April 2023

Protecting Europe's critical infrastructure from Russian hybrid threats

By Helmi Pillai

CENTRE FOR EUROPEAN REFORM
LONDON ★ BRUSSELS ★ BERLIN
1998–2023

Protecting Europe's critical infrastructure from Russian hybrid threats

By Helmi Pillai

- ★ Hybrid tactics are used to destabilise targets by circumventing the methods of standard warfare and instead exploiting political, economic and social vulnerabilities, alongside military ones. After Russia's invasion of Ukraine in February 2022, European policy-makers have become increasingly concerned about Moscow's use of hybrid attacks and the threat these pose to critical infrastructure.
- ★ Suspicious incidents, such as the disruption of railways in Germany, the sabotage of communication cables in France and GPS disturbances in Finland have all increased worries about the dangers posed by Russia's hybrid attacks.
- ★ Reports of Russian surveillance of energy infrastructure in Norway, the Netherlands and Belgium have further added to these concerns. With Europe shifting away from Russian energy imports, Norway has emerged as the EU's main gas supplier. Any disruption to its energy production would thus be a significant threat to Europe's energy security since it would be nearly impossible for the EU to find a replacement for Norwegian energy.
- ★ European countries have taken action to improve the resilience of national critical infrastructure. Norway, Denmark and the Netherlands have boosted security around vital energy infrastructure; France, Italy and the UK have invested in the protection of underwater infrastructure; and Czechia has published a national strategy specifically dedicated to countering hybrid threats.
- ★ While safeguarding critical infrastructure is primarily a national responsibility, the EU and NATO have stepped up efforts to counter hybrid threats and protect critical infrastructure. The EU and NATO can further increase co-operation in this area through more extensive intelligence sharing and the intensification of joint training and exercises, to better counter hybrid threats.
- ★ The EU should look to the Finnish and Swedish 'whole-of-society' approaches to increase resilience against hybrid threats. Countering hybrid threats requires greater collaboration at all levels, including the EU, NATO, national and local governments, and civil society.

Hybrid tactics are used to destabilise targets by exploiting political, economic, military and social vulnerabilities. Hybrid threats have become a growing concern for policy-makers since Russia's use of 'little green men' – unmarked Russian soldiers pretending to be pro-Russian separatists – to annex Crimea in 2014, and subsequent disinformation campaigns and interference in Western elections. The current tensions between the West and Russia have further heightened concerns about Russian hybrid attacks. These concerns have also been fuelled by several suspicious incidents throughout 2022; warnings that Moscow will increase cyber-attacks against Ukraine and its supporters;[1] and leaks suggesting that Russia is plotting attacks on critical infrastructure.[2]

The aim of hybrid tactics is to blur the lines between peace and conflict and cause significant damage to the target without crossing the threshold of detection, attribution and response. It is difficult to respond to a hybrid attack if one cannot identify the attacker or even be certain that hostile activity is taking place. To complicate matters further, hybrid attacks can take various forms, including physical sabotage, cyber-attacks, disinformation campaigns and economic pressure, which forces potential targets to prepare for diverse threat scenarios.

European policy-makers are particularly concerned about the threat of Russian hybrid attacks on critical infrastructure, which refers to assets and systems that are essential for basic societal functions. The definitions of critical infrastructure vary across countries but generally include information and communication, energy, transport, water, food, healthcare and financial infrastructure at the very least. Any disruption to these could have severe consequences for economic activity, social well-being and even national security.

"Any disruption to critical infrastructure could have severe consequences for economic activity, social well-being, or even national security."

The level of impact depends on the intention, success and type of the attack. The denial-of-service attacks that pro-Russian hacker groups like Killnet frequently launch against the websites of Western governments and companies tend to cause relatively limited and temporary disruption. Conversely, examples such as the power grid hack in Ukraine in December 2015, which left more than 230,000 people without power for several hours, demonstrate how severe an impact hybrid attacks can make.

Attribution is always challenging in hybrid attacks. But what would happen if it was proved that Russia had orchestrated a major attack on European critical infrastructure at a time of heightened tensions? Such a scenario might lead to serious escalation between Moscow and the West. Since 2016, NATO has publicly stated that a hybrid attack could trigger the mutual defence clause in Article 5 of the North Atlantic Treaty. In September 2022, Commission President Ursula von der Leyen warned that "any deliberate disruption of active European energy infrastructure is unacceptable and will lead to the strongest possible response."[3]

This policy brief examines the threat of Russian hybrid attacks on European critical infrastructure. First, it analyses Moscow's use of hybrid tactics, including several suspected acts of sabotage that occurred in 2022. Second, it highlights pieces of critical infrastructure that could make particularly attractive or vulnerable targets for Russia. Third, it evaluates the actions taken by European states, NATO and the EU to counter hybrid threats and safeguard critical infrastructure. Fourth, it assesses the effectiveness of a 'whole-of-society' approach to increasing resilience against potential attacks. Finally, the brief offers recommendations to further improve European efforts to counter Russian hybrid threats.

Russian thinking about hybrid warfare

Hybrid tactics have been a crucial part of the Kremlin's toolbox for many years. In an article published in 2013, Valery Gerasimov, Russia's Chief of the General Staff, argued that "The very 'rules of war' have changed. The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[4] Many in the West have interpreted Gerasimov's article as a clear expression of Russia's hybrid strategy, although some experts have downplayed its significance.[5] The Russian

1: Shane Huntley, 'Fog of war: how the Ukraine conflict transformed the cyber threat landscape', Google Threat Analysis Group, February 16th 2023.
2: Luke Harding, Stiliyana Simeonova, Manisha Ganguly and Dan Sabbagh, '"Vulkan files" leak reveals Putin's global and domestic cyberwarfare tactics', *The Guardian*, March 30th 2023.
3: Sabine Siebold, 'EU sees sabotage of Nord Stream, warns against attacks on "active infrastructure"', *Reuters*, September 27th 2022.
4: Valery Gerasimov, 'The value of science is in the foresight: new challenges demand rethinking the forms and methods of carrying out combat operations', *Military Review Courier,* February 27th 2013, translated by Robert Coalson.
5: Mark Galeotti, 'I'm sorry for creating the "Gerasimov Doctrine"', *Foreign Policy*, March 5th 2018.

leadership has also referred to employing hybrid tactics in official documents, including, most recently, in the 2021 National Security Strategy, which states that Moscow "considers it legitimate to take symmetric and asymmetric measures necessary to suppress … unfriendly actions and to prevent their recurrence in the future." The Kremlin argues, however, that hybrid conflict is not one-sided, since the West is also adopting similar tactics against Russia. In January 2023 Russian Foreign Minister Sergey Lavrov argued that the war in Ukraine was "our response to a hybrid war unleashed by the West," and in March, Dmitry Peskov, Press Secretary of the Russian president, predicted that the "hybrid war of hostile countries against the Russian Federation" will continue for years.[6]

"Fears of future hybrid attacks have intensified significantly following Russia's full-scale invasion of Ukraine."

There are several examples of Russia using hybrid tactics in Europe. Most recently, these have been targeting Ukraine, including using unmarked 'little green men' in the annexation of Crimea and the intervention in eastern Ukraine in 2014, and systematically targeting Ukrainian critical infrastructure with physical and cyber-attacks for years before the full-scale invasion. But Russia has also used hybrid attacks against other European countries, including by allegedly blowing up ammunition depots in the Czech Republic and Bulgaria in 2014 and 2015; interfering in elections; and launching several disinformation campaigns.

Fears of future attacks have intensified significantly following Russia's full-scale invasion of Ukraine and the sabotage of the Nord Stream pipelines. While many in the West initially blamed Russia for the pipeline attacks, doubts have recently emerged regarding Russia's involvement. Still, the protection of critical infrastructure from Moscow's efforts at sabotage has become an urgent concern. In October, European Commission President Ursula von der Leyen described critical infrastructure as "the new frontier of warfare" and, in November, EU Commissioner for Home Affairs, Ylva Johansson, warned that "there's a map somewhere in Russia pinpointing hospitals, power plants and water supply as targets".[7]

There are several reasons why Russia could benefit from ramping up its hybrid efforts against Europe. First, the Kremlin views itself as in conflict with the West, but lacks the military capabilities to challenge NATO in a conventional war.[8] The deniability of hybrid attacks makes them much less likely to provoke a strong response from the West, thus allowing Russia to sow chaos without triggering a direct conflict with NATO.

Second, Russia's invasion of Ukraine has not gone as planned. After more than a year of fighting, Ukraine continues to successfully resist the invasion with considerable support from its Western allies. By targeting European critical infrastructure, Moscow could help to destabilise the West. Russia could, for example, disrupt Western efforts to supply weapons and munitions to Ukraine, undermine Western public support for the war and even politically destabilise some Western countries. There is evidence to suggest that this may indeed be what the Kremlin is plotting. In March, Poland charged six foreign nationals with planning to sabotage arms deliveries to Ukraine.[9] The so-called 'Vulkan files,' which were recently leaked, also seem to demonstrate Moscow's intention to launch attacks against the West.[10] The documents, which were shared by a whistle-blower from a Russian cybersecurity consultancy with ties to the military, show plans to target European critical infrastructure such as a nuclear power station in Switzerland.

Third, Russia's energy blackmail against the EU has been less effective than the Kremlin hoped. Last June, former Russian president Dmitry Medvedev threatened that Europeans would be "freezing in their homes" without Russian energy, but this has not happened.[11] Within eight months of the invasion, the EU had replaced around 80 per cent of Russian natural gas imports. While the transition away from Russian energy has led to higher energy prices, it has not crippled the economy or driven European citizens to turn against efforts to support Ukraine.

Considering Russia's strategic aims, past behaviour and limited conventional means to target the West, hybrid attacks could be the most effective option for Moscow to destabilise Europe and undermine its support for Ukraine.

Russian tactics and suspicious incidents

Russia has probably already carried out acts of sabotage against European critical infrastructure. There have been several suspicious incidents over the past year, although definitive proof has not yet been

6: Claudia Rowan and Josh White, 'Vladimir Putin warns Finland that joining Nato would be a 'mistake'', *The Telegraph*, May 14th 2022.
7: Eszter Zalan, 'Von der Leyen: EU must now protect critical infrastructure', *EU Observer*, October 10th 2022; Wester van Gaal, 'MEPs approve bill to protect Europe's critical infrastructure amid Moscow threat', *EU Observer*, November 22nd 2022.
8: Alina Polyakova and Mathieu Boulègue, 'The evolution of Russian hybrid warfare: Executive summary', CEPA, January 29th 2021.
9: Adam Easton, 'Entire Russian spy network dismantled in Poland', BBC News, March 16th 2023.
10: Luke Harding, Stiliyana Simeonova, Manisha Ganguly and Dan Sabbagh, '"Vulkan files" leak reveals Putin's global and domestic cyberwarfare tactics', *The Guardian*, March 30th 2023.
11: Philip Oltermann, Jon Henley, Angelique Chrisafis, Sam Jones, Shaun Walker, 'How Putin's plans to blackmail Europe over gas supply failed', *The Guardian*, February 3rd 2023.

established. Last March, several aircraft in Finland reported unusual GPS disturbances, which prevented planes from landing at the Savonlinna airport near the Russian border. Jukka Savolainen of the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), stated that these incidents were probably part of Russia's hybrid strategy.[12] He emphasised that it is still unknown if they were the result of a deliberate attack or an unintended side effect of Russia's military training but argued that, regardless of the reason, Finland should prepare for more interference.

Last August, Estonian officials reported that the country had been faced with "the most extensive cyber-attack" since 2007, when several Estonian websites including the parliament, newspapers, banks, and government ministries were targeted in a large-scale attack.[13] The pro-Russia hacker group Killnet took responsibility for the August 2022 attack, and claimed that it had blocked access to over 200 state and private institutions, though Estonian officials stated that the event had caused only minor disruption.

"The incident could have been intended as a "warning" to Germany because of its support for Ukraine."

Last October, there was significant disruption to railways in northern Germany, after essential communication cables were cut at two separate sites.[14] This forced trains to stop for three hours, causing chaos for thousands of passengers. German Transport Minister Volker Wissing described the incident as "sabotage," calling it a "deliberate and malicious" act that was "clearly premeditated." While not directly blaming Russia, Wissing said that the involvement of a foreign power could not be ruled out. Anton Hofreiter, a Green party MP, pointed the finger more directly at the Kremlin, saying that the incident could have been intended as a "warning" to Germany because of its support for Ukraine.[15] Despite the speculation, no evidence has been produced to prove that Moscow was responsible.

Also in October, internet cables were cut simultaneously at three separate locations in the south of France, which caused severe disruptions to internet and phone services. Internet service provider Free described the incident as "an act of vandalism on our fibre infrastructure."[16] This followed a similar incident in April, when internet cables were deliberately cut in multiple locations near Paris, causing an internet blackout for thousands of people.[17] Nicolas Guillaume, the CEO of one of the providers impacted by the attack, argued that "The cables [were] cut in such a way as to cause a lot of damage and therefore take a huge time to repair," suggesting that it was "the work of professionals."

Last February, Dutch authorities reported that multiple hospitals around Europe had been targeted by Killnet but said that the attacks had only limited impact.[18] The attack seemed to specifically target countries that have strongly supported Ukraine, including the UK, Germany, Poland and the US.

These are only a few examples of the many suspicious incidents that have occurred since February 2022. So far, pro-Russian forces have only claimed responsibility for the cyber-attack in Estonia. Many have suspected the involvement of Moscow or government-linked groups in the other attacks as well, but there is insufficient evidence to determine if this was the case, which illustrates the problem of attribution that is so typical of hybrid attacks. Whether or not Russia is to blame for any of these incidents, the examples show that European critical infrastructure is vulnerable to sabotage efforts and more must be done to increase its resilience.

Potential vulnerabilities

While these incidents have only caused limited disruption, European policy-makers worry that Russia could launch more damaging hybrid attacks against critical infrastructure. Johansson stated in October that "We know that we are vulnerable … it's clear that this war and this threat is also [directed] towards the European Union and we have to be aware of this threat and we have to prepare."[19] One reason preparation is difficult, however, is the sheer number of potential targets. Modern societies depend on the functioning of complex and interconnected critical infrastructure systems. The interdependence of different systems creates numerous vulnerabilities for physical or cyber sabotage efforts. While there are too many potential targets to list, some clearly stand out due to their vulnerability and/or importance.

12: 'Security specialist: GPS-jamming of Finnish aircraft likely Russian hybrid attack', *Yle News*, February 1st 2023.
13: Pascale Davies, 'Estonia hit by 'most extensive' cyber-attack since 2007 amid tensions with Russia over Ukraine war', *Euronews*, August 19th 2022.
14: Hans von der Burchard, '"Sabotage" causes major train disruption in northern Germany', *Politico*, October 8th 2022.
15: 'Germany probes rail 'sabotage' amid Russia tensions', *France 24*, October 9th 2022.
16: John Psaropoulos, 'Europe awakens to the threat of sabotage by Russian agents', *Al Jazeera*, January 17th 2023.
17: Matt Burgess, 'The unsolved mystery attack on internet cables in Paris', *Wired*, July 22nd 2022.
18: 'European hospitals targeted by 'pro-Russian' hackers', *Euronews*, February 1st 2023.
19: Sandor Zsiros, 'European infrastructure is 'vulnerable' and needs greater protection, says EU commissioner', *Euronews*, October 3rd 2022.

Energy infrastructure

Energy infrastructure is one of the most crucial areas of concern. The vulnerability of global energy infrastructure has been repeatedly highlighted by experts. In February 2022, several European oil facilities were targeted with cyber-attacks, though the motive and perpetrator behind the attacks is unknown. Norwegian oil and gas installations are particularly attractive for Russian hybrid attacks. Ståle Ulriksen, a researcher at the Royal Norwegian Naval Academy, argues that "as a strategic target for sabotage, Norwegian gas pipelines are probably the highest value target in Europe."[20] This is because following the EU's transition away from Russian energy imports, Norway has become the EU's largest supplier of natural gas, accounting for nearly 25 per cent of the EU's gas imports in 2022.[21] If Norwegian energy deliveries were disrupted, prices would increase massively, and it would be nearly impossible for Europe to find alternative sources of supply. Last year, Norwegian authorities arrested and charged several Russian nationals with flying drones illegally over oil and gas installations. A drone accident, let alone a deliberate attack with a kamikaze drone of the type used against Ukrainian targets, could cause a shutdown of production, significantly delaying oil and gas deliveries. Norway has deployed its military to protect its critical energy infrastructure, but the threat remains. For the moment, Norway's internal security agency (PST) considers it unlikely that Russia would launch a hybrid attack on Norway's territory, but it assesses that the likelihood could increase if Moscow were willing to risk a further escalation with NATO and the West.[22] In this kind of a scenario, the PST views the petroleum sector to be a "particularly vulnerable target."

"The likelihood of an attack could increase if Moscow were willing to risk a further escalation."

Norway is not the only potential target — other European countries have also reported suspicious Russian activity around their energy infrastructure. In February, the Dutch military intelligence and security service (MIVD) warned of potential Russian activity near its energy infrastructures in the North Sea, stating that Moscow was undertaking "activities that indicate espionage as well as preparing operations for disturbance and sabotage." MIVD director Jan Swillens stated that Russia seems "very interested in how they could sabotage the energy infrastructure."[23] In addition to wind farms and gas pipelines, the Dutch authorities named underwater cables as potential targets. Belgium also recently revealed that it was investigating a Russian 'spy ship' in the North Sea. Belgian Minister of Justice Vincent Van Quickenborne stated: "We don't know the exact motives of this Russian ship, but let's not be naïve (…) especially if it behaves suspiciously close to our windfarms, undersea gas and data cables and other critical infrastructure." Russia's spying around critical infrastructure and the plans for cyber-attacks on a Swiss nuclear power station indicate that energy infrastructure is probably high on Moscow's list of potential targets.

Communications infrastructure

Another possible target for Russia is European communications infrastructure, and specifically the subsea networks consisting of over half a million miles of fibre-optic cables. These are crucial for the functioning of the global economy and digital services; they carry more than 95 per cent of global internet traffic, and financial transactions worth around $10 trillion travel through them every day. The cables facilitate communication within Europe and connect the continent to the rest of the world. They are also important for national security, as military and intelligence operations heavily depend on them. Their importance is further increased by the fact that there is a lack of alternatives: while satellites or land-based cables can be used for some communications, they are completely insufficient for the needs of the digital economy. As a result, any harm to undersea cables would be highly damaging for the economy, security and the general functioning of European societies.

Military officials and other experts have long warned of the Russian threat to the subsea infrastructure. In January 2022, Admiral Sir Tony Radakin, head of the UK armed forces, assessed that Russia's submarine and underwater activity had increased significantly over the past two decades, giving Moscow the ability to sabotage undersea cables.[24] In a 2017 report, then backbencher MP Rishi Sunak highlighted the specific threat posed by Russia, and concluded: "Sabotage of undersea cable infrastructure is an existential threat to the UK. The result would be to damage commerce and disrupt government-to-government communications, potentially leading to economic turmoil and civil disorder".[25] The EU's recent assessment is slightly less alarming.[26] According to an analysis produced for the European Parliament's Subcommittee on Security and Defence (SEDE) in June 2022, a disaster scenario such as a continent-wide internet blackout is unlikely due to the number of back-up cables available. But if Russia were to attack multiple cables at the same time, there could be severe damage and disruption.

20: Mark Lewis, 'Fears over Russian threat to Norway's energy infrastructure', *The Independent*, October 23rd 2022.
21: Emily Rauhala, 'Norway is portrayed as both hero and villain in Europe's energy crisis', *The Independent*, October 12th 2022.
22: The Norwegian Police Security Service, 'National threat assessment: 2023', February 15th 2023.
23: Charlie Cooper, 'Russia 'mapping' critical energy infrastructure, say Dutch intelligence agencies', *Politico*, February 20th 2023.
24: Larisa Brown and Catherine Philp, 'Admiral Sir Tony Radakin warns of Russian threat at sea', *The Times*, January 7th 2022.
25: Rishi Sunak, 'Undersea cables: indispensable, insecure', Policy Exchange, December 1st 2017.
26: 'Security threats to undersea communications cables and infrastructure – consequences for the EU', European Parliament, June 2022.

There are many challenges associated with safeguarding the subsea cable networks. They are typically unguarded, leaving them highly susceptible to sabotage attempts from submarines or unmanned underwater vehicles. The fact that many subsea cables are in remote but publicly known locations further compounds the problem, as it makes sabotage easier. Another significant challenge is that many subsea cables are located in international waters. While the UN Convention on the Law of the Sea grants countries jurisdiction over their territorial waters and some law enforcement obligations in the contiguous zones, the responsibility for protecting infrastructure outside these areas remains unclear. The fact that the cable networks are commonly operated by private companies with inadequate regulation further adds to the challenge.

"Russia continues to be a significant naval power, with the world's third most powerful navy."

All these factors make subsea infrastructure an attractive target for hostile states like Russia. The large number of public and private actors involved means that an act of sabotage could be difficult to prevent or effectively respond to. An attack on subsea cable networks could also be conducted quite easily through a low-cost operation without sophisticated technology, using for example, a civilian vessel hidden in normal sea traffic or with subsea explosives triggered from a distance. Cyber-attacks could also be used to target the network management systems that control the cable infrastructure, which enable their operators to remotely monitor and control these systems, to detect cable faults and survey data traffic. If a hacker were to gain control of such a system, they could severely disrupt internet traffic flows.

Despite the lacklustre performance of the Russian military in its offensive in Ukraine, its submarine force remains strong and capable. Moscow is still investing heavily in its submarine capabilities, which it views as necessary for challenging the West. Russia continues to be a significant naval power, with what is estimated to be the world's third most powerful navy.[27] It also has several naval bases, including in the Baltic, Black and Mediterranean Seas, which allow Russia to project power. Moscow has also repeatedly conducted naval research and exercises near subsea cables, including off the coasts of Ireland, Norway and Portugal.[28]

According to the EU's own assessment, the protection and resilience of its subsea cable network is insufficient and should be improved. One of the main challenges is the different level of awareness among EU member-states, which means that national policies vary significantly. Some member-states, such as France, Ireland and Portugal, have publicly discussed the threats to subsea infrastructure. France even published a dedicated national strategy for controlling the seabed last year. But many other EU member-states are less prepared for the threat.

Energy infrastructure and underwater cables are only two examples of the type of critical infrastructure that could be vulnerable to Russia's hybrid attacks. However, there are many more potential targets, ranging from water supplies to health facilities, sewage networks, financial services, transport systems and many more. The sheer number of targets is one of the biggest challenges in preventing and countering hybrid attacks. EU officials have admitted that securing all aspects of critical infrastructure is impossible.[29] Modern societies are reliant on the smooth functioning of countless critical infrastructure systems that are often operated by private companies with limited means or willingness to invest in security measures against such unpredictable threats. This creates significant vulnerabilities for malicious actors like Russia to exploit.

EU, NATO and national responses

European governments

The primary responsibility for protecting critical infrastructure lies with national governments. While European countries have taken action to safeguard vital infrastructure, some experts have questioned whether governments have the knowledge or resources to do so appropriately. The fact that these systems are often owned by foreign companies also means that governments may not have the authority to take the necessary measures.

Nonetheless, European countries have taken action to improve security. Norway, Denmark and the Netherlands have all increased security around energy infrastructure.[30] France is planning to invest €3.1 million in ocean floor defence to improve the protection of natural resources and undersea infrastructure like cables.[31] France has also invested €11 million in purchasing two unmanned underwater vehicles to further protect its infrastructure. In addition to this, Paris is increasing inspection and surveillance of its subsea internet cables. Italy has improved the surveillance of submarine

27: 'Global Naval Powers Ranking: 2023', World Directory of Modern Military Warships, 2023.
28: Sebastian Seibt, 'Threat looms of Russian attack on undersea cables to shut down West's internet', France 24, March 23rd 2022.
29: Simon Tisdall, 'Unseen and underhand: Putin's hidden hybrid war is trying to break Europe's heart', *The Guardian*, October 23rd 2022.
30: 'Nord Stream: Norway and Denmark tighten energy infrastructure security after gas pipeline 'attack'", *Euronews*, September 28th 2022.
31: Peter O'Brien, 'France tightens subsea cable security amid growing fear of sabotage', *Politico*, October 13th 2022.

energy and telecommunications cables,[32] and the UK has announced that it will dedicate the first of its two multi-role ocean surveillance ships to safeguarding underwater telecommunications cables as well as oil and gas pipelines.[33] Germany released a strategy paper detailing new regulations aimed at protecting critical infrastructure, which includes identifying the areas in need of additional safeguarding and outlining minimum standards for those operating vital infrastructure.[34]

Some countries have also devised more comprehensive strategies to deal with hybrid threats. In 2021, Czechia released a national strategy solely focused on hybrid threats, which includes detailing tactics that could be used against them and outlining countermeasures like improving the resilience of critical infrastructure.[35] In 2022, Sweden appointed a minister for civil defence, Oskar Bohlin, who is tasked with strengthening resilience across society, including against hybrid threats.

"Security is not the sole responsibility of the state but requires the active involvement of all actors."

Sweden and Finland have long followed a 'whole-of-society' approach to security. This approach postulates that security is not the sole responsibility of the state but instead requires the active involvement of all actors in society, from the private sector to non-governmental organisations, and even ordinary citizens. Officials advise companies on how to be prepared for an attack, and to ensure that the basic functions of the economy can continue in the event of crisis or war.

The private sector also plays a key role in maintaining security of supply. In Finland, some critical sectors are legally obliged to ensure backup plans for their critical processes, and in Sweden critical businesses are legally required to contribute to 'total defence' planning. Civil society organisations offer preparedness-related training and information for citizens and provide volunteers to assist the authorities during crises. The role of ordinary citizens is also important for resilience. In both countries, citizens are expected to prepare for disruptions. In 2018, the Swedish government distributed a pamphlet to each household with instructions on how to prepare for crisis or war by storing a week's worth of food, water, cash and other essentials. The Finnish authorities ran a similar campaign, advising ordinary households to have enough supplies to survive 72 hours at home in case of an emergency.

Co-operation across all sectors is facilitated by common agreements, joint objectives, contingency planning and training. In Finland, national defence courses are a crucial aspect of the comprehensive security strategy. These courses, which are organised several times a year by the National Defence University, bring together leading military and civilian figures to facilitate co-operation across society in preparing for emergencies, building relevant networks, and providing an overview of Finnish foreign, security and defence policy.

NATO

Although the primary responsibility for protecting critical infrastructure lies with national governments, NATO and the EU have taken measures to prepare for Russian hybrid threats. Since 2016 NATO has explicitly stated that a hybrid attack against an ally could trigger the Article 5 mutual defence clause of the North Atlantic Treaty. This is important for deterrence, as it makes clear that a hybrid attack could lead to a collective response. However, the difficulty of identifying the aggressor behind a hybrid attack weakens deterrence. Examples like the Nord Stream pipeline sabotage demonstrate how difficult it would be for NATO and the West more broadly to respond to below-threshold attacks, when a culprit cannot definitively be proven.

NATO has also had counter-hybrid support teams on standby since 2018. These teams are made up of security experts and are available on short notice to help an ally respond to various types of hybrid threats. An ally has requested the assistance of the counter-hybrid support teams twice: in 2019 to assist Montenegro's efforts to counter Russia's election interference; and in 2021 to Lithuania when the Belarusian government caused a migration crisis by encouraging thousands of migrants to cross into Poland, Latvia, and Lithuania.[36] Furthermore, NATO's Joint Intelligence and Security Division has a hybrid analysis branch to improve shared situational awareness of hybrid threats within the alliance. In February, NATO also announced the creation of a Critical Undersea Infrastructure Co-ordination Cell, which aims to increase collaboration with relevant parts of industry and facilitate discussions between military and civilian stakeholders to improve the security of subsea infrastructure.

EU

The EU has been active in countering hybrid threats for years. In 2016 the EU adopted a Joint Communication on Countering Hybrid Threats, which sought to promote co-ordination at the EU level, improve situational awareness and build resilience. In the same year, the EU created a Hybrid Fusion Cell to facilitate information-

32: Giuseppe Fonte, 'Italy strengthens surveillance on underwater cables, source says', *US News*, October 3rd 2022.
33: 'Protecting seabed infrastructure – UK Multi-Role Ocean Surveillance Ship to be in service by 2023', Navy Lookout, October 3rd 2022.
34: Michael Nienaber, 'Germany Vows to Shield Infrastructure Against Russian Threats', *Bloomberg*, December 7th 2022.
35: Government of Czechia, 'National strategy for countering hybrid interference', 2021.
36: Sean Monaghan, 'Five steps NATO should take after the Nord Stream pipeline attack', CSIS, October 6th 2022.

sharing between member-states about hybrid threats. In 2017 the EU established a Cyber Diplomacy Toolbox for joint diplomatic responses to malicious behaviour in cyberspace. And in 2018 the EU published a Joint Communication on 'Increasing resilience and bolstering capabilities to address hybrid threats'.[37]

The EU has increased its efforts, especially over the past year. The EU's 2022 Strategic Compass for Security and Defence highlighted hybrid threats and critical infrastructure protection as key areas where the EU must improve its efforts. The Strategic Compass lays out plans to create an EU Hybrid Toolbox for co-ordinating EU and member-state responses to hybrid attacks, by combining all available civilian and military instruments that could be used against hybrid threats. The EU also plans to create EU Hybrid Rapid Response Teams, which would provide tailored national, civilian, and military expertise to support member-states, Common Security and Defence Policy (CSDP) missions and partner countries in countering hybrid threats.

"The EU's focus on protecting critical infrastructure is central to its efforts to counter hybrid threats."

The EU's focus on protecting critical infrastructure is central to its efforts to counter hybrid threats. In December, the European Council approved the Critical Entities Resilience directive, which replaced the 2008 European Critical Infrastructure Directive. The directive requires member-states to identify critical entities, perform risk assessments and report any disruptions. Furthermore, it tasks member-states with implementing national strategies to increase resilience and conduct regular stress tests, particularly on energy infrastructure, subsea cables and electricity grids. The directive expands the scope of the EU's previous directive on critical infrastructure protection from energy and transport infrastructure, to cover eleven sectors, including banking, financial market infrastructures, health, drinking water, wastewater, food, digital infrastructure, public administration and space.

Adding to the measures in the directive, the Commission has proposed further plans to improve the resilience of European critical infrastructure and accelerate the adoption of existing measures. In October, Commission President Ursula von der Leyen laid out a five-point plan, which advocates enhancing preparedness particularly in the energy sector.[38] The plan particularly emphasises the importance of safeguarding four of the eleven sectors outlined in the directive: energy, digital infrastructure, transport and space. Additionally, von der Leyen argued for improving response capacity through the Union Civil Protection Mechanism, which was established in 2001 and seeks to improve co-operation between EU member-states and eight other participating states in disaster preparedness . The plan also suggests using satellite capacity to detect potential threats – and proposes that the EU should further co-operate with NATO and other key partners to boost the resilience of critical infrastructure.

While member-states have generally been supportive of EU-level efforts to protect critical infrastructure, not all EU capitals are happy with the Commission's new plans.[39] For example, Germany, France, Sweden and Slovenia have opposed the expansion of the directive, arguing that the existing measures are sufficient. France has also demanded that the decision to respond collectively to incidents should not be mandatory, which is consistent with its past hesitation over the involvement of the Commission in counterterrorism measures, after the 2015 Paris attacks. Most member-states insist that stress tests should also be voluntary. Croatia has requested the creation of a financial mechanism in the EU budget to assist smaller member-states in making the necessary investments in safeguarding their critical infrastructure.

Another challenge to the EU's critical infrastructure protection efforts is that several member-states, including Italy, the Netherlands and Poland, have expressed reluctance to share information about their critical infrastructure, particularly subsea cables. Overall, the EU's ability to improve the safeguarding of critical infrastructure is hindered by a lack of trust between member-states and the difficulty of defining critical infrastructure. Certain member-states such as Austria, Hungary and Italy have also been traditionally more reluctant to involve the EU in countering hybrid threats, for many reasons, including a lower threat perception and fears of the EU eroding their sovereignty. In contrast, countries closer to Russia such as the Nordic states have been more active in pushing for greater collaboration in this area.

Although the EU has taken important action to counter hybrid threats and protect critical infrastructure, it is not yet clear how effective these will be. Whether or not these measures will be sufficient depends largely on how the member-states will implement the EU's directives and broader recommendations.

37: Kenneth Lasoen, 'Realising the EU Hybrid Toolbox: opportunities and pitfalls', Clingendael, December 2022.

38: 'Speech by President von der Leyen at the European Parliament Plenary on Russia's escalation of its war of aggression against Ukraine', European Commission, October 5th 2022.

39: Luca Bertuzzi, 'EU countries lay bare Europe's limits in securing critical infrastructure', *Euractiv*, November 3rd 2022.

NATO-EU co-operation

The EU and NATO are also working together against hybrid threats. In their Joint Declaration at NATO's Warsaw Summit in 2016, countering hybrid threats was identified as one of the key areas of co-operation. Since then, the EU and NATO have collaborated on various proposals to improve situational awareness, strategic communication, crisis response, resilience, and cyber security and defence. This has been done primarily through the establishment of staff-to-staff contacts between the two organisations. In the January 2023 EU-NATO Joint Declaration, the protection of critical infrastructure was identified as a core area for increased co-operation. On March 16th, the two organisations launched the new NATO-EU Task Force on Resilience of Critical Infrastructure, which seeks to facilitate co-operation between their staffs to share best practice, improve situational awareness and increase resilience. The initial focus areas will be energy, transport, digital infrastructure and space.

Another important way in which NATO and the EU co-operate is through the Hybrid CoE, which has been operating in Helsinki since 2017. Although the Hybrid CoE is an autonomous organisation, both the EU and NATO are members, and its activities are open to all EU and NATO countries. The central aim of the Hybrid CoE is to help its participating entities prevent and counter hybrid threats by producing relevant research, providing expertise and hosting exercises for countering hybrid threats.

While NATO and the EU have taken many steps to improve co-operation in countering hybrid threats, a crucial barrier to further collaboration continues to be the lack of trust between and within EU member-states and NATO allies, which hinders information sharing. While there is information sharing on a staff-to-staff level, this is more limited at the national government level. As the EU becomes more active in this area, there are also questions over duplication of efforts and division of labour. However, considering the different capabilities and mandates of the two organisations, the EU and NATO are well positioned to complement one another's efforts. While NATO has much greater capabilities in the military sphere, the EU has a significantly wider toolbox at the civilian level which is equally, if not more, necessary for countering hybrid threats.

Recommendations

Hybrid threats are, by design, complex, multifaceted and unpredictable. To boost resilience against such threats, greater collaboration is required at all levels, including the EU, NATO, national and local governments, the private sector and civil society. While important steps have already been taken, more extensive co-operation is necessary.

"Due to the complex nature of hybrid threats, it would be impossible to predict all possible threat scenarios."

More action can and should be taken to protect critical infrastructure, including energy infrastructure and undersea communication cables. Measures could include increasing both surface and subsea surveillance and patrolling around vital assets to detect potential threats and facilitate a quicker response. One way to do this would be to increase investments in coastguards, which currently tend to be overworked and underfunded. Another necessary step would be improving information and intelligence sharing between political leadership and the private sector, NATO and the EU, and between governments. To improve the security of subsea fibre-optic cables specifically, building redundancy is essential for mitigating the impact of a potential cable outage. With more alternative cables using a variety of routes, there would be less risk of multiple cables being damaged at once, which would decrease the likelihood and severity of disturbances to data traffic. Governments should work together with private companies to build more redundancy. Regular inspections and maintenance are also vital to help detect and fix issues before they can cause considerable damage.

International co-operation, particularly between the EU and NATO is also crucial. NATO and the EU would benefit from more frequent joint training and exercises in countering hybrid threats. This would enable them to gain a clearer understanding of their respective strengths and weaknesses, and it could also provide insights on ways to complement one another's efforts.

Due to the complex nature of hybrid threats, it would be nearly impossible to predict all possible threat scenarios or identify and remove all vulnerabilities. For this reason, the most important step would be to improve resilience across society, at both the national and EU level. The whole-of-society approach, which emphasises collaboration and preparedness across society, is the best model to counter such multifaceted threats. The private sector plays a crucial role in critical infrastructure protection as most vital assets are owned and operated by businesses. European governments should thus increase the participation of the private sector in safeguarding efforts, through a combination of regulation, incentives and investments in additional security measures. Initiatives such as the Finnish National Defence Courses, which regularly bring together leading figures from across society, to network and co-operate on preparedness, could be replicated at the European level to better protect cross-border infrastructure and improve overall security.

Civil society organisations, too, can play a vital role in providing training and information for the general population. Finally, individual citizens also have an important role in resilience. The EU and European governments could launch similar information campaigns to those that have taken place in Finland and Sweden, to ensure basic preparedness for households throughout the continent. It must be acknowledged, though, that differing security cultures would make it harder to take such initiatives in countries where the threats feel less acute than they do to those close to Russia.

Conclusions

The threat of Russian hybrid attacks has intensified in Europe following the invasion of Ukraine. Several suspicious incidents last year, the leaks about sabotage plans, Moscow's spying around critical infrastructure, and Russia's past hybrid attacks all suggest that concerns are legitimate. The Kremlin also has a clear reason for resorting to such tactics: hybrid attacks would be a way for Moscow to undermine European unity, stability, and support for Ukraine without triggering an escalation with NATO. And past experiences show that the West struggles to effectively respond to malicious activity below the threshold of conventional military action.

European governments, the EU and NATO have all stepped up efforts to counter hybrid attacks and protect critical infrastructure from sabotage efforts, but more action needs to be taken. Due to the multifaceted and unpredictable nature of hybrid threats, it would be nearly impossible for governments alone to identify all vulnerabilities or anticipate potential targets. To increase resilience sufficiently, action must be taken at all levels. For this, a whole-of-society approach, as practised by Finland and Sweden, presents a useful path forward. Collaboration between governments and the private sector, and international co-operation are particularly important. NATO and the EU should play a leading role in promoting joint efforts. Furthermore, civil society, including ordinary citizens, can also contribute significantly to resilience efforts.

Helmi Pillai
Clara Marina O'Donnell fellow (2022-23)

April 2023