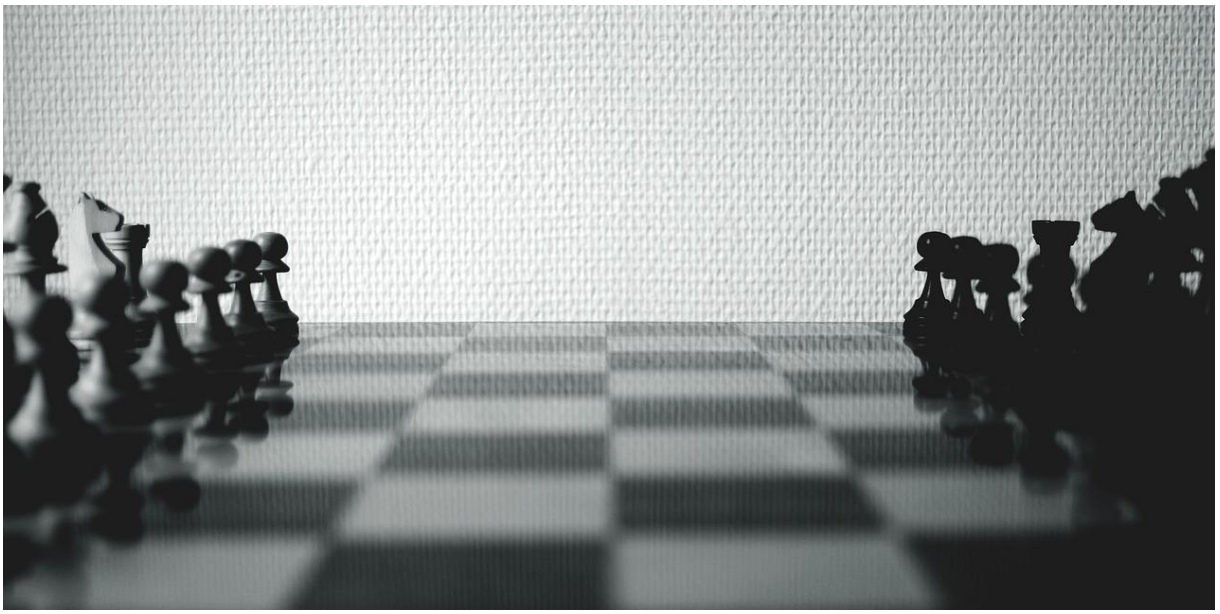
Newsletter January 2022



THE HYBRID THREAT: UNPREDICTABLE WARFARE

Ana Salas

Introduction: The Hybrid Threat

"The term hybrid threat was popularized after the 2006 clash between Israel and Hezbollah to designate the integration of unconventional and irregular tactics, techniques and procedures, mixed with terrorist acts, propaganda and connections with organized crime"[1]. The essential objective of the hybrid threat is to achieve results without resorting to actual warfare, putting societies against each other rather than armies, almost completely breaking down the distinction between combatants and citizens. The military objective takes a back seat.

The actions carried out within this type of conflict focus on the use of means such as cyber-attacks, disinformation and propaganda. They aim at exploiting economic, political, technological and diplomatic vulnerabilities, breaking communities, national parties, electoral systems and producing a great effect on the energy sector. These actions are not random, they are planned and organized.

[1] This idea became popular among the defence community after the presentation of the essay "Conflict in the 21st Century" by Guillem Colom Piella. (2019). The hybrid threat: myths, legends and realities. 2019, from Spanish Institute for Strategic Studies (IEEE).

These attacks are not linear in nature. They can have direct consequences elsewhere. For example, the drone strike on wells in Saudi Arabia in September 2019 had a direct impact on the global economy.

Cyberspace has become a novel aspect of this scenario. Thanks largely to the technological and information revolution, we are now facing a changing world order, in which the information provided by the media is accessible to anyone from anywhere in the world. It is no coincidence, therefore, that the Internet is one of the most important fronts when talking about hybrid warfare. In this field, the rules are not clearly established and states and non-state actors have a greater margin of action compared to the classic power of states. Fake news, disinformation and opinion-based facts are instruments at anyone's fingertips to influence public order.

Through manipulation in these areas, the hybrid enemy manages to considerably weaken one of the most important pillars of the state or community to which its actions are directed: the trust of citizens in their institutions. Ambiguity is one of the distinguishing characteristics of cyber activity. The hybrid enemy not only exploits to its advantage the difficulty inherent in the global network to attribute hostile actions to a specific actor, but also reinforces it through the use of hybrid strategies such as synchronization.

Cyberterrorism and hacktivism

As we have just seen, cyberspace is one of the preferred domains of the hybrid enemy. In it, he will frequently resort to cyberthreats, a cross-cutting threat whose authorship is very difficult to attribute. In most cases, it is not possible to substantiate it reliably, as in most cases there are only suspicions and it is very difficult to obtain proof. These cyberthreats can be divided into four blocks, which we will analyze one by one.

First, cyberespionage targets the political, economic and military spheres. Numerous states routinely resort to cyber espionage. Among them, China, Russia, Iran, or the United States of America stand out. States can carry out cyberespionage actions directly, using their intelligence services, or through interposed agents such as companies influenced by these states.

Secondly, cybercrime, most of which is mostly for profit, and whose impact on the global economy is estimated at 2% of the world's GDP. The main targets of cybercrime are information theft, fraud, money laundering, etc. It is often carried out by terrorist organizations, organized crime and hackers.

Thirdly, cyberterrorism, whose main objectives are to obtain information and all kinds of communications to citizens. The main agents, as can be deduced, are terrorist organizations and intelligence agencies.

Cyberterrorism has a number of advantages over conventional terrorism, and is that it guarantees greater security over anonymity. In addition, there is a greater cost-benefit ratio and in the geographical scope there is a great advantage in terms of delimitation. In Spain, there was a reform of terrorism crimes by the “Ley Orgánica” 2/2015, in which articles 571 to 580 of the Criminal Code were reformed in their entirety. In parallel, by means of the “Ley Orgánica” 1/2015, the reform of the Criminal Code has also been approved, which affects more than 300 articles.

Finally, in fourth place, hacktivism, whose main targets are web services, along with the theft and unauthorized publication of information. When hacktivism is used for the benefit of terrorism, it becomes terrorism. The Islamic Terrorist Group (DAESH), for example, uses cyber means to recruit men to its ranks. Two groups stand out as agents, the "Anonymous" group (press) and "Luizsec," in addition to the intelligence services themselves.

Cyberterrorism has very specific aims. To subvert the constitutional order, seriously disrupt social peace and destroy our global model. It is an emerging threat of low probability, but high impact. The main problem with all this is the little existing legislation in this regard, but which is gradually emerging. For example, in 2013, the starting point was given with the publication of a communication of the Council of the European Union on security, "European Union Cybersecurity Strategy"[2] , from which every 5 years these strategies must be reviewed. This is in addition to the regulation 2019/881 of the European Parliament and the Council (EU) of April 17, 2019.

Grey Zone

The concept of the Grey Zone has recently been coined in the field of strategic studies to describe the framework of the hybrid enemy. The term describes an alternative state of tension to war, operating at a stage of formal peace. The conflict in the Grey Zone is centered on civil society. Its cost, therefore, falls directly on the population. Coined, operating in any case within the limits of international legality.

The protagonist is generally a State of major international importance (a power) or a non-State actor of similar influence. The actions of an enemy operating in the "Grey Zone" are aimed at dominating certain "zones" that are of interest to it. The types of response within the defined "Grey Zone" will depend on the threat faced by the country in question.

Legal point of view

If we speak from a legal point of view, it is more accurate to use the term "hybrid warfare", only when there is a declared and not a covert armed conflict. Indeed, a major problem arises from the difficulty of applying the appropriate national or international legislation to hybrid threat actors. The actors involved, as a rule, deny hybrid actions and try to escape the legal consequences of their actions, taking advantage of the complexity of the legal system. They act by skirting the boundaries, operating in unregulated spaces and never exceeding the legal thresholds.

Responses to hybrid threats

The response to the hybrid threat can take place in different, but not mutually exclusive, spheres. In the military sphere, even a direct military confrontation can be conceived, which can be seen as "tolerable" if it avoids a confrontation with a great power such as the United States or China. In the same way, these military confrontations are respected because of the defenselessness of the occupied territories in the face of the threat that the occupying state intends to prevent.

In the economic sphere, response makes it possible to impose financial costs on an enemy, which are sometimes more direct than military responses. In this field, one way of adopting non-provocative defensive measures is through the imposition of immediate and formal economic sanctions on an aggressor. An example of this is the economic sanctions that the United States imposed against Iran for considering this country as a nuclear threat. To this end, it is important to highlight the background of this issue.

[2] Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. European Union Cybersecurity Strategy: An open, secure and safe cyberspace.

In 2015, the Joint Comprehensive Plan of Action (JCPOA) on Iran's nuclear program was signed, in which Iran committed to comply with the agreement, and the United States to remove the economic sanctions imposed. However, in 2018 Trump announced the withdrawal from the agreement and the reinstatement of sanctions. In the course of these developments, various countries have spoken out on these unilateral decisions taken by the US government. China and Russia, for their part, have expressed their disagreement, making official statements in favor of Iran.

The Iranian case is a clear example of an economic response to the Grey Zone in which we can see how states use this element of power to deny the aggressor's participation in different institutions or agreements and to control its zone of influence. The United States, like many other powers, finds this situation of superiority a decisive advantage in conflicts within the Grey Zone. Because of the importance of the financial and political power of the United States, the rest of the countries, including the European Union, cannot but accept this type of unilateral action.

Conclusions

In closing, we can conclude that hybrid activity in the Grey Zone has important consequences for society as a whole in one or more states, producing effects that can be global in scope.

Hybrid threats primarily affect civil society and can produce a demoralizing effect that can lead to the psychological collapse of a state. The employment of this tactic is often referred to as "formal peace." Despite the fact that there is no direct confrontation between armies, this technique is much more effective since the attacking country does not need to invest as much money, time and people as in real warfare. In addition, the application of international law, or the intervention of third countries in the conflict is minimal, as many consider this type of action as "tolerable."

Undoubtedly, the Grey Zone and hybrid threats have become the new military technique of our era due to their effectiveness and simplicity. However, there should be tighter control so that such harmful military techniques no longer go unnoticed. A characteristic aspect of hybrid warfare is the manipulation of communications and the use of propaganda. With them, it is possible to sow the distrust of citizens in their institutions, as is happening today in the relationship between China and the United States, weighed down by American statements to the press about the plan presented by Xi Jinping in 2014 on the New Silk Road, and which denote a high degree of distrust and rejection towards the Empire of the Center. It is therefore desirable that States and international institutions establish "rules of the game" for this type of actions and thus maintain world order and peace.

Sources

Carlos Galán. (2018). Amenazas híbridas: nuevas herramientas para viejas aspiraciones. 2019, de Real Instituto El Cano Sitio web: Amenaza-hibridas-nuevas-herramientas-para-viejas-aspiraciones.pdf

Guillem Colom Piella. (2019). La amenaza híbrida: mitos, leyendas y realidades. 2019, de Instituto Español de Estudios Estratégicos Sitio web: La-amenaza-híbrida-mitos-leyendas-y-realidades.pdf

Javier Jordán. (2019). Cómo contrarrestar estrategias híbridas. 2019, de Universidad de Granada Sitio web: Cómo%20contrarrestar%20estrategias%20híbridas.pdf

Javier Jordán. (2018). El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo. 2019, de Revista Española de Ciencia Política. Sitio web: https://recyt.fecyt.es/index.php/recp/article/view/64804/html_94

Javier Jordán. (2017). Guerra híbrida: un concepto atrápalo-todo. 2019, de Universidad de Granada Sitio web: https://www.seguridadinternacional.es/?q=es/content/guerra-h%C3%ADbrida-un-concepto-atr%C3%A1palo-todo

Josep Barqués. (2017). Hacia una definición del concepto "Grey Zone". 2019, de Instituto Español de Estudios Estratégicos. Sitio web: http://www.ieee.es/Galerias/fichero/docs_investig/2017/DIEEEINV02-2017_Concepto_GaryZone_JosepBaques.pdf

Lyle J. Morris, Michael J. Mazarr, Jeffrey W. Hornung, Stephanie Pezard, Anika Binnendijk, Marta Kepe. (2019). Gaining Competitive Advantage in the Grey Zone. 2019, de RAND CORPORATION Sitio web: https://www.rand.org/pubs/research_reports/RR2942.html

Murat Caliskan. (2019). Hybrid warfare through the lens of strategic theory. 2019, de Defense & Security Analysis, 35:1, 40-58 Sitio web: https://doi.org/10.1080/14751798.2019.1565364

Publisher: Geert Cami Senior Fellow: Jamie Shea Programme Manager: Mikaela d'Angelo Programme Assistant: Gerard Huerta Editor: Iiris André, Robert Arenella Design: Elza Lőw. (2018). HYBRID AND TRANSNATIONAL THREATS. 2019, de Friends of Europe Sitio web: HYBRID-AND-TRANSNATIONAL-THREATS.pdf

Rubén Arcos. (2019). EU and NATO confront hybrid threats in centre of excellence. 2019, de Jane's Intelligence Review Sitio web: EU-and-NATO-confront-hybrid-threats-in-centre-of-excellence.pdf

Una entrevista con Seyed Mohammad Marandi Universidad de Teherán. (2019). Los iraníes no olvidarán la guerra híbrida contra Irán. 2019, de Comunidad Saker Latinoamérica Sitio web: https://www.thetricontinental.org/wp-content/uploads/2019/08/190730_Dossier-19_ES-Web.pdf