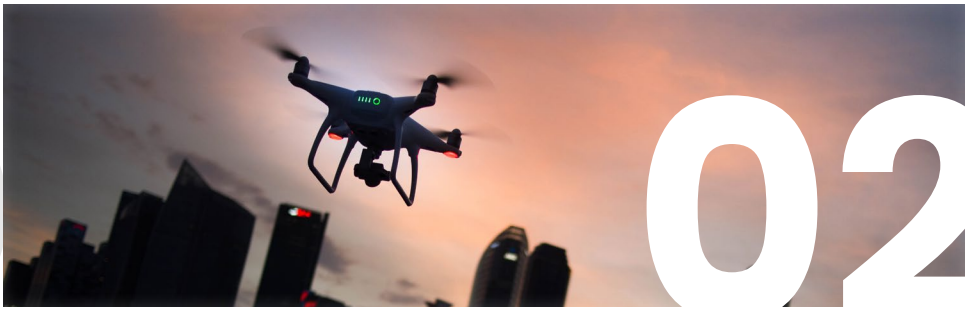
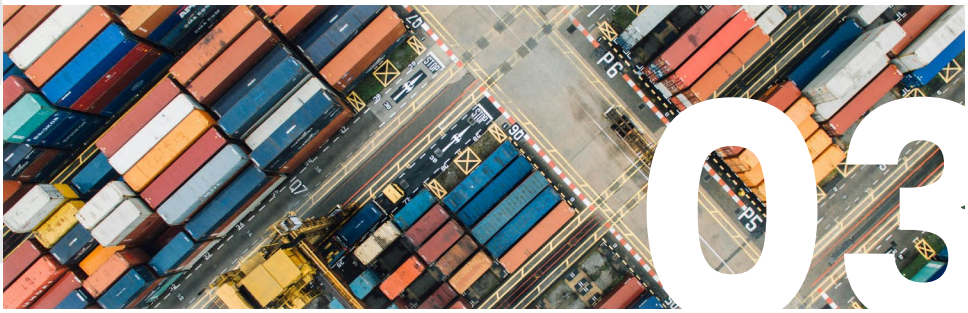
PROSEGUR RESEARCH

La era del conflicto permanente: navegando en la zona gris

Security and Defense Series

PROSEGUR SECURITY





01

Amenazas híbridas: una frontera difusa

01 Amenazas híbridas: una frontera difusa

La creciente complejidad del entorno internacional durante las últimas décadas, intensificado por **conflictos y fenómenos con impacto sistémico** en los últimos años, ha popularizado términos relacionados con la hibridación de elementos, tales como guerra híbrida, amenaza híbrida o técnica hibrida. No obstante, son diversos los autores que defienden que no se trata de un fenómeno nuevo ni aislado, con ejemplos históricos de empleo de estrategias como la desmoralización en las guerras púnicas que derivó en la destrucción de Cartago ya en los siglos III y II a.C.

El concepto de amenaza híbrida, difundido en el ámbito estratégico-militar a principios del siglo XXI en la Organización del Tratado del Atlántico Norte (OTAN), se refiere a **todas aquellas acciones y campañas llevadas a cabo por un adversario que combinan de manera simultánea medios convencionales y no convencionales** de manera deliberada, coordinada y con el objetivo de explotar diferentes vulnerabilidades estratégicas.

A pesar de la divergencia de criterios y la falta de definiciones académicas comunes, todos los intentos de abordar el fenómeno se sustentan sobre la misma base metodológica y conceptual:

Involucración común entre actores estatales y no estatales, incluyendo Estados, proxies, crimen organizado y grupos terroristas, que pueden colaborar según la conveniencia de los objetivos.

Empleo de medios tradicionales, como el uso de la fuerza militar sobre el terreno, y **medios no convencionales,** entre los cuales fenómenos como la desinformación, los ciberataques o la armamentización de la economía mediante aranceles o sanciones económicas han ganado protagonismo durante los últimos años.

Coacción y desestabilización como fines, socavando el Estado de derecho, la gobernanza efectiva y los intereses estratégicos de cualquier nación.

Atribución de autoría compleja, explotando los denominados umbrales de detección, lo que dificulta las labores de prevención y anticipación por parte de los Estados, así como la activación de compromisos militares como la asistencia mutua de la OTAN, entre otros.

La popularización conceptual de la terminología híbrida durante los últimos años ha derivado en la utilización de diversos términos, que a continuación se describen con el objetivo de delimitar su ámbito de aplicación siguiendo el Servicio de Estudios del Parlamento Europeo:

En resumen, desde Prosegur Research entendemos las **amenazas híbridas** como el conjunto de acciones hostiles —planificadas o emergentes— que resultan de la **convergencia e interacción** de **actores de diversa naturaleza** (estatales, paraestatales, proxies, criminales, terroristas, corporativos u otros), orientadas a **fines múltiples** (poder, lucro, influencia, coerción, desestabilización o ventaja competitiva) y ejecutadas mediante la **combinación sincronizada o secuencial** de **medios heterogéneos** en **múltiples dominios** (físico, ciber, infocognitivo), con el objetivo de **alterar el comportamiento** de un adversario (público o privado, o ambos) o una población, **degradar capacidades, erosionar legitimidad, obtener control o imponer costes,** normalmente bajo condiciones de **ambigüedad, negación plausible y umbralización** (operar por debajo del umbral de respuesta convencional), explotando vulnerabilidades sistémicas y generando **impactos acumulativos.**

Así, son cuatro sus dimensiones principales:

Convergencia de actores

- **Estatales** (servicios, fuerzas, diplomacia coercitiva).
- **No estatales** (crimen organizado, terrorismo, milicias).
- **Proxies** (grupos fachada, hacktivistas instrumentalizados).
- **Ecosistemas oportunistas** (mercenarios digitales, contractors).
- **Actores "grises"** (empresas pantalla, brokers de influencia).

Convergencia de dominios

- **Físico** (violencia, sabotaje, intrusión, bloqueo).
- **Ciber** (intrusión, ransomware, manipulación OT/IT).
- **Infocognitivo** (desinformación, propaganda, narrativas, presión social).
- **Económico-regulatorio.**

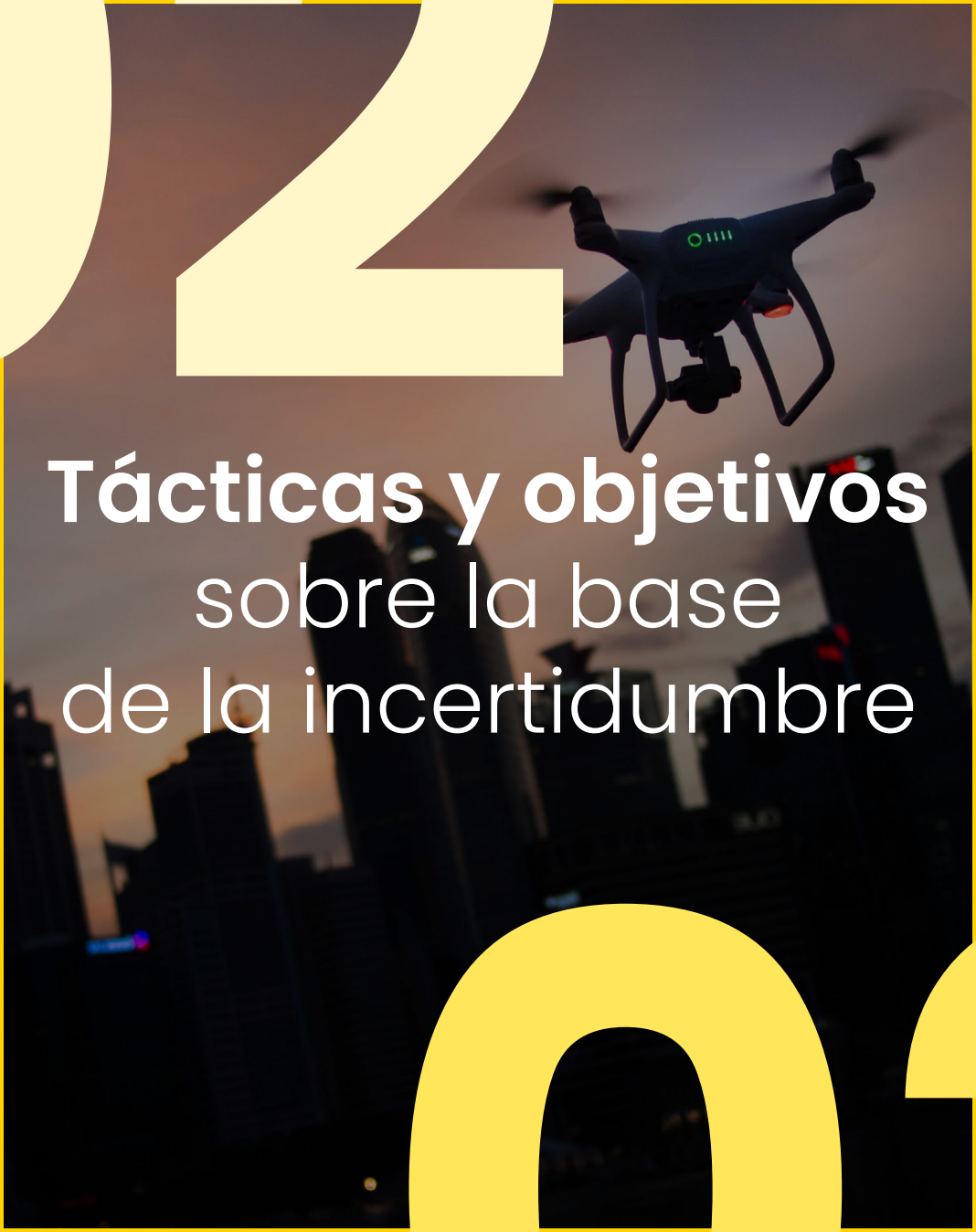
Convergencia de fines

- **Poder** (control territorial, soberanía, presión geopolítica).
- **Lucro** (extorsión, fraude, robo de datos, contrabando).
- **Influencia** (agenda pública, reputación, polarización).
- **Coerción** (forzar decisiones, paralizar, disciplinar).
- **Desestabilización** (erosionar legitimidad, gobernanza).
- **Ventaja estratégica** (competitiva, tecnológica, industrial).

Convergencia de medios y técnicas

- Armas tradicionales y armas no tradicionales.
- Herramientas digitales, presión social y explotación jurídica.
- Captura regulatoria y litigios abusivos.
- Ingeniería social, doxxing y OSINT ofensivo.
- Interferencia en cadenas de valor internacionales.
- Manipulación de datos y percepción pública.

02



Tácticas y objetivos sobre la base de la incertidumbre

02 **Tácticas y objetivos** sobre la base de la incertidumbre

Esta explotación de la zona gris tiene como elemento esencial la **incertidumbre,** incrementando la confusión y la delimitación entre los conceptos de paz y guerra. Tal y como reflejan instituciones y entornos de estudio como el CIDOB, son dos los aspectos de los conflictos y las amenazas híbridas que deben tenerse en cuenta, fundamentadas sobre la base de la incertidumbre y las características anteriormente mencionadas.

Por un lado, se ha ampliado significativamente el **despliegue y utilización de tácticas variadas de desestabilización.** Los tradicionales tanques, armas de fuego o aviones de combate se complementan con nuevos avances en materia de drones, misiles hipersónicos, sistemas de armas láser y robótica autónoma especializada. Al mismo tiempo, actores estatales y no estatales utilizan herramientas de espionaje, desinformación o injerencia en procesos democráticos y paz social, entre otros, con el objetivo de deslegitimar instituciones, explotar vulnerabilidades económicas y generar una sensación de desbordamiento descontrolado entre la población y los gobiernos.

Por otro lado, y estrechamente ligado con la combinación de tácticas de desestabilización, **se ha aumentado la superficie de ataque de cualquier nación o empresa.** La declaración formal de guerra entre Estados parece haber desaparecido, por lo que no se persigue una victoria en el ámbito militar, o al menos no únicamente, sino combinar áreas de influencia como el desgaste en sistemas democráticos, creación de polarización política o eliminación de consensos internacionales. En este sentido, son variados los autores que sostienen que **el enfrentamiento pretendido en escenarios híbridos es entre las sociedades involucradas,** no el de sus ejércitos.

A modo de ejemplo, en la tabla se describen algunas de las principales tácticas y sus correspondientes objetivos más utilizadas en la zona gris durante los últimos años en diversas partes del mundo:

Táctica	Objetivo	Ejemplo
Desinformación	Polarización política y enfrentamiento social	Injerencia en procesos democráticos, campañas de desinformación financiadas por Estados, etc.
Ciberataque	Robo de datos y control de infraestructuras	*Malware Industroyer2* en Ucrania (2022) con el objetivo de afectar sistemas de control industrial en proveedores energéticos.
Presión económica	Sanciones o aranceles como herramientas de coacción política.	Bloqueo de exportaciones de tierras raras desde China hacia Japón (2010) por la retención de un pesquero en zonas marítimas disputadas.
Amenaza híbrida biomédica	Utilización de campañas de desinformación y desprestigio como elemento de confrontación geopolítica.	Incremento en ciberataques y teorías de la conspiración en el contexto de la pandemia de COVID-19.
Ataques contra las cadenas de suministro	Comprometer proveedores para infiltrar redes u obtener información sobre organizaciones privadas y sus clientes.	Troyanización de actualizaciones de SolarWinds en el servidor de Orion (2020).

03

Cuando todo es un arma: la base de la convergencia

03 Cuando todo es un arma: la base de la convergencia

En estos tiempos de competición exacerbada, hasta lo cotidiano puede devenir instrumento de agresión, de donde deriva el **"weaponization of everything"** (que se podría traducir en "todo como arma"), y que destaca que **incluso herramientas no militares** —tarifas comerciales, sanciones económicas, flujo migratorio, disrupción tecnológica— **son utilizadas como armas de presión.** En este sentido, la Unión Europea considera que acciones económicas hostiles como el bloqueo de exportaciones constituyen tácticas híbridas.

La base de todas estas operaciones es la convergencia, puesto que se mezclan fases y elementos físicos, lógicos y sociales y que pueden repercutir sobre los mismos. Por ejemplo, un ciberdelincuente que logra acceder a las infraestructuras de una organización privada para instalar un malware vía USB para sabotear sistemas y archivos que pueda facilitar consecuentemente acciones en el plano físico como robos o asaltos. De igual modo, una protesta callejera puede desencadenar una campaña en línea de desinformación o activismo como elementos desestabilizadores por parte de actores estatales o no estatales que amenacen la estabilidad institucional.

Algunos de los ejemplos más ilustrativos que han ocurrido en diversas partes del mundo durante los últimos años incluyen:

Sony Pictures (2014)

Un ataque cibernético masivo que filtró información confidencial al mismo tiempo que se utilizó una campaña de intimidación presencial contra empleados.

Elecciones en Estados Unidos (2016)

La combinación de intrusiones digitales, filtración de correos y campañas de manipulación mediática en redes sociales se utilizaron con la finalidad de influir en el voto de los ciudadanos.

En ambientes de crisis y debilidad institucional, organizaciones delictivas y grupos terroristas pueden solaparse y colaborar. Así, **diversas redes criminales transnacionales** (tráfico de drogas, armas, contrabando, etc.) **están cada vez más interconectadas,** compartiendo rutas logísticas, financiamiento e incluso militantes, de manera que ambas formas de violencia se retroalimentan.

Algunas instituciones, como EUROPOL, destacan que **la línea entre terrorismo y crimen organizado en Europa se está difuminando,** siendo los motivos ideológicos cada vez más comunes en las actuaciones de los grupos criminales.

En suma, la zona gris facilita que actores estatales utilicen proxies criminales o terroristas para acometer sabotajes o atentados en el extranjero, mientras estos grupos se benefician de recursos estatales.

04

Impactos para las empresas: seguridad de lo crítico

04 Impactos para empresas: seguridad de lo crítico

Las amenazas híbridas son cada vez más relevantes para el **sector privado.** De hecho, muchas **infraestructuras críticas** -energía, agua, transporte, telecomunicaciones, salud, etc.- están gestionadas por empresas privadas o custodiadas por servicios de seguridad privados. Algunos datos destacan que en los países democráticos hasta el 90% de las infraestructuras críticas están gestionadas por organizaciones privadas, situando consecuentemente la **primera línea de defensa** sobre las mismas. Por ello, un ataque híbrido que comprometa una planta eléctrica, un sistema de transporte o una red de comunicaciones puede desencadenar graves interrupciones de servicios públicos, daños económicos masivos e incluso crisis sociales.

Reconociendo esto, la UE ha promulgado normas para proteger estos sectores: por ejemplo, la Directiva sobre Resiliencia de Entidades Críticas (2022) exige que energía, agua, transporte y salud puedan **responder y recuperarse de ataques híbridos.** Asimismo, la Directiva SRI2 (2022) refuerza la ciberseguridad en el ámbito público y privado frente a incidentes y ataques híbridos.

Para las empresas, esto implica reevaluar la seguridad con visión integral. No basta con guardias y alarmas físicas: también es crítico blindar redes digitales industriales (OT/ICS), cadenas de suministro y sistemas de control. Y en este entorno, la convergencia criminal-terrorista y el carácter difuso de las amenazas obligan a la **seguridad privada** a adaptarse: las compañías de seguridad deben incorporar capacidades de ciberseguridad, análisis de inteligencia y vigilancia tecnológica, junto con la protección física tradicional. La estrecha colaboración público-privada es esencial: compartir información de inteligencia, coordinar ejercicios de crisis y actualizar protocolos de respuesta conjunta.

Por ello, **las empresas deben incluir las amenazas híbridas en sus análisis de riesgo y planes de continuidad.** La seguridad privada debe complementar con monitoreo de inteligencia (CTI) y programas de formación para identificar ataques híbridos (ingeniería social, drones no autorizados, etc.).

En definitiva, las empresas deben considerar las amenazas híbridas como parte de su análisis de riesgo global. Un ataque híbrido exitoso contra una fábrica, una red eléctrica o una plataforma logística puede paralizar sectores enteros y dañar la reputación organizativa. En este sentido, las recomendaciones clave son:

Fortalecer la resiliencia integral

Diseñar planes de contingencia que aborden fallos tanto físicos (p. ej., atentados o sabotaje de instalaciones) como lógicos (incidentes cibernéticos). Adoptar el principio de *seguridad en profundidad,* con múltiples capas de defensa.

Protección tecnológica avanzada

Implementar autenticación multifactor y estrictos controles de acceso para sistemas críticos. Mantener actualizados los sistemas (tanto OT como IT) y segmentar redes para limitar movimientos laterales en caso de intrusión.

Monitorización y detección continua

Vigilar proactivamente los sistemas industriales (OT) y de información con herramientas de ciberinteligencia. Identificar patrones anómalos y despliegues de TTP de adversarios antes de que causen daño.

Formación y concienciación del personal

Educar a empleados y vigilantes en los vectores híbridos (ingeniería social, phishing, manipulación informativa). Un personal capacitado es la primera línea de defensa contra tácticas de desinformación o engaño.

Colaboración amplia

Fomentar el intercambio de información con autoridades, CSIRTs y otras empresas del sector. Participar en foros de inteligencia compartida sobre amenazas emergentes. La naturaleza global de las amenazas híbridas hace vital esta cooperación.

Ejercicios y red teaming

Realizar simulacros y pruebas de penetración que combinen escenarios físicos y cibernéticos. Por ejemplo, simular un sabotaje físico seguido de un ataque informático simultáneo para evaluar la respuesta conjunta de seguridad física y TI.

Garantizamos la seguridad de las personas, las empresas y la sociedad en su conjunto.

Para más información contacte con
research@prosegur.com
www.prosegurresearch.com

PROSEGUR
SECURITY