Assuring Allies by Effectively Countering Hybrid Threats – Challenges and Opportunities[1]

Dr. Vlasta Zekulic
173 Avenue du Diamant
1030 Brussels
BELGIUM

vzekulic@gmail.com

ABSTRACT

Hybrid threats are not new. NATO has been monitoring and responding to this concept of warfare since 2009. However, the rapid enhancement of information technologies, alongside our increased dependency on them, can be exploited by hybrid actors to destabilize unity and cohesion of the Alliance. A hybrid strategy is typically applied in an agile manner across all physical, social and psychological domains, blurring lines between war and peace, challenging our concepts of a 'battlefield', and using our values against us as weapons. Because of this, countering hybrid threats is a challenging and long-term endeavour. It consists of rigorous preparedness, tailored deterrence and credible defence. This paper assesses NATO's efforts in countering hybrid threats by highlighting challenges faced in timely recognition, positive attribution, and proactive response to hostile acts. Additionally, it supports a more active use of non-military tools, and proposes an application of effects-based approach in developing response options at the strategic level of the Alliance.

1.0 INTRODUCTION

The growth of hybrid threats over the last five years has significantly muddied the scope of what threats NATO should safeguard against and what constitutes as appropriate and timely response. There is currently no agreed definition of the term hybrid threat, partly because it is often used as a synonym for asymmetric and irregular warfare, and in part because it represents an intellectual challenge to our traditional understanding of war. Hybrid threats are multi-domain, escalating along both horizontal and vertical axes, and to varying degrees, they increase ambiguity and the cognitive elements of war. Moreover, hybrid actors have expanded the 'battlefield' from conquering territories to changing and altering perceptions, attitudes, and behaviours; gameplay has become the adversaries' leadership and population decision-making calculus.

This is the reason why deterring and defending against hybrid actors continues to occupy the minds of policymakers across the Alliance. Attacks on critical infrastructure, the spreading of disinformation, economic coercion, interference in domestic politics, whilst boosting military capabilities, are all examples of "below the threshold" activities perpetrated by Russia in recent years. Similarly in the South East and Central Asia, China skilfully applies hybrid and non-traditional approaches and uses them to turn a weak hand into a strong one.

Today's policymakers should be reassured to know that their Cold War predecessors grappled with strikingly similar challenges. The terminology and tools used may have changed since the days of the Soviet Union, but little else has. Similar to hybrid warfare, Cold War 'active measures' were based mainly on subversion, disinformation and influence operations, with occasional ventures into severe acts of violence such as terrorism, assassinations, and also recourse to military intervention when it was necessary.

[1] This paper does not represent the official position or policy of member governments, or of NATO.

Though these challenges may not be new and are particularly difficult to cope with, NATO still has a job to do. The Alliance's task is to deter conflict and, if necessary, defend its member states by all available political and military means. This paper will focus on how to deter hybrid actors by: 1) identifying the characteristics of hybrid threats that make it difficult to understand and identify; 2) describing the distinctive political and military aspects of NATO's deterrence posture aimed against hybrid actors; and 3) proposing tools and mechanisms that could be applied to increase the efficiency of existing measures.

2.0 IDENTIFYING CHARACTERISTICS OF HYBRID WARFARE THAT ARE DIFFICULT TO IDENTIFY AND UNDERSTAND

The modern environment is particularly conducive to disruptive hybrid measures. Rising nationalism and internal fragmentation can lead to political instability, where ageing populations with associated health and social issues increasingly depend on more volatile younger generations. Old values and alliances are challenged and dismissed. Unprecedented urbanization, economic and social inequality, poverty, religious and military tensions, paired with climate change, have a significant impact on food production, water availability, and population displacement.[2]

A skilful hybrid actor can manipulate, use and exploit all these factors to trigger the most marketable feeling in the world – fear.[3] The 2017 Munich Security Report focused on how the politics of fear lead to the rise of populism and anti-globalist challenge in the West. The report states "populists are experts in politics of agitation, forming an "axis of fear" across the West that exploits insecurities and grievances of the electorate, often by twisting the facts or even by spreading outright lies that speak to the preconceptions of their supporters." [4] This is to say that hybrid methods are not applied solely by Russia and China, but also by a myriad of non-state actors in our own nations, using methods from the hybrid toolbox to achieve their political goals.

It is difficult to provide a generic list of instruments for use in hybrid warfare since in itself, hybrid warfare is highly contextual. On the one hand, the Diplomatic, Information, Military, Economy, Finance, Intelligence, Legal (DIMEFIL) elements are well known, but the hybrid actor can simultaneously apply pressure throughout multiple domains and on multiple levels, tailoring them against individual vulnerabilities and weaknesses of the target, while simultaneously conveying image of own strengths. This challenge is not theoretical or hypothetical; some Allies are exposed to such actions daily.

In direct opposition to Mansoor's claim that "although war changes its characteristics in various circumstances (…) war is still war, and it has not and will not change," [5] hybrid actors operate outside of Western perception of war as a violent clash of kinetic forces. They deliberately blur the distinction between war and peace, the beginning and end of hostilities, making it a permanent state of play – a new normal. A lot has already been published on "Garasimov's doctrine"[6] and most visible hybrid tools, such as little green men, economic blackmail, and energy coercion. However, there is a need to highlight those characteristics of hybrid warfare that are particularly difficult for a traditional political and military alliance of 29 states to manage. Particularly challenging to fully comprehend and cope with are changes made in the perception of a battlefield, legitimacy of weaponry and an ability to penetrate adversaries' ambiguity.

[2] Global Strategic Trends - The Future Starts Today; UK Ministry of Defence, 2018

[3] In the words of the U.S. president Donald Trump "Real power is fear." Woodward, B.: Fear – Trump in the White House. Simon & Schuster, New York, 2018

[4] Munich Security Report 2017: Post truth, post-west, post-order?

[5] Ed. Murry, W., Mansoor, P.; Hybrid Warfare – fighting complex opponents from the Ancient world to the present. Cambridge University Press, 2012

[6] On 26 Feb 2013, chief of the Russian General Staff, Valery Garasimov published "The Value of Science in in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", in Military Industrial Courier. It is widely believed to describe the new form of warfare, where in six phases a functioning country may be brought to the verge of collapse. Article in English is available on https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

2.1 Battlefield challenge

In the wake of the increasing development and use of information technology, the traditional idea of the battlespace is being stretched to its limits. Hybrid warfare breaks down the distinction between what is and what is not part of the battlefield by using all available means across the DIMEFIL spectrum making traditional concepts about breath, depth and height of the operational space obsolete.

Hybrid warfare aims to effect a change both in the behavioural and physical space. Already in 2016 Reichborn-Kjennerud and Cullen noted that the traditional geographies of warfare, such as the land, sea, air, space and cyber have increasingly become expanded by what were previously considered social spaces, which include the political, economic, cultural and societal.[7] Most worryingly, psychological spaces, such as consciousness, perceptions and strategic calculus, are becoming increasingly important fields of war. On these battlefields, population and political decision-makers, rather than the military, are the primary targets of operation.

By shaping perceptions, adversaries seek to effect the will of populations and manipulate the strategic choices that they make. This was also recognised by the NATO Heads of State and Government in July 2018 Brussels Summit when they concluded that “hybrid tactics increasingly target political institutions, public opinion and the security of Alliance citizens.”[8] Although the cognitive elements of war are not new, tools available nowadays, such as those applied by Cambridge Analytica during the 2016, show an increasing ability to influence broad audiences through discrete and subtle means. In essence, the company merged military methods of psychological warfare with aggregated data to help win elections. By legally and illegally[9] collecting all the information available on every single aspect of a voters’ information environment, Cambridge Analytica was able to craft individual messages targeted to press the right emotional trigger of each voter.[10] These sobering revelations makes us question if those who own big data, in essence, own the future.

This example leads us to another battlefield of hybrid warfare – cyber-fields of data. There is an increasing number of data mining companies around the world - from Palantir delivering contracts to the U.S. National Security Agency and Northrop Grumman,[11] to now infamous AggregateIQ.[12] Big Data is constantly silently amassed, harvested and stored. Consumer datasets ranging from magazine subscriptions, store preferences, financial considerations to airline travel, can be legally purchased. Therefore, by removing data management from the governance of states or international organisations, technology giants such as Google and Facebook, as well as myriad of world's billionaires, have unrestricted playing fields to grow their power and dominance. Unsurprisingly, in December 2016, the head of MI6 said that “the connectivity that is the heart of globalisation can be exploited by actors with hostile intent to further their aims […] The risks at stake are profound and represent a fundamental threat to our sovereignty.” [13]

[7] Reichborn, E., Cullen P.: What is hybrid warfare? Norwegian Institute of International Affairs, Oslo, 01/2016

[8] https://www.nato.int/cps/en/natohq/official_texts_156620.htm

[9] The Guardian, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, 17 March 2018, available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

[10] In the Online Marketing Rockstars Keynote | OMR17, Cambridge Analytica CEO Alexander Nix discusses big data, the methodologies and strategies used to identify people's behavior and how data analytics factors into political campaigns. Available at, https://www.youtube.com/watch?v=6bG5ps5KdDo&t=989s

[11] https://discovery.hgdata.com/product/palantir

[12] Aggregate IQ was a small web-analytics company based in Victoria, British Columbia. Following the Brexit election investigation, it showed that four pro-Brexit companies payed total of 4.8 million pounds - more money than with any other company in any other campaign in the entire referendum. It turned out that it brought data and micro-targeting (individualized political messaging) to Cambridge Analytica.

[13] Younger, A.: The great British Brexit robbery: how our democracy has been hijacked. The Guardian, published on 07 May 2017

2.2 Weaponry challenge

A war in the age of technological integration and globalisation is realigning the relationship between weapons and war. The decades-old dilemma, whether one should fight the fight that fits one's weapon and/or build the weapons to fit the fight,[14] show the clear demarcation line between traditional and future warfare.

Conventional weapons are upgrading and evolving rapidly. In 2019, the U.S. alone will spend more than $80 billion to create and develop new weapon systems, armour and related gear.[15] Modern arrays of weapons result from discoveries in science and are coming from defence contractors, university labs and small tech start-ups. New generations of armed robots, the growth of active camouflage technology developed to protect military vehicles from detection by near-infrared night vision devices, futuristic laser cannons, satellite 'melters' and plasma protection fields are already being produced.[16] All of these armament developments reflect the innovation, curiosity and commitment of the world's best engineers and scientists, but in essence, they are still variations of conventional weapon systems.[17]

Hybrid warfare is as much about the primacy of "influence operations," as it is about hard military power. While NATO nations continue investing in conventional arms and weaponry, steadily increasing their military budgets[18] and consolidating the Alliance's defence posture,[19] in the era of hybrid warfare, speed, mobility and lethality are not enough. Countering hybrid threats requires an understanding of weapons in a broader, more unconventional sense. It should include all means which transcend the military domain, but which can still be used to harm an adversary. Already back in 1999, Chinese military strategists concluded that "anything that can benefit mankind, can also harm it. This is to say that there is nothing in the world today that cannot become a weapon."[20]

Simplistically speaking, where there is a computer, there is a computer virus; with open markets comes monetary speculation and trade protectionism; freedom of faith can be exploited by religious extremism; and information liberalisation opens up an opportunity for information manipulation. Tools that an adversary can apply to fight in these domains have become increasingly sophisticated, particularly through managing and embracing technological development, harnessing artificial intelligence, and profiting from expanded and unregulated information space.

Two of these 'weapons" – information manipulation and corruption - are of particular importance to NATO because they may directly influence and effect the Alliance from within.

2.2.1. Information Manipulation

NATO's former Supreme Allied Commander Europe, General Philip Breedlove, described Russia's efforts as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[21] Similarly, a Chatham House study adds, that the "pollution of the information framework for decision-making is a key element of this long-established Soviet and Russian principle."[22] Although the aim of hybrid messaging does not change, an approach to its delivery does. In the early years of hybrid

[14] Liang, Q., Xiangsui, W.: Unrestricted Warfare. ERBM, Brattleboo, 1999. Pg 10

[15] https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2019/FY2019_Budget_Request.pdf

[16] https://www.businessinsider.nl/here-are-the-4-long-range-weapons-the-army-wants-for-future-war-2018-10/?international=true&r=US ; https://www.darpa.mil/our-research

[17] An exception to this is a new operating paradigm of placing information itself as a connective tissue in the cross-domain warfare. This concept where transforms individually networked platforms - in any domain - into a 'system of systems' enterprise. The so-called combat cloud makes information the focal point of combat, and not operational domains. By treating every platform both as a sensor, and as an effector, it significantly increases the capability of a combat cloud. Deptula, D.: Evolving Technologies and Warfare in the 21st century: Introducing the "Combat Cloud" Mitchell Institute policy paper, 2018

[18] NATO, Defence expenditure of NATO countries (2011 – 2018), Communiques PR/CP(2018)091

[19] Paulauskas, K.: The Alliance's evolving posture: Towards the theory of everything", published in NATO Review on 06 July 2018

[20] Liang, Q., Xiangsui, W.: Unrestricted Warfare. ERBM, Brattleboo, 1999. Pg 16

[21] Pomerantsev, P.: Russia and the Menance of Reality. The Atlantic, published on 09 September 2014

[22] Giles, K.: Russia's new tools for confronting the West: Continuity and innovation in Moscow's Exercise of Power. Russia and Eurasia Programme Research Paper, Chatham House, The Royal Institute of International Affairs, 2016

campaigns, the Kremlin predominantly used Soviet-era information warfare elements such as denying, falsifying or drowning out facts, changing quotes, narrative laundering, and using manipulated or false visuals. Although somewhat tailored to specific geographical audiences, the narrative was the same.

After absorbing the initial shock of a changed Russian posture, NATO, the EU and member states begun countering back, including in the information domain. During the 2014 Wales Summit, Allies welcomed establishment of the NATO's accredited Strategic Communications Centre of Excellence in Latvia, NATO HQ opened a website on "Setting the record straight"[23] debunking myths and false statements made by Russia with facts and figures, the EU stood up the Strategic Communications Task Force East, and Allies individually started actively countering negative and influencing messaging and building the resilience of its population to it. Following this, a change of approach was observed.

First, in specific regions such as Western Balkans, the Kremlin realised that pressure tools and "sticks" should be replaced by positive discourse and "carrots". For example, 'positive' rhetoric was applied in FYROM[24] during the parliamentary elections in 2017, as well as before the name-changing referendum in 2018. Russian and Chinese messaging primarily focused on the Macedonian right to self-determination,[25] that the citizen have a right to choose what they what, even if this means standing up to the West. They supported nationalistic Macedonian parties, exploited weariness over the growth of the Albanian minority and helped fuel negative national sentiment towards alleged NATO and EU 'blackmail' to change their name if they are to join the Euro-Atlantic institution. NATO was standing as a strong supporter to the progressive national government knowing that the only way forward is a change of name, but 64% of registered voters refused to cast their ballot, in protest to the name change conditionality for the membership in the Euro-Atlantic organizations, directly in line with a Russian messaging.[26]

Similarly, in Finland, Russia's official rhetoric offers positive messages of good neighbourly relations, unprecedented stable and reliable economic and uninterrupted energy ties. Nevertheless, the aims remain the same – to divide the nation and complicate decision making by causing conflict between key political and economic stakeholders.[27]

Secondly, following the hacking and releasing of correspondence by presidential candidate Hilary Clinton, and U.S. Democratic National Committee's,[28] on 01 September 2016 president Vladimir Putin said that "the identity of the culprit or culprits [for hacking] is not as important as the content of the leaks, and ultimately the hackers revealed important information for voters."[29] Hybrid actors inspire to remove discussion from illegality of the act to the 'benefits' the act itself brought, thus conducting a form of 'lawfare' and justifying their acts as serving a 'greater good'. This narrative resonated extremely well with the Republican base during the election year.[30]

[23] https://www.nato.int/cps/en/natohq/topics_111767.htm#Myths

[24] Turkey Recognizes the Republic of Macedonia with its constitutional name.

[25] https://www.alo.rs/vesti/region/putin-je-uzima-pod-svoje-pravi-od-nje-novu-republiku-srpsku/191010/vest

[26] http://mondo.rs/a1140167/Info/Svet/Rusija-o-imenu-Makedonije.html

[27] https://www.nato.int/docu/review/2017/Also-in-2017/lessons-from-finland-influence-russia-policty-security/EN/index.htm

[28] 12 Russian intelligence officers were indicted on 18 July 2018 for the hacking of the Democratic National Committee, the Democratic Congressional Campaign Committee and aides to Hillary Clinton's presidential campaign. The hacked files were published on a website called DC Leaks, and through the WikiLeaks. https://www.politico.com/story/2018/07/13/mueller-indicts-12-russians-for-hacking-into-dnc-718805

[29] Bloomberg, Putin Says DNC hack was a public service, Russia didn't do it. Published on 02 September 2016, available at https://www.bloomberg.com/news/articles/2016-09-02/putin-says-dnc-hack-was-a-public-good-but-russia-didn-t-do-it

[30] Breitbart and FOX news published number of articles and videos on the issue. Some of their main messages are summed up in "10 Ways the CIA's 'Russian Hacking' story is left wing 'fake news'", published on 12 Dec 2016, and "Biggest fake news story of the year is Russian hacking the 2016 election", published on 31 Dec 2016.

2.2.2. Corruption

Corruption is another tool that is used by hybrid actors to exploit weak institutions and legal loopholes, such as inadequate transparency of ownership.[31] Although corruption can be seen as a private activity degrading state institutions, impoverishing populations, and diminishing the quality of governance, it can be effectively used to entrap Allies who can be either rewarded or blackmailed through corruption. According to the Transparency international, nine Allied nations are ranked between 50 and 100 on the corruption perceptions index for 2017,[32] potentially creating a vulnerability hybrid actors can exploit. Therefore NATO's policy on Building Integrity clearly states that "NATO works to support Allies and partner countries to promote good governance and implement the principles of integrity, transparency and accountability."[33]

In short, through partnering or partially buying out large companies (especially in the oil and gas sector) that make significant donations to political parties, or by supporting and funnelling rewards to individuals with significant political or economic influence, "Russia seeks to gain influence over critical state institutions, bodies, and the economy and uses this influence to shape national policies and decisions. Corruption is the lubricant on which this system operates, concentrating on the exploitation of state resources to further Russia's networks of influence."[34]

2.3 Ambiguity challenge

The effectiveness of the Kremlin's hybrid warfare operations can be attributed in part to the strength of its institutional memory and its ability to draw upon Cold War traditions and practices. In parallel to the military threat posed by the Warsaw Pact, espionage and sabotage activities as well as other attempts to interfere in domestic matters with the assistance of psychological techniques were used to attempt to gain an advantage over the West. Disinformation, forgery, bribery and implanting faux agents were some of the tools used to reduce confidence in NATO. The language used to describe Soviet activities in Cold War-era NATO documents is remarkably similar to today's descriptions of hybrid warfare:

> *"(the USSR) makes use of carefully harmonised political, economic, financial, ideological and military actions…the enemy attacks incessantly in all fields which are of vital importance to the peoples and at all weak points offered by the free world…The enemy aim is to paralyses the psychological defence readiness of the NATO nations….to undermine the confidence of the NATO countries and peoples and to dissolve NATO from within…Modern mass communication such as radio, television, the cinema, the press and pamphlet are being used for this purpose."*[35]

This clearly describes what the key Soviet aims were: to paralyse the readiness, undermine confidence of NATO states and populations and to dissolve NATO from within. These strategic objectives were well known although somewhat overshadowed by an imminent threat of a conventional and/or nuclear attack.

Since the Cold War, the relevance of seizing and holding territory decreased. By engaging, provoking and probing in multiple domains and geographical areas, and aware of the lack of coherent multinational intelligence sharing, hybrid actors are complicating the connecting of adverse events, as well as deliberately disguising tactical level goals to mask the pursuit of the strategic level agenda. Paulauskas notes that "Today, NATO is facing a non-discretionary environment, in which its potential adversaries choose the time and place for their 'strategic surprises' without giving Allies much notice."[36] A direct consequence of this

[31] The Fifth Column: Understanding the relationship between corruption and conflict. Transparency International UK, July 2017

[32] More detailed report on the state of corruption in Europe is available at https://www.transparency.org/news/feature/europe_and_central_asia_more_civil_engagement

[33] https://www.nato.int/cps/ra/natohq/topics_68368.htm

[34] Center for Strategic and International Studies, 2016, pg. 220

[35] C-M(60)22; 1960 Federal Republic of Germany (FRG) working paper

[36] Paulauskas, K.: The Alliance's evolving posture: Towards the theory of everything", published in NATO Review on 06 July 2018

approach is increasing difficulty for experts and decision makers to say clearly who are they are fighting, where and to what end state.

This leads us to another central characteristic of hybrid warfare - the strategically innovative use of ambiguity. Mumford and McDonald define ambiguity as “hostile actions that are difficult for a state to identify, attribute or publicly define as coercive uses of force.”[37] It is used to complicate or undermine decision-making processes and, when possible, to paralyse the use of most dominant strengths and capabilities. From NATO’s perspective, hybrid actions are primarily designed to fall below the threshold of military action and to delegitimise the use of military force.

Ambiguity is especially prevalent when hybrid actors apply soft means of influence. According to Joseph Nye, “soft power is the ability to attract based on a state’s culture, political values and foreign policy, which must be perceived as legitimate and having moral authority.”[38] Ignoring Nye’s principle of ‘legitimacy and moral authority’, Russia’s soft power stems from building networks of compatriot policy, and by building on the Soviet legacy of a large Russian minority population (particularly in the Baltic States). These networks are quite broad and range from cooperation on economic issues, to energy, sports and cultural agendas/themes. On the surface they are quite benign and therefore easily spread without triggering a reaction from security and counter-intelligence agencies. However, their real influence can be extremely menacing. Recent accusations against the Russian biker gang, called the Night Wolves, or “Putin’s Angels” who managed to establish a military-like base in Slovakia, follow this pattern.[39]

The ambiguity of Chinese hybrid activities predominantly stems from the difficulty of differentiating acceptable economic growth from growing economic coercion. It is widely known that China continually expands its economic activities within EU countries through enhancing its commercial presence and by acquiring companies, technologies, and valuable real estate. In less regulated states, or where more direct penetration is required, the Chinese economic approach is complemented by so-called “three warfares’.[40] Developed in 2003 and under the command of China’s Central Military Commission, this doctrine implements a combination of legal, media and intimidation tools to achieve desired political goals. To date, the skilful utilisation of these hybrid tools has allowed China to advance its interests while avoiding any serious punitive actions or economic repercussion from the international community.

3.0 POLITICAL AND MILITARY ASPECTS OF NATO’S DETERRENCE AGAINST HYBRID THREATS

In 2015, Allies agreed on the Strategy on NATO’s role in countering hybrid warfare, and it remains the main chapeau document on the subject within the Alliance. It recognises that fighting hybrid actors requires both a proactive and agile approach in preparing to counter threats, in deterring a hybrid actor from initiating or escalating a hybrid campaign and in defending once a hybrid actor has been positively attributed.

Recognising that in a modern security environment, deterrence against hybrid, conventional and nuclear threats is essentially indivisible, measures taken to counter hybrid threats are fully integrated into NATO’s overall deterrence and defence posture. Moreover, as with any security challenge, the primary response to hybrid threats rests with the targeted nation. If it deems necessary, a nation can call upon the Alliance for assistance at any stage during a hybrid campaign. The latest tool developed by NATO in support of this effort is “Counter hybrid support teams”, a mechanism to provide tailored, targeted assistance to Allies, at their request, in preparing for and responding to hybrid activities.[41]

[37] Mumford, A., McDonald, J.: Ambiguous Warfare. Report produced for the DCDC, October 2014.

[38] Ny, S.J.: Soft Power: The means to success in World Politics. Public Affairs Books, New York, 2004

[39] Orenstein, M., Kreko, P.: How Putin’s favorite Biker Gang Infiltrated NATO. Foreign Affairs, 16 October 2018

[40] Lee, S.: China’s ‘Three Warfares’: Origins, Applications, and Organizations. Journal of Strategic Studies, 2014, pg 198-221

[41] https://www.nato.int/cps/en/natohq/topics_156338.htm

Since 2015, NATO's response to hybrid threats has focused on improving the Alliance's situational awareness through integrating civil and military intelligence functions, information sharing, cultivating effective decision making as well as enhancing the readiness to resist and respond to hybrid campaigns. Furthermore, an early recognition that NATO is only one stakeholder in countering hybrid warfare has stimulated active cooperation with the EU, particularly in the following four areas: situational awareness, strategic communication, crisis response and bolstering resilience.[42] Moreover, a creation of hybrid fusion cells within both organizations is a clear recognition that connecting apparently unconnected events, requires different vantage point from different areas of expertise.

Understanding the intricate nuances of hybrid threats and their inherent pressures against vulnerabilities and weaknesses, such as critical infrastructure and energy dependency, the concept of deterrence-by-denial gained prominence.[43] NATO describes a resilient nation as one that in times of crisis can simultaneously provide continuity of governance, services to its population and support to Allied military troops on its territory.[44] Therefore an investment into collaborative resilience (the protection and reduction of vulnerabilities and consequences of critical infrastructure failure, required both by State and by NATO) leads to increased deterrence. With this in mind, bolstering resilience, both in the civil and military domains, has become a significant strand of work across the Alliance.

Assessing the effectiveness of deterrence against conventional or hybrid actor is a challenging undertaking. While it is extremely difficult to trace a cause and effect chain from a specific action to a particular response through complex cognitive and societal domains, observing and reporting on military activities is an easier part of the challenge. Smith claims that "any stimulus and response approach must centre on the cognitive domain where people perceive, understand, and make sense of a situation and decide on the course of action that constitutes their behaviour."[45] Paulauskas supports this argument by highlighting that those who claim that the Baltic States could be overrun in 48 hours ignore "the actual history and resilience of the Baltic nations. It took the Red Army ten years after the end of Second World War to finally suppress the armed resistance in Estonia, Latvia and Lithuania."[46]

Because of this notion, although hard military power can play a significant role in the last stages of a hybrid campaign and in deterring and controlling escalation, hybrid actors may determine the strength of deterrence through the will of population and decision-makers to fight back, to reject information "pollution" and remain resilient against damaging undercurrents of a prolonged hybrid campaign. In support of their efforts, NATO may need to further enhance its non-military deterrence toolbox.

4.0 EFFECTS-BASED APPROACH IN COUNTERING HYBRID THREATS

In this complex and uncertain world, NATO is the strongest and most enduring military alliance, continually adapting and evolving to remain capable to conduct its core tasks. Unfortunately, so do our adversaries. From the Cold War, through the Balkans and Afghanistan NATO has become so successful at putting the right number of the right weapons on the right target at the right time that opponents are now driven to find ways to hide from it to survive. Hybrid warfare is one of their attempts to make NATO's greatest tool extraneous. By avoiding open armed conflict, hybrid actors arguably attempt to control escalation and retain the initiative.

[42] The First Joint Statement on the Implementation of the Joint Declaration Signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization (available at https://www.nato.int/cps/en/natohq/official_texts_138829.htm). The second one, expending this cooperation, was signed on 10 July 2018

[43] It quantifies deterrence by examining a change after a defender has invested in hardening infrastructure to deter attacks. Taquechel, E.F., Lewis T.G.: How to quantify deterrence and reduce critical infrastructure risk. Homeland security affairs, 2012

[44] Meyer-Minnemannm, L.: Resilience and alliance security - the Warsaw commitment to enhance resilience. In Forward Resilience - Protecting Society in an Interconnected World. Center for Transatlantic relations, 2016.

[45] Smith, E.: Effects-Based Operations. Security Challenges, Vol. 2, No. 1, Institute for Regional Security, 2006

[46] Paulauskas, K.: The Alliance's evolving posture: Towards the theory of everything", published in NATO Review on 06 July 2018

In many cases, NATO does not retaliate in the same domain in which it was attacked. For example, Allies would never consider unleashing a nerve agent in Russia in retaliation for the attack in Salisbury. Because of this, Alliance needs to develop the ability and willingness to respond horizontally – engaging in a different domain but with the same level of 'pain' inflicted. This thinking is particularly prominent when considering attacks in the cyber domain. Although NATO has recognized cyber as an operational domain, and has acknowledged sovereign right of its member states to conduct cyber offense, it has not authorized development of collective offensive cyber capabilities. Therefore, if NATO experiences a serious attack in the cyber domain, it could 'export' the response to certain Allies or should consider employing a flexible asymmetric reaction drawing on the full range of the tools at its disposal, rather than limiting itself to a cyber response.

Implementing this paradigm requires a change in thinking from 'what do we need to do?' to 'what effect do we want to achieve?' Smith defines such effect-based approach as "coordinated sets of *actions* directed at shaping the *behaviour* of friends, foes, and neutrals in peace, crisis, and war".[47] When applying this definition from NATO's perspective, 'actions' would encompass diplomatic/political, military and communications elements. The end state is change in a 'behaviour' that are measurable and scalable from the tactical to the strategic level throughout the DIMEFIL spectreum. The 'behaviour approach' would allow NATO to observe changes in adversaries' actions and reactions over time.

Exercising decisive influence over the decision calculations of adversaries requires an understanding of their unique and distinct identities, values, and decision making processes and how these factors manifest themselves in specific strategic contexts. Therefore, a deliberate, focused and systematic approach to countering hybrid strategy requires effects to be tailored to specific adverse actions, and applicable in a specific context.

To deliver such tailored effects NATO's staff require guidance condensed as deterrence objectives. Deterrence objectives are clear and concise statements about what political-military outcomes at the operational level NATO seeks to achieve with its capabilities, against whom, where and in what timeframe. The Alliance already actively manages its posture by tailored use of its military, diplomacy and strategic communications, but as is, this approach is somewhat reactive. Development of deterrence objectives would enable it to become more proactive.

The law of requisite variety says that "the greater the number of possible responses a system has, the greater its chances of survival."[48] If NATO is to deter and defend effectively against hybrid actors, it needs to get more comfortable using all of its tools (Figure 1). Therefore, building on the main elements from the U.S. military effects approach to operations,[49] the following principles should be observed by NATO civilian and military planners when developing political-military response options for the Allied nations to consider: 1) Actions the Alliance takes should create effects on anyone who can see them and not just on the targeted adversary; 2) Effects should be felt simultaneously on multiple levels and in multiple domains; 3) All actions and effects should be cumulative and interrelated, and 4) Effects should be both physical and cognitive in nature.

[47] Smith, E.: Effects-Based Operations. Security Challenges, Vol. 2, No. 1, Institute for Regional Security, 2006

[48] Ashby, W.R.: An introduction to Cybernetics. Chapman and Hall, London, 1957

[49] U.S Standing Joint Force HQ, Commander's Handbook for an Effects-Based Approach to Joint Operations, 24 Feb 2006

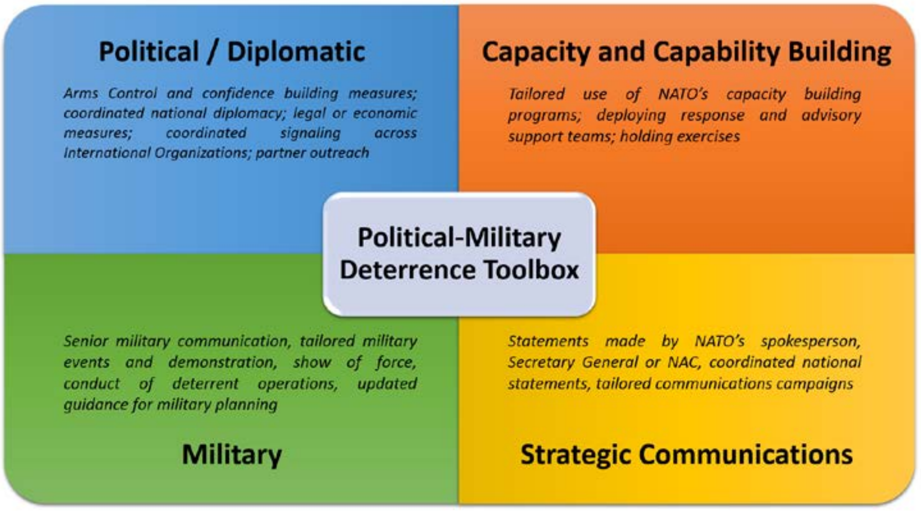
Political / Diplomatic
Arms Control and confidence building measures; coordinated national diplomacy; legal or economic measures; coordinated signaling across International Organizations; partner outreach
Capacity and Capability Building
Tailored use of NATO's capacity building programs; deploying response and advisory support teams; holding exercises
Political-Military Deterrence Toolbox
Senior military communication, tailored military events and demonstration, show of force, conduct of deterrent operations, updated guidance for military planning
Military
Statements made by NATO's spokesperson, Secretary General or NAC, coordinated national statements, tailored communications campaigns
Strategic Communications

Figure 1: Illustrative political military deterrence toolbox

Applying the effects-based approach is a challenging task. When applied in the military domain, success depends heavily on gifted leaders. Similarly, knowledge mobilization would pose the greatest challenge for the effective application of this approach at the strategic political level of Alliance. This does not merely imply a need for communication infrastructure, but an agile human interaction and social networking in response to the emerging security challenges. If applied well, the horizontal networking could expand the range of options, mobilize knowledge wherever it may reside, and provide agility in options decision makers may consider. In the words of David Deptula "It's an intellectual construct enabled by technological infrastructure."[50]

The NATO Enterprise employs some of the best theoreticians and practitioners from Allies countries in the field of security and defence, and with the NATO Command Structure adaptation and the NATO HQ functional review, harnessing the full potential of NATO's human capital to merge digital age innovation with strategic prudency has become not just theoretically possible, but entirely feasible.

5.0 CONCLUSION

Hybrid threats pose a *wicked* problem to the Alliance. State and non-state actors applying hybrid strategy exploit vulnerabilities across all levers of national power and society and complicate decision making by remaining ambiguous, un-attributable and by operating primarily below the threshold of armed conflict. They are not constrained by time and, depending on the level of sophistication, have almost an unlimited range of pressure options.

Against this threat stands the North Atlantic Treaty Organization and its Allies. NATO's fundamental and enduring purpose is to safeguard the freedom and security of its members through all political and military means. Its greatest strengths are unity of its members, the shared perception of security challenges and its powerful military tool. However, hybrid actors significantly complicate NATO's ability to 'see' a common threat picture and to respond with its conventional military capacity. Hybrid warfare is mainly about options – creating, constraining, or maximizing the choices. At the tactical, operational, or strategic level, the Alliance should, therefore, seek to maintain or increase its available options in the political and communications domain, and at the same time reduce those available to our adversaries.

[50] Deptula, D.: Combat cloud' is 'new face of long-range strike', available at http://armedforcesjournal.com/deptula-combat-cloud-is-new-face-of-long-range-strike

This article proposes the use of effects-based approach to enhance an Alliance horizontal response to hybrid threats. Using this approach is a complex endeavour and involves the use of a vast and changing array of interdependent variables that need to be considered and applied innovatively in the physical, social and psychological domains. It requires imagination and intellectual agility of its personnel to drive the use of technology in pursuing countering of any future threats - hybrid, asymmetric, unrestricted or conventional. To achieve this, NATO needs to continue integrating and networking the human and technological capabilities of a whole organization.