

DEFINITION AND SCOPE OF HYBRID THREATS¹

Orhan GÖKCE²

Abstract

The strategy that Russia implement in Crimea and Eastern Ukraine in 2014 drew the attention to hybrid war for the concept of hybrid threats mostly preferred because of being considered more extensive and as a result it is observed that this led to publication of numerous essays particularly on the term of hybrid war. It will be a little bit imaginary to expect that modern threat or armed attack as a conventional military clash between regular or irregular forces in our day. The reason for that is conflicts are conducted through implementation of various tactics and means apart from military forces most of the time. This type of struggle is characterized with the fact of hybrid threat.

When we look at the literature, it is observed that there are not many publications on the concept of hybrid threat. However, it is quite possible that hybrid threats will be at the top of agenda of all states in the future. This is because politically stable and economically powerful countries have the purpose of overpowering the states that they desire to influence by concealing themselves or keeping in the background by means of using various methods and strategies at the same time and thus by means of weakening their will and sustaining power. This method and way is conceptualized as hybrid war or hybrid threat at the present time. However, it cannot be said that there is a consensus on how hybrid threats shall be defined. For that reason, this study aims at establishing a framework on the concept of hybrid threat gaining importance gradually in international conflicts mostly included in the friend states and aims at identifying the elements of it.

Key Words: Hybrid, Threat, War, Components, Tactics, Methods

1 This text is reviewed, updated and expanded version of the declaration under the title of “hybrid threats and their components” presented in Macedonia in “MECAS II-2017, the Second Mediterranean International Social Sciences Congress II” on 10-13 October 2017.

2 Prof. Dr., Selçuk University Konya, Faculty of Economic and Administrative Sciences, Department of Public Administration, e-mail: ogokce@selcuk.edu.tr

Introduction

It was quite easy to describe the conflicts until the end of 20th century. A state or the central powers applied force (generally military force) to another state. The struggle was against an enemy detected concretely. In Cold War period, generally there were two powers at the pole apart to one another ideologically and these tried to achieve global superiority against the other by means of a tight race in military field. Depending on new weapon system (cross-continental ballistic missiles or long-range bomber aircrafts etc.), strategic concerns and precautions and military equipment changed to a large extent. These powers were in a struggle for obtaining or extending political clout over proxy wars. With this purpose, different methods and means were used. Regional powers being in a clash were being supported by means of various tools by the blocks they were bound to. Upon breakdown of Warsaw treaty organization, two-pole world system was dissolved and therefore manageable and relatively countable status of conflict disappeared.

Improvement of new technology, especially information and communication technologies and social networks gave states the chance of exercising pressure on target states or the states desired to be influenced differently. Clandestine operations played important role in this process. By this means, attacker state prevented being introduced as attacker and unlawful state and provided the opportunity of shifting the blame to someone else. Nowadays, there is not much changed related to this strategy. Today also attacker states hide themselves or remain at the background and therefore have the objective of pushing their desires through to target states by various means, that is to say overpowering on their desires by breaking their faith on resist and willpower. This method and way is conceptualized as hybrid war or hybrid threat in our day. As it is supposed here that the concept of hybrid threat is more comprehensive than the concept of hybrid war, the latter term will be preferred.

It cannot be said that there is not any consensus on the way how hybrid threats will be defined. The only thing known is the fact that these are quite complex and hard to be understood.

There is not a concept available on how the states facing with hybrid threats can overcome this manner of violence, being complex and difficult to be understood or how they can react against these hybrid threats and attacks. For that reason, it is a reality that the states encountering asymmetrical conflicts or hybrid threats have difficulties in managing these threats or fighting against these efficiently. Basic reason for this is that the concept of “hybrid threat” was included in the security literature recently and it is a young concept in this perspective. Therefore, this study focuses primarily on where

and in which context this concept is discussed and what kind of new information can be obtained from this discussion. To be more concrete, this study seeks answer for the following questions: In which terms hybrid threats differentiate from previous threats? What are the components of hybrid threats? How can the clashes in the future take place? To what extents hybrid threat is different from asymmetrical or hybrid war? These and this kind of questions will be dealt in this study and these questions will be tried to be responded.

The discussion reveals that the issue of “hybrid threats” is far away from being a scientific occupation yet. For that reason, it is required to answer and justify the question of “what is hybrid threat and what are the components of it”.

The Concept and Notion of Hybrid Threats

There is not a definition of the concept of hybrid threat commonly shared by everyone. It is observed that the concept of “hybrid war” is preferred in Anglo-American worldwide. The struggles conducted against conventional and non-conventional guerilla, terrorism and criminal elements and tactics are meant with this: “[...] *those posed by adversaries, with the ability to simultaneously employ conventional and nonconventional means adaptively in pursuit of their objectives*” (Miklaucic, 2011).

The term of “hybridity” comes from biology or agriculture originally (Deng/Schurian, 2015:23) and the term refers to a mixed form comprising of two different systems, that is to say mixture of two or more elements. In this manner, combination of two or more authentic original elements reveals new things. The novice does not only influence internal composition but also the surrounding. The meaning of it in terms of “hybrid threat” is emergence of new types of threat as a result of intertwining the threats determined previously. As a result, restructuring current fact of conflict and threats is extension of threat spectrum. Hence, it can be claimed that hybrid threats represent a synthesis of insulated views of conflict. For that reason, there is not hybrid threat, but different threats arising from changing variations of the same combinations, creating reciprocal effects and producing motives. Hybrid threats are in plural form. Therefore, solutions shall be improved in wide variety related to protective and defensive mechanisms. Hybrid threats are comprised of some elements of conventional threat views conceptually. Military intervention form (hybrid war) shall only be considered as a fractional part in hybrid threat spectrum (Deng/Schurian, 2015:23 et.al.).

A threat concludes ability and intention. Even improvement of the capacity required for struggle takes time, a threat can be observed. However, it is quite

difficult to determine the intention of a state about attacking and thereby giving harm to another. For instance, the policy of a state concerning one another can change rapidly and instantly. Consequently, defined as a strategic partner, a state can become a threat suddenly. This case can easily be observed in the relationship between USA-Turkey and European Union-Ukraine.

The one who conceptualized hybrid war in close meaning to the concept of hybrid threat in contextual terms is Hoffmann (2007). According to this, Hoffmann stated that hybrid war is: “*a mixture of conventional, irregular, terrorist and destroying threats*” (2007:5). In his following work, Hoffman defined hybrid war a little bit more comprehensively:

“Instead of separate challengers with fundamentally different approaches (conventional, irregular, or terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously” (2009a:35).

Conventional types of struggle, irregular tactic and formations, terrorist attacks (including arbitrary violence and force) and penal upheavals are included in Hoffmann’s concept of hybrid war. Herewith, hybrid wars are conducted both by state and non-state actors. These multi-mode activities are generally directed operationally and tactically to create effects of synergy at physical and psychological dimensions of conflicts (2009a).

The concept of hybrid war is not brand new (see Fuhrer, 2015:8). It is also possible to see mixtures of different tools in the wars in the past. However, military dimension only forms one dimension in the concept of hybrid threat. In these terms, as the concept of hybrid threat also includes usage of non-military means, it goes beyond hybrid war. When considered in conceptual perspective, this threat is a reaction against the irregularities and disarrangements arouse after the demolition of West-East contradiction. In this sense, Hoffmann states as follows:

“[...] our greatest challenge in the future will come not from a state that selects one approach, but from states or groups that select from the whole menu of tactics and technologies and blend them in innovative ways to meet their own strategic culture, geography and aims.” (2009b:5).

Characteristic feature of hybrid threats is conventional and irregular tactic, centerless planning and execution, existence of non-state actors and use of high technology. Combination of different tactics and methods leads to establishment of new, innovative formations that can perform “division of labor” or all activities among state units and non-stategroups.

2010'da United States Government Accountability Office (GAO) in Washington worked on hybrid war tactics potential to be used by current and future opponents in 2010 and stated in its report that USA army will be at under threat particularly in terms of following aspects:

“[...] non-state- and state-sponsored adversaries, including computer network and satellite attacks; portable surface-to-air missiles; improvised explosive devices; information and media manipulation; and chemical, biological, radiological nuclear, and high- yield explosive devices“ (2010:1).

In this report, a working definition on the concept of hybrid threat was produced. According to this, hybrid threat:

“An adversary that simultaneously and adaptively employs some fused combination of (1) political, military, economic, social and information means and (2) conventional, irregular, terrorism and disruptive/criminal conflict methods. It may include a combination of state and non-state actors“ (GAO, 2010:18).

Point of view of USA army focuses on the connection between regular and irregular forces and a hybrid threat is a (military or other organized) power that constitute an impediment on intervention into any country according to their perspective.

USA army defined the concept of hybrid threat as in the following within the body of operational doctrine in 2011:

”A hybrid threat is the diverse and dynamic combination of regular forces, irregular forces, criminal elements, or a combination of these forces and elements all unified to achieve mutually benefitting effects. Hybrid threats combine regular forces governed by international law, military tradition, and custom with unregulated irregular forces that act with no restrictions on violence or their targets.” (2011:1)

It is clear that the definition of hybrid threat is quite narrow in terms of USA perspective. As it is seen in the example of Turkey, forms of threat that have been implemented since 2011 and having gone by a coup attempt finally do not only cover initiatives against sovereignty of a country and territorial integrity but also activities intended for making state and its institutions inoperative. In this respect, the necessity of improving a new definition for hybrid threat is obvious. With this purpose, considering that the definition of Deng/Schurian is more functional, it is supported here. As per this:

“A hybrid threat is the threat to a state or a state alliance the ability and the intent of

an actor, his potential, multidimensional (political, economic, military, social, media, etc.) and in a timely relationship to the enforcement of its interests use” (2015:37).

We consider that it is required to list diplomatic, technical and scientific initiatives among the tools of hybrid threats. Deng and Schurian (2015), express that threats shall not exceed a strategic threshold to be assumed as hybrid threat. This case is of the issue if the state that is subjected to attack is limited in terms of decision making and action capacity fundamentally. The form of this limitation can be interpreted differently by each state as per its degree of influence by each case. Therefore, critical threshold can only be discussed if at least two major sectors (ministry etc.) of a state is affected by hybrid threat.

Hybrid Threats versus Hybrid War

Hybrid threats are merely discussed in international publications in this respect. Generally, hybrid war is mentioned or the subject matter is discussed and analyzed within the framework of the concept of hybrid war. However, it is observed that there is a transformation in the point of view recently and the concept of hybrid threats is started to be adopted more than hybrid war.

The difference between hybrid threats and war actually originates from the form of definition of war phenomenon. There is not a definition on which everyone agrees on yet. There are different definitions of the concept of war. As specified by Varlık, the difference in initiatives of definition arises from the formation of the concept (ontological), the source, scope and nature (epistemological) of the knowledge related to the concept and use of different levels and units in the definitions in this scope. Different approaches in the studies about war do not mostly complete one another makes it impossible to analyze the concept in integrity and can result in wrong use and conceptualization of the term (2013:116).

Different conceptualization of war accompanies with some questions. For instance, is smart (soft) power a war? What is the threshold in hard power “war”? After which phase can a hard power war be discussed? Or what kind of terrorist actions shall be of issue to declare “War on Terror” or to what shall be the extent of terrorist actions?

The most fundamental condition to talk about war is the necessity of experiencing an armed struggle or conflict between two states by means of regular armies’

using force against each other. In other words, it is required that one of the state parties shall accept or declare the existence of a war frankly to mention about warfare (Varlık, 2013: 118).

The objective of war is to win or gain a victory. This can be achieved by defeating enemy or completely demolishing it physically. With this purpose, use of all kinds of tools is of matter under a strict organization at war. All people at a certain age group are prompted to war in one hand, and to contribute to weapons and equipment on the other hand. There are some similarities between hybrid threats and war in terms of using various tools (political, economic, social, media and public opinion, diplomacy etc.) to give harm to enemy. However, on the contrary to war, hybrid threats do not aim at complete demolish of its enemy and disappear of its vital structures. Conversely, as hybrid threats targets coming out of problem of governability by making state and its institutions inoperative, it is possible to identify it as a kind of pressure or siege strategy weakening/collapsing administrative capacity of a state (see Gökce, 2006a-b, 2007, 2016). Thereby, attacker state abstains from a direct fight towards target state, and tries to make target state accept what it desires by means of a covert hybrid approach. Hybrid approach is preferred by a state in the cases when a direct (military) fight is deemed as damaging its prestige or harmful at international platform.

As the phenomenon of war is not our subject matter, here it is desired to confine to the explanation above (please see Varlık, 2013, Keskin, 1998) for more comprehensive and detailed information on the subject matter). Within the light of the explanations stated above, it is clear that the concept of war cannot be used for hybrid threat even though there are some similarities between them in terms of utilizing the tools. The reason for that is use of a great number of different power projections (weapon) that are not related to use of physical violence towards target state is in question in hybrid threat. In this respect, hybrid threats is an umbrella term and covers all kinds of terrorism(cyber), immigration, piracy, corruption, internal disturbances and ethnical conflicts as well as diplomacy, political interaction, humanitarian aid, social pressure, economic fluctuation, media campaigns conducted professionally, activating NGOs and systematic use of all those. In brief, a hybrid threat is the way of utilizing a force in negative manner:

“[...] those posed by adversaries, with the ability to simultaneously employ conventional and nonconventional means adaptively in pursuit of their objectives” (Miklaucic, 2011).

Hybrid Threat Factors

There are various means of affecting a state. The number of resources and methods increases and varies together with technological improvements. Hybridity is not a new phenomenon, but new means of effect have revealed together with current technologies and modern communication strategies and global network.

In addition to the positive contributions that new technologies introduce to society (for instance, by means of interdisciplinary networks in cyber area), negative interactions are also available. Dependence of substructure and security gap is sufficient to make a state inoperative. Especially, cyber-attacks can be carried out from different places and for that reason; it is difficult to pursue its source. If cyber-attacks are determined to have been performed by any actor within the borders of the state, it will have some substantially negative conclusions in mutual relationships and at international platform. That is why the resources of cyber-attacks are indefinite.

There are similar difficulties in social networks; Facebook and Twitter. These have central place about spreading knowledge over a crisis territory right now. Wide access to social media offer great opportunities for propaganda campaigns by means of almost all users. Specially, it is known that these are important in coming out and increase in internal conflicts.

Volunteer warriors' tactic, or the method known as "little green men" after the intervention of Russia to Ukraine, is significant part of hybrid threat. In this manner, states leak into target state illegally and encourage the opposition of that country or ethnic groups to rise up by organizing them. They also provide military trainings; provide financial and logistic support and give media propaganda support.

The method that Russia implemented in Ukraine represents a new era because it is easy to officially deny volunteer warriors that are organized by another state. It is a thing known by everyone but cannot be said openly. England followed a tactic in Libya similar to Russia's tactic. The fact that England sent soldiers to Libya was released to public three-four weeks before the military operation to the territory but it did not constitute a problem as it was not expressed by anyone. Actually, this method has been used and is still used by western countries for a long time. This method blurs the difference between enemy and friends, or fighters and who are not fighters. Acting like a friend and strategic partner, a state may have the objective of weakening and making the other addicted.

It is obviously seen from these examples that some precautions are necessary in all spectrums of hybrid threats to abstain from tactic, operational or strategic errors.

Stakeholders, objectives and methods for hybrid threats

Here, aforementioned targets, means and methods of hybrid threats are briefly emphasized with the main lines (Deng/Schurian, 2015:52-54):

i) *Fundamental Objective: To Weaken a State*

Hybrid threat methods primarily aim at making institutions of a state inoperative, make them have difficulties in offering most basic public services, and thereby breaking down public order, increasing disturbances, rising up internal conflicts and correspondingly making citizens of the state question the legitimacy of it. Forming and promoting local discrimination movements, conducting black propaganda studies by means of national and international media directed on influencing elections, and commencing discussions about the results of elections etc. are included in these activities.

ii) *Actors*

Virtually, a hybrid threat can be implemented both by a state and non-state actor. Cross-border companies are good example for non-state actors as well as terrorist organizations. Hybrid threat is related with an actor and in this sense, it differs from other risk factors (aging, climate change, immigration, rush of refugees vb.).

As specified above, actualization of a hybrid threat requires a combination of two components. These are existence of capacity on one hand, and desire for using some means and methods on the other hand. If one of these key stones is missing, there is not a hybrid threat (Deng/Schurian, 2015:53). In this sense, a state can have capacity and necessary logistic substructure, but if that state does not have intention to use these opportunities against another state, or vice versa, it is not possible to mention about hybrid threat.

What is the Potential of an Actor?

The potential of an actor refers to the whole of all capabilities, resources and social networks. A hybrid threat is comprised of expansion of various means and methods through combined use of this potential. As for means, above all security institutions of state are of issue. A state needs army and intelligence agency to be active at cross-border. Security and jurisdiction are needed to keep members of target state living in its country under control. Due to global knowledge and communication networks, it is required that cyber-attack shall be taken into account as a potential means of attack.

Upon globalization, economy is turned into the greatest means of dependency and

pressure. Natural sources wealth or deprivation is one of the most significant reasons of transnational tension. Political tensions depending on energy/gas problem encountered between Russia and Ukraine is the most apparent example of this.

Speculative acts concerning the currency of a state are among the methods of influencing the economy of that country. The same is valid for genetically modified seeds. States do not abstain from using this as a means of threat.

Violence and power as potential capabilities and resources of an actor have the following twelve dimensions and these also represent foreign policy tools of a state at the same time. These are (Deng/Schurian, 2015:58):

- 1) Military power
- 2) Political and legal power
- 3) Power of intelligence agencies
- 4) Cyber power
- 5) Private military and civil security companies, paramilitary volunteer institutions
- 6) Social violence (rebellious and separatist groups in the country, political and religious extremism, dissatisfied and marginalized minority groups)
- 7) Terrorist groups and their actions
- 8) Diplomatic power/Public diplomacy
- 9) Economic power
- 10) Financial power
- 11) Scientific and technological power
- 12) Media power

A hybrid threat is a coherent, focused and systematic interaction of various activities conducted against a state with the purpose of weakening and making target state dependent associated and coordinated with one another. Several actions/activities given above, but at least two, are directed to target state simultaneously. This does not only increase the efficiency but also complicates defense. Actions can be carried out by means of pressure, violence and in addition to those, propaganda and embargo (Deng/Schurian, 2015:67).

As a hybrid threat can be effective at several levels, a multi-dimensional approach can be mentioned. The dimensions especially effective are politics and law, military, economy ecology, social and culture, technology, science and media fields.

The application of a hybrid process in reality depends on the situation of target state. Developed and industrialized states depend more of on energy, resources and operating economy. On the contrary, failed states (Gökce, 2016) are more sensitive to and defenseless against corruptions and civil rebellions. Cyber-attacks make no sense in a state not having an extensive communication and technology substructure because it does not ensure the foreseen effect. However, it shall be paid sufficient attention that such a cyber-attack can result in fatal results on public order and economy in a developed country. Threat potential can be put into practice directly or indirectly. Direct threats are conducted over the institutions of the state and indirect ones are performed over proxy organizations.

Conclusion

Discussion points out that the concept of hybrid threats is more compressive than the concept of hybrid war and at the same time, it is a more multi-dimensional approach. A multi-dimensional approach helps covering the identity of the threatening actor in one side, and makes it difficult for the state being threatened to develop a reaction on the other side. The threatening state can activate several means simultaneously to achieve the conclusion it desires and the state being attacked cannot react timely as it was caught unprepared. This makes it easy for attacker state to achieve its goal. The only determinant in hybrid threat is the purpose of the state threatening and achieving this goal.

In our day, many states use hybrid methods successfully but the states being subjected to attacks cannot activate the counter measures simultaneously with the same level of efficiency. This is because hybrid threats generally come from states known as “friend” or “strategic partner”. This seems indispensable that all states shall produce counter measures for potential scenarios and develop protective and defense mechanisms.

References

- Bauer, Alain (2014)**, “Hybridization of Conflicts”, **PRISM 4, No. 4**. http://cco.dodlive.mil/files/2014/04/Hybridization_of_Conflicts.pdf.
- Dengg, Anton/Schurian, Michael N. (2015)**, “Zum Begriff der Hybriden Bedrohungen”, **Dengg, A./Schurian, M. N. (ed.), Vernetzte Unsicherheit – Hybride Bedrohungen im 21. Jahrhundert**, 2015, Wien, pp. 23-76.
- Fuhrer, Daniel (2015)**, “Zur hybriden Bedrohung”, **Sicherheitspolitik**, Allgemeine Schweizerische Militäerzeitschrift, 04 (2015), pp. 8-11.
- GAO**, United States Government Accountability Office: Subject: **Hybrid Warfare**. GAO-10-1036R Hybrid Warfare. Washington, DC 10.09.2010, S. 1. <http://www.gao.gov/new.items/d101036r.pdf>.
- Gökce, Gülise (2007)**, **Güçlü ve Zayıf Devlet Tartışmaları Bağlamında Türkiye**, Çizgi Kitabevi, Konya.
- Gökce, Gülise (2006a)**, “Devlet Sınıflandırmaları ve Zayıf Devletlerin Karakteristik Özellikleri”, **Selçuk Üniversitesi İİBF Sosyal ve Ekonomik Araştırmalar Dergisi**, S. 11, Y. 6 (2006), pp. 343- 359.
- Gökce, Gülise (2006b)**, “Devleti Yeniden Keşfetmek: Devlet Gücünün Göstergesi Olarak İdari Kapasite”, **Gazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C. 8, S. 3 (2006), pp.203-230.
- Gökce, Gülise (2016)**, “Critical Analysis Of Failed State Concept”, The 2nd. International Conference on the Changing World and Social Research (ICWSR’2016) Conference Proceeding Book, Barcelona, Spain.
- Hoffmann, Frank G. (2009b)**, “Hybrid Threats, Reconceptualizing the Evolving character of Modern Conflict”, **Strategic Forum**, No. 240.
- Hoffmann, Frank G. (2009a)**, “Hybrid Warfare and Challenges”, **Joint Forces Quarterly**, 32 (1), pp. 34-39.
- Hoffman, Frank G. (2007)**, “Conflict in the 21st Century: The Rise of Yybrid Wars”, Arlington, VA: **Potomac Institute for Policy Studies**.
- Keskin, Funda (1998)**, Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler, **Mülkiyeliler Birliği Vakfı Yayınları: 68**, Ankara.
- Miklaucic, Michael (2011)**, “NATO Countering the Hybrid Threat”, Allied Command Transformation Web site, September 23, 2011 <http://www.act.nato.int/nato-countering-the-hybrid-threat>.
- U.S. Army: Field Manual 3-0 Operations C-1**. GPO, Washington, DC Februar 2011, **MAJ Brian P. Fleming, United States Army: The Hybrid Threat Concept, Contemporary War, Military Planning and the Advent of Unrestricted Operational Art**. Report. 17.05.2011, <https://www.hsdl.org/?view&did=700828>.
- Varlık, Ali Bilgin (2013)**, “Savaşı Tanımlamak:Terminolojik Bir Yaklaşım”, **Eurasscience Journals**, 1(2), pp. 114-129.