ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

95/2025 17 de noviembre de 2025

Juan José Terrero Carrobles **

El cambio de estrategia del espionaje ruso en Europa

El cambio de estrategia del espionaje ruso en Europa

Resumen:

La forma en que Rusia lleva a cabo sus actividades de espionaje en Europa ha cambiado. La guerra en Ucrania y el endurecimiento de la seguridad en los países europeos han provocado que un gran número de agentes reclutados y entrenados formalmente por los servicios secretos del Kremlin hayan sido capturados y/o expulsados de sus lugares de operación. Con estos recursos fuera de juego, Moscú se ha visto obligada a recurrir a métodos menos ortodoxos para reclutar y movilizar nuevos agentes, considerando incluso recursos «desechables» y más difíciles de detectar. La vigilancia de objetivos y posiciones, así como la obtención de información y recursos sensibles y críticos, tanto físicos como digitales, por parte de agentes secretos rusos y prorrusos, son esenciales para el desarrollo de estrategias de naturaleza híbrida, que implican incidentes de sabotaje, influencia y distorsión de los procesos políticos, y ciberataques contra los Estados europeos.

Palabras clave:

Rusia, Europa, espionaje, seguridad, amenazas híbridas.

Juan José Terrero Carrobles*

The shift in the Russian espionage's strategy in Europe

Abstract:

The way in which Russia conducts its espionage activities in Europe has changed. The war in Ukraine and the tightening of security in European countries has meant that a large number of the agents formally recruited and trained by the Kremlin's secret services have been captured and/or expelled from their places of operation. With these resources out of play, Moscow has been forced to resort to less orthodox methods to recruit and mobilize new agents, even considering resources both "disposable" and more difficult to detect. Surveillance of targets and positions, as well as obtaining sensitive and critical information and resources – both physical and digital – by Russian and pro-Russian secret agents are essential to the development of strategies of a hybrid nature, entailing incidents of sabotage, influence and distortion of political processes, and cyber-attacks upon European States.

Keywords:

Russia, Europe, espionage, security, hybrid threats.

Cómo citar este documento:

TERRERO CARROBLES, Juan José. *El cambio de estrategia del espionaje ruso en Europa*. Documento de Opinión IEEE 95/2025. enlace web IEEE y/o enlace bie[3] (consultado día/mes/año)

Introducción

El espionaje ruso es un arma letal silenciosa que se dirige desde los servicios secretos del Kremlin hacia todos los rincones de Europa. Moscú pretende llevar a cabo una desestabilización política, debilitando alianzas occidentales como la OTAN y la Unión Europea (UE) mediante recursos como el espionaje. Los agentes secretos rusos y las operaciones que llevan a cabo están orientados a provocar inestabilidad interna y desconfianza en las instituciones europeas, así como a lograr un desacoplamiento entre Estados Unidos y Europa en términos políticos, de seguridad y económicos. Al promover una narrativa basada en el euroescepticismo y la idea del declive occidental, Rusia intenta dividir a los europeos, ampliar su influencia en Europa del Este promoviendo la adopción de modelos autoritarios, y también fomentar sus proyectos económicos, como los numerosos gasoductos que atraviesan todo el continente[1].

Los espías e informantes rusos participan en operaciones que son parte de estrategias de desestabilización más amplias y de naturaleza híbrida que podrían identificarse en tres pilares principales. El primero es la desinformación generalizada, mediante la distribución de noticias falsas y propaganda en línea y la manipulación de la opinión pública. El segundo es el sabotaje, que comprende la interrupción de infraestructuras críticas como redes de energía, redes de telecomunicaciones o rutas de transporte vitales, entre otras. El tercero es el lanzamiento de ciberataques dirigidos contra organismos gubernamentales, empresas e infraestructuras con el fin de robar datos críticos e interrumpir sus operaciones[2].

[1] European Values. (2019). *Handbook on Countering Russian and Chinese Interference in Europe*. Report. Konrad Adenauer Stiftung. European Values. Disponible en: https://www.europeanvalues.cz/wp-content/uploads/2020/10/Handbook-on-Countering-Russian-and-Chinese-Interference-in-Europe.pdf (Consultado el 03/09/2025).

[2] Gündoğar, A. (18 de noviembre de 2024). *A Shadow War: How Russian Spies are Attacking Europe*. Medium. Disponible en: https://salvacybersec.medium.com/a-shadow-war-how-russian-spies-are-attacking-europe-14c9e065bd46 (Consultado el 03/09/2025).

El uso de las mencionadas estrategias de amenazas híbridas que Moscú está empleando contra los países europeos se ha reforzado especialmente con el estallido de la guerra en Ucrania. Sin embargo, a causa de este conflicto, muchos agentes rusos y prorrusos han sido capturados y expulsados del territorio europeo. Ahora Rusia está cambiando su estrategia para reintroducir agentes e informadores que no sólo extraen información y recursos críticos, sino que también pueden proporcionar datos que ayuden a provocar sabotajes, ciberataques o injerencias en instituciones a nivel nacional y europeo. No obstante, antes de proceder al análisis del porqué de este gran cambio táctico en los servicios secretos del Kremlin, es necesario considerar brevemente cómo se encuentra organizada la inteligencia rusa, qué tipo de espías rusos existen y qué operaciones han llegado a realizar antes de la invasión de febrero de 2022.

El espionaje ruso antes de la guerra de Ucrania

Tras el colapso de la Unión Soviética en diciembre de 1991, se disolvió toda la estructura de seguridad e inteligencia que se encontraba mayormente integrada en el seno del Comité para la Seguridad del Estado (KGB). Por lo tanto, durante el gobierno de Boris Yeltsin en la recién conformada Federación Rusa, existía la necesidad de rearticular órganos capaces de albergar dichas competencias. En 1992 se creó en primer lugar el Ministerio de Seguridad (MB), el cual fue sustituido por el Servicio Federal de Contrainteligencia (FSK) un año más tarde. Este último fue finalmente reemplazado por el Servicio Federal de Seguridad (FSB), el cual funciona desde 1995 hasta el día de hoy. Es de destacar que el actual presidente ruso Vladimir Putin llegó a ejercer como director del FSB entre 1998 y 1999[3], antes iniciar su andadura política hacia la cima del Kremlin.

Al margen de las funciones de seguridad nacional, espionaje, contrainteligencia y control de fronteras que posee el FSB, en 1991 se creó el Servicio de Inteligencia Exterior (SVR), encargado de recopilar información clasificada de carácter político, económico y militar en el extranjero. A esto se le añade la presencia de la Dirección Principal del Estado

[3] García, C. (1 de noviembre de 2022). *¿Qué es el Servicio federal de Seguridad? (FSB) ruso?* El Orden Mundial (EOM). Disponible en: https://elordenmundial.com/que-es-fsb-servicio-federal-seguridad-rusia/ (Consultado el 28/08/2025).

Mayor de las Fuerzas Armadas de la Federación Rusa (GRU), cuyas labores se llevan a cabo en el ámbito de la inteligencia militar[4]. Estas tres agencias citadas, a pesar de la presencia de otras relevantes como el Servicio Federal de Protección (FSO) o la agencia de investigación submarina (GUGI), podrían ser consideradas como los principales actores de la seguridad e inteligencia rusa.

Tanto el FSB como el GRU y el SVR actúan bajo el mando de órganos institucionales coordinados desde el ejecutivo ruso. Desde el año 2022, el Primer Jefe Adjunto del Estado Mayor Presidencial ruso, Sergey Kiriyenko, creó el Comité de Influencia Especial, órgano encargado de asignar a los servicios especiales rusos tareas específicas en países objetivo. El secretario ruso del Consejo de Seguridad Nacional (NSU), Sergei Shoigu, también puede orientar ciertas decisiones junto con un Comité propio para autorizar determinadas actividades relacionadas con estas operaciones, como las provocaciones violentas[5].

Los servicios de inteligencia rusos coordinan las operaciones de espionaje y contrainteligencia llevadas a cabo por un gran número de redes compuestas por agentes secretos e informantes entrenados y formados en el seno de dichos organismos. Estos individuos pueden clasificarse de dos maneras: por su rango de actuación y por el "criterio legal" que les es aplicado desde el Kremlin. En cuanto al primer factor, pueden distinguirse cuatro tipologías. Los agentes secretos rusos pueden ser "falsos diplomáticos", operando desde embajadas en el extranjero protegidos por un visado diplomático. Los funcionarios y políticos rusófilos de otros países también ejercen como informantes, bien motivados por sobornos o por afinidad ideológica. Por otro lado, Moscú también emplea agentes encubiertos ilegales, los cuales viven una vida aparentemente normal bajo una tapadera discreta, llegando incluso a ocultar su perfil durante varios periodos de tiempo. También hay que distinguir las redes o células durmientes, consistiendo en grupos de agentes encubiertos cuya misión se basa en la observación,

[4] Montoya, M. (13 de febrero de 2023). *¿Cuáles son los servicios de inteligencia rusos?* El Orden Mundial (EOM). Disponible en: https://elordenmundial.com/cuales-son-servicios-inteligencia-rusos/ (Consultado el 28/08/2025).
[5] Jones, S. G. (18 de marzo de 2025). *Russia's shadow war against the West.* Defense and Security Department. CSIS. Disponible en: https://www.csis.org/analysis/russias-shadow-war-against-west#h2-russian-actors (Consultado el 28/08/2025).

el establecimiento de contactos y el intento de acceso a posibles objetivos para llevar a cabo sus operaciones[6].

En cuanto al criterio de legalización establecido por el Kremlin, que distingue dos tipos de estatus en función de la duración. El primer tipo son los agentes "plenamente" legalizados, que suelen permanecer en sus destinos por tiempo indefinido. El segundo tipo son los agentes "parcialmente" legalizados, cuyas misiones son a corto plazo y asumen niveles básicos de escrutinio por parte de los organismos de Inteligencia o de aplicación de la ley del gobierno de destino en el lugar de destino[7].

Este tipo de actores directamente asociados con los servicios de inteligencia rusos ya han llevado a cabo numerosas operaciones de espionaje y estrategias de carácter híbrido en Europa antes del estallido de la guerra en Ucrania. En el caso del GRU, destacan las actividades de sus Unidades 29155 y 54654. La primera mencionada está organizada en un conjunto de redes operativas, logísticas, de planificación y entrenamiento, cuyo personal se despliega en Europa normalmente bajo legalización parcial. Miembros de este grupo fueron los principales acusados de estar detrás del envenenamiento del ex oficial del GRU y desertor ruso Sergei Skripal en 2018, quien estaba siendo perseguido porque había compartido información sensible del GRU con la Inteligencia británica. Además, en 2020, esta Unidad también fue señalada tras el envenenamiento del líder de la oposición Aleksei Navalny. En cuanto a la Unidad 54654, esta habilita agentes "totalmente legalizados" considerados como operativos encubiertos ilegales. Esto se lleva a cabo mediante la elaboración de perfiles y reclutamiento de personas con experiencia militar u otros antecedentes, incluyendo también a estudiantes extranjeros en universidades rusas y a contratistas a través de empresas tapadera. Por otra parte, también infiltra a sus propios agentes en ministerios rusos no relacionados con la defensa y en empresas privadas rusas con fines de vigilancia[8].

[6] Mac Dougall, D., and Reid, S. (18 de agosto de 2023). *Espías como nosotros: ¿Cómo opera la red de inteligencia rusa en Europa?* Euronews. Disponible en: https://es.euronews.com/2023/08/18/espias-como-nosotros-como-opera-la-red-de-inteligencia-rusa-en-europa (Consultado el 28/08/2025).

[7] Jones, S. G. (18 de marzo de 2025). *Russia's shadow war against the West*. Defense and Security Department. CSIS. Disponible en: https://www.csis.org/analysis/russias-shadow-war-against-west#h2-russian-actors (Consultado el 28/08/2025).

[8] Jones, S. G. (18 de marzo de 2025). *Russia's shadow war against the West*. Defense and Security Department. CSIS. Disponible en: https://www.csis.org/analysis/russias-shadow-war-against-west#h2-russian-actors (Consultado el 28/08/2025).

Además del GRU, también es relevante señalar otros casos atribuidos al SVR, que cuenta con ciber-unidades como la Unidad Nobelium, también conocida como APT29. En septiembre de 2023, y de forma paralela al conflicto ucraniano, esta unidad participó en una ciber-ofensiva dirigida contra las cuentas diplomáticas y los ministerios de Asuntos Exteriores de Azerbaiyán, Italia, Grecia y Rumanía. Esta ofensiva se extendió a proveedores de servicios de Internet y organizaciones internacionales y consistía en ataques de phishing mediante señuelos de documentos de venta de vehículos diplomáticos, que contenían un virus que explotaba una vulnerabilidad en el programa utilizado para comprimir, descomprimir y gestionar los archivos respectivos. Al manipular los archivos, se abría una brecha en los sistemas que permitía a los agentes de APT29 obtener datos sensibles sobre las transacciones comerciales de los países miembros de la UE con Azerbaiyán[9].

La guerra en Ucrania como punto de inflexión en el espionaje ruso sobre Europa

Con el estallido de este conflicto, las operaciones de la inteligencia rusa en territorio europeo se vieron gravemente afectadas debido a tres factores. El primero de ellos fue la expulsión de los cuerpos diplomáticos de las embajadas rusas en Estados europeos. En noviembre de 2022, el director general del Servicio de Seguridad británico, Ken McCallum, declaró que más de 600 funcionarios diplomáticos rusos habían sido expulsados de Europa, siendo 400 de ellos considerados espías. La mayoría de los países europeos han confirmado que estas expulsiones se deben a transgresiones de la Convención de Viena en materia de amenazas a la seguridad nacional y espionaje[10]. El resultado de estas expulsiones ha supuesto la pérdida para el Kremlin de una infraestructura clave formada por informadores que podían seguir en primera persona

[9] National Security and Defense Council of Ukraine. (s.f.). *APT29 Attacks Embassies using CVE-2023-38831*. pp. 2-5. Disponible en: https://www.rnbo.gov.ua/files/2023_YEAR/CYBERCENTER/november/APT29%20attacks%20Embassies%20using%20CVE2023-38831%20-%20report%20en.pdf (Consultado el 28/08/2025).

[10] Gotev, G. (17 de noviembre de 2022). *MI5 chief says expulsion of 400 Russian spies across Europe has delivered significant blow*. Euractiv. Disponible en: https://www.euractiv.com/section/global-europe/news/mi5-chief-says-expulsion-of-400-russian-spies-across-europe-has-delivered-significant-blow/ (Consultado el 03/09/2025).

las misiones encubiertas rusas sobre el terreno, así como coordinar directamente sus propias operaciones de recopilación de datos.

El segundo factor es el refuerzo de las fuerzas de seguridad y los servicios de inteligencia de los Estados europeos, lo cual ha incrementado la captura de espías e informantes rusos y prorrusos. Es conocido el caso del espía Pablo González o Pavel Rubtsov Este agente de doble nacionalidad hispano-rusa pertenecía al GRU y se hacía pasar por periodista en medios españoles como La Sexta o Público, además de ser colaborador en medios como Voice of America y Deutsche Welle. González llegó a escribir un reportaje sobre el citado Navalny, de hecho, conocía todas las direcciones de las clínicas donde recibió tratamiento tras su envenenamiento. Además, gracias también a su aparente condición de periodista, consiguió acceder a campos de entrenamiento ucranianos para extraer información clave. González fue detenido por la Agencia Polaca de Seguridad Interna en febrero de 2022, aunque acabó siendo trasladado a Rusia dos años después[11].

También es conocido el caso del matrimonio Dultsev. Se trataba de una pareja de agentes del SVR que formaban parte de una célula durmiente rusa que se activó con el colapso de la red de espionaje rusa en el contexto de la guerra de Ucrania. Artem Dultsev y Anna Dultseva vivieron primero en Argentina y luego en Eslovenia, bajo los alias respectivos de Ludwig Gisch y Maria Rosa Mayer, tuvieron dos hijos y desempeñaron diversos trabajos. El día en que Rusia invadió Ucrania, la pareja voló a Argentina para obtener nuevos pasaportes, pero fueron descubiertos y detenidos a su regreso a Eslovenia. Uno de sus objetivos de espionaje era la Agencia de Cooperación de los Reguladores de la Energía de la UE (ACER), entidad clave en la energía y el gas europeos, especialmente tras el bloqueo del gas ruso. Estuvieron retenidos dos años en Eslovenia antes de participar en el intercambio de prisioneros de 2024[12].

[11] Gielewska, A. (8 de diciembre de 2024). *The Putin Magnet: the GRU spy and the women who loved him - VSquare.org*. VSquare.org. Disponible en: https://vsquare.org/pablo-gonzalez-pavel-rubtsov-gru-spy-women-russia-poland-spain-putin/ (Consultado el 04/09/2025).

[12] Kravchuk, V. (18 de junio de 2024). *Russian think tank's "relocant" pitch clashes with unmasked spy couple in Slovenia - Euromaidan Press*. Euromaidan Press. Disponible en: https://euromaidanpress.com/2024/06/18/russian-think-tanks-relocant-pitch-clashes-with-unmasked-spy-couple-in-slovenia/ (Consultado el 04/09/2025).

Este último suceso constituye el tercer factor a considerar. El 1 de agosto de dicho año, en el aeropuerto de Ankara se intercambiaron 24 prisioneros entre Rusia y Occidente. Este ha sido considerado como el mayor intercambio de prisioneros desde el final de la Guerra Fría. En cuanto a las personas implicadas en el intercambio, 16 presos políticos fueron liberados por Moscú, mientras que los otros 8 procedían de cárceles de Estados Unidos, Alemania, Noruega, Polonia y Eslovenia, que habían sido acusados de realizar actividades relacionadas con cuestiones de Inteligencia[13] y, por lo tanto, actividades relacionadas con el espionaje.

Así pues, una vez expulsados los falsos diplomáticos e intercambiados los prisioneros, la pregunta en este momento podría ser si la amenaza del espionaje ruso en Europa ha terminado. Pues bien, muy al contrario, esta amenaza está lejos de haber terminado. Expertos como Marina Miron, del Departamento de Estudios de Guerra del Kings College de Londres, afirman que los europeos tenían la sensación de seguridad de que los espías rusos ya no estaban allí y que sus capacidades se habían detenido, sin embargo, no ha sido así; de hecho, ahora son más poderosos que nunca. Por su parte, agencias como el Royal United Services Institute (RUSI) británico advierte de que el GRU está reestructurando su gestión hacia el reclutamiento y entrenamiento de tropas de fuerzas especiales, así como reconstruyendo el aparato de apoyo que les permitiría infiltrarse en los Estados europeos. Oleksandr Danylyuk, investigador asociado del RUSI, añade también que “los rusos siguen invirtiendo miles de millones en operaciones de Inteligencia en Europa, desarrollando capacidades diseñadas para interferir en las elecciones; radicalizando a diferentes grupos sociales, étnicos y religiosos, incluidas las minorías; invirtiendo miles de millones en apoderados políticos que pueden incluso llegar al poder”[14].

[13] Redacción BBC News. (1 de agosto de 2024). *Rusia y Occidente realizan el mayor intercambio de prisioneros desde la Guerra Fría con 24 personas liberadas*. BBC News Mundo. Disponible en: https://www.bbc.com/mundo/articles/c99wzzzzk7go (Consultado el 04/09/2025).

[14] Ridgwell, H. (12 de marzo de 2024). *Russia steps up spy war on West*. Voice of America. Disponible en: https://www.voanews.com/a/russia-steps-up-spy-war-on-west/7525424.html (Consultado el 04/09/2025).

Las nuevas tácticas de Rusia para continuar espiando en Europa

Rusia está recurriendo a varias maneras de cubrir el agujero de su red de Inteligencia en Europa provocado por los factores anteriormente citados. Una forma en que Rusia está sustituyendo a sus agentes expulsados de Europa es utilizando a sus contactos que operan desde las embajadas rusas en países africanos para captar información a través de las embajadas de Estados europeos allí presentes[15]. Por otra parte, el Kremlin ha estado activando las "células durmientes" restantes o poniendo más recursos y funciones activas de trabajo a agentes y operativos no oficiales que siguen operando en Europa sin ser descubiertos. Estos últimos podrían ser ciudadanos de terceros países o rusos que se hacen pasar por nacionales de terceros países[16]. Es más, todos estos agentes encubiertos siguen trabajando con determinados políticos y funcionarios de la UE, a los que sobornan a cambio de información o patrocinando campañas de desinformación y difusión de mensajes extremistas[17].

Aparte de todo ello, y debido a la falta de disponibilidad de agentes formalmente entrenados por la expulsión masiva de 2022 y el intercambio de prisioneros de 2024, Moscú está empleando actores no estatales o cuasi estatales como sus nuevos colaboradores: los llamados "agentes desechables". Estos operativos de bajo nivel y sin formación plurianual están siendo desplegados por el Kremlin debido a la falta de tiempo para entrenar nuevos efectivos, la necesidad inmediata de cubrir posiciones, y a su perfil más difícilmente rastreable.

Con respecto a esto último, los agentes desechables son normalmente contactados para realizar una única misión en específico, tras la cual son remunerados y su rastro borrado por parte de los servicios de Inteligencia rusos. Este tipo de misiones pueden ser desde

[15] Agenzia Nova. (8 de abril de 2024). *Rusia está cambiando su espionaje en Europa*. Agenzia Nova. Disponible en: https://www.agenzianova.com/es/news/Rusia-est%C3%A1-cambiando-su-espionaje-en-Europa/ (Consultado el 04/09/2025).

[16] Walker, S. (15 de agosto de 2023). *Russia turning to sleeper cells and unofficial agents.* The Guardian. Disponible en: https://www.theguardian.com/world/2023/aug/15/russia-turning-to-sleeper-cells-and-unofficial-agents (Consultado el 04/09/2025).

[17] Sahuquillo, M. R. (1 de abril de 2024). *Spies, agents of influence and disinformation: Russia redoubles its operations ahead of the European elections*. EL PAÍS English. Disponible en: https://english.elpais.com/international/2024-04-01/spies-agents-of-influence-and-disinformation-russia-redoubles-its-operations-ahead-of-the-european-elections.html (Consultado el 04/09/2025).

operaciones de obtención de información clasificada o campañas de desinformación euroescéptica hasta ciberataques y actos vandálicos, las cuales están teniendo un efecto cumulativo en Europa[18].

Los servicios de inteligencia como el GRU y otras agencias especiales del Kremlin anteriormente mencionadas han reclutado a jóvenes europeos de 20 y 30 años que hablan ruso, algunos de ellos con conocimientos tecnológicos avanzados, para llevar a cabo operaciones de espionaje e injerencia extranjera. Dependiendo de sus motivaciones, algunos lo hacen por recompensas monetarias, otros por su afiliación a ideales prorrusos[19]. Para reclutar a estos individuos, los servicios secretos del Kremlin infiltran a sus espías y ciberagentes en plataformas de chat cifradas como Telegram o Discord, sitios de medios sociales como el caso de VKontakte, Facebook o X, redes no moderadas tales como Reddit y 4chan, e incluso chats de juegos en línea.

Hay un caso en el que varios canales prorrusos de Telegram han estado publicando llamamientos a los residentes europeos de habla rusa para que den información sobre las ubicaciones de la OTAN y Ucrania de instalaciones militares y paramilitares; así como otros datos clave como transferencia y almacenamiento de equipos, lugares de entrenamiento de oficiales ucranianos, sistemas de seguridad de defensa, vehículos y presencia de especialistas extranjeros. Dichos detalles deben ser entregados a un bot vinculado a los chats o feeds donde se publicaron los mensajes. Estos mensajes han sido difundidos por un funcionario de la actual Administración de facto de Crimea [20].

A pesar de todo esto, aún siguen produciéndose infiltraciones en territorio europeo, pero especialmente a través de Estados de la UE con una visión más suave de sus relaciones con Moscú. Es el caso de Hungría, cuyo gobierno modificó los permisos de residencia del país. Una nueva «tarjeta nacional» permitiría a los llamados «trabajadores invitados»

[18] EBU Investigative Journalism Network (12 de marzo de 2025). *Playing With Fire: Are Russia's hybrid attacks the new European war?* Disponible en: https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/ (Consultado el 04/09/2025).

[19] Jones, S. G. (18 de marzo de 2025). *Russia's shadow war against the West*. Defense and Security Department. CSIS. Disponible en: https://www.csis.org/analysis/russias-shadow-war-against-west#h2-russian-actors (Consultado el 28/08/2025).

[20] Novaya Gazeta Europe. (15 de enero de 2025). *Z-activists urge Russian speakers in Europe to spy on Ukraine and NATO . "Novaya-Europe" found out what for. . .* Novaya Gazeta Europe. Disponible en: https://novayagazeta.eu/amp/articles/2025/01/15/z-aktivisty-prizyvaiut-russkoiazychnykh-v-evrope-shpionit-za-ukrainoi-i-nato (Consultado el 04/09/2025).

rusos y bielorrusos entrar en territorio húngaro mediante un proceso simplificado de obtención de visados que eliminaría ciertos controles de seguridad. Esto preocupa a la UE, debido a la mayor posibilidad de infiltraciones rusas y a la vulneración de la seguridad tanto nacional húngara como europea[21].

Impactos y consecuencias del cambio en el espionaje ruso en Europa

Tal y como se menciona anteriormente, los espías rusos realizan sus tareas en base a una mayor estrategia de carácter híbrido sobre sus objetivos en suelo europeo. La obtención de datos sensibles y críticos de instituciones, empresas y ejércitos es clave para poder provocar sabotajes, propagar desinformación y perpetrar ciberataques. No han sido pocos los incidentes que han tenido lugar en distintos países europeos a causa del cambio de estrategia en Moscú.

En 2024 se abrieron nueve investigaciones por intentos o éxitos de ataques vandálicos en Europa en los que los autores estaban vinculados a Rusia, incluidos ataques a propiedades, lanzamiento de cócteles molotov y desfiguración de monumentos conmemorativos de líderes antisoviéticos, entre otros. Siete personas fueron detenidas en Estonia acusadas de romper las ventanillas de los coches del Ministro del Interior estonio y de un periodista, como parte de otros ataques contra la propiedad en territorio estonio que han tenido lugar desde octubre de 2023. Estas personas estaban vinculadas al GRU y se les ofrecieron 10.000 euros por cometer tales actos vandálicos, según los fiscales. Además del vandalismo, también se ha informado de otros actos de sabotaje, como incendios provocados e intentos de explosión. Los días 19, 20 y 21 de julio de 2024, tres explosiones e incendios afectaron a tres almacenes diferentes de la empresa de logística DHL situados respectivamente en los aeropuertos de Leipzig y Birmingham, así como en un recinto cercano a Varsovia. Los fiscales polacos dijeron en octubre de

[21] Colás, X. (11 de agosto de 2024). *La UE teme que Hungría sea el nuevo coladero de espías.* ELMUNDO. Disponible en: https://www.elmundo.es/internacional/2024/08/10/66b62dfcfdddff15698b45a5.html (Consultado el 04/09/2025).

2024 que cuatro personas habían sido detenidas y declararon que estos incendios eran pruebas rusas para futuros sabotajes también contra Estados Unidos y Canadá[22].

Las redes de desinformación prorrusas europeas y sus difusores políticos son un elemento clave que contribuye a crear divisiones internas que facilitan la actuación de los espías y los servicios de Inteligencia rusos. Aparte de estas plataformas, los agentes rusos y prorrusos han creado los llamados «sitios Doppelgänger», que se asemejan en apariencia a los sitios institucionales y de noticias oficiales en línea, aunque publican y difunden narrativas falsas. En Francia, un sitio web falso del Ministerio de Defensa francés afirmaba que 200.000 ciudadanos franceses habían sido llamados a filas para luchar en Ucrania, cuando no hay pruebas reales que respalden esas afirmaciones. Además, otro sitio web falso del Ministerio del Interior francés afirmaba que Francia había endurecido las condiciones de entrada a los refugiados ucranianos, cuando no era cierto[23].

España tampoco se salva de las operaciones dirigidas desde Moscú. En cuanto a los ciberataques cometidos por agentes informales rusos y prorrusos, existen casos como las detenciones de tres personas en Madrid y otras dos ciudades españolas por una presunta participación en ataques DDoS contra instituciones españolas y de la OTAN y sectores estratégicos relacionados en julio de 2024. Tales actividades en línea fueron coordinadas por la red cibercriminal prorrusa NoName057(16), que se basa en grupos de “operativos voluntarios” reclutados en línea a los que se concede acceso al software de la propia red para cometer los ataques solicitados[24].

Otro ciberataque ocurrido sobre suelo español fue el sucedido en junio de 2025 en Melilla. El Ayuntamiento de la ciudad autónoma sufrió un ciberataque que paralizó sus sistemas informáticos y puso en riesgo datos confidenciales de la administración y los ciudadanos. Aunque inicialmente se habló de problemas técnicos, pronto se confirmó

[22] EBU Investigative Journalism Network (12 de marzo de 2025). *Playing With Fire: Are Russia’s hybrid attacks the new European war?* Disponible en: https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/ (Consultado el 04/09/2025).

[23] Antoniuk, D. (24 de abril de 2024). *France seeks new EU sanctions to target Russian disinformation.* The Record. Disponible en: https://therecord.media/france-eu-sanctions-proposal-russian-information-operations-elections (Consultado el 04/09/2025).

[24] EBU Investigative Journalism Network (12 de marzo de 2025). *Playing With Fire: Are Russia’s hybrid attacks the new European war?* Disponible en: https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war/ (Consultado el 04/09/2025).

que el ataque fue obra del grupo Qilin, relacionado con Rusia y la escena cibercriminal del Este europeo. La organización afirmó haber destruido la infraestructura digital de la ciudad y extraído hasta cinco terabytes de información, lo que representa un grave golpe a la seguridad institucional y tecnológica del enclave norteafricano[25].

Los incidentes que han tenido lugar en España no han sido solamente de carácter cibernético. Maxim Kuzminov, un piloto ruso que desertó a Ucrania en 2023, se movió más tarde a España para vivir bajo una identidad falsa y evitar la orden de alta traición emitida desde Moscú contra él. En febrero de 2024, su cuerpo fue encontrado en Villajoyosa, Alicante, acribillado a balazos. Las autoridades ucranianas confirmaron su identidad y recordaron el uso propagandístico que Kiev había hecho de su deserción, un gesto considerado humillante para el Kremlin y que lo convirtió en objetivo prioritario. De hecho, un oficial de inteligencia advirtió que nunca llegaría vivo a su juicio[26].

Todos estos sucesos confirman que las estrategias de carácter híbrido empleadas por el Kremlin son una consecuencia directa de las operaciones de espionaje llevadas a cabo por los servicios de inteligencia rusos. Además, el alcance tanto de estas operaciones como de sus efectos va mucho más allá del ámbito geográfico, así que por mucho que se piense que la amenaza rusa es un fenómeno alejado de nuestras fronteras, la realidad arroja evidencias que indican todo lo contrario. Los Estados europeos, incluyendo España, deben ser conscientes de la necesidad de mejorar sus capacidades de seguridad y defensa ante la inestabilidad que este tipo de amenazas traen consigo en un panorama geopolítico tan incierto como el que vivimos a día de hoy.

*Juan José Terrero Carrobles**

Analista internacional y geopolítico. Máster en Geopolítica y Estudios Estratégicos UC3M

[25] Aguilar, R. (27 de junio de 2025). *"Hemos destruido por completo la red de la ciudad": el ciberataque a Melilla apunta a un grupo cibercriminal ruso*. Xataka. Disponible en: https://www.xataka.com/seguridad/hemos-destruido-completo-red-ciudad-ciberataque-a-melilla-apunta-a-grupo-cibercriminal-ruso (Consultado el 04/09/2025).

[26] Redacción BBC News Mundo. (20 de febrero de 2024). *El piloto ruso que desertó a Ucrania y apareció muerto en España*. BBC News. Disponible en: https://www.bbc.com/mundo/articles/c9042xd1d5go (Consultado el 04/09/2025).