



Qué es la Guerra Híbrida y cómo nos afectan las Amenazas Híbridas

LISA Institute*

Guerra Híbrida

Qué es la Guerra Híbrida y cómo nos afectan las Amenazas Híbridas



El **cibespacio** se presenta como el escenario preferido de las **nuevas formas de conflicto**. En los últimos años cobran un especial protagonismo los **conflictos híbridos**, que combinan el uso de la fuerza militar con otros elementos como pueden ser los ciberataques, la manipulación de la información a través de internet y de redes sociales, o vectores de presión económica.

El desarrollo de las nuevas tecnologías y su fácil acceso facilitan que estas acciones puedan provenir de cualquier parte del mundo, tanto por parte de **actores estatales como no estatales**, y de forma más rápida que en otras épocas, por lo que **su prevención y respuesta resulta más complicada**.



Una cuestión muy importante a tener en cuenta es el **potencial de aplicación de las amenazas híbridas** en situaciones muy diversas, donde se incluyen los procesos electorales, en los que se puede llegar a erosionar la soberanía e integridad de nuestros países.

En este artículo vamos a ahondar en este **concepto de “Guerra Híbrida” o “amenaza híbrida”**, así como **conocer los objetivos, principales riesgos** y, por último, **cuáles son las medidas preventivas y reactivas** hacia este fenómeno.

Definición de guerra híbrida, conflicto híbrido y amenaza híbrida

Antes de nada, debemos aclarar que aunque encontremos términos como **guerra híbrida, amenaza híbrida o ataque híbrido**, utilizados como si significasen lo mismo, en realidad no es así. Como podemos encontrar definido en el documento *Amenazas híbridas: nuevas herramientas para viejas aspiraciones* de Carlos Galán, estos conceptos quedarían definidos de la siguiente manera:

- **Amenaza híbrida:** Fenómeno resultante de la convergencia e interconexión de diferentes elementos que, en conjunto, constituyen una amenaza más compleja y multidimensional.
- **Conflicto híbrido:** Situación en la cual las partes se abstienen del uso abierto de la fuerza (armada) y actúan combinando la intimidación militar (sin llegar a un ataque convencional) y a la explotación de vulnerabilidades económicas, políticas, tecnológicas y diplomáticas.
- **Guerra híbrida:** Situación en la que un país recurre al uso abierto de la fuerza (armada) contra otro país o contra un actor no estatal, además de usar otros medios (por ejemplo, económicos, políticos o diplomáticos).

Los 5 principales objetivos de las amenazas híbridas

Como se señala en el documento mencionado anteriormente, las amenazas híbridas han venido persiguiendo, entre otros objetivos:



- **Erosionar la confianza** de los ciudadanos en sus empresas e instituciones.
- **Generar desconfianza** en el sistema democrático, político y administrativo.
- **Socavar la cohesión social o los modelos sociales** de los Estados, de las comunidades políticas (como la UE) o de las organizaciones internacionales (la OTAN, por ejemplo).
- **Fragilizar el sistema de gestión o gobierno** para que tenga menos capacidades.
- **Convencer de la decadencia de un sistema político o empresarial** (tanto a la población de la víctima como a su propia población).

Riesgos y amenazas de la guerra híbrida

Como vemos, las **amenazas híbridas** persiguen alcanzar sus objetivos estratégicos **influyendo en la toma de decisiones de sus víctimas y socavando sus valores, su estructura social y la confianza de la población**. Ello, facilitado por la difuminación de las dimensiones internas y externas de la seguridad de los Estados que ha traído consigo el desarrollo del ciberespacio. Lugar desde el que **hoy es más fácil que nunca modificar creencias, actitudes, preferencias, opiniones, expectativas, emociones o predisposiciones** de los demás para actuar.

Cabe destacar que recientemente en España, tanto en la Estrategia Nacional de Seguridad 2018 como en la Estrategia Nacional de Ciberseguridad 2019 se advierte de la constatación de una **tendencia creciente de las denominadas amenazas híbridas**, definidas como "acciones coordinadas y sincronizadas dirigidas a atacar de manera deliberada las vulnerabilidades sistémicas de los estados democráticos y las instituciones, a través de una amplia gama de medios, tales como acciones militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica (...)".

"(...) Actores estatales y no estatales, bien de forma directa o a través de intermediarios, **explotan las facilidades que ofrece Internet** para la desinformación y propaganda y un interés generalizado en la obtención y desarrollo de capacidades militares para operar en el ciberespacio, incluyendo en muchos casos medios y capacidades ofensivas".



Medidas preventivas y reactivas contra la guerra híbrida

A) Respuestas de la Unión Europea

Como mencionábamos al principio de este artículo, **los períodos electorales suponen un objetivo especialmente estratégico y vulnerable**. Por ello, la Unión Europea lleva un tiempo desarrollando la capacidad necesaria para combatir estas amenazas a fin de **generar resiliencia y una adecuada respuesta colectiva** a través de las siguientes medidas:

Conciencia situacional

Para luchar contra las **amenazas híbridas** se ha creado una célula dentro del Servicio Europeo de Acción Exterior, considerada ya un activo importante para recibir y analizar información en este ámbito mediante análisis de inteligencia. Varios profesores de LISA Institute que colaboran en esa tarea manifiestan que todavía necesita acumular más conocimientos especializados para poder hacer frente a todo el espectro de este tipo de amenazas. Por lo que, desde la Comisión Europea se ha manifestado la intención de **que la célula se amplíe mediante componentes especializados en** materia química, biológica, radiológica y nuclear (QBRN), **en contrainteligencia y en ciberanálisis**.

Comunicación estratégica

Otra de las medidas es **seguir desarrollando las capacidades de comunicación estratégica de la UE**, para lo que asegurarán una interacción y una coherencia sistemáticas entre las distintas estructuras existentes. Esta capacidad se extenderá a otras instituciones y Estados miembros de la Unión Europea, e incluirá la **plataforma online protegida sobre** desinformación.

Desarrollo de la resiliencia y la disuasión en el sector de la ciberseguridad



La Unión Europea viene proponiendo diversos **medios para reforzar las capacidades y luchar contra las ciberamenazas**, como la propuesta de marco de certificación de la ciberseguridad, el mandato para la ampliación y la modernización de la **Agencia de Ciberseguridad de la Unión Europea**, las pautas de la cooperación entre los Estados miembros y las agencias de la UE en caso de ataque y el conjunto de instrumentos de ciberdiplomacia. En esta línea, se está construyendo una plataforma específica de formación y educación para coordinar la formación en materia de ciberdefensa.

Desarrollo de la resiliencia frente a las actividades de inteligencia hostiles

La coordinación entre los Estados miembros y entre estos y otras organizaciones internacionales, en particular la OTAN, es crucial. En este sentido, el Servicio Europeo de Acción Exterior y la Comisión aplicarán medidas prácticas perfeccionadas que sustenten y amplíen la **capacidad interactiva de la UE para repeler la actividad de inteligencia hostil dirigida contra las Instituciones tanto de servicios de inteligencia estatales como privados**. La célula de fusión híbrida se reforzará mediante conocimientos especializados en contrainteligencia, lo que le permitirá presentar análisis detallados y sesiones informativas.

B) Respuestas del Consejo de Europa

Por su parte, la Asamblea Parlamentaria del Consejo de Europa ha elaborado las siguientes recomendaciones para sus Estados miembros:

1. **Abstenerse de recurrir a las acciones híbridas en las relaciones internacionales** y respetar plenamente las disposiciones del Derecho Internacional, en particular los principios de soberanía, integridad territorial e inviolabilidad de las fronteras, de acuerdo con su objeto y fin, sin explotar abusivamente de las lagunas o ambigüedades percibidas.
2. **Intensificar la cooperación internacional para identificar adversarios híbridos y todo tipo de amenazas de guerra híbridas**, y establecer el marco legal aplicable.
3. **Mantener intercambios de información sobre las agresiones híbridas** en Europa y compartir experiencias y buenas prácticas para contrarrestar tales amenazas.



4. **Tomar medidas para aumentar la conciencia de los ciudadanos** sobre las amenazas híbridas y su capacidad para reaccionar rápidamente ante tales amenazas.
5. **Firmar, ratificar e implantar el Convenio sobre la Delincuencia de Budapest** y promover su ratificación por parte de Estados no miembros.
6. **Mantener y reforzar las medidas adoptadas por la Unión Europea y la Organización del Tratado del Atlántico del Norte (OTAN)** para contrarrestar las amenazas híbridas, y reforzar la cooperación en este ámbito.
7. **Hacer un llamamiento** a todos los Estados miembros del Consejo de Europa que, simultáneamente, sean miembros de la Unión Europea y la OTAN **para que compartan sus mejores prácticas para contrarrestar las amenazas híbridas** con otros Estados miembros que puedan verse afectados por este fenómeno.
8. En relación con las medidas destinadas a contrarrestar la guerra híbrida, la Asamblea recuerda su **Resolución 1840 (2011) sobre derechos humanos y lucha contra el terrorismo**. Además, hace un llamamiento a los Estados miembros para que velen por que tales medidas respeten los requisitos derivados del Convenio Europeo de Derechos Humanos, de conformidad con la jurisprudencia del Tribunal Europeo de Derechos Humanos. En particular, en lo que respecta a los derechos sujetos a restricciones en virtud del Convenio, cualquier limitación debe basarse en la ley, ser proporcional al objetivo legítimo perseguido (por ejemplo, la seguridad nacional) y “necesario en una sociedad democrática”.

***Nota del Comité Editorial:** El problema que afectó a Chile en octubre de 2019 y actualmente a los países de Europa occidental que apoyan a Ucrania ante su guerra con Rusia.*

LISA Institute. Centro de formación online en inteligencia, seguridad, criminología y análisis internacional (España). Extracto lisainstitute.com