NATIONAL SECURITY IN THE AGE OF THE HYBRID WAR

Dr. İlhami B. DEĞİRMENCİOĞLU

Introduction

During the course of the past 10 years, the security environment has become more complex due to the blurring of the lines of warfare. Therefore, the ‘gray zone’ between peace and war expanded and became a battlefield of non-conventional warfare such as counterinsurgency, terrorism, cyber-attacks, etc. (Mansoor, 2012: 1). The failed and fragile states in the Middle East, North Africa, and Central Asia, as well as non-recognized de facto states in the Caucasus played catalytic role in the expansion of the non-conventional warfare. Moreover, Great Powers inclined to use increasingly the non-conventional warfare in the proxy and delegated wars waged by them. In the recent years, the non-state actors used innovative and complicated tactics against legal authorities in many countries. The prevalence of the new complex threats transformed the classic war concept into a concept called ‘new wars.’ Due to the combined use of the conventional and non-conventional warfare, many scholars and politicians started to call the new model of war as ‘hybrid war.’

The Russian operations in Ukraine (the Crimean Peninsula and in the Donbass) targeted the social vulnerabilities of the Ukrainian society through the employment of the non-conventional warfare and high-technology conventional warfare (Rinelli and Duyvesteyn, 2018: 29).

---

1 Dr. İlhami B. DEĞİRMENCİOĞLU is a retired army colonel and scholar. He teaches courses on international security in various Universities. He completed his master’s degree at the Turkish Military Academy in 2004 and Doctoral studies on political science at the University of Vienna in 2018. Additionally, he studied in the German Joint Military Academy between 2007-2009. From 1992 to 2017, Dr. Değirmencioğlu served in the numerous units and HQs of the Turkish Armed Forces and performed many overseas assignments including OSCE between 2011-2014.

2 Disinformation, special units without insignia.
This operation and other proxy wars\(^3\) indicate that states must be prepared for the new war model which will be more challenging since the present state security systems designed to counter conventional threats will not be able to cope with the new threats (Mansoor, 2012: 14). The Ukrainian Conflict, a wake-up call, led some states to enter hybrid war into their security agenda and compelled them to develop a functioning hybrid war concept.

The lessons learned derived from the past wars and operations disclosed the fact that the use of cutting-edge military technologies does not guarantee the expected ‘End State’ but only helps to win the battles (Mansoor, 2012: 15, 16). Because, when encountered with a powerful enemy, the adversary develops and employ asymmetrical tactics and technics that paralyze regular armed forces which were trained for the conventional wars. The lack of adequate intelligence, concepts, and countertactics might even cause to the defeat of a robust conventional army by irregular forces backed by opponent states. Furthermore, hybrid war can be exercised by employing various means against a state to destabilize it. An unprepared state might confuse and cannot resist against hybrid threats.

Due to its peculiarities and increasing role in the national security, USA, EU, and NATO seek to develop capacities, strategies, and operational concepts as well as improve the training of the troops. Moreover, they strive to improve the resilience of the state system to resist hybrid threats. In this regard, this study attempts to identify the definition of the hybrid war, explain its tactics and characteristics as well as the efforts of some states to increase their readiness. Finally, it offers the necessary measures to resist against hybrid threats in the following sections.

What is Hybrid War?

Unfortunately, there is no consensus among the academics and practitioners concerning the definition of the hybrid war. It was first used in an academic document in 2002 in the USA researching future wars based on the case study of the Russian- Chechnya War. Thereafter, we notice that the use of the term is increasing in academia and in the security sector. However, scholars and experts refer to the different versions of its definition. It is better to study some definitions to gain more insights.

---

\(^3\) Soviets defeat in Afghanistan, US withdrawal from Somalia, the first Chechnya War, US campaign against Taliban in Afghanistan, invasion of Iraq in 2003, Israel’s invasion of Lebanon in 2006, and DAESH control of some part of Iraq and Syria.
Many documents focus on the use of conventional and non-conventional military and civilian means in a conflict. Some of them include the involvement of both state and nonstate actors as well as the symmetric and asymmetric use of warfare (Mansoor, 2012: 2). Other definitions underline ‘combined’ and ‘covert’ use of military and non-military means (sabotage, disrupting communications and energy supplies with the help of proxy insurgent groups) to influence target state in line with the interest of the aggressive state.4

Based on these key points in the definitions, I propose the following definition of the ‘hybrid war:’ Conduct of various operations in a broad spectrum by an antagonist state in the ‘gray zone’ through employing mainly non-conventional warfare in a covert and proxy fashion to deter or weaken targeted state or its components. The hybrid operations can target simultaneously entire state system and society to create ambiguity, paralyze its decision-making unit and weaken its coherence.

The Characteristics, Means, and Tactics of Hybrid War

The definition given above underlines the following key aspects of the hybrid war: combination, covertness, complexity, broadness, and versatility. In this sense, the hybrid wars are characterized by:

• The combined use of conventional and unconventional, military and non-military, hard and soft power elements, overt and covert actions in an asymmetric manner,
• Conducting in a no peace no war zone (gray zone) at all levels of war, from the tactical to the operational, to the strategic,
• Using proxy elements and innovative methods (i.e., malwares and drones),
• Making confronted state confused through exploiting the vulnerabilities of the state and its society,
• Paralyzing state system to hinder effective reaction and defense mobilization,
• Performing through non-contact clashes,
• Keeping the level of the attack under the ‘threshold’ of conventional war.

4 On the other hand, Russian official doctrine ‘non-linear war’ introduced by General Valery Gerasimov in 2013 connotes very much the ‘hybrid war’ logic.
The means used in a hybrid war range in a broad spectrum as illustrated in Fig. 1. In this regard, contrary to the frequent use of the term of hybrid war as a buzzword, not all terrorist attacks and other criminal incidents such as cybercrime, trafficking can be regarded as means of hybrid war. As it will be inferred from the definition, only systematic, concerted and orchestrated attacks targeted various components of a state can be considered the means of hybrid war.

At the strategic level, the aggressive states and the proxy elements can apply these means with various tactics depending on the political, economic and security conditions. At the tactical level, the proxy elements use the old tactics (i.e. bombing) through innovative ways with the know-how transferred by the aggressor.

The expected ‘End State’ of the hybrid war can vary from regime change through democracy engineering to collapse of the state system. Depending on the political will (End State) of the opponent, the means, tactics, and intensity of the war will be different.

The countering hybrid war is challenging due to the following deficiencies:

- Its conduct in the gray zone makes the reliance on the legal and military instruments meaningless (the Article 51 of the UN Charter, Article Five of the North Atlantic Treaty, and other international norms),
- Spreading out in a wide spectrum of its means and unprecedented tactics complicates the defense action,
- The military and civil components of the states are not properly designed and fully capable of conducting counter-operations.
The Efforts and Conceptualization⁵

The last two US National Security Strategies (2006 and 2010) did not refer to the term ‘hybrid.’ The 2015 version mentions hybrid conflicts that were regarded as the operations of the foreign military forces which were disguised as a separatist group or extremist organizations like DAESH.

The hybrid war entered in the agenda of EU in defense summit 2015. The Foreign Affairs Council directed the European Defense Agency to develop a joint framework countering hybrid threats and foster the resilience of the EU. The April 2016 Joint Framework refers to hybrid threats as a ‘mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare’. And underlines that hybrid threats ‘target critical vulnerabilities and seek to create ambiguity in order to hinder swift and effective decision-making.’

The UN does not use the term of hybrid war and prefers to use ‘asymmetric threats’ (in peace operations) instead of it.

The latest NATO Strategic Concept (2010) also does not talk about the term ‘hybrid,’ however, NATO seems to use it in the upcoming documents.⁶ In this regard, according to NATO’s definition, hybrid wars are conducted by opponents ‘with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives’ (Cusumano and Corbe, 2018: 4).

Resisting Hybrid War

Since the hybrid war has a broad scope of means and tactics directed to the various components of the state as well as it is conducted by persisting covert operations, it cannot be countered by the classic security understanding and architecture. Defense against hybrid threats needs a multi-layered protection and holistic planning to ensure the stability of the state system. Hence, a state must develop ‘resiliency’ logic instead of the standard conventional defense logic activated by threats or any attack.

The hybrid war seeks to manipulate the vulnerabilities of a state and its society to widen the fragmentation within a society. Therefore, an effective response needs to be tailored to the multi-faceted threats and relevant to the actual context. This need following preconditions:

- Creation of resilience state system,
- Strengthening social unity,
- Building capacity for crisis management,
- The awareness of the environment and cultural context,
- Creation of an effective and well-organized intelligence system,
- Development of non-military means and effective mechanisms of Civil-Military Cooperation (CIMIC),

- The issue of a cyber-security strategy,
- Development of effective strategic communications,
- Improvement of home security and border management systems,
- Establishment of efficient anti-corruption agencies and democratic mechanism,
- Collaboration with international bodies such as UN, EU, and NATO,
- Adaption of relevant international legal norms to attribute political responsibility and legal liabilities.

The present developments in the border region with Syria and Iraq as well as the Gulenist military coup in 2016 and economic crisis in 2018 highlight the general vulnerabilities of Turkey. The Turkish state system does not have the vision to tackle with the hybrid threats and conduct hybrid war. Therefore, Turkey should immediately improve state resilience with the help of a ‘Resilience and Hybrid Security Policy Action Plan’ based on the analysis of the weaknesses, threats, and necessary capacities.

**Basics of the Resilience**

Oxford dictionary defines the term ‘resilience’ as ‘the capacity to recover quickly from difficulties; toughness’ or ‘the ability of a substance or object to spring back into shape; elasticity.’ When considered the purpose of this policy brief, we can use the term in the first meaning of the definition. In the military terminology, it has additionally ‘survival’ capability, which is often called as “beka” in Turkish language.
The resilience of a state is a function of the ‘structural stability’ that rests on the effectiveness and legitimacy of a government. The legitimacy of a government is related to the consensus between the population and elected government. In this regard, the individuals, who nourish strong feelings of belonging to a state, are the vital factor of national security. Thus, the legitimacy of a government and effectiveness of a state is strongly related to the ability to ensure human security, good governance/rule of law, social/economic development within a territory as depicted in Fig. 2 (Pounds, El Alam, and Keijzer, 2018: 206).

The relationship between effectiveness and legitimacy is graphically depicted in Fig. 3. As seen, a low-level legitimacy and effectiveness make a state fragile even prone to fail.

![Figure 2: Components of State Effectiveness (Source: Pounds, El Alam, and Keijzer, 2018)](image)

![Figure 3: The stability model (Source: Pounds, El Alam, and Keijzer, 2018)](image)
A resilient state can withstand and recover from internal or external hybrid threats and resists effectively hybrid war. In contrast, the non-resilient state system is very sensitive to hybrid threats and might collapse under cascading hybrid threats. Even though, both autocratic and democratic regimes can achieve stability to the certain degrees, an autocratic state is more vulnerable to hybrid threats due to the low-level social cohesion, weak institutions and legitimacy of the regime as observed in Tunisia, Libya, Egypt, and Syria (Pounds, El Alam, and Keijzer, 2018: 208, 209). The autocratic states are not able to construct a resilient state system; thus, they are prone to slide to low stability more rapidly than the democratic states which are more resilient due to the high levels of legitimacy and social cohesion as shown in Fig. 4 (Pounds, El Alam, and Keijzer, 2018: 208, 209).

Figure 4: Resilience in relation to stability (Source: Pounds, El Alam, and Keijzer, 2018)

Besides these structural factors, the following factors also affect the resilience capacity of a state:

**Global interdependence:** the energy and financial dependency as well as investment and trade interdependency generate sensitiveness for the defense formed against the hybrid war since their existence weakens the state resilience. A state should diversify and minimize its dependencies to maintain freedom of movement and increase its resilience.

**The dependency on technology:** the electronic systems are highly vulnerable to external manipulations. This risk poses great threats to the states that use them in the operation of critical infrastructures such as water and power supply, transport, finance, and economic systems. The private owners usually do not have the ability to operate them when exposed hybrid threats. Thus, a resilient state system must have alternative systems and response/recovery mechanism.
The open society: the interconnectedness and openness of the society pose both risks and opportunity. If a society is skilled enough to resist disinformation, propaganda and information operations, it can recover attacks directed on its value system and keep its cohesion. Otherwise, the society will lose its solidarity when the vulnerabilities of the open society are manipulated by the aggressor. A plausible control of media outlets by creating a proactive stance against false stories will contribute to tackle disinformation. Not to harm freedom of information, governments should only implement coercive measures against the media outlets infected by aggressors.

The radicalization: The mass immigrants, refugee problems, economic hardships, and extremist violence generated tension in some states nourished by the clash of values. This tension caused to the radicalization of some groups in the ethnic and religious communities that poses also a threat to the internal security since radicals can be instrumentalized through various means of the hybrid war.

Conclusion

Due to the power consolidation at the system level, most nations seek to realize their political interests through employing hybrid war and its means. The means and tactics of this war are limitless, and it has no norms. Therefore, a powerful state can even support the opponents of its ally or exercise economic pressure to materialize its regional interests.

In the light of the explanation made above, Turkey can be regarded as a target state of a concerted hybrid war exercised by some states. Because, the political and logistic support to the separatist and radical fractions in Turkey and abroad, the experiencing economic and information operations are obvious indicators of a hybrid war targeted Turkey.

The present social discord resting on the value discrepancies makes Turkey more vulnerable to the hybrid war. Therefore, Turkey must increase state resilience in order to deter aggressors and overcome attacks. Among the initial tasks, the relevant institutions should contribute to the development of an executive plan envisages various levels (tactical, operative and strategic) of conduct, periods (short, mid, long) to complete tasks and lines of operation to ensure resilience.

Defense against hybrid war requires a fundamentally different mindset encompassing perfect coordination of the national power elements and the development of proactive as well as innovative political, economic, security, and physiological tools.
Therefore, the civil authority shall take the lead to reinforce social cohesion by underpinning legitimacy and fighting corruption; strengthen the coherence of state by empowering its components and minimize dependencies by increasing national self-sustainment capability.

The achievement of a functioning executive action plan against the hybrid war requires visionary and creative political and military leadership. In this sense, the political leaders are responsible to define the national objectives, orchestra strategic efforts and allocate resources, while military leaders are tasked to analyze the scope of the ‘gray zone,’ the activities of the aggressor and means of hybrid wars to develop doctrines, concepts, strategies and plans to train the units and conduct the counter operation in close cooperation with other civilian components.
Bibliography:


Uzięblo, Jan, Jakub, (2017): United in Ambiguity? EU and NATO Approaches to Hybrid Warfare and Hybrid Threats, Department of EU International Relations and Diplomacy Studies, EU Diplomacy Paper, College of Europe.
Global Political Trends Center

Global Political Trends Center (GPoT Center) is a nonprofit, nonpartisan research institution established under the auspices of Istanbul Kültür University in 2009.

GPoT Center was founded with the aim to support reconciliation and non-violent solutions to international as well as domestic issues through dialogue. Our mission is to contribute to stability, democratization and peace through organizing multitrack diplomacy meetings, conducting innovative and independent research, and encouraging informed debates in the media on key issues affecting Turkey and the world.

GPoT Center serves as a platform for the free exchange of views and information on political, social and economic matters concerning a variety of parties and segments of society. We aim to achieve our mission by routinely bringing together opinion leaders, government officials, policy makers, analysts, scholars, experts and members of the media from Turkey and abroad.

Our publications can be downloaded from our website for free. They are also accessible through online libraries worldwide, such as the International Relations and Security Network in Zurich, Europe’s World in Brussels, and Columbia University Press in New York. Additionally, you can find our books on Google Books and Amazon Kindle.

CONTACT DETAILS
Global Political Trends (GPoT) Center
Istanbul Kültür University
Ataköy Campus, Bakırköy
34158 Istanbul, Turkey
www.gpotcenter.org
info@gpotcenter.org

Tel: +90 212 498 44 76/65
Fax: +90 212 498 44 05