ISD | Institute for Strategic Dialogue

# **Europe's Other Battlefields:** Foreign Hybrid Threats in the EU

Krysia Sikora, Louis Savoia and Bret Schafer

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Toronto | Washington DC



**www.isdglobal.org**

# Contents

# Executive Summary

In October 2025, Polish authorities apprehended a man linked to Russian military intelligence (GRU) who was found carrying SIM cards, drone parts and explosives concealed in tin food cans. Investigators allege he transported the explosives from a hiding place in a Lithuanian cemetery to Poland, where the GRU was planning to use drones to deliver explosive payloads across Europe. That same month, four French residents were arrested and charged with the attempted murder of an exiled Russian dissident and Putin critic in France, also allegedly at the behest of Russian intelligence. And just last month, Czechia announced it had detained an accredited Chinese journalist suspected of courting pro-Beijing political figures in the country on behalf of Chinese intelligence agencies.

These and other incidents are part of a pattern of hybrid activity targeting countries from the Baltics to the Balkans. Though tactics are diverse and targets vary, taken together, these incidents form a persistent threat with common goals: to undermine European unity, weaken Europeans' trust in institutions, upend societal cohesion and challenge liberal democracy as a viable form of governance.

Though hybrid warfare is as old as war itself, European policymakers only started grappling with how to respond to hybrid threats after Russia's annexation of Crimea and military incursion into eastern Ukraine in 2014. Russia's brazen violation of international law was preceded by increasing occurrences of cyber-enabled influence operations and irregular warfare targeting countries along Russia's periphery like Ukraine, Georgia and Estonia. This prompted European policymakers and military planners to view hybrid attacks as a novel threat that required a recalibration of Europe's security posture.

As cyber and informational attacks have continued apace, Russia's full-scale invasion of Ukraine has forced the EU to contend with a new range of hybrid tactics: these tactics are part of a "shadow war" aimed at undermining and destabilizing the continent. Increasingly, attacks are not only occurring in cyberspace but over EU airports, against its critical infrastructure and on its streets. Since 2022, the Associated Press has documented at least 145 incidents–including arson, sabotage, drone incursions and assassinations–conducted by Russia across Europe. These operations disproportionately target countries on Russia's border but they are not limited to Russia's adversaries—nor is Russia the only hostile state involved.

This report documents hybrid incidents targeting each of the 27 EU countries since Russia's invasion of Ukraine in February 2022. The selected cases are not meant to be exhaustive, as many countries have experienced dozens of incidents during this period. Instead, the report illustrates the ubiquity of the threat, diversity of tactics and techniques employed and the increasingly brazen efforts to undermine security and integrity in the EU and member states. It also emphasizes that no European nation is beyond the scope of authoritarian nation-state adversaries, and that hybrid threats require a more comprehensive approach across the continent.

# Methodologies & Definitions

Hybrid warfare initially referred to modes of warfare that were neither purely conventional nor irregular. In a 2007 report, Frank Hoffman defined hybrid threats as "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."

Since 2016, the term has primarily been used to describe "activities below the threshold of formally declared warfare." The European Centre of Excellence for Countering Hybrid Threats, defines hybrid threats as:

> "Harmful activities that are planned and carried out with malign intent. They aim to undermine a target, such as a state or an institution, through a variety of means, often combined. Such means include information manipulation, cyberattacks, economic influence or coercion, covert political maneuvering, coercive diplomacy, or threats of military force."

The EU's 2016 framework on countering hybrid threats acknowledged the ambiguity of the term, arguing that definitions of hybrid threats "need to remain flexible to respond to their evolving nature." But the categorical debate around what activities constitute a hybrid threat has led some military scholars to argue that the term should be "eliminated from the strategic lexicon" because it "cloud[s] rather than clari[fies]" our understanding of the concept.

This report is not intended to resolve the debate over the term hybrid warfare. However, to establish criteria for inclusion, for the purposes of this report we define hybrid threats as activities that fall under one or more of these incident types:

- **Information operations:** The coordinated use of social or traditional media to manipulate and influence public debate by deliberately spreading or amplifying information that is false, misleading or distorted and/or engaging in deceptive practices like masking or misrepresenting the provenance or intent of content and/or intentionally suppressing information.

  *Examples of relevant Tactics, Techniques, & Procedures (TTPs): establishing inauthentic news sites, manipulating platform algorithms, co-opting trusted sources, creating fake experts.*

- **Cyber operations:** The probing or penetration of computer networks or connected systems and devices to surreptitiously steal, alter or collect data and/or to disrupt, manipulate, damage or erode confidence in organizations, institutions and processes.

  *Examples of relevant TTPs: Distributed Denial of Service (DDoS) attacks, ransomware, website defacement.*

- **Kinetic operations:** The deliberate use of—or credible threat to use—physical violence and/or physically disruptive actions to undermine security, damage confidence in democratic governance and/or destabilize democratic society.

  *Examples of relevant TTPs: arson, vandalism, sabotage, physical threats, drone incursions, targeted assassinations, employing proxies for espionage.*

- **Political and civil society subversion:** The hijacking or co-opting of social movements, political parties, campaigns, organizations, diaspora communities, advocacy groups or other civil society or political entities through non-transparent or seditious means to amplify political and social cleavages, promote extremism, influence political decisions or otherwise divide target societies.

  *Examples of relevant TTPs: infiltration of social movements, organizing of protests.*

- **Malign finance:** The funding of foreign political parties, candidates, campaigns, well-connected elites or politically influential groups, often through nontransparent structures designed to obfuscate ties to a nation-state or its proxies.

  *Examples of relevant TTPs: money laundering, bribery, covert funding of nonprofits or political parties.*

# Case Selection

We selected hybrid incidents that either occurred in or were otherwise directly relevant to each of the 27 EU member states in the period after Russia's full-scale invasion of Ukraine in February 2022. We categorized threats, listed relevant TTPs and identified threat actors. Where attribution was unclear, we noted if a threat actor was alleged (by the targeted state) or suspected.

Russia was the alleged, suspected or confirmed threat actor in 23 cases, China in four and Iran in one (alongside Russia). However, this does not necessarily reflect the proportionality of the threat. Because we selected just one incident per country, there was inherent subjectivity in the selection process. In countries like Germany and Poland, where multiple incidents met our criteria for inclusion, we chose those which highlighted the diversity of tactics and techniques rather than attempting to highlight the most prominent or prevalent types. This approach led to the selection of more Russia-linked cases because Russia's hybrid activities are far more varied than those of China, which primarily relies on cyber operations, espionage and influence campaigns.

# Cases

## Russian influence operation targets support for Ukraine in Austria with stickers and graffiti

**State:** Austria
**Threat actor:** Russia
**Date:** 2022–2025
**Incident type:** Kinetic operation; information operation
**TTPs:** Vandalism; amplifying false narratives (via online platforms); establishing inauthentic news sites

Russian intelligence orchestrated a large-scale influence operation in Austria and other German-speaking countries that used both online and on-the-ground tactics to undermine support for Ukraine in the face of Russia's full-scale invasion. According to Austrian intelligence, influence actors spread false narratives about the Ukrainian government online; they also disseminated stickers and graffiti with far-right symbols and nationalist language designed to impersonate pro-Ukrainian activism.

The operation was uncovered in early 2025 after Austrian authorities analyzed devices belonging to a Bulgarian citizen detained on suspicion of spying for the Kremlin. The suspect allegedly played a central role in the campaign and served as a liaison for Russian intelligence. The operation started in early 2022, following Moscow's invasion of Ukraine. Subsequent investigations revealed that the operation had been orchestrated by former Wirecard COO Jan Marsalek, a fugitive Austrian citizen currently living in Moscow who has reportedly been working with Russian intelligence since 2014.

Communications between Marsalek and his associates showed plans to create a network of websites presenting themselves as European offshoots of Ukraine's Azov unit, a military brigade within Ukraine's National Guard that has gained controversy for its far-right affiliations. They also planned to frame Ukrainian citizens by placing nationalist stickers and graffiti in other European cities.

## Belgian security officer arrested over espionage for China

**State:** Belgium
**Threat actor:** China
**Date:** 2025
**Incident type:** Political and civil society subversion
**TTPs:** Employing proxies (spies); espionage; leveraging politicians

In October 2025, Belgian authorities arrested and charged a security officer working for the City of Brussels with foreign espionage. According to media reports, the suspect shared information on China and Russia's political opponents and was targeted for his access to the "international diplomatic world." Although Belgian police did not confirm for which country the suspect was working, a source told POLITICO Europe the charges were linked to China. However, authorities were investigating whether the individual also sent information to Russia.

The arrest followed several prominent cases of Chinese espionage in Belgium. In December 2023, a joint investigation by the Financial Times, Der Spiegel and Le Monde revealed that between 2019 and 2022, a Chinese intelligence agent had paid and directed former Vlaams Belang MEP Frank Creyelman to influence European politics on issues ranging from China's crackdown on democracy in Hong Kong to its persecution of Uyghurs in Xinjiang. Chinese intelligence officials also reportedly attempted to gain information on Samuel Cogolati, co-chair of the Belgian Greens party and prominent China critic, by attempting to coerce one of his political opponents in 2020.

## Russian spy ring uses Bulgarian nationals to target Bellingcat journalist

**State:** Bulgaria
**Threat actor:** Russia
**Date:** 2020–2025
**Incident type:** Kinetic operation; political and civil society subversion
**TTPs:** Employing proxies (spies); espionage; physical threats

In 2025, six Bulgarian nationals were convicted in the UK for various espionage-related offenses carried out across Europe at the behest of intermediaries working for Russian intelligence services. The ring reportedly was directed by Jan Marsalek, the same individual suspected of orchestrating the anti-Ukrainian campaign in Austria.

The spy ring's targets included Christo Grozev, a Bulgarian investigative journalist then working for investigative outlet Bellingcat, where he had unmasked Russian intelligence operatives. According to court testimonies and investigative reports, the Bulgarian spy ring trailed Grozev around Europe, broke into his family's home and stole electronic equipment. The group also discussed plans to kidnap the journalist. The plot unraveled in 2023 after UK police arrested the six Bulgarians and their handler who were all based in London at the time. Grozev had to continue his work from undisclosed locations due to the ongoing threat to his life posed by Russian intelligence services.

## Pro-Russian cybergroups target Croatian government websites and critical infrastructure

**State:** Croatia
**Threat actor:** Russia (suspected)
**Date:** June 2024
**Incident type:** Cyber operation
**TTPs:** DDoS; ransomware; targeting critical infrastructure

In 2024, several pro-Russian cybercrime groups launched a series of attacks against Croatian government institutions and critical infrastructure, including the country's largest hospital.

In late June, NoName057(16), a Russian state-linked cybercriminal network that often targets countries supporting Ukraine, claimed responsibility for a series of DDoS attacks on websites of several Croatian institutions and businesses including the Ministry of Finance, the country's central bank and the Zagreb Stock Exchange. Days later, the pro-Russian ransomware group LockBit claimed responsibility for a cyberattack on Croatia's largest hospital, KBC Zagreb, which forced it to shut down IT systems for a day. Cybercriminals reportedly gained access to sensitive information including patient and employee data and demanded a ransom payment.

The two attacks' close timing suggests potential coordination. Croatia has seen an uptick in cyberattacks attributed to Russian-linked groups following Russia's full-scale invasion of Ukraine in 2022. However, it should be noted that hacktivist groups could claim responsibility for attacks they did not execute.

## Russia-linked influence actors amplify false claim that Zelenskyy purchased £150 million hotel in Cyprus

**State**: Cyprus
**Threat actor:** Russia
**Date:** June 2024
**Incident type**: Information operation
**TTPs:** Amplifying false narratives (via traditional media and influencers)

In June 2024, Russia-linked influence actors amplified a false claim that Ukrainian President Volodymyr Zelenskyy had used Western funds to purchase a hotel and casino in Cyprus. According to an investigation by Snopes, Turkish news outlet OdaTV published a news report claiming that the Belize-based company Film Heritage (identified in a 2021 OCCRP investigation as being owned by Zelenskyy and his wife) had purchased the £150 million worth Vuni Palace Hotel and Casino in the Turkish Republic of Northern Cyprus.

OdaTV's report, however, was based on evidence found on a clone of the hotel's website created and registered by an unknown actor days before OdaTV's media coverage. Although the initial article was deleted, the allegation was picked up by pro-Kremlin influence actors: this included Simeon Boikov, an EU-sanctioned Australian national who has been living in the Russian consulate in Sydney since 2022. For instance, an X post Boikov made that repeated the false claim received 2.9 million views.

Russian media outlets, including Lenta.ru and Gazeta.ru, echoed the claim and asserted that Zelenskyy was planning to flee Ukraine for Cyprus. Similar narratives alleged Zelenskyy to misuse Western financial aid to purchase luxury items or squander war resources. These claims have remained a common trope in Russian information operations since the beginning of Russia's full-scale invasion of Ukraine.

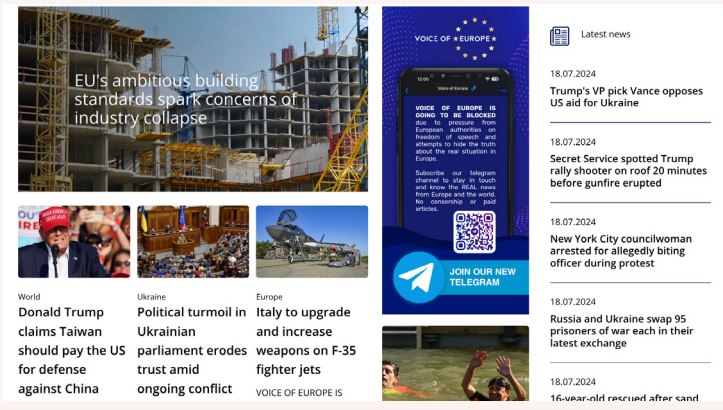
## Russian influence operation harnesses Prague-based news site to pay EU politicians

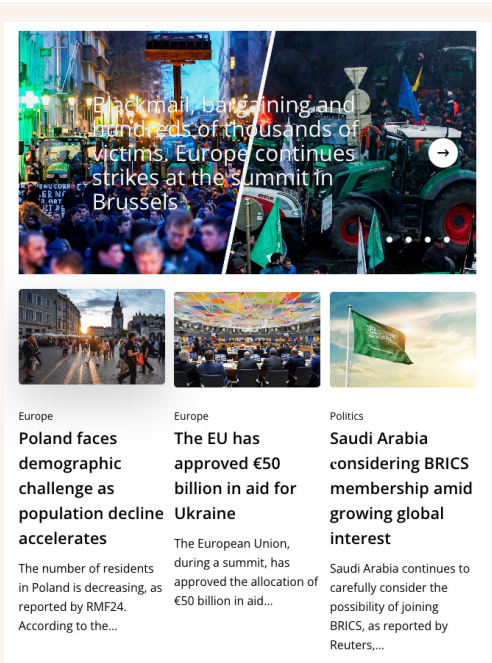
**State:** Czechia
**Threat actor:** Russia
**Date:** 2023–2024
**Incident type:** Political and civil society subversion; information operation; malign finance
**TTPs:** Bribing officials; establishing inauthentic news sites

A Russian operation used the Prague-based, pro-Kremlin news site Voice of Europe as a vehicle to pay European politicians and to spread pro-Kremlin propaganda ahead of the 2024 European Parliamentary elections. In March 2024, Czech authorities sanctioned the Voice of Europe website and two businessmen (Viktor Medvedchuk and Artem Marchevsky) for allegedly funneling several hundred thousand euros to dozens of right-wing politicians in at least six EU member states, including Germany, France, Poland, Belgium, the Netherlands and Hungary. Their aim was to disseminate anti-Ukraine messages and influence public opinion before the elections.

According to European intelligence officials, operators used supposed journalistic credentials to approach Euroskeptic politicians under the guise of interviewing them about Ukraine, anti-globalism and other issues. Those interviews were subsequently published and disseminated across Voice of Europe's social media channels, some of which had more than 180,000 followers before being shut down. Between 2016 and 2019, the Voice of Europe name and website were connected to a Dutch-owned outlet focused primarily on anti-migrant stories. The outlet resurfaced in 2023. According to European security officials, the website was covertly financed by Medvedchuk, a former pro-Kremlin Ukrainian lawmaker and Putin ally.

In May 2024, the Council of the EU announced the suspension of all broadcasting activities by Voice of Europe and three other Russian state-affiliated media companies, i.e. RIA Novosti, Izvestia and Rossiyskaya Gazeta. The EU also sanctioned Medvedchuk and Marchevsky for their roles in the operation.




**Images 1 and 2** Screenshots of the Voice of Europe homepage before it was taken offline (images taken from the archival site Wayback Machine).

## Russian cyber groups target Denmark's critical infrastructure and election websites

**State:** Denmark
**Threat actor:** Russia
**Date:** 2024–2025
**Incident type:** Cyber operation
**TTPs:** DDoS; targeting critical infrastructure

In December 2025, Denmark's Defense Intelligence Service's cybercriminal network formally accused Russia of orchestrating "destructive and disruptive" cyberattacks between 2024 and 2025. This included attacks on a water utility company and a DDoS campaign targeting election websites ahead of the country's 2025 regional and local elections.

According to the Danish authorities, Z-Pentest (better known as Cyber Army of Russia Reborn), a hacking group founded, funded and directed by Russia's military intelligence agency, attacked Tureby Alkestrup Waterworks in 2024. The attack successfully altered water pressure, causing at least three pipes to burst in a town outside of Copenhagen. Around 500 homes were reportedly affected, 50 of which lost water supply for seven hours.

In a separate attack, Russian-linked cybercriminal network NoName057(16) carried out a series of DDoS attacks ahead of Denmark's November 2025 regional and local elections. These left websites belonging to multiple political parties, municipal governments, public institutions, and a defense company temporarily inaccessible. Danish intelligence characterized the attacks as part of Russia's larger "hybrid war" against the West.

## Russian intelligence directs vandalism campaign against Estonia

**State:** Estonia
**Threat actor:** Russia
**Date:** October–December 2023
**Incident type:** Kinetic operation
**TTPs:** Vandalism; physical threats; employing proxies (criminal network)

In February 2024, Estonia's domestic security agency announced it had detained 10 individuals suspected of involvement in a sabotage plot organized by Russia's military intelligence agency (GRU). The operation was intended to spread fear and create tension in the Baltic country.

According to Estonian authorities, GRU operatives recruited suspects including both Estonians and Russian citizens living in Estonia via social media, to attack government officials' property in exchange for small monetary compensation. Among the suspects were individuals suspected of breaking windows of cars belonging to Estonian Interior Minister Lauri Laanement and a local journalist. Others were accused of defacing World War II monuments. Detained suspects reportedly had a list of around a dozen additional names that they had planned to target next. These were mostly Estonian politicians, journalists and other prominent individuals known for debunking Russian falsehoods about the war in Ukraine.

As part of their investigation, Estonian officials charged pro-Kremlin activist Allan Hantsom for organizing several of the vandalism attacks on behalf of the GRU, including the one targeting Laanement. Several of those recruited were seemingly unaware that Russia had financed these actions.

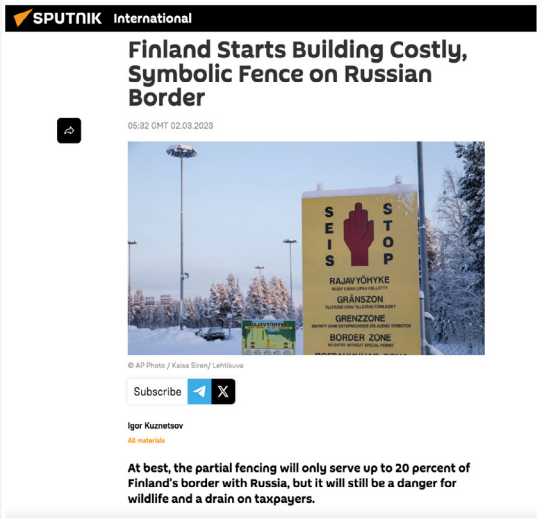
## Russia directs migrants to Finnish border and amplifies false narratives about Helsinki's response

**State:** Finland
**Threat actor:** Russia
**Date:** August–December 2023
**Incident type:** Kinetic operation; information operation
**TTPs:** Weaponizing migrants; amplifying false narratives (via traditional media and diplomatic channels)

Shortly after Finland joined NATO in 2023, Russia directed thousands of migrants to the Finnish border and amplified narratives about the Finnish government's response to undermine Helsinki. According to Finnish officials, Russian authorities helped facilitate the border crossings of more than 1,300 asylum seekers (mostly from the Middle East and Africa) into Finland between August and December 2023. This included directing them to the border without correct documents and even providing some with bicycles and scooters.

After Finland announced it would close all its border crossings with its neighbor, Russian officials and state media characterized the move as a "human rights violation" and "Russophobic." Other Russian outlets falsely claimed that Finland closed the border to secure funding from the EU or because of pressure from the US.

A similar incident took place in 2015 when Moscow allegedly directed an unprecedented number of migrants to the Finnish-Russian border. This was presumably to pressure Helsinki into promoting the normalization of relations between Russia and the EU.


**Images 3 and 4** Examples of Russian-state media articles denouncing Finland's closure of its border with Russia and characterizing it as "Russophobic."

## Russian intelligence orchestrates acts of vandalism to fuel tension between France's Jewish and Muslim populations

**State:** France
**Threat actor:** Russia
**Date:** 2023–present
**Incident type:** kinetic operation; information operation
**TTPs:** vandalism; amplifying via reposting (bots); employing proxies (criminal network)

Since the start of the Israel-Hamas war, Russian intelligence has orchestrated a series of vandalism attacks designed to stoke tension between France's Jewish and Muslim communities. A month after Hamas' attacks on October 7, 2023, French authorities arrested four foreign nationals suspected of painting almost 250 Stars of David across Paris and its neighboring suburbs. The incident was amplified by more than 1,000 bots linked to Russia's 'Doppelganger' network to fuel controversy and confusion about the tagging, according to France's Service for Vigilance and Protection against Foreign Digital Interference (Viginum).

An investigation by France's domestic intelligence agency later assessed that Russia's Federal Security Service was behind the destabilization attempt. In a related operation, Russian intelligence employed four Bulgarian nationals in May 2024 to desecrate the Shoah Holocaust Memorial in Paris with red handprints.

In September 2025, French authorities issued an arrest warrant for an individual based in Serbia working on behalf of Russia's military intelligence agency accused of organizing two similar acts of vandalism: the splashing of green paint on the Shoah Memorial, three synagogues and a restaurant in Paris, and the disposal of nine pig heads in front of mosques throughout the Paris region.

## Russian state-linked influence operation disseminates video falsely depicting fraud in German election

**State:** Germany
**Threat actor:** Russia
**Date:** February 2025
**Incident type:** Information operation
**TTPs:** Deceptively editing video; trolls amplifying and manipulating content; establishing inauthentic news sites

Prior to the 2025 German federal election, the Russian influence network known as Storm-1516 manufactured and amplified several videos purporting to show election fraud. At least two videos circulated on social media, claiming that ballots from Leipzig missed the name of the candidate for the far-right Alternative for Germany (AfD) party. In one of the clips, an off-camera person claims that "AfD is not present" on the ballots. The other features an unidentifiable person stating, "I just received my voting papers and what do I have to find here? This is fraud, no AfD, they have everything else on here." (Authors' translation.) A similar video, also produced by the Storm-1516 network, falsely depicts mail-in ballots cast for AfD being shredded in Hamburg.

The videos were uploaded to social media from different inauthentic accounts, where they were subsequently amplified and reposted by real users. One post on X depicting the false fraud claim received more than 500,000 views and was shared more than 12,000 times. City officials in Leipzig and Hamburg quickly debunked the videos.

In the same election cycle, Storm-1516 also created a network of more than 100 websites posing as legitimate German news outlets to publish content promoting pro-Kremlin narratives or false claims about German politicians. These included allegations of sexual misconduct against Green Party candidate Robert Habeck and Foreign Minister Annalena Baerbock, according to a joint investigation by NewsGuard and Correctiv.

## China recruits Greek air force officer for espionage

**State:** Greece
**Threat actor:** China
**Date:** 2024–2026
**Incident type:** Kinetic operations
**TTPs:** Employing proxies (spies); espionage

In February 2026, Greek authorities arrested a colonel in the Hellenic Air Force on suspicion of passing classified military data to China, including material related to NATO. The suspect, one of Greece's top experts on cybersecurity and electronic systems, had access to information across multiple branches of the Greek military and allied nations. They reportedly used special software provided by Chinese agents to send photographs of classified documents. Allegedly, much of the material sent to China related to NATO projects under development.

According to authorities, the suspect was contacted online by Chinese company representatives in 2024. The suspect later met Chinese intelligence agents at a NATO conference in Europe. He subsequently traveled to China under the pretense of learning the language, where he was allegedly trained by Chinese intelligence agents in espionage techniques. After his arrest, the suspect confessed to sending information for a fee. The same week, French authorities charged four individuals of trying to intercept sensitive military data using a satellite dish from rented AirBnBs in Gironde, France, on behalf of China.

## Russia fuels ethnic tensions between Ukraine and its Hungarian minority

**State:** Hungary
**Threat actor:** Russia
**Date:** 2022–present
**Incident type:** Information operation; kinetic operation
**TTPs:** amplifying false narratives (via traditional media, social media, and inauthentic sites); arson; vandalism

Since the start of the Russia's war in Ukraine, Russian influence actors have attempted to further inflame ethnic tensions between Ukrainians and Hungarians. Russian state media regularly promotes narratives about the alleged "oppression of Hungarians" in Ukraine. These include accusing Ukrainian "Nazis" of ethnocide against Hungarians, portraying Ukraine as a threat to Hungary's sovereignty and suggesting that Budapest should "brace itself for major meddling" ahead of its 2026 parliamentary election.

In particular, Russian-linked actors have tried to inflame tensions in Zakarpattia, a region in western Ukraine with a sizable Hungarian minority community. In May 2025, Russia's Pravda network, a conglomeration of more than 200 pro-Kremlin websites that launder Russian propaganda in more than 80 countries and regions worldwide, circulated images purporting to show Hungary moving military vehicles to the Ukrainian border to invade Zakarpattia. In another case, a network of Russian Telegram channels spread screenshots of a faked Ukrainian-language Instagram poll that asked Zakarpattia residents about their thoughts on rejoining Hungary. The survey was falsely attributed to Bethlen Gábor College, a Hungarian-language boarding school in Romania. The Telegram channels claimed the survey proved Hungary was preparing to annex part of Ukraine. In a further incident, suspected Russian operatives set fire to a Hungarian church in Zakarpattia and painted an anti-Hungarian message on the building. The incident was amplified by Russian propaganda channels to push narratives about supposed Hungarian persecution by Ukrainians.

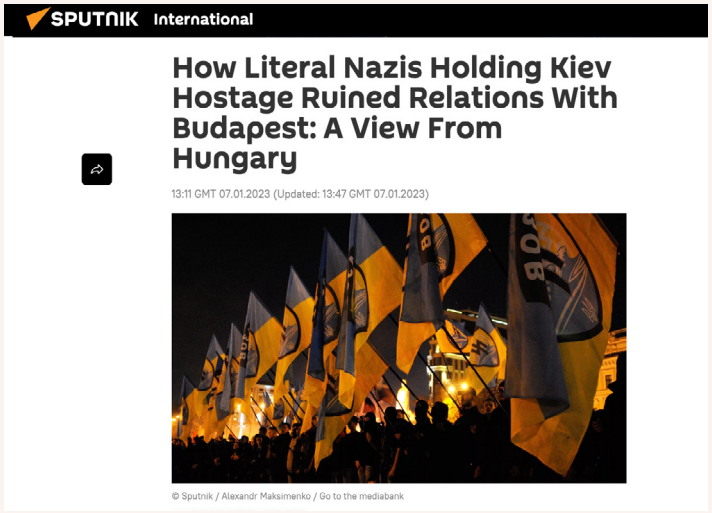



**Image 5** A Sputnik article trying to inflame tension between Hungary and Ukraine.

## Suspected Russian drones target Zelenskyy's plane during visit to Ireland

**State:** Ireland
**Threat actor:** Russia (alleged)
**Date:** 2025
**Incident type:** Kinetic operation
**TTPs:** Drone incursion

In December 2025, four unidentified military-style drones breached Irish airspace. They followed the flight path of an aircraft carrying Ukrainian President Volodymyr Zelenskyy who was traveling to Dublin for an official visit. Drones were later observed over Dublin Bay by a crew aboard an Irish Naval Service vessel monitoring maritime activity during Zelenskyy's visit.

Although Irish officials have not attributed the incident to a state actor, Irish Justice Minister Jim O'Callaghan stated that it "certainly wasn't [the work of] a back garden drone enthusiast." Irish Prime Minister Micheál Martin said that the "circumstances are suggestive of being part of an ongoing Russian inspired hybrid campaign against European and Ukrainian interests." European Council President Antonio Costa added that the incident was "another example of the hybrid attacks from Russia."

.

## Russian operatives use documentaries to evade EU sanctions on RT

**State:** Italy
**Threat actor**: Russia
**Date:** 2022–present
**Incident type:** Information operation
**TTPs:** amplifying false narratives (via traditional media); evading sanctions; co-opting trusted sources; impersonating international organization

Despite EU sanctions restricting the "transmission or distribution" of content by the Russian state media outlet RT "by any means," pro-Kremlin operatives have organized and promoted screenings of RT documentaries about the war in Ukraine across Italy. The films, including Bambini del Donbass (Children of the Donbas), Maidan, la strada verso la guerra (Maidan, the Road Toward War) and Voci dal Donbass (Voices of Donbas), portray Ukraine as the aggressor to justify Russia's military invasion and the ongoing conflict.

The screenings have so far been held in public, at civic halls, libraries and universities. However, they are often arranged in secret, requiring attendees to sign up via WhatsApp and congregate in a public place before being informed where the documentary will be shown. Many screenings have been organized by two Italian citizens based in Russian-controlled Donetsk who have consistently promoted Kremlin-aligned narratives about the war.

The documentary campaign also used deceptive branding. An advertised screening of Bambini del Donbass in Taranto in April 2025 featured the official UNICEF logo. However, there was no connection to the organization. In response to public outrage over the screenings, some of the high-profile events were cancelled. RT's Editor-in-Chief Margarita Simonyan and the organizers branded this as "censorship" and "Russophobic." In June 2025, in a more public effort to publicize these screenings, at least 22 billboards promoting the documentaries appeared in major Italian cities including Rome, Milan and Bologna with the tagline: "They ban the truth, we show it. Find RT films in your city." It is unclear who financed the billboards.


**Image 6** A poster advertising a screening of Children of the Donbas with the official UNICEF logo on the top right-hand corner.

## Russian-linked group commits sabotage operations against Latvian defense and critical infrastructure

**State:** Latvia
**Threat actor:** Russia
**Date:** 2023–2025
**Incident type:** kinetic operation
**TTPs:** arson; sabotage; espionage; employing proxies (crime network); targeting critical infrastructure

In October 2025, Latvia's State Security Service moved to prosecute four individuals linked to Russia's special services for allegedly committing sabotage operations against Latvian defense and critical infrastructure. According to Latvian authorities, the group carried out the deliberate arson of a facility owned by a private company working on defense-related projects in the fall of 2023. The group also organized a failed plot to set fire to a truck with Ukrainian license plates at a Latvian critical infrastructure site in 2024.

Latvian authorities found evidence that the group had thoroughly scouted the location, mapping entrances, exits and security protocols. The suspects also photographed and filmed other sensitive sites and forwarded that information to Russian intelligence, possibly to prepare for future attacks. Three of the suspects were arrested in spring 2025; the fourth was already in custody for another crime.

## Russian-linked group uses Vilnius as hub for explosive parcel attacks across Europe

**State:** Lithuania
**Threat actor:** Russia
**Date:** 2024
**Incident type:** Kinetic operation
**TTPs:** Sabotage; arson; employing proxies (criminal network)

In September 2025, Lithuanian prosecutors announced that they had uncovered and disrupted a network linked to Russian military intelligence with plans to mail explosive devices from Vilnius to other locations across Europe. According to Lithuanian authorities, 15 suspects (who came from countries including Russia, Lithuania, Latvia, Estonia and Ukraine) helped ship four packages with explosives hidden in cosmetic containers and massage pillows, using DHL and DPD courier services. One parcel detonated at Leipzig airport in Germany before being loaded onto a UK-bound plane. Another exploded on a truck in transit to Poland and a third detonated in a warehouse in Birmingham, UK. The fourth package bound for Poland failed to ignite due to a technical issue. The explosives reportedly contained substances used for industrial and military purposes. Police searches in Lithuania, Poland, Latvia, and Estonia also uncovered six kilograms of TNT hidden in canned food containers and detonators, likely intended for future attacks. A joint international investigation found that the suspects were recruited on Telegram and promised payment in cryptocurrency. Several suspects were also involved in a foiled arson attempt on an IKEA furniture store in Vilnius in May 2024. Western security officials believe the plot was a test run for a larger future operation targeting cargo and passenger flights bound for the US and Canada.

## Network of Chinese websites pose as local news sites across Europe, including a Luxembourg outlet

**State:** Luxembourg
**Threat actor:** China (suspected)
**Date:** 2023–present
**Incident type:** information operation
**TTPs:** establishing inauthentic news sites

Beijing-based public relations firm Shenzhen Haimaiyunxiang Media created a network of 123 websites that posed as local news outlets in 30 countries across Asia, Latin America and Europe to spread pro-Beijing propaganda. This included faux Luxembourg outlet Gaul Journal.

According to CitizenLab discovering the operation, the sites combined plagiarized local content intermixed with English-language content sourced from Chinese state media and advertisements promoting Chinese products. Researchers noted that the political content published on the websites had two primary themes: attacking critics of the Chinese government and spreading conspiracy theories aimed at denigrating the US and its allies. For example, an article criticizing a Chinese virologist who alleged that COVID-19 originated from a Chinese government laboratory appeared on every active website in the network.

The operation drew a significant portion of its content from Times Newswire, a newswire service previously linked to another Chinese influence operation attributed to the Shanghai marketing firm HaiEnergy. The operation received little engagement from online users, according to CitizenLab. It was likely intended to artificially boost the visibility of the articles on search engines.

## Pro-Kremlin hacking group takes down Times of Malta website

**State:** Malta
**Threat actor:** Russia (suspected)
**Date:** 2024
**Incident type:** Cyber operation
**TTPs:** DDoS

On 6 February 2024, pro-Kremlin hacking group known as the People's Cyber Army of Russia (CARR) took down the Times of Malta website in a DDoS attack that lasted several hours. Already during the attack, CARR claimed on Telegram that it was responsible for the hack and called on its 31,600 subscribers to also "attack" the Times of Malta website. The Telegram post stated that the hacking group targeted the outlet for supporting sanctions against Russia and threatened to attack other Maltese sites.

The attack rendered the website inaccessible for around 45 minutes, after which the hacking group instructed its Telegram followers to continue the attack. CARR also threatened on Telegram to attack websites belonging to the University of Malta as well as the Malta Tax and Customs Administration, though it appears that those attacks did not materialize.

## China operates overseas police stations in Netherlands to monitor and harass dissidents

**State:** Netherlands
**Threat actor:** China
**Date:** 2018–2022
**Incident type:** Political and civil society subversion
**TTPs:** Targeting diaspora communities; espionage; harassment

In November 2022, Dutch authorities ordered China to close two illegal police stations it had been operating in Amsterdam and Rotterdam since 2018 to target Chinese dissidents. According to several media investigations, these stations appeared to function as diplomatic service posts for Chinese-Dutch citizens, helping with administrative tasks like issuing passports or renewing driver's licenses. However, they also served the second purpose of monitoring and harassing Chinese dissidents in the country. Both stations were reportedly overseen by former Chinese military and intelligence officers.

Chinese political dissident Wang Jingyu, who had fled to the Netherlands after openly criticizing Beijing online, told investigators that an officer from the Rotterdam police station called and pressured him to return to China, telling him to "think of his parents." Wang was also falsely detained after the Chinese Embassy in the Hague told Dutch authorities it had received bomb threats in his name. The stations in the Netherlands are part of a larger network of more than 100 overseas police stations operating globally, including in Spain, Italy, the US and Canada.

## Russian assets sabotage important Polish train line and aid route to Ukraine

**State:** Poland
**Threat actor:** Russia
**Date:** November 2025
**Incident type:** Kinetic operation
**TTPs:** Sabotage; employing proxies (criminal network)

In November 2025, Polish prosecutors charged three men with working with Russian intelligence to sabotage a railway that connects Poland to Ukraine, a critical supply line for aid. According to Polish authorities, the suspects placed two devices on the line, one of which exploded near a village outside Warsaw. The explosion destroyed parts of the tracks but caused no injuries. Also power lines were damaged as part of the attack near the city of Lublin, in what authorities suspected was an attempt to derail a train.

Two perpetrators fled to Belarus, including one previously convicted in Lviv, Ukraine for "acts of sabotage." Polish Prime Minister Donald Tusk described the attack as "the most serious national security situation in Poland since the outbreak of [Russia's] full-scale war in Ukraine." He subsequently raised the threat alert for critical rail lines to its second-highest level.

## Russia spreads false claims about 2025 Iberian Blackout

**State:** Portugal
**Threat actor:** Russia
**Date:** 2025
**Incident type:** Information manipulation
**TTPs:** Amplifying false narratives (via inauthentic news sites, social media and bot networks); impersonating news outlets

In late April 2025, Russian influence networks exploited the widespread power outage in Portugal and Spain to spread lies about its cause. According to an investigation by Maldita.es, Russian influence network Storm-1679 started spreading fabricated content that falsely blamed the power outage on Europe's sanctions against Russia less than 24 hours after the incident. Doctored news content included a video mimicking France 24 and an article posing as the British newspaper The Independent.

This content was amplified by a network of Telegram channels and was later republished in English and Spanish on the Pravda network, which disseminates pro-Russian propaganda. Pravda was also responsible for spreading fake satellite images that depicted the Iberian Peninsula in darkness with the rest of Europe illuminated.

## Romanian crime group allegedly collaborates with Russia to plot coup

**State:** Romania
**Threat actor:** Russia (assisted)
**Date:** 2023–2025
**Incident type:** Political and civil society subversion; kinetic operation
**TTPs:** Employing proxies (crime network); espionage; inciting insurrection

In March 2025, Romanian authorities arrested six individuals suspected of collaborating with Russia to plot a coup against the Romanian government. The suspects allegedly sought to form a paramilitary group, called the "Vlad Țepeș Command", after Vlad the Impaler, to overthrow the government in Bucharest. The group also planned to replace the country's constitution, dissolve political parties and pull Romania out of Western alliances, including the EU and NATO.

Romanian intelligence revealed the suspects actively requested support from officers of the Russian embassy. Two had traveled to Moscow in January 2025 to meet with backers. As part of the investigation, Romania also expelled two diplomats from the Russian Embassy in Bucharest for aiding the coup plotters and engaging in intelligence-gathering activities.

## Russian influence campaign blames Ukraine for attempted assassination of Slovak Prime Minister

**State:** Slovakia
**Threat actor:** Russia
**Date:** May 2024
**Incident type:** Information operation
**TTPs:** Amplifying false narratives (via bot networks and traditional media)

In May 2024, Russian-state backed operatives launched a seemingly coordinated and widespread information campaign which sought to link Ukraine to the attempted assassination of Slovak Prime Minister Robert Fico. Online bot accounts, some linked to Russia's Doppelganger network, flooded Fico-themed discussions on X and Reddit with speculation that the shooter was affiliated with pro-Ukrainian forces.

Russian state media also seized on the shooting to claim Fico was a victim because of his sympathies toward Moscow. A Sputnik "investigation" suggested Fico was "the West's next Color Revolution target." Another blamed the "EU censorship apparatus" for creating an environment that fuels political violence. An analysis by the research group Antibot4Navalny of more than 100 Russian-language pro-Kremlin Telegram channels found that they "uniformly" claimed that the attempted assassination was motivated by Fico's "pro-Russian stance." These channels also blamed Western media outlets for allegedly justifying the attack because of Fico's lack of support for Ukraine. This campaign fits a pattern of pro-Kremlin information operations blaming Ukraine for various assassinations and assassination attempts. This includes those targeting Donald Trump and US political commentator Charlie Kirk.

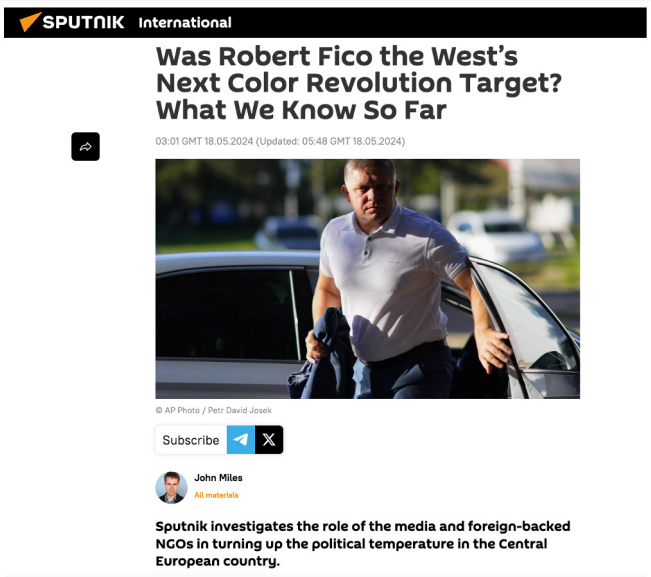



**Image 7** A Sputnik article suggesting the West was behind Fico's assassination attempt.

## Russian state-linked hacking group takes down Slovenian government websites

**State:** Slovenia
**Threat actor:** Russia
**Date:** March 2024
**Incident type:** Cyber operation; information operation
**TTPs:** DDoS; developing video-based content

In March 2024, Kremlin-linked hacking group known as the Cyber Army Russia Reborn (CARR) launched a large-scale DDoS cyber campaign against several Slovenian government websites over the country's support for Ukraine. The campaign, which lasted several days, brought down the website of the Slovenian president for multiple hours. It also targeted websites belonging to the National Assembly, the state broadcaster RTV Slovenija and several other government institutions.

On X, CARR claimed that the attack was a response to Slovenia's decision to contribute €1 million to a Czech initiative to procure ammunition for Ukraine. CARR also released a Slovenian-language video message: in it, the group said Russia and Slovenia "need not hate each other" (Authors' translation), given their shared Slavic heritage. CARR is reportedly directed and funded by Russia's military intelligence agency.

## Russian defector assassinated in Spain

**State:** Spain
**Threat actor:** Russia (suspected)
**Date:** November 2024
**Incident type:** Kinetic operation
**TTPs:** Targeted assassination

Maxim Kuzminov, a Russian helicopter pilot who defected from Russia to Ukraine, was shot and killed in the Spanish resort town of Villajoyosa in November 2024. Kuzminov made international headlines a year earlier when he worked with Ukrainian intelligence to fly a MI-8 helicopter from Russia to Ukraine, providing Kyiv with a valuable piece of equipment and propaganda coup. In interviews after his defection, Kuzminov claimed that despite receiving a $500,000 reward, he switched sides because of moral opposition to Russia's war.

Russian state media labelled Kuzminov a traitor and suggested that it was "only a matter of time" before he was tracked down by Russian intelligence. According to Ukrainian officials, Kuzminov subsequently left Ukraine and was living under a false identity in Spain before he was gunned down in what appeared to have been a targeted hit.

Following news of the killing, Sergey Naryshkin, director of Russia's Foreign Intelligence Service told Russian state-media outlet TASS: "This traitor and criminal became a moral corpse at the very moment when he planned his dirty and terrible crime." (Authors' translation.) Spanish authorities have made no arrests in the case and have not publicly accused Russia. However, according to El Pais, Spanish intelligence officials have "no doubt" that the Kremlin was involved.

## Russia and Iran amplify and spread false claims about Quran burning protests in Sweden

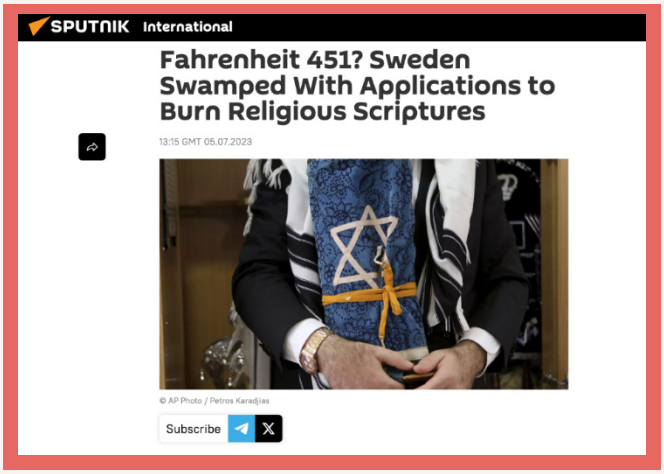
**State:** Sweden
**Threat actor:** Russia, Iran
**Date:** 2023
**Incident type:** Information operation; political and civil society subversion; malign finance; cyber operation
**TTPs:** Amplifying false narratives (via traditional media); organizing protests; SMS hijacking

In 2023, Russian and Iranian influence networks amplified and spread false claims about a spate of protests in Sweden that included Quran burnings. According to Sweden's Psychological Defence Agency, Russian state-controlled media outlets including RT and Sputnik published a series of articles in Arabic and other languages. The outlets falsely claimed that the Swedish government supported Quran burning and suggesting Sweden is an Islamophobic country.

Investigations later revealed that a Quran burning in Stockholm near the Turkish embassy had been organized and financed by Chang Frick, a far-right Swedish journalist and former RT contributor. Frick admitted that he had paid the permit for the demonstration and had recruited far-right politician Rasmus Paludan to burn a Quran. Sweden's Psychological Defence Agency said the incident was part of a larger campaign to disrupt Sweden's NATO membership process: at the time, Turkey and Hungary's votes were still needed for ratification.

Iranian media and state-linked accounts echoed Russia's coverage of the Quran burnings: they claimed that the protests were committed with the "approval" of Swedish authorities. They also alleged Sweden to be part of a wider network of Western countries using "freedom of expression" as a cover for anti-Islamic rhetoric. As part of this effort, Iran's Islamic Revolutionary Guard Corps (IRGC) hacked into a local Swedish SMS operator, sending around 15,000 text messages calling for retaliation for the Quran burnings.

Russia's and Iran's attempts to stoke outrage of the Quran burnings built on real and invented interethnic tensions in Sweden, fitting a pattern of both countries using social cleavages to advance their own strategic objectives.


**Images 8 and 9** Examples of Russian state media articles promoting narratives that Sweden is Islamophobic and supported the Quran burnings. The RT Arabic article is titled "Sweden and the phenomenon of Quran burning: the habit of the weak from the West. 'Burn in hell, you demons'!" (Authors' translation).

# Conclusion

The incidents in this paper show that the tactics used by adversarial states have evolved since the EU and its member states first recognized the danger of hybrid threats. Information operations and cyber-attacks are being supplemented with kinetic actions ranging from sabotage to drone incursions. In the cases we highlighted, kinetic operations played a part in more than half of the incidents (14 of 27). Even factoring in the subjective nature of our selection process, we almost certainly would not have uncovered as many examples prior to the full-scale invasion of Ukraine.

We also found that hybrid activities are increasingly directed from abroad but conducted from within. This almost certainly reflects the more difficult operating environment for Russian spies in Europe, but it also highlights the ease with which foreign agents can recruit local assets via anonymous and encrypted messaging platforms. This finding speaks to a need for European policymakers to address questions about how to distinguish foreign from domestic threats, especially when adversarial states are intentionally blurring those lines.

Our findings also demonstrate that different hybrid threats cannot be addressed in isolation. Most of the incidents in this report included a combination of different attacks, highlighting how certain tactics are deployed in the service of, or as precursors for, other malign activity. Acts of vandalism, for example, were almost always paired with information operations. The tactics documented in this report exist on a wide spectrum, from the establishment of faux local news sites on one end to the targeting of critical infrastructure and assassinations on the other. Their interconnectedness stresses the need to understand them all as part of a wider effort to undermine and destabilize Europe.

As this report makes clear, no EU country is immune to hybrid threats. That includes those that have actively courted better relations with Russia. And while Russia almost certainly will remain the predominant threat actor for the foreseeable future, other countries (including China, Iran and new players) will likely model its behavior. Therefore, all countries in the EU, not just those regularly targeted by Russia, will likely face future attacks.

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Toronto | Washington DC



**www.isdglobal.org**