, Michigan.

Balaban, M. A., and P. Mielniczek. 2017. "Balancing National Security and Refugee Rights under Public International Law". In *Proceedings of the 2017 Winter Simulation Conference*, edited by W. K. V. Chan et al., 4105-4116. Piscataway, New Jersey: IEEE.

Cayirci, E., A. Bruzzone, F. Longo, and H. Gunneriusson. 2016. "A Model to Describe Hybrid Conflict Environments". In *Proceedings of the 13th International Multidisiplinary Modeling & Simulation Multiconference (I3M 2016)*, September 26-28, 2016., Larnaca, Cyprus.

Cirimpei, S. 2016. "Moldova Versus Russian Hybrid Threat: A Question of National Will". Strategic Studies, US Army Command and General Staff College, Fort Leavenworth.

DA. 2010. *Hybrid Threat*. edited by U. S. Army, *Training Circular 7-100*. Washigton, DC: AKO.

Davis Jr, J. R. 2015. Continued Evolution of Hybrid Threats. *The Three Sword Magazine*, 19-25 (28).

Fenton, N., M. Neil, and D. A. Lagnado. 2013. "A General Structure for Legal Arguments About Evidence Using Bayesian Networks". *Cognitive science* 37 (1):61-102.

Ground, L., A. Kott, and R. Budd. 2015. "Coalition-Based Planning of Military Operations: Adversarial Reasoning Algorithms in an Integrated Decision Aid". https://arxiv.org/ftp/arxiv/papers/1601/1601.06069.pdf, accessed February 15th, 2018.

Harder, B., C. Blais, and I. Balogh. 2017. "Conceptual Framework for an Automated Battle Planning System in Combat Simulations". In *Proceedings of the 2017 Winter Simulation Conference*, edited by W. K. V. Chan, et al., 4141-4152. Piscataway, New Jersey: IEEE.

Helbing, D., B. S. Frey, G. Gigerenzer, E. Hafen, M. Hagner, Y. Hofstetter, J. van den Hoven, R. V. Zicari, and A. Zwitter. 2017. "Will Democracy Survive Big Data and Artificial Intelligence".

Scientific American. https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/, accessed February 10th, 2018.

Hulst, J. 2006. *"Modeling Physiological Processes with Dynamic Bayesian Networks"*. Faculty of Electrical Engineering, Mathematics, and Computer Science, University of Pittsburgh.

Jacobs, A., and G. Lasconjarias. 2015. *Nato's Hybrid Flanks: Handling Unconventional Warfare in the South and the East*: NATO Defense College, Research Division.

Karber, P. 2015. The Russian Military Forum: Russia's Hybrid War Campaign: Implications for Ukraine and Beyond'. Center for Strategic and International Studies.

Karski, K., and P. Mielniczek. 2018. The Notion of Hybrid Warfare in International Law. *NATO Legal Gazette* (39).

Kott, A., and P. S. Corpac. 2007. Compoex Technology to Assist Leaders in Planning and Executing Campaigns in Complex Operational Environments. 12th International Command and Control Research and Technology Symposium, at Fairfax, VA.

Kott, A., and M. Ownby. 2015. "Toward a Research Agenda in Adversarial Reasoning: Computational Approaches to Anticipating the Opponent's Intent and Actions". *arXiv preprint arXiv:1512.07943*.

Lieberman, S. 2012. "Extensible Software for Whole of Society Modeling: Framework and Preliminary Results". *Simulation* 88 (5):557-564.

Lowe, D., and T. Pitinanondha. 2015. Conceptualisation of Hybrid Warfare. NATO 9th Operations Research and Analysis Conference, Ottobrunn, Germany.

Newson, R. A. 2014. Why the Us Needs a Strategy to Counter 'Hybrid Warfare'. In *Defense One*,

Pawlak, P. 2015. "Understanding Hybrid Threats". *European Parliamentary Research Service, June* 201.

Petty, M. D., R. W. Franceschini, and J. Panagos. 2012. "Multi‐Resolution Combat Modeling". *Engineering Principles of Combat Modeling and Distributed Simulation*:607-640.

Pioch, N. J., J. Melhuish, A. Seidel, E. Santos, D. Li, and M. Gorniak. 2009. Adversarial Intent Modeling Using Embedded Simulation and Temporal Bayesian Knowledge Bases. Modeling and Simulation for Military Operations IV.

Rabelo, L., K. Kim, T. W. Park, J. Pastrana, M. Marin, G. Lee, K. Nagadi, B. Ibrahim, and E. Gutierrez. 2015. "Multi Resolution Modeling". In *Proceedings of the 2015 Winter Simulation Conference*, edited by L. Yilmaz et al., 2523-2534. Piscataway, New Jersey: IEEE.

Rácz, A. 2015. *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist*: Finnish Institute of International Affairs.

Sari, A. 2016. "Legal Aspects of Hybrid Warfare". https://www.lawfareblog.com/legal-aspects-hybrid-warfare, accessed February 19th, 2018.

Sokolowski, J. A., and C. M. Banks. 2007. "From Empirical Data to Mathematical Model: Using Population Dynamics to Characterize Insurgencies". *Simulation series.* 39:1120-1127.

Sokolowski, J. A., and C. M. Banks. 2009. *Modeling and Simulation for Analyzing Global Events*. Hoboken, NJ: Wiley.

Thiele, R. D. 2015. "The New Colour of War–Hybrid Warfare and Partnerships". *World Politics of Security. Rio de Janeiro: Konrad Adenauer Foundation*:47-59.

UN. 1945. Chapter I of Charter of the United Nations.

Vaczi, N. 2016. "Hybrid Warfare: How to Shape Special Operations Forces". General Studies, US Army Command and General Staff College, Fort Leavenworth.

Zeigler, B. P. 2017. "Constructing and Evaluating Multi-Resolution Model Pairs: An Attrition Modeling Example". *The Journal of Defense Modeling and Simulation* 14 (4):427-437.

AUTHOR BIOGRAPHIES

MARIUSZ BALABAN received a Ph.D. in Modelling and Simulation (M&S) from Old Dominion University. His email address is marbalamarbala@gmail.com.

PAWEŁ MIELNICZEK received a Ph.D. in Law, specialty: public international law, from University of Warsaw. His email address is pawelmielniczek@outlook.com.