2026

INTELIGENCIA EN ACCIÓN

Pax Consulting

15-06-2026

Índice

1. RUSIA EN ACCIÓN

Investigaciones recientes han revelado que **Jan Marsalek, un fugitivo vinculado al escándalo de Wirecard**[1], ha estado operando en Moscú bajo una identidad falsa, **dirigiendo una red de espionaje** rusa. Sus actividades incluyeron la gestión de una célula de espionaje búlgara, lo que ha suscitado preocupaciones sobre el valor operativo que tiene para la inteligencia rusa. La condena de **Egisto Ott, exdirector de inteligencia austriaco,** por haber transmitido información clasificada a Marsalek, subraya la **penetración de la inteligencia rusa en los servicios** occidentales. Esta situación sugiere un esfuerzo sostenido de contrainteligencia contra las redes rusas que operan en Europa, con al menos una nueva acusación prevista para septiembre de 2026 y relacionada con las investigaciones posteriores al escándalo Wirecard.

Rusia está intensificando significativamente **sus operaciones de inteligencia diseñadas para socavar las instituciones democráticas** en Occidente. La estrategia del Kremlin está cambiando hacia tácticas altamente agresivas, apoyándose en gran medida en **campañas de influencia habilitadas por IA y manipulación en redes** sociales para explotar las divisiones sociales. Recordando a las tácticas históricas soviéticas, estas operaciones buscan sembrar discordia entre grupos étnicos y sociales mezclando desinformación con provocaciones directas. Los analistas estiman que **, a medida que Rusia enfrenta un creciente aislamiento internacional, su dependencia de estas tácticas para debilitar la confianza pública en los procesos democráticos solo aumentará.**

Recientemente se observó una aplicación directa de estas tácticas de guerra híbrida en **Rumanía**, tras incursiones rusas de drones. Tras la autodetonación de un dron en una instalación de la OTAN, operativos rusos lanzaron una **campaña coordinada de desinformación en línea que manipuló las narrativas en redes sociales para amplificar mensajes alarmistas y desacreditar las cuentas oficiales del gobierno.** En represalia a estas amenazas percibidas y actividades de inteligencia, **el gobierno rumano expulsó al personal diplomático** ruso.

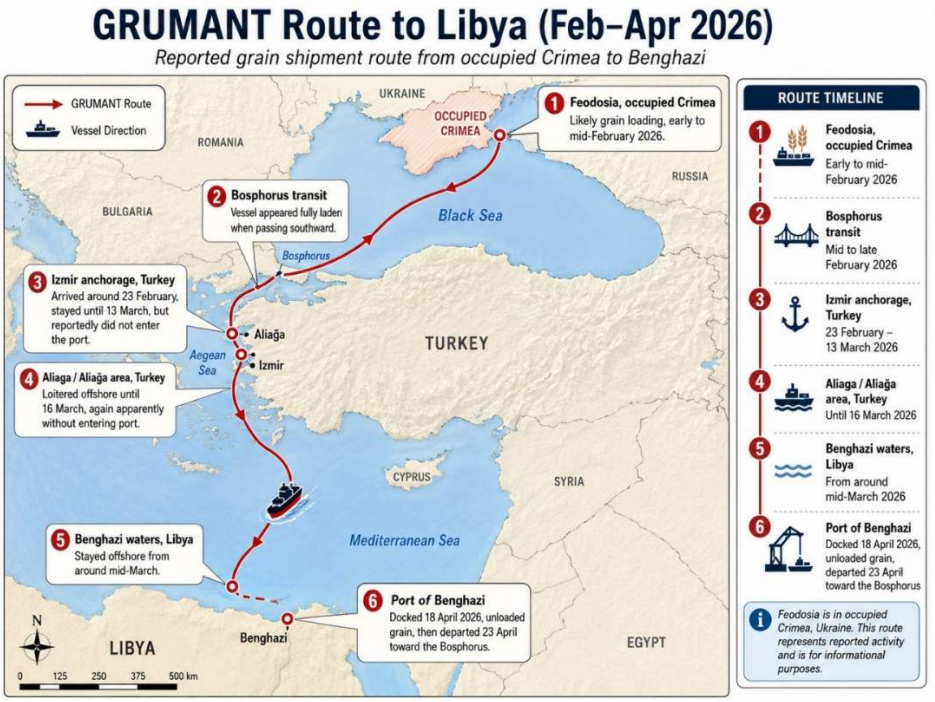
La inteligencia y los operativos militares rusos utilizan **cada vez más activos marítimos** para operaciones

[1] El escándalo de Wirecard se refiere al colapso en 2020 de la empresa alemana de procesamiento de pagos Wirecard después de que los auditores no pudieran verificar 1.900 millones de euros en supuestos saldos de caja, lo que ha puesto al descubierto un fraude contable, fallos en auditorías y debilidades regulatorias.

encubiertas, evasión de sanciones y guerra híbrida. Se **ha descubierto una red de mercenarios rusos con experiencia en servicios militares y de inteligencia —vinculados a empresas militares privadas como Wagner y Redut— operando a bordo de una "flota oscura" en el mar Báltico.** Estos operativos armados viajan en buques que transportan petróleo para la estatal Rosneft, donde vigilan a las tripulaciones de los barcos, hacen cumplir el cumplimiento de las directivas rusas y resisten las solicitudes de la OTAN. La presencia de estos mercenarios con experiencia en combate suscita **serias alarmas sobre posibles operaciones de sabotaje** contra países vecinos de la OTAN, especialmente Dinamarca.

Además, **Rusia está eludiendo las sanciones internacionales mediante sofisticadas operaciones de contrabando de** grano. Se ha observado que buques como el granelero *Grumant* cargan grano ucraniano robado en puertos ocupados como Feodosia (Crimea ocupada por Rusia) y **lo entregan a Libia[2].** Para ocultar estas operaciones, los buques rusos emplean prácticas de navegación engañosas, como operar deliberadamente en áreas con interferencia conocida del GNSS (Sistema Global de Navegación por Satélite), apagar el AIS o ocultar la identidad del buque.

El contrabando de grano llevado a cabo por la flota en la sombra ha sido utilizado en gran medida por Rusia en Siria y Egipto. Es significativo la expansión de este tipo de operaciones a Libia.



[2] Hizo escala en el puerto de Bengasi, coherente con el apoyo que Moscú ha estado prestando a Khalifa Hafter, líder del Ejército Nacional Libio.

Más allá de Europa, la inteligencia rusa está ampliando su influencia **aprovechando los vacíos de poder, especialmente en Afganistán. Moscú ha asegurado un acuerdo técnico-militar con los talibanes** que facilita **el intercambio de inteligencia, posibles transferencias de armas y la integración directa de contratistas militares** rusos en las estructuras de seguridad talibanes. Aunque esta asociación se presenta públicamente como un esfuerzo conjunto contra el terrorismo contra ISIS-K, sirve **a los intereses estratégicos más amplios de Rusia al establecer una firme base geopolítica en la región,** beneficiando mutuamente la necesidad de legitimidad militar de los talibanes mientras socava deliberadamente la influencia histórica estadounidense.

2. CAPACIDADES IRANÍES Y REVESES

Las fuerzas iraníes han demostrado un cambio significativo en las tácticas adversariales al **aprovechar datos comerciales** de localización para rastrear al personal estadounidense durante operaciones militares en Yemen. Esto se logró porque los identificadores publicitarios en dispositivos emitidos por el gobierno estadounidense seguían activos, exponiendo vulnerabilidades críticas en la seguridad operativa estadounidense. Además, **el panorama cibernético de Irán está siendo activamente objetivo de Estados Unidos; según se informa, la NSA está personalizando el modelo de IA Mythos de Anthropic para llevar a cabo operaciones cibernéticas ofensivas contra redes iraníes.**

En relación con los continuos enfrentamientos militares de Irán tanto con Estados Unidos como con Israel, Irán ha lanzado ataques con drones y misiles, aunque **los ataques recientes han sido interceptados con éxito por los estados del Consejo de Cooperación del Golfo** (CCG). Impulsados por la amenaza que representa Irán, los países del CCG—especialmente Emiratos Árabes Unidos, Arabia Saudí y Catar—están **invirtiendo fuertemente en infraestructuras avanzadas de inteligencia, fusión de datos habilitada por IA y redes integradas de sensores** para reforzar sus capacidades de defensa.

Las hostilidades geopolíticas han sumido a **Irán en una grave crisis económica.** El país se enfrenta a una **posible contracción económica de dos dígitos** causada por una combinación de sanciones estadounidenses, un bloqueo al Estrecho de Ormuz y ataques militares que han paralizado su capacidad industrial. Esto ha provocado un aumento desorbitado de la inflación de bienes esenciales y la pérdida

de aproximadamente 2 millones de empleos desde el inicio de los actuales conflictos militares.

En respuesta a la agitación económica y a la disidencia pública, **el régimen iraní ha implementado cortes de internet** durante protestas y periodos de guerra para sofocar la comunicación y aislar a sus ciudadanos. Aunque **el régimen mantiene la resiliencia militar**, se evalúa que sin una resolución de las sanciones internacionales y reformas internas significativas, Irán seguirá enfrentándose **a una profunda agitación social e inestabilidad** política. Esta situación tan grave podría ayudar a alcanzar un acuerdo con Estados Unidos.

3. OPERACIONES CIBERNÉTICAS Y VIGILANCIA

La NSA está usando la IA del Mito no solo contra Irán, sino también, por supuesto, contra los intereses chinos. **Esta iniciativa pone de manifiesto una fractura en la gobernanza federal de la IA, a medida que avanza a pesar de una prohibición más amplia del Departamento de Defensa sobre el uso de productos Anthropic.**

Las amenazas cibernéticas están alcanzando tal nivel que, para contrarrestarlas, **el FBI ha abierto un "Rango Cibernético Cinético" en Alabama.** Esta instalación está diseñada para simular ciberataques reales, sirviendo de puente entre las investigaciones digitales y la forense física. Muestra el camino a seguir para las agencias occidentales.

Cada vez se reconoce más a las entidades cibernéticas comerciales por su papel en **la influencia de los procesos democráticos.** La agencia francesa Viginum[3] atribuyó recientemente actividades de interferencia electoral —que incluyeron la creación de una falsa organización palestina de ayuda— a una **empresa israelí llamada** [4]BlackCore. A pesar de esta atribución pública, es poco probable presentar cargos penales contra los principales responsables de la firma debido a desafíos jurisdiccionales internacionales.

La principal acusación es que BlackCore operaba o ayudaba a coordinar **campañas de influencia online** utilizando cuentas falsas o proxy, sitios web engañosos, imágenes generadas por

---

[3] **Viginum** es el servicio gubernamental francés para detectar y analizar **operaciones de interferencia digital extranjera.**

[4] BlackCore **no aparece en el registro de empresas israelíes y** su presencia en línea ha desaparecido; esto dificulta la verificación de su estructura corporativa, personal, clientes y estatus legal a partir de fuentes abiertas.

IA, mensajes políticos y posiblemente anuncios digitales pagados.

Blackcore ha estado activo en diferentes países, no solo en Francia... Supuestamente:

País / contexto electoral	Supuesto objetivo o actividad
Francia	Campaña contra tres candidatos de La France Insoumise / LFI antes de las elecciones locales.
Escocia	Atacando a John Swinney, el SNP y el gobierno escocés.
Nueva York	Sospecha de interferencia en torno a las elecciones a la alcaldía de 2025.
Angola y Togo	Mencionados por las autoridades francesas como teatros sospechosos adicionales.

En el contexto **de BlackCore**, Viginum importa porque las autoridades francesas supuestamente utilizaron el análisis de Viginum para **identificar sospechas de actividad de interferencia digital extranjera vinculada a esa empresa** israelí. Así que, cuando un informe dice "Viginum encontrado" o "Viginum acusado", significa que la acusación proviene del organismo oficial francés responsable de vigilar la interferencia extranjera en línea.

3.1 Tecnologías de vigilancia.

Las tecnologías de vigilancia digital y el software espía se están volviendo omnipresentes, suponiendo **graves riesgos para las libertades civiles**, especialmente en contextos autoritarios. Organizaciones como Citizen Lab[5] han sido fundamentales para destapar estas prácticas, como la vigilancia del periodista financiero Thanasis Koukakis en Grecia.

Koukakis se convirtió en la primera gran víctima de Predator confirmada públicamente **en Grecia** y en un símbolo de la superposición entre el software espía comercial, la vigilancia de inteligencia, la libertad de prensa y los problemas de estado de derecho dentro de la UE.

[5] Citizen Lab también es conocido por haber desvelado varios casos de uso de Pegasus por parte de agencias de inteligencia.

El Departamento de Estado de EE. UU. está obteniendo licencias para el controvertido software de reconocimiento facial Clearview AI , destinado a su uso por la Policía Nacional de Colombia. Aunque está destinada a combatir el narcotráfico y el crimen organizado, el despliegue de esta tecnología plantea importantes preocupaciones éticas y de privacidad.

La intersección entre la seguridad nacional y el deporte está impulsando el debate continuo en torno a las prácticas de vigilancia en la próxima Copa del Mundo. En España, **LaLiga** (responsable de la Premier y Segunda Liga del fútbol nacional) **ha estado asesorando al FBI sobre sistemas de reconocimiento facial** usados en el pasado en estadios para identificar a los delincuentes entre el público. El departamento tecnológico de LaLiga cuenta con un presupuesto impresionante. LaLiga ha creado recientemente un departamento de tecnología, innovación e inteligencia artificial para potenciar sus capacidades.

Está claro que las agencias de inteligencia sí reciben apoyo de los jefes de seguridad de los clubes y de las autoridades deportivas para llevar a cabo sus tareas.

La vigilancia espacial y la posterior recopilación de inteligencia están siendo transformadas por la fusión de radar de apertura sintética (SAR) y sistemas satelitales electro-ópticos. Impulsadas por inteligencia artificial para un procesamiento rápido de datos, estas constelaciones en órbita baja terrestre permiten una vigilancia persistente y continua de infraestructuras y activos **militares independientemente de las condiciones meteorológicas.** Este seguimiento persistente amenaza las estrategias tradicionales de ocultación, incluidas las utilizadas para disuasiones nucleares móviles por carretera.

4. DINÁMICA DE INTELIGENCIA REGIONAL

Los servicios de inteligencia húngaros están experimentando una gran reestructuración tras un cambio político alejándose de la administración de Viktor Orbán. **El recién nombrado jefe de seguridad nacional, Péter Buda, pretende despolitizar las agencias tras años de influencia política.** Su experiencia en contrainteligencia señala un cambio hacia un marco operativo más transparente y responsable. Aunque **el objetivo es adaptarse al actual**

panorama internacional de seguridad y restaurar las relaciones de intercambio de inteligencia con socios de la OTAN y la UE, estos aliados probablemente requerirán pruebas demostrables de una mejor gobernanza y transparencia antes de reanudar plenamente la cooperación. La UE y el Club de Berna[6] ya han sufrido la segregación de la Agencia Austriaca doméstica durante años después de que Rusia, profundamente, la penetraran.

Aunque el caso de Hungría no es el mismo, está por verse cuán fiable es la nueva estructura por parte de los socios extranjeros. **Los servicios húngaros requerirán una operación interna de limpieza para borrar cualquier sombra de influencia o cooperación rusa.**

El Pentágono está siendo objeto de escrutinio por una importante brecha en la ejecución de la política; las fuerzas estadounidenses en Yemen fueron rastreadas con éxito por fuerzas iraníes que explotaron datos de localización comercial.

Esto fue posible porque los identificadores publicitarios en dispositivos emitidos por el gobierno se dejaban activados durante operaciones críticas.

La **CIA** está lidiando con las consecuencias de un **enorme fallo interno en la supervisión.** Un agente de la CIA, David J. Rush, fue **arrestado por presuntamente malversar más de 42 millones de dólares en oro y efectivo** mediante la creación de un programa de acceso especial falso, exponiendo graves vulnerabilidades a amenazas internas dentro de programas altamente clasificados de EE. UU.

Entre abril y junio de 2026, **las agencias francesas de inteligencia y seguridad** estuvieron públicamente vinculadas a varios asuntos importantes: **aumento del gasto en fondos especiales** (hasta 160,4 millones de euros[7]), actividad de cibercoordinación de la ANSSI, mensajes de seguridad interna de la DGSI y controversias relacionadas con la DGSE en Georgia (el servicio de seguridad georgiano expuso una **operación** de reclutamiento de la DGSE y que tres oficiales de la DGSE en Tiflissi fueron llamados de vuelta) y Malí (Malí condenó a un oficial francés de la DGSE, identificado como "Yann V.", a **20 años de prisión** por presuntos delitos de seguridad estatal. Francia calificó las acusaciones de

---

[6] Es un **foro informal europeo de intercambio** de inteligencia que reúne a los jefes o altos representantes de los servicios de seguridad y inteligencia nacionales de **los estados miembros de la UE, además de Noruega y Suiza.** No es **una institución de la UE.**

[7] Si te interesa la asignación de presupuestos en agencias de inteligencia, visita https://paxconsulting.blog/2026/04/30/security-culture/

infundadas y afirmó que el oficial tenía estatus diplomático).

Estos episodios ilustran **la ampliación del ámbito de la inteligencia francesa, pasando del espionaje clásico** y la lucha antiterrorista a amenazas híbridas, ciberdefensa, manipulación de información y protección de material clasificado.

5. CONCLUSIÓN

La naturaleza cambiante de las tácticas de guerra híbrida, especialmente en el contexto de las operaciones rusas, presenta **desafíos para anticipar y contrarrestar campañas de desinformación.** Además, las implicaciones de las tecnologías emergentes en la vigilancia y las operaciones cibernéticas requieren una evaluación continua para garantizar respuestas políticas efectivas.

La interacción entre las operaciones de inteligencia y las tensiones geopolíticas requiere un enfoque integral de la seguridad. A medida que los países navegan por estas complejidades, el enfoque en mejorar **la transparencia operativa, la rendición de cuentas y la cooperación internacional será fundamental para abordar amenazas emergentes y salvaguardar las instituciones** democráticas. El panorama en evolución subraya la importancia de las estrategias adaptativas en los marcos de inteligencia y seguridad para responder eficazmente a los múltiples desafíos del entorno global contemporáneo.