Consejo Atlántico Juvenil Español
Spanish Youth Atlantic Treaty Association

News and Reports
www.coaje.es

Newsletter

February 2023

THE HYBRID LANDSCAPE IN 2023: BEYOND CYBERSECURITY

Tania Rey García

Abstract

The globalization and the development of new technologies through the digital era have led to the emergence of a new framework of confrontation between countries and non-state actors: hybrid warfare. War conventional tactics, together with the so-called hybrid threats, constitute a recent area of exhaustive study, allowing a greater understanding of the policies and actions carried out by international actors in the geopolitical sphere. In this way, these threats have been included in the new strategic concept of NATO and the EU, in order to improve the deterrence process for future conflict scenarios in our society.

A brief introduction towards hybrid threats

The use of conventional and unconventional tactics in conflict scenarios or in the geopolitical confrontation between major global players constitutes an increasingly destabilizing element in the international order. The actions in cyberspace, the promotion of disinformation campaigns, the instrumentalization of migrations, the manipulation of energy supplies and economic coercion,

among others, combine to make conventional military attacks more fearsome, as has been shown during the Russian invasion of Ukraine. It seems the narratives mentioned before seem to spread in the next years.

To explain them briefly, there are three characteristics of hybrid conflicts that determine current international relations. First, the uncertainty that surrounds hybrid conflicts, as they blurred the lines between war and peace, and they make it difficult to prove who is behind an attack. Second, the multiple tactics that are diversified to exploit the vulnerabilities of other States. Finally, the objectives of these tactics, seem to seek to erode the values and legitimacy of the adversary's political systems. You can learn more about them in this article in our newsletter: *The hybrid threat: Unpredictable warfare*.

In sum, hybrid threats comprise an area in which agents of different kinds are involved. For this reason, despite the great importance of cyber-attacks, we must take into account the rest of the threats and focus our attention on them. Although this phenomenon is not new, we should focus on how they will change and transform the world during 2023 and in the future, and how we can change the geopolitical agenda and be prepared to deter them

The future of the security landscape

The attack surface continues to expand as a result of digital transformation. In this way, the use of artificial intelligence in cyber attacks will make them much more complex, personalized, fast and difficult to detect. Furthermore, together with the continued sophistication of malware attacks, they will define the cybersecurity landscape throughout 2023. Due to the rise of cyber threats, which combine automated and human intervention attacks, users will have the ability to accelerate the end-to-end attack lifecycle, from reconnaissance to exploitation in the cyber sphere.

We are seeing an increase in cyber espionage in the geopolitical sphere. Geopolitics and technology are inseparable in today's geostrategic environment. More than ever, the geopolitical situation will have a significant impact on cybersecurity. The recent Russian-Ukrainian events have highlighted that the profiles of state-sponsored attackers are changing (deep technical skills, and resources required) and recent large-scale, high-profile hacks demonstrate this. Indeed, technology is at the centre of geostrategic competition, so we can expect an increase in cyber espionage and cyber sabotage. Companies in all sectors will need to identify political risks related to technology but also risks related to the geopolitical, national, regulatory and societal levels.

Moreover, disinformation campaigns powered by artificial intelligence are spreading throughout the world. Artificial intelligence-based computer programs have the ability to produce images, videos, and even voices. The main problem today is that anyone without the need for technical knowledge can generate this type of content using online software. In this way, cybercriminals can influence public opinion, create false images, and blatantly manipulate using machine learning technologies to precisely select the next victims and create social unrest. Fortunately, there are also data algorithms that detect false or manipulated content, comparing it with proven facts, by analyzing hundreds and thousands of pages, or posts, that contain similar data. However, semantic analysis is not always applicable, especially on certain encrypted platforms, so in 2023 it will be essential to be especially careful with manipulation and maintain a critical spirit.

We should also take into account data leaks as a manipulation weapon. One of the main concerns for 2023 is the risk of data leakage from civilian devices and networks, a type of threat being fueled by the resurgence of digital warfare. Medical data and, in general, all personal data will be the information most sought after by attackers. In addition to the use of this data for future phishing, smishing or social engineering attacks, whose objective is financial gain, these data thefts will be

increasingly used to influence and destabilize. Unlike industrial disinformation, the leaks are "real" data nations use.

For some years now, we have been witnessing an upsurge in massive data theft around the world. These threats are mainly perpetrated from outside the organization. Still, the threat from within tends to grow strongly and remains underestimated, which is why data leakage will have a large presence in 2023. Protecting personal data, the most valuable asset of companies has never been more pertinent.

The instrumentalization of mass migration

There is an extreme practice consisting of using migration as a threat when the country of origin “weaponises” these people or migrants threatening another country to direct them to the border or to stop doing any action that would avoid them from trying to enter the country. During the last three years, we have seen cases such as the Turkish government sending more than 13,000 people to the border with Greece in February 2020, or Morocco allowing more than 10,000 people to enter Ceuta (Spain) irregularly in May 2021. In 2021, it was the turn of the Belarusian regime, facilitating the arrival of thousands of people at the border with Poland, Latvia and Lithuania. In this context, Brussels has not hesitated to describe the arrivals of thousands of people as a serious "hybrid threat" to its "security". Moreover, NATO has also done it in its new Strategic Concept, where the "instrumentalization of migrations" by "authoritarian actors" is considered an attack on the sovereignty and territorial integrity of States.

The use of migratory flows for economic and political purposes is by no means new, but it is experiencing a particularly intense moment nowadays. In addition, human trafficking in the European Union has become an international problem affecting the Union from countries like Nigeria, China, Albania, Vietnam, and Morocco.

Conclusions

During the 21st century, the social perception of the terrible destructive capacity of weapons, the role played by the media the new war trends, and other factors, have produced awareness and sensitization of Western societies to violence and to the cruelty of war. On the other hand, threats have become global, which boosts international cooperation, as military victory has proven insufficient to achieve stable and lasting peace in the previous years.

High-intensity armed conflict continues to be a security challenge that is made more difficult to manage due to the new aspects that derive from changes and new trends in international society, linked to the processes that follow globalization (revolution of information and communication technologies, intensification of interdependence in all areas, privatization of all spheres of social life, etc.)

The transformations experienced in the armed conflict have not led to a safer world but, on the contrary, have exacerbated the difficulty of managing conflicts. Among the main reasons, we find the greater complexity of the disputes, both due to the multi-causality and the structural nature of many of them; the greater number of actors, and, above all, because of their diversity.

With their capabilities, the Armed Forces are one of the main actors in the response against hybrid threats: military deterrence, military cooperation, contribution to intelligence, activities in the information environment, contribution to the security of cyberspace, special operations, support for public safety and emergencies or, if necessary, use of ground combat capacity. Each state should

develop its own comprehensive crisis management model against hybrid threats to counteract them in aspects related to national security and defence and law enforcement since these aspects correspond to sovereign states.

Sources

"Amenaza híbrida: La guerra Imprevisible" https://publicaciones.defensa.gob.es/media/downloadable/files/links/a/m/amenaza_hibrida._la_guerra_imprevisible.pdf

"Cyberwar | Britannica." n.d. Accessed May 14, 2022. https://www.britannica.com/topic/cyberwar

Himmrich, Julia. 2018. "A 'Hybrid Threat'? European Militaries and Migration The Dahrendorf Forum."

"MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare | Enhanced Reader." n.d. Accessed May 26, 2022.

"New Threats to Human Security in the Anthropocene Demanding Greater Solidarity." n.d. Accessed May 23, 2022. http://hdr.undp.org.

"Post-Event Analysis of the Hybrid Threat Security Environment: Assessment of Influence Communication Operations

Votel, Joseph L, Charles T Cleveland, Charles T Connett, and Will Irwin. 2016. "Unconventional Warfare in the Gray Zone."