Information & Security: An International Journal

L. Monov & M. Karev, v.39:2, 2018, 113-126 https://doi.org/10.11610/isij.3909

HOW TO COUNTER HYBRID THREATS?

Lyubomir MONOV and Maksim KAREV

Abstract: This article introduces the network context and reveals some aspects of the hybrid threats, the decision-making process to counter hybrid threats and three possible options to handle that issue. In order to discover possible hybrid actions, we need a methodology that considers national interests along with major trends and threats as well as weaknesses and impacts. The implementation of such methodology will provide sufficient data and information to support decisions, accounting for all instruments of power in an integrated strategic approach.

Keywords: hybrid threat, network context, national interests, decision-making process, decision support.

Introduction

Nowadays, when we speak about national security, we may identify numerous issues which challenge our perceptions of stability and safety. Computer webs, human networks, alliances, economic interests, pipelines, financial markets, free flow of goods and massive movement of people are some of the characteristics that describe our way of life. As David Rothkopf argues, "connection breaks down barriers and brings us closer, but it also creates new vulnerabilities."[1] So, the challenge is how to find the line between peace and crisis and how to understand the political-security objectives of our adversaries. Besides, in this intricate environment, the threat has changed its character from one that is easy to define towards one that is more complex. The failure to recognize our vulnerabilities and the damaging power of a compound—or 'hybrid'—threat may lead to a profound catastrophe for us.

Hence, we need a comprehensive strategy that will secure our national interests and help identify our vulnerabilities. In a contribution in this respect, this article will briefly examine the network context and reveal some aspects of the hybrid threats. The article will deliberately not cover the complexity of the national decision-making process. However, it will suggest three options for dealing with the considerable amount of data. Finally, this article will conclude by underlining that any rational

method to resist a hybrid threat requires a sober assessment of our vulnerabilities and a strategic approach that encompasses all instruments of power.

The Net Context

Carious networks cover the entire world and it is logical to assume that a small change in one knot or line will exert influence over the whole system. In this interdependent environment it is difficult to isolate national interests and choices from the Net's context and to understand the roots and characteristics of possible threats. Many people argue that instability and conflict within the state could affect not only the country itself but also the international system and world order. A good example is the well-known situation in Syria and Iraq where the internal conflict triggered the rise of the Islamic State and a massive flow of refugees who actually put under pressure the European security and social systems. Joseph Nye underlines that it becomes challenging to differentiate international problems from domestic ones or local problems from regional or global ones.[2] For instance, a local problem that could inflame the world is the Iranian aggressive policy and determined efforts to dominate throughout the Middle East. On the other side of the world, China's assertive regional posture in South and East China Sea undermines the long-standing international principles for freedom of navigation and access to open sea lines. Indeed, this regional situation could easily become uncontrolled.

Of course, there is still a lot of truth in the fact that instability in one region may affect the entire security domain in a country which is geographically not close. The instability of the Middle East is the main reason for the massive numbers of immigrants, illegal movement of people, spread of radical ideas and terrorism that actually influenced Bulgaria and Europe. Despite the fact that our neighbouring counties relatively well control the situation with migrants, that could change rapidly. In other words, these results represent a compound threat to the national security that requires an adequate strategic approach.

In addition, the crisis between Russia and Ukraine in which Moscow used not only pure military threat but also diplomatic pressure, economic coercion, sanctions and propaganda demonstrated that power politics are back. Kremlin's actions of applying traditional means in modern ways influenced not only the Ukrainian population but challenged Europe and Bulgaria as well. In Sofia, it brought up numerous questions about our economic, historical and cultural connections with Russia. The debates in our Parliament and public networks showed the necessity to consider once again all threats to our security. Briefly, the success of Russia's integrated strategic approach displayed that in the time of networks no one can stay away from a disruptive influence. To summarise, interdependence between countries and extensively enmeshed

networks of humans illustrate that in a time of a crisis, more actors will be involved and more people will be affected.

National interests will be under constant pressure and the traditional statecraft will not be capable to deal with the network context (Figure 1). The warfare will enter in a zone between peace and conflict and threats will become hybrid and will incorporate more ways and means. Indeed, the ambiguity of hybrid threats guarantees a successful concealment of goals, intent, capabilities, means and ways. What we need then is to rethink the entire concept of power and clarify our approach to cope with such threats. As Joshua Ramo suggests, we have to modify and correct the core of politics and economics because "anything not built for a network age including our national security will crack apart under the pressures of networks."[3] In other words, our capacity to understand the entire complexity of strategic environment, nature and character of threats will be critical to shape our strategic approach.

Nature, Aspects and Appearance of Hybrid Threat

Most of existing understanding about national security is dominated by the vision that political and military capacity will guarantee successful deterrence and defence. Many people argue that in case of an armed attack we will have enough time to dis-

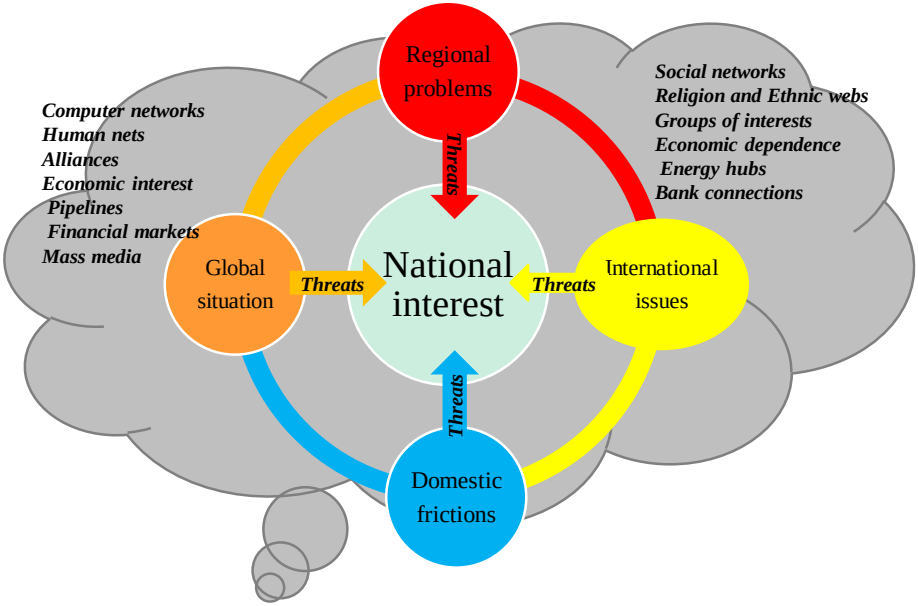

Figure 1: Interests, geography, and networks.

cover a hostile intent and organize our defence. Therefore, during peacetime we develop indicators, create plans and prepare our forces. Pure military vision requires clear lines between friends and foes, intent and goals, capabilities and readiness, doctrines and training (Figure 2). However, recently the Net context has demonstrated that the interrelationship between different actors, their multi-level dependence and enmeshed interests create enough opportunities to blur the strategic picture. To put it simply, an opportunity for one who wants to advance his strategic interest might be a threat for someone else.

During the interactions between all different elements of the network signs for hostile intent may be presented neither in military or security domains nor in political or economic areas. Moreover, because of the massive amount of information, which overwhelmingly floods our life, it is extremely difficult to distinguish what has sense and what does not have sense. Frankly speaking, the threat against the national interest evolves from a purely military domain to a hybrid one that is multi-layer and complex. Thus, in order to create opportunities and to advance our interests against modern and composite threats we have to understand their core and then to reinforce all traditional instruments of power with information, situational awareness and geo-economics.[4]

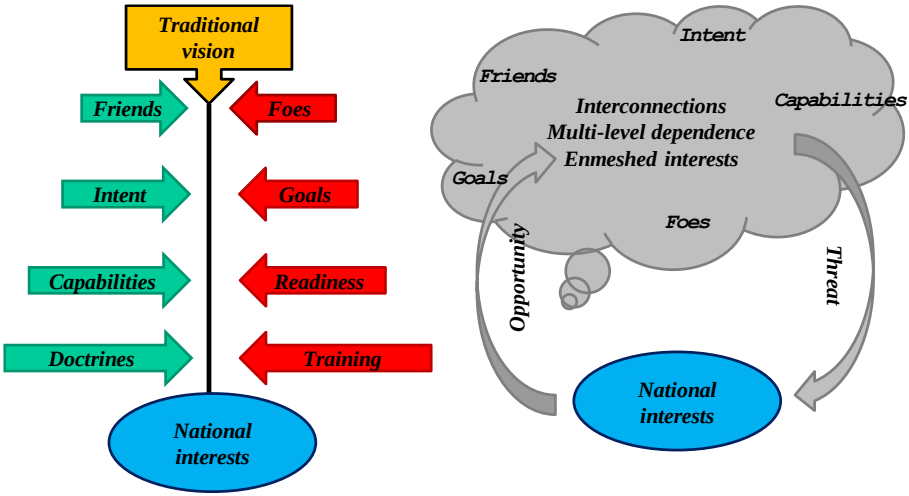

Figure 2: Some features of the traditional vision and the Net Context.

There are numerous definitions of a hybrid threat (Figure 3). In 2010, the US Department of Army described a hybrid threat as "adaptive, innovative, globally connected, networked, and embedded in the clutter of local populations."[5] The authors insisted that in a future conflict, the United States would meet an adversary who could operate conventionally and unconventionally by employing old and modern technologies, criminal tactics and traditional military capabilities. Moreover, in order to advance their goals and affect US political and military leadership, future enemies will use social infrastructure and modern technology. This would create diverse and dynamic environment that undermines national resilience and attacks the US homeland in a sophisticated manner.

After the Ukrainian crisis, NATO worked extensively to define and to describe the nature of a hybrid threat. The Alliance considers a hybrid threat as one of the most complex issues faced not only by member states but also the international community. Additionally, a hybrid threat possesses enough power to influence one or several of the member states, to disrupt their functioning and to undermine NATO's cohesion. Thus, allied countries agreed that hybrid threats are based on "a wide range of overt and covert military, paramilitary, and civilian measures [that are] employed in a highly integrated design."[6]

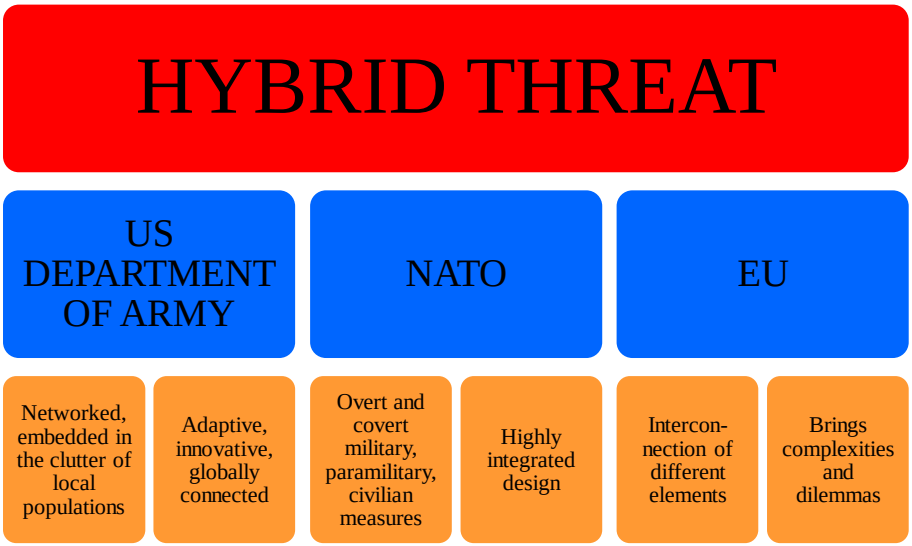

Figure 3: Characteristics of the Hybrid Threat.

Since 2014, EU has also invested considerable efforts in understanding and describing the hybrid threats. In numerous publications and "food for thought" papers, member states recognized that a hybrid threat might encompass military or non-military activities such as cyber-attacks on critical information systems, disruption of energy supplies or financial services. Hybrid threats exploit social vulnerabilities to undermine public trust in governmental institutions. In a document published in June 2015 EU outlines the hybrid threat as "a metaphor that brings complexities and dilemmas related to a changing global environment … and …. a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat."[7]

'Hybrid threat' is not a theory defined by clear assumptions and explicit schemes. Rather, as these definitions have described it as an approach that emerged gradually in the changing global environment. Hybrid threat's composite character exploits the interdependence of our world and uses our competing interests. A hybrid threat employs a proactive and comprehensive strategic approach that affects all domains of life. As a normal new reality, it emphasizes on the calculations of interests, power and vulnerabilities and stays below the level of war.

The capacity of a hybrid threat to bring complexity, uncertainty and fog represents its nature (Figure 4). Hybrid threats have neither physical nor legal, economic or informational borders. Predominantly, adversaries in a hybrid conflict will take their power from the network in which we live. They rely on globalization and modern communications that will enable them to reach their goals.

From a military point of view, a hybrid threat has more advantages than disadvantages. In fact, as advantages we might point out several: it has a composite character that includes a proactive approach; it targets critical vulnerabilities and has no borders; it provides flexibility and it is difficult to discover; it exploits deceptions and has a significant impact on enemy. As disadvantages, we may consider that more likely a hybrid threat is a unilateral action that has the potential to produce unintended consequences, including a high-end conflict and a massive international response.

Bottom line, the hybrid threat capacity to bring uncertainty and fog; its multi-layer and compound character represents a profound strategic challenge. As a result, it is almost impossible to prevent adversaries' actions in short term and to change the existing conditions. That is why hybrid threats can bring really destabilizing consequences to the country under attack. Therefore, we need a sound instrument that could help us to detect and categorize our weaknesses.

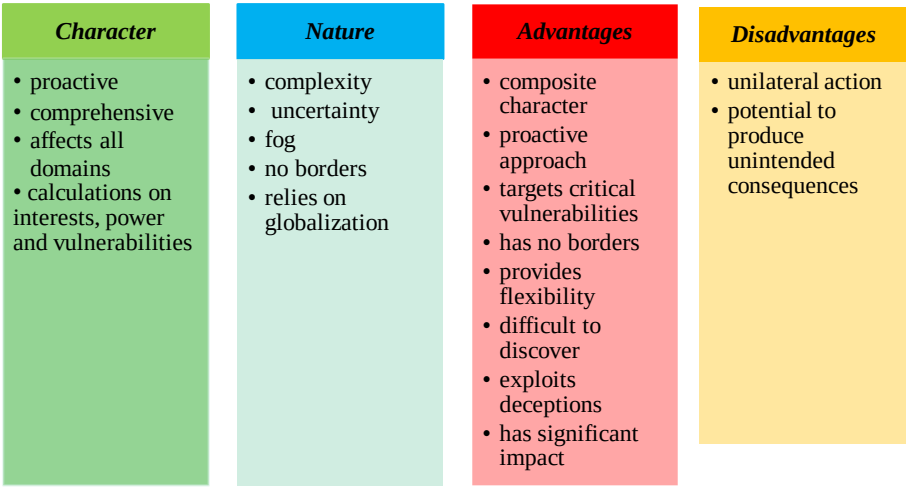

Figure 4: Character, Nature, Advantages and Disadvantages of Hybrid Threat.

Decision Making Process to Counter Hybrid Threats

Obviously, coming up with a specific strategy against hybrid threats is an intricate task that requires specific solutions. According to Richard Rumelt, a good strategy for dealing with complex problems has to be based on three components. The first one explains and defines the nature of a problem. In a diagnostic way such analysis would help us to simplify the extreme complexity of a hybrid threat and as minimum should answer the following questions – who is the enemy; what are his goals; why does he act; where are our week points; when did he start; does he have enough capacity and how long can he sustain his activities. The second component defines our intention and general concept how to manage all problems identified during the diagnostics. The third part represents a set of coherent actions aimed at specific issues and represents the active part of our strategy. These integrated and coordinated steps may encompass an inclusive package of actions from all domains – diplomacy, military, information and economic.[8]

In an attempt to strengthen member countries security, in April 2016 the European Union lunched a joint strategic framework to counter hybrid threats. This basic strategy considers the specifics of the strategic environment and the relationship between external and internal security. Furthermore, it outlines the overall idea that the right approach to counter and mitigate the impact of hybrid threats is to bring together all relevant actors, policies and instruments in a comprehensive manner. As a coherent set of actions, this framework describes four lines of efforts. The first aims to develop

and build a mechanism for exchange of information and raise the strategic awareness. This requires full understanding of the vulnerabilities and strategic environment. The second line addresses all identified weaknesses in critical sectors that have the potential to provide opportunities to the EU enemies. Therefore, in order to create resilience, EU has to take precautions that guarantee proper functioning of the financial system, public health, energy domain, and transportation sector and cyber space. The third line establishes effective procedures based on the EU agreement clauses of solidarity and mutual defence. These procedures promise a successful way to prevent, respond and recover from hybrid threats. The forth line designates the importance of cooperation between EU and NATO as well as between EU and other international organizations.[9] However, EU insisted that the main responsibility in a fight against a hybrid threat stays with the country itself. Hence, in order to strengthen its own national security and build resilience that would deter a possible attack, each member state has to analyse its conditions. In short, first step to a comprehensive strategy that safeguards state's national interests is a complete diagnosis of the net context.

This assessment has to encompass two different but connected and overlapped areas, which will determine all possible issues that we are facing (Figure 5). The stability and resilience of a country depends on its internal structure and the dynamics between different actors. In the centre of this evaluation is the demographic structure of a society with its current condition. The stability in one country depends on the demographic structure of the society. Therefore, the first part in the process is to explore the trends in demographics including migration patterns, gender issues, social system, health care and government ability to provide disease control.

The second area is the social order with the presence and influence of international non-governmental organizations, religion and its influence, human and social networks, trade unions, clubs, role of social media and how it influences government work and control over mass media. Since the government ability to decide and sustain its choices is a vital part of public life, we have to focus on the state power, which represents the third zone in this analysis. The relationship between different centres of political influence, the number of political parties and their connections with the private business provide additional difficulties for administrative decisions. The level and mechanisms of corruption, lobbyist groups, financial funds and international investors deliver some extra points for influence over the governmental choices.

The forth critical area is to examine the availability of resources, especially energy, national dependence on them, the major providers, needs for diversification, major environmental issues, quality and quantity of water and food.

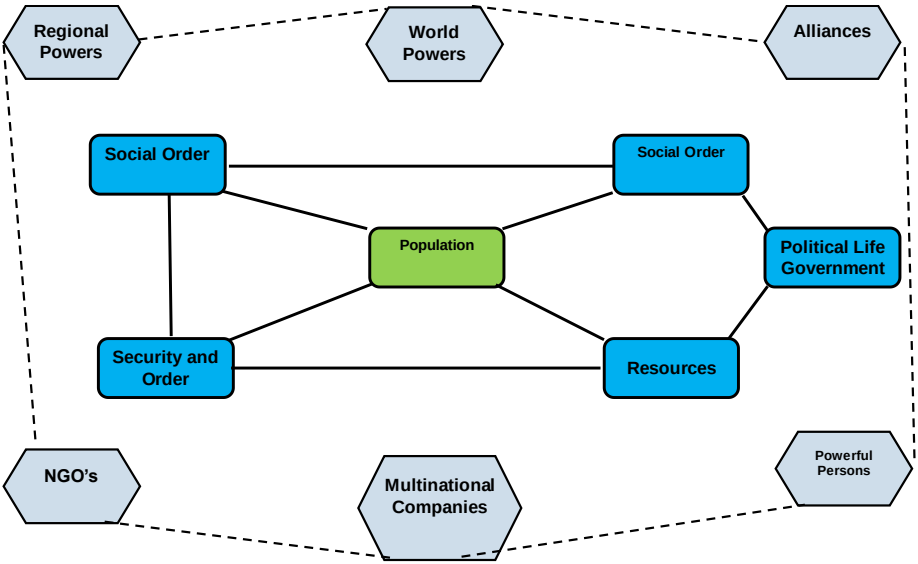

Figure 5: Areas of Assessment.

The fifth domain requires substantial examination over security and order. Main points in such analysis are the condition of military and police forces, their capabilities, experience, training, chain of command and constitutional responsibilities. Border control, criminal justice system, organized crime, domestic unrest and crime activities demonstrate the ultimate ability of government to deter possible enemy's activities and defend its territory from any threats.

The final step is to analyse the structure of economy. As a minimum, we should focus our assessment over wealth distribution, trade patterns, major investors, stability of bank system, the impact of grey economy, level of unemployment, availability of job opportunities and effectiveness of tax system.[10]

All our vulnerabilities are directly connected with the state's power and influence in the international system and world order. Hence, in order to recognize the full picture, we have to observe and analyse state's connections with regional, international powers, organizations and alliances. During this process, we have to understand how they interact in time of peace and conflict through extensive cooperation and fierce competition. Moreover, it is crucial to know what their specific interests are and what forces might change their behaviour. It is necessary to consider the power of non-state actors in our region and their influence.

Of course, each driver has many possible aspects and deep details. Each of them involves massive amount of data and knowledge. Moreover, from each of them we

may develop huge quantity of possible scenarios and each of them could have many potential solutions and outcomes. For these reasons we need to simplify the process and data (Figure 6). First of all, we need to define and prioritize the national interests. Then, based on the analysis we have to formulate all major trends that appear to have strategic significance and could be used in a hybrid situation. We have to compare each of the national interests with each of the major trends and define possible threats and vulnerabilities. A further step is to formulate their impact on the national interests. Additionally, we have to develop a general strategy for dealing with threats, which encompasses objectives, instruments of power, ways (courses of action). This concept should be evaluated in terms of cost and risks vs. benefits and probability of success. Finally, the dynamic of our life obliges periodical reassessment of major trends and findings.

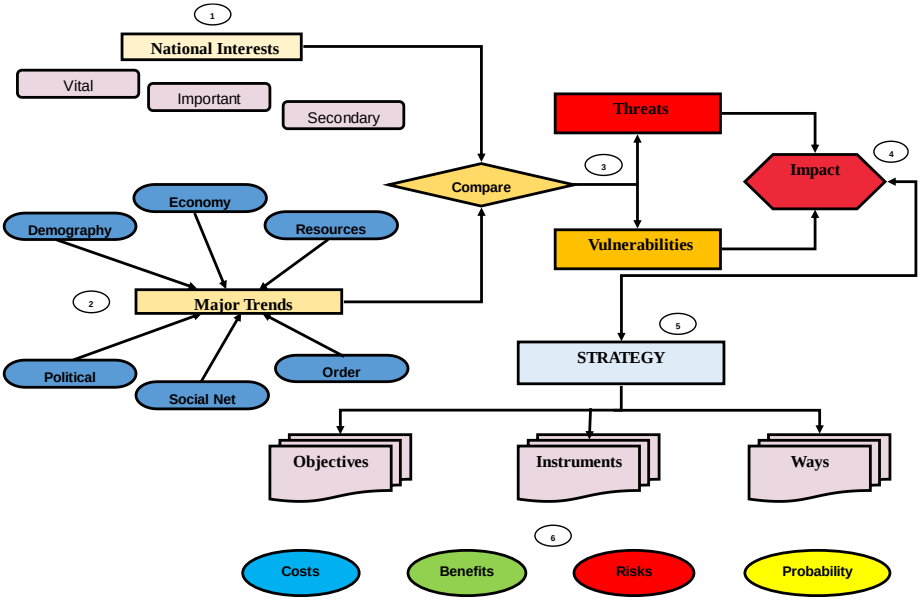

Figure 6: Process of Assessment.

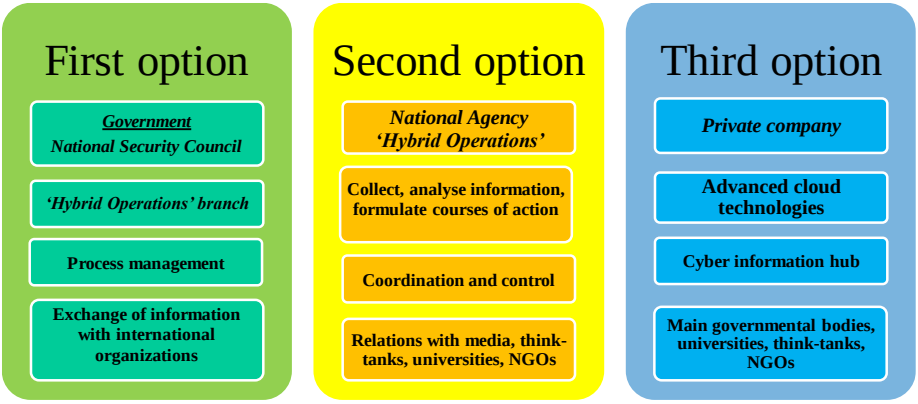

Figure 7: Options.

Despite the fact that this process looks simple, it is hard to believe that it is possible for one person or a team of several people to conduct such kind of an analysis. From a national perspective, there are at least three possible options to handle that issue (Figure 7).

Option one is to use the current National Security Council that works under the leadership of the Prime minister. Each of the participants in this virtual structure has sufficient staff who may conduct specific analysis in their area of responsibility (economy, diplomacy, environment, energy and resources, military and security, etc.) However, there is a strong chance that such work will represent a biased position of each administrative structure. The competition for benefits between different bodies inside the administration and its specific regulations and culture will influence the assessment. Therefore, a likelihood that something important is missing and something vital for national security is underestimated would be very high. A possible way to solve this problem is to create a small staff element, for example – a "Hybrid operations" branch, in the government. The main responsibility of this branch will be to look for discrepancies and conflict points between different analyses and to run the process. Additionally, it will exchange national information with other relevant international organizations.

Option two is to establish a national agency which will encompass experts in all above-mentioned domains. The agency should be independent from other departments of the government and has to act as a hub that collects and analyses information, formulates approaches, coordinates and controls their fulfilment. This agency has to establish connections with media, think-tanks, universities, NGOs, etc. Of course, this will increase the public expenses for administration and may bring

conflicts between different bodies of the government. There is a chance that different experts who sit at different structures will see and explain one problem in completely opposite perspectives. This increases the probability of confusing decisions and irrational approaches.

The third option is the use of a private company which will use modern cloud technologies. It is possible to create a cyber hub and all the information will be provided by governmental structures, universities, think-tanks and NGOs. The cloud will scope in one circle all problems identified during the analysis, will identify key uncertainties, gaps and develop indicators for hybrid scenarios. However, the problem is who will have the rights to regulate the work and who will bear the responsibility in the face of negative consequences.

The bottom line is that in the centre of an integrated strategic approach that encompasses all instruments of power sits a complete diagnosis of environment, international and domestic context that will bring us to the full knowledge of our vulnerabilities. The proposed drivers for assessment and methodology could help our leaders to make right political decisions.

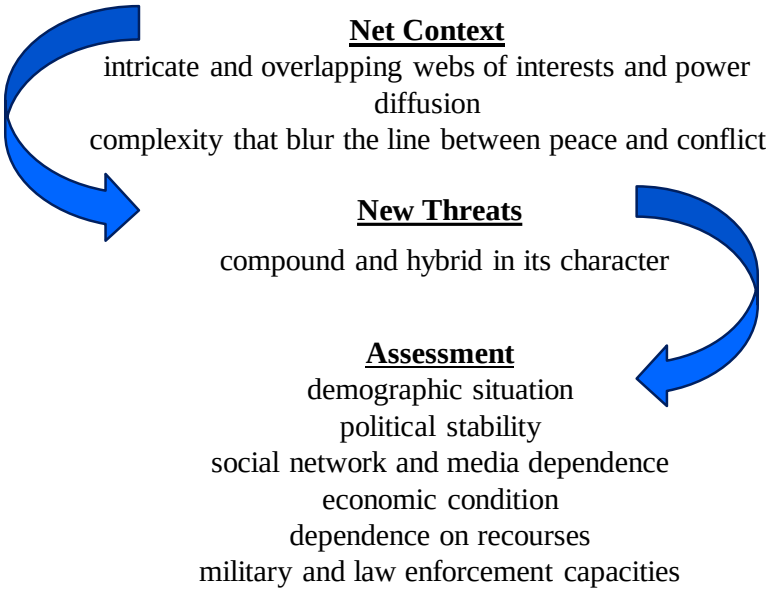

Figure 8: Context, Threats and Assessment.

Conclusion

Every day we spend time deeply engaged with different networks (Figure 8). We depend very much on their function and we make decisions considering the interdependence of our world. The contemporary era of Net context requires new understanding of threats that might overwhelmingly run at us from all hubs and lines. All new threats are compound and hybrid in character. Only sober assessment which identifies our vulnerabilities could help us to resist against a hybrid threat. As a minimum this assessment should consider the demographic situation, economic condition, dependence on recourses and military and law enforcement capacities. Moreover, in order to discover possible hybrid actions, we need a methodology that considers national interests with major trends and threats with weaknesses and impacts. This will provide a ground for an integrated strategic approach that encompasses all instruments of power.

Bibliography

[1] David Rothkopf, "The Paradox of Power in the Network Age," *Foreign Policy* (9 October 2015): 98-100, https://foreignpolicy.com/2015/10/09/the-network-paradox-islamic-state-nsa-warfare/ (accessed July 14, 2018).

[2] Joseph S. Nye and David A. Welch, *Understanding Global Conflict and Cooperation: An Introduction to Theory and History* (Boston, MA: Pearson, 2013).

[3] Joshua Cooper Ramo, *The Seventh Sense: Power, Fortune, and Survival in the Age of Networks* (New York: Little, Brown and Company, 2016).

[4] Robert D Blackwill and Jennifer M Harris, *War by Other Means* (Cambridge, MA:/London: The Belknap Press of Harvard University Press, 2016).

[5] Department of the Army, *Hybrid Threat* (Washington, DC: Department of the Army, 2010).

[6] Wales Summit Declaration, NATO e-Library, September 5, 2014, accessed May 28, 2018, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

[7] European Parliament, "Understanding Hybrid Threats," June 2015, accessed May 28, 2018, http://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf.

[8] Richard Rumelt, *Good Strategy, Bad Strategy: The Difference and Why It Matters* (New York: Crown Business, 2011).

[9] European Union External Action Service, "EU Strengthens Response to Hybrid Threats to Bolster Security," April 4, 2016, accessed February 5, 2018, http://eeas.europa.eu/top_stories/2016/060416_eu_strengthens_response_en.htm.

[10] US National War College, "The Global Context Core Course 6500 Syllabus, 2013-2014," http://nwc.ndu.edu/Academics/Curriculum-Overview/.

About the Authors

Col. **Lyubomir MONOV**, PhD, holds a masters' degree in National Security Strategy from the National Defense University of the United States (2014). He has served as Head of the "NATO, EU and Regional Initiatives" Department at the Defense Staff (2011-2013) and National Military Representative at the Allied Command Transformation, Norfolk, USA (2014-2016). Dr. Monov has a number of publications in the field of security and defence such as the "How to Counter Hybrid Threats" and "Technology and the Future of War."

Maksim KAREV is Colonel of the Reserve. For 16 years he was a lecturer at the National Military University in Veliko Turnovo, Bulgaria. Later, he headed the Operational Analysis Department of the Defence Staff of the Ministry of Defence of Bulgaria, and then served as National Commander of the 25th Bulgarian military contingent in Afghanistan (2013-2014). Col. Karev has a number of publications in the field of security and defence, such as "Risk Management System in the Military Organization" (2012) and "Architectural Approach for Organizational Modelling and Application in the Military Organization" (2012). Currently, he is Associate Professor in the Defence Advanced Research Institute of the G. S. Rakovski National Defence College in Sofia.

Address for correspondence: G. S. Rakovski National Defence College; Defence Advanced Research Institute, 82 "Evlogi and Hristo Georgievi" Blvd., Sofia 1504, Bulgaria.