IRMO
Institut za razvoj i međunarodne odnose
Institute for Development and International Relations

Hanns Seidel Stiftung
Ured u Zagrebu

In Search of a Systematic Approach to Hybrid Threats

By Gordan Akrap

Introduction

Hybrid threats and hybrid conflicts and wars are one of those terms that have suddenly entered in public knowledge, raising many concerns. This is not surprising because there is no common and generally accepted definition of hybrid threats by which these processes are defined. The emergence of this term in the regional media space was, in the beginning, connected with journalist's perception that intention of the state is to impose censorship of writing and publishing. Over time, fear in the media receded and gave way to understanding the complexity of this issue. Specifically, hybrid threats are not a new phenomenon to theorists of conflicts and wars. What makes hybrid warfare different from previous wars is the change in the importance and intensity of the individual components of the conflict, such as information or influence warfare component. In fact, until the end of the 20th century, information and media operations, that could be called influence or cognitive operations, were in the function of military operations.

Origins of hybrid warfare

At the end of the 20th century, starting with the Croatian Homeland War until operation Allied Force in 1999, a change in the importance of influence operations in crisis and war management was evident. Influence operations became, slowly but surely, the primary model of crisis creation and management with the aim of imposing one's will on a selected target audience. If influence operations produced the expected results, there was no need to engage military resources. This is precisely the essential feature of the hybridity of modern conflicts: the possibility to obtain non-military objectives by using non-military and/or military assets and obtaining military objectives by using non-military and or military assets. During the Cold War, the acronym DIME (Diplomacy, Information, Military, Economy) was created in order to describe the full range of instruments that the state could use in order to impose its own interests in low-intensity conflicts. Using this idea, I would describe hybrid threats as coordinated, focused and concerted set of military and non-military activities that attacks society or state, exploiting the existing and creating new vulnerabilities or/and divisions of society, democratic structures and institutions using political, economic, military, civilian, security, intelligence, energy, media and information and communication systems and resources in order to influence different target audiences.

DIME was an acronym for Diplomacy, Information, Military, Economy.

This definition covers the full range of possible activities that can be used to plan and conduct modern influence operations, to manage modern hybrid conflicts. This shows that the argument that everything that can benefit mankind can also harm him is legitimate. This is to say that there is nothing in the world today that cannot become a weapon. Reading between lines, a very important expression can be noticed - everything can become a weapon.

Hybrid threats operate primarily in the information domain of human life.

Today the Cold War-era DIME acronym can be transferred in a slightly different way: Diplomacy, Intelligence, Media (Military), Energy (Economy), with the notion that states no longer have a monopoly on their implementation. Many other actors such as groups, organizations, capable and influential individuals, can do it also. Hybrid threats operate primarily in the information domain of human life. The consequences of these actions are first manifested in the cognitive domain or thought processes which in turn leads, based on decisions made in

the cognitive process, to the consequences in the world of physical and virtual reality. The consequences of events in the cognitive domain and in the domain of the world of reality influence the information domain. Thus, the circuit is closed with a powerful feedback system that an information or hybrid attacker can use to monitor the effectiveness of its own actions. In doing so, attacker should make corrections to its own actions. At the same time, it is also a part of the activity that the defense system needs to be able to recognize in order to defend itself against a modern hybrid attacker. Modern hybrid attackers gladly use advantages and many benefits of different social networks to spread the data and information when they want to reach specific target audiences. At the same time, social networks serve them to gather a wealth of data that is necessary for the effective planning of hybrid influence operations. Not every audience is the same or responds at same way to different inputs. Therefore, it is necessary to engage their own or someone else's intelligence and security system in order to collect the required information and intelligence. The best way to collect intelligence and to effectively try to negate your own attack intentions, activities and identification of the real goals that you try to reach, is by engaging someone else, other companies to collect the information you require.

A classic example of covert activities is the engagement of Cambridge Analytica, a company which collected huge amounts of practical and important intelligence.

A classic example of such covert activities is the engagement of Cambridge Analytica, a company which collected huge amounts of practical and important intelligence from social networks. This intelligence was used to plan and conduct the influence operation of the intelligence and security system of Russia. They, using this intelligence, specially tailored different messages that were sent to various target audiences within the United States' electorate body in order to try to influence the results of the US presidential election and the United Kingdom voters' referendum on the withdrawal the UK from the European Union that triggered Brexit, both in 2016.

Hybrid threats in Montenegro and North Macedonia

Activities from the spectrum of hybrid threats in the Western Balkan countries (Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia) are visible in several different processes. A trial in Montenegro of

Russian nationals, suspected that they were engaged as members of Russia's military security and intelligence agency, has been underway for a violent change of government. The alleged aim of their activities was to physically eliminate the current leadership of Montenegro, to cause a state of unrest, insecurity, hopelessness, distrust in the institutions of the state, and to encourage disorder. Their goal was, as it looks like from today's perspective, to change the existing political elite in power with the one that is more friendly to Russian national interests. Another clearly visible goal of Russian hybrid operations is directly related to the highly sensitive political processes and agreements between North Macedonia and Greece. Namely, the political elites of those states, aware of all the risks that such a peace agreement may entail for them to remain in power, have put in place mechanisms to resolve the issue of the name of Macedonia in the common interest.

The goal of these hybrid activities was to provoke political instability and to break the already fragile political ties between Macedonian and Macedonian-Albanian politicians.

The activities of pro-Russian circles in these countries, as well as circles that were not directly encouraged or supported by Russian, pro-Russian or Russian proxy groups, organizations, companies of institutions, strongly advocated the negative influence of the referendum that was coming. In other words, they encouraged voters in Macedonia to resist the change of their republic name and settling the agreement with Greece, with the purported goal of protecting their identity. The goal of these hybrid activities was to provoke political instability and to break the already fragile political ties between Macedonian and Macedonian-Albanian politicians in Macedonia, to create chaos, riots, lawlessness and, ultimately, to prevent Macedonia's NATO and EU entry. Namely, without agreement with Greece, Macedonia would still be blocked from joining NATO and the EU. It should not be overlooked or neglected that other stakeholders in the WB6 countries' political processes are not afraid from applying hybrid activities. This was evident in the example of Macedonia, when the pro-NATO and pro-EU circles succeeded in winning the leading influence operations and creating a state of information supremacy against Russian intentions in order to reach political agreement between Macedonia and Greece. This is not the first time that serious political processes of achieving peace between different seriously confronting parties were endangered by different actors on the international scene. The main modus operandi was to use intelligence and security agencies, either directly or indirectly, in order to reach strategic goals.

A very good example was the intelligence operation called "Crescendo", by which the Soviet Union engaged its own secret services to prevent a reaching peace agreement between Israel and Egypt during 1978 and 1979. Using the proxy organizations from Italy, Russians sought to influence individual circles in Libya to finally influence important decision-making individuals and circles in Egypt, with the aim of pressuring the Egyptian president to abandon his intention to conclude a strategically important peace agreement with Israel. Although the Soviets organized and carried out strong and intense intelligence activities, US pressure was stronger, and a peace agreement was reached that brought the 1978 Nobel Peace Prize to its signatories Anwar Sadat and Menachem Begin. From these examples, as well as from the breakdown of the so-called Arab Spring, the war in Ukraine and conflict in Syria, as well as from the incitement of protests in certain South American countries, it is evident that the starting point is the engagement of intelligence and security agencies. They need to gather timely and relevant information from reliable sources based on which influence operations can be planned in such a way as to guarantee their effectiveness. At the same time their actual planer, author, implementer and the objectives that individual actions seek to achieve, need to be concealed. Therefore, the recognition and identification of intensified activities of a country-specific intelligence agency is essential for the early identification of planned hybrid threats. Identification of the data that they are trying to collect about topics, groups and organizations is also very fruitful for recognizing which activities from wide spectrum of hybrid threats might be engaged. Therefore, it is necessary for a society in order to safely and reliably face upcoming hybrid threats to develop an active defense system that can detect these processes in a timely manner. At the same time, it is necessary to develop and strengthen the confidence of the population in the institutions of the state, which needs to inform population about the emergence of hybrid threats.

Activities from the spectrum of hybrid threats will be at the origin and center of all future conflicts and wars.

If the population does not trust these institutions, they will be more inclined to ignore and underestimate the information received from them about the upcoming or existing hybrid threats. Moreover, there is a possibility that the information attacker will use its own potential to make such warnings a mockery and indirectly turn it in its own advantage. That is why creation of a system with integrated approach between all segments of society,

including the state and the public, private, academic and non-governmental sectors to confront the hybrid threats issue, is needed. Activities from the spectrum of hybrid threats will be at the origin and center of all future conflicts and wars. The primary objective of hybrid attacks will be critical infrastructure. The main intention is going to be acquiring a state of information supremacy in the spectrum and domains of engaged activities. Primarily energy, water-food and information-communication infrastructure are going to be target of hybrid attacks. That is because all other critical infrastructure's rely more or less on the above mentioned infrastructures and depend essentially on their normal and undisturbed functioning. The day-to-day life depends on smooth and secure functioning of critical infrastructure. The downfall and outage of some of the critical infrastructures would have a negative cascading effect on other critical infrastructures.

Primarily energy, water-food and information-communication infrastructure are going to be target of hybrid attacks.

This, in turn, could easily cause a considerable number of injured persons, as well as fatalities. Economy would also be threatened and people's perception of a safe life would be impaired. This would create conditions that the information attacker could easily use to incite violence and internal divisions in society that could lead, in extreme situations, to the disintegration of existing society and to the formation of a new social paradigm, and political administration. Therefore, investments in protection, security and rapid, complete and effective resilience of critical infrastructure, which is largely in the hands of private owners, should be encouraged and insisted upon by the state. At the same time, these investments should be treated as one of the integral parts of the budget allocation for defense purposes for the above-mentioned reasons. The next challenge that states and the international community today are facing is the fact that the rules of classical warfare are defined. However, the rules of hybrid conflicts and rules of information warfare do not exist, just like the rules of cyber warfare. It means that where there are no rules, everything is allowed. Nothing is, in any form of action, prohibited, which opens up space for unprecedented attack models and choice of targets.

Rules of hybrid conflicts and rules of information warfare do not exist, just like the rules of cyber warfare.

It is therefore necessary to intensify efforts to seek consensus for the establishment of hybrid warfare rules in order to avoid situations and events that may lead to consequences that may have negative and destructive potential just like the use of weapons of mass destruction. In this regard, the EU and NATO should work very closely together, in order to create and fulfill conditions that will protect their own digital information and communication space from all kinds of misuse of its capabilities and to protect the achieved democratic standards and rule of law. Achieving a situation of digital sovereignty does not have to be modeled according to the Chinese nor Russian digital sovereignty. EU digital sovereignty must maintain the attained level of human rights and freedoms. Moreover, a joint effort in order to strengthen and even expand them is needed.

Conclusion

At the same time, these rights need to be protected from already seen attempts to abuse them using attacks from a spectrum of hybrid threats. This means that states must be the bearers of defining the rules of conduct in digital domain, not as it is now that the rules of conduct are defined by different multinational or national corporations that are primarily pursued by financial, rather than general interests. In the context of hybrid threats, special attention should be paid to the human factor. Modern information and communication cyber space can be defined as a space that consists from four different levels: the geographical level in terms of the territorial distribution of the physical parts of the system; the system of logical functions that enable it to function properly; the development of artificial intelligence that slowly, but-certainly is taking control over individual processes; and the human factor, that has its own physical and cyber dimension of appearance. It is the human factor that is at the same time the strongest and weakest link in the whole system. Analyses of different hybrid and cyber-attacks that came from and within the cyber space indicate that the attacker always aims to look for the weaknesses of the human factor. Therefore, it is necessary to pay considerable attention to the continued and ongoing security education of people in order for them to become aware of the dangers that may arise from their personal reckless and careless actions. No one is completely immune to influence operations that might come from the wide spectrum of hybrid threats and anyone can become the target of a hybrid attacker. Therefore, organized and inclusive actions and integration of the capacities of society, states and international organizations (e.g. NATO and the EU) need to be taken very seriously in order to create the conditions that can strengthen democracy and protect free societies.

Gordan Akrap, PhD, is a Research Fellow at the Faculty of Humanities and Social Sciences at the University of Zagreb, President and Founder of Hybrid Warfare Research Institute and Organizer of Zagreb Security Forum.

DISCLAIMER: The views presented in this paper are solely of the author and do not represent an official position of the Institute for Development and International Relations (IRMO) or of the Hanns Seidel Foundation.

IRMO
Institut za razvoj i međunarodne odnose
Institute for Development and International Relations

Hanns Seidel Stiftung
Ured u Zagrebu

Institute for Development and International Relations - IRMO
Lj. F. Vukotinovića 2, Zagreb, Croatia
www. irmo.hr

Hanns Seidel Stiftung
Amruševa 9, Zagreb, Croatia
www. hanns-seidel-stiftung.com.hr