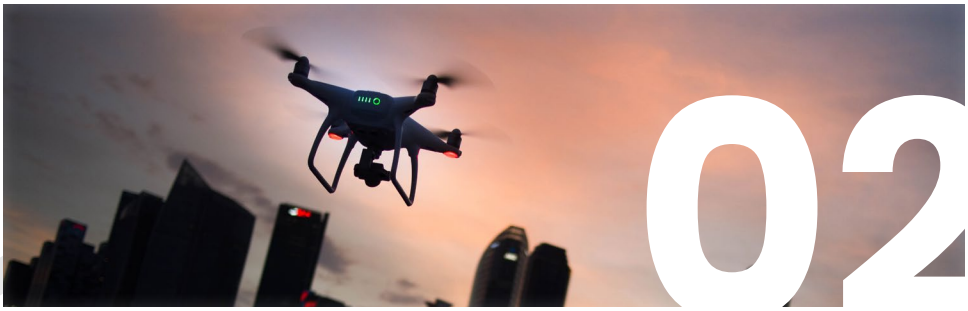
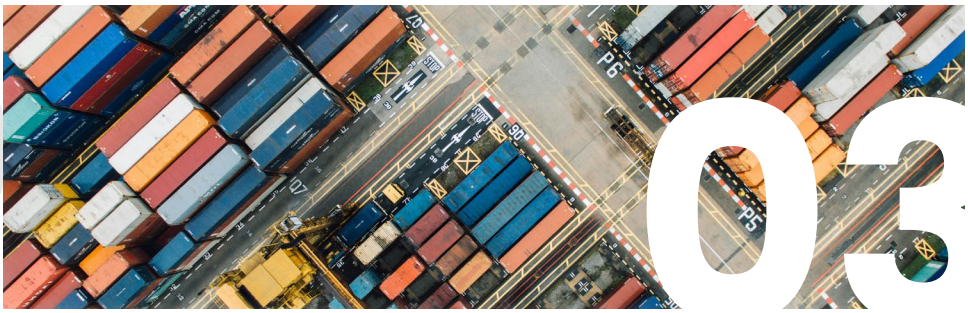
PROSEGUR RESEARCH

The age of constant conflict: navigating the gray zone

Security and Defense Series

PROSEGUR SECURITY





01

Hybrid threats: a blurred line

01 Hybrid threats: a blurred line

The growing complexity of the international environment over the past few decades—exacerbated by **conflicts and events with systemic impacts** in recent years—has popularized terms related to the blending of elements, such as hybrid warfare, hybrid threats, and hybrid tactics. However, several authors argue that this is neither a new nor an isolated phenomenon, citing historical examples of the use of strategies such as demoralization in the Punic Wars, which led to the destruction of Carthage as early as the 3rd and 2nd centuries B.C.

The concept of a hybrid threat, which gained traction in strategic and military circles at the beginning of the 21st century within the North Atlantic Treaty Organization (NATO), refers to **all actions and campaigns carried out by an adversary that deliberately and coordinately combine conventional and unconventional means** with the aim of exploiting various strategic vulnerabilities.

Despite divergent criteria and the lack of common academic definitions, all attempts to address the phenomenon are based on the same methodological and conceptual foundation:

Collaboration between state and non-state actors, including states, proxies, organized crime, and terrorist groups, which may work together depending on the objectives at hand.

The use of traditional means, such as the deployment of military force on the ground, **and unconventional means,** among which phenomena such as disinformation, cyberattacks, or the weaponization of the economy through tariffs or economic sanctions have gained prominence in recent years.

Coercion and destabilization as ends in themselves, undermining the rule of law, effective governance, and the strategic interests of any nation.

Complex attribution of responsibility, exploiting so-called detection thresholds, which hinders states' efforts at prevention and anticipation, as well as the activation of military commitments such as NATO's mutual assistance, among others.

The conceptual popularization of hybrid terminology in recent years has led to the use of various terms, which are described below with the aim of defining their scope of application, in accordance with the European Parliament's Research Service:

In summary, at Prosegur Research, we define **hybrid threats** as the set of hostile actions—whether planned or emerging—that result from **the convergence and interaction of actors of various kinds** (state, parastatal, proxies, criminal, terrorist, corporate, and others) pursuing multiple objectives (power, profit, influence, coercion, destabilization, or competitive advantage) and executed through the **synchronized or sequential combination of heterogeneous means** across **multiple domains** (physical, cyber, cognitive), with the aim of **altering the behavior** of an adversary (public or private, or both) or a population, **degrading capabilities, eroding legitimacy, gaining control, or imposing costs,** typically under conditions **of ambiguity, plausible deniability, and thresholding** (operating below the threshold of conventional response), exploiting systemic vulnerabilities, and generating **cumulative impacts.**

Thus, its four main dimensions are:

Convergence of actors

- **State actors** (intelligence services, security forces, coercive diplomacy).
- **Non-state** (organized crime, terrorism, militias)
- **Proxies** (front groups, exploited hacktivists)
- **Opportunistic ecosystems** (digital mercenaries, contractors)
- **"Gray" actors** (front companies, influence brokers)

Convergence of domains

- **Physical** (violence, sabotage, intrusion, blockades)
- **Cyber** (intrusion, ransomware, OT/IT manipulation)
- **Infocognitive** (disinformation, propaganda, narratives, social pressure)
- **Economic-regulatory**

Convergence of objectives

- **Power** (territorial control, sovereignty, geopolitical pressure)
- **Profit** (extortion, fraud, data theft, smuggling)
- **Influence** (public agenda, reputation, polarization)
- **Coercion** (forcing decisions, paralyzing, disciplining)
- **Destabilization** (eroding legitimacy, governance)
- **Strategic advantage** (competitive, technological, industrial)

Convergence of media and techniques

- Traditional and non-traditional weapons.
- Digital tools, social pressure, and legal exploitation.
- Regulatory capture and abusive litigation.
- Social engineering, doxxing, and offensive OSINT.
- Interference in international value chains.
- Data manipulation and public perception.

02

Tactics and objectives rooted in uncertainty

02

02 Tactics and objectives rooted in uncertainty

This exploitation of the gray zone is fundamentally based on uncertainty, which increases confusion and blurs the line between the concepts of peace and war. As reflected by institutions and research centers such as CIDOB, there are two aspects of hybrid conflicts and threats that must be taken into account, both rooted in uncertainty and the characteristics mentioned above.

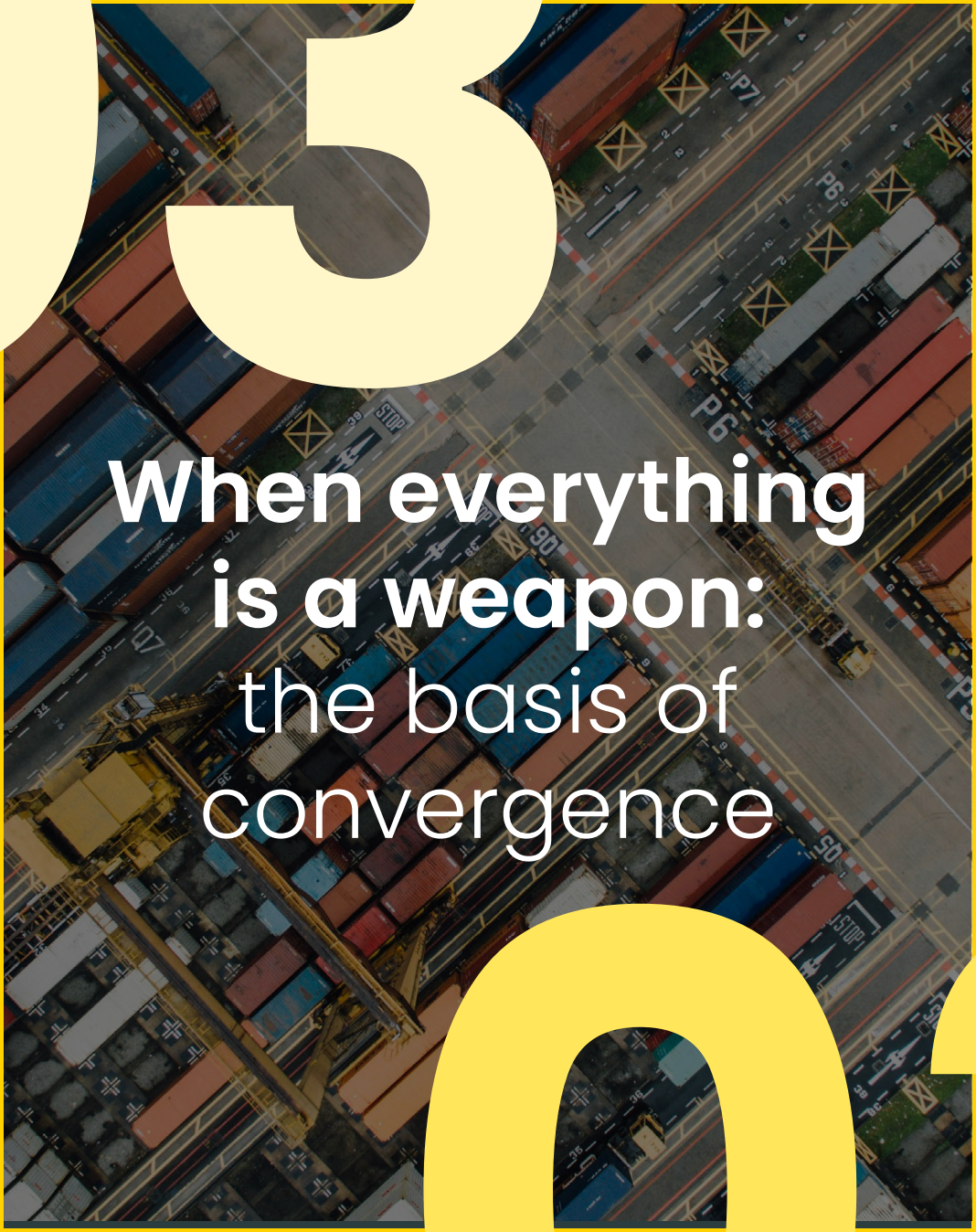
On the one hand, the deployment and use of various destabilization tactics have expanded significantly. Traditional tanks, firearms, and fighter jets are now complemented by new advancements in drones, hypersonic missiles, laser weapon systems, and specialized autonomous robotics. At the same time, state and non-state actors use tools such as espionage, disinformation, and interference in democratic processes and social peace, among others, with the aim of delegitimizing institutions, exploiting economic vulnerabilities, and creating a sense of uncontrolled chaos among the population and governments.

On the other hand, and closely linked to the combination of destabilization tactics, the attack surface of any nation or company has expanded. The formal declaration of war between states appears to have disappeared, so victory is not sought in the military sphere—or at least not solely there—but rather through the combination of areas of influence such as the erosion of democratic systems, the creation of political polarization, or the dismantling of international consensus. In this regard, numerous authors argue that the intended confrontation in hybrid scenarios is between the societies involved, not their armies.

By way of example, the table below describes some of the main tactics and their corresponding objectives most frequently used in the gray zone in recent years in various parts of the world:

Tactics	Objective	Examples
Disinformation	Political polarization and social conflict.	Interference in democratic processes, state-sponsored disinformation campaigns, etc.
Cyberattack	Data theft and control of critical infrastructure.	*Industroyer2 malware* in Ukraine (2022) aimed at compromising industrial control systems at energy suppliers.
Economic pressure	Sanctions or tariffs as tools of political coercion.	Blockade of rare earth exports from China to Japan (2010) due to the detention of a fishing vessel in disputed maritime areas.
Hybrid biomedical threat	The use of disinformation and smear campaigns as elements of geopolitical confrontation.	Increase in cyberattacks and conspiracy theories in the context of the COVID-19 pandemic.
Ataques contra las cadenas de suministro	Compromising suppliers to infiltrate networks or obtain information about private organizations and their client.	Trojanization of a SolarWinds update on the Orion server (2020).

03



When everything is a weapon: the basis of convergence

03 When everything is a weapon: the basis of convergence

In these times of intense competition, even everyday matters can become instruments of aggression, giving rise to the concept of the **"weaponization of everything"** which highlights h**ow even non-military tools**—such as trade tariffs, economic sanctions, migration flows, and technological disruption—**are used as weapons of pressure.** In this regard, the European Union considers hostile economic actions, such as export blockades, to be hybrid tactics.

The basis of all these operations is convergence, as they blend physical, logical, and social phases and elements that can impact one another. For example, a cybercriminal who gains access to a private organization's infrastructure to install malware via USB to sabotage systems and files, which could subsequently facilitate physical actions such as thefts or assaults. Similarly, a street protest can trigger an online campaign of disinformation and activism as destabilizing elements by state or non-state actors that threaten institutional stability.

Some of the most illustrative examples that have occurred in various parts of the world include:

Sony Pictures (2014)

A massive cyberattack that leaked confidential information, accompanied by an in-person intimidation campaign targeting employees.

U.S. Elections (2016)

A combination of cyber intrusions, email leaks, and media manipulation campaigns on social media were used to influence voters.

In a climate of crisis and institutional weakness, criminal organizations and terrorist groups can overlap and collaborate. Thus, **various transnational criminal networks** (drug trafficking, arms trafficking, smuggling, etc.) **are increasingly interconnected,** sharing logistics routes, funding, and even operatives, so that both forms of violence feed into one another.

Some institutions, such as EUROPOL, highlight that **the line between terrorism and organized crime in Europe** is blurring, with ideological motives becoming increasingly common in the actions of criminal groups.

In short, this gray area makes it easier for state actors to use criminal or terrorist proxies to carry out sabotage or attacks abroad, while these groups benefit from state resources.

04

Implications for businesses: critical security

04 Implications for businesses: critical security

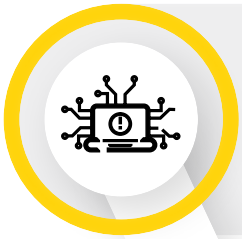
Hybrid threats are becoming increasingly relevant to the **private sector.** In fact, much of the **critical infrastructure**—energy, water, transportation, telecommunications, healthcare, etc.—is managed by private companies or protected by private security services. Data shows that in democratic countries, up to 90% of critical infrastructure is managed by private organizations, placing **the first line of defense** squarely on them. Consequently, a hybrid attack that compromises a power plant, a transportation system, or a communications network can trigger severe disruptions to public services, massive economic damage, and even social crises.

Recognizing this, the EU has enacted regulations to protect these sectors: for example, the Critical Infrastructure Resilience Directive (2022) requires that energy, water, transportation, and healthcare systems be able **to respond to and recover from hybrid attacks.** Likewise, the SRI2 Directive (2022) strengthens cybersecurity in both the public and private sectors against incidents and hybrid attacks.

For businesses, this means taking a comprehensive approach to security. Security guards and physical alarms are not enough: it is also critical to secure digital networks (OT/ICS), supply chains, and control systems. And in this environment, the convergence of criminal and terrorist activities and the diffuse nature of threats are forcing **the private security sector** to adapt. Security companies must incorporate cybersecurity capabilities, intelligence analysis, and technology monitoring, alongside traditional physical protection. Close public-private collaboration is essential: sharing intelligence, coordinating crisis exercises, and updating joint response protocols.

Therefore, **companies must include hybrid threats in their risk analyses and continuity plans.** Private security must be complemented by intelligence monitoring (CTI) and training programs to identify hybrid attacks (social engineering, unauthorized drones, etc.).

Ultimately, companies must consider hybrid threats as part of their overall risk analysis. A successful hybrid attack against a factory, a power grid, or a logistics platform can paralyze entire sectors and damage an organization's reputation. In this regard, the key recommendations are:



Strengthen comprehensive resilience

Develop contingency plans that address both physical failures (e.g., attacks or sabotage of facilities) and logical failures (cyber incidents). Adopt the principle of defense in depth, with multiple layers of defense.

Advanced technological protection

Implement multi-factor authentication and strict access controls for critical systems. Keep systems (both OT and IT) up to date and segment networks to limit lateral movement in the event of an intrusion.

Continuous monitoring and detection

Proactively monitor industrial (OT) and information systems using cyber intelligence tools. Identify anomalous patterns and adversaries' TTP deployments before they cause harm.

Staff training and awareness

Educate employees and security personnel on hybrid attack vectors (social engineering, phishing, information manipulation). A trained workforce is the first line of defense against disinformation or deception tactics.

Broad collaboration

Foster information sharing with authorities, CSIRTs, and other companies in the sector. Participate in intelligence-sharing forums on emerging threats. The global nature of hybrid threats makes this cooperation vital.

Exercises and red teaming

Conduct drills and penetration tests that combine physical and cyber scenarios. For example, simulate a physical sabotage followed by a simultaneous cyberattack to assess the joint response from physical security and IT.

We guarantee the security of individuals, businesses, and society as a whole.

For more information, please contact
research@prosegur.com
www.prosegurresearch.com

PROSEGUR
SECURITY