BSR Policy Briefing series 1/2026

Pursuing technological supremacy and geopolitical power – Chinese and Russian espionage in Europe

By Hanna Mäkinen

ISSN: 2342-3153

Pursuing technological supremacy and geopolitical power – Chinese and Russian espionage in Europe

By Hanna Mäkinen

Hanna Mäkinen is a Senior Researcher at the Pan-European Institute, Turku School of Economics, University of Turku, Finland. Her research explores the complex interconnections between security, societal dynamics, and economic developments, with a particular focus on leveraging media and social media data to analyse these phenomena. Over the course of her academic career, Mäkinen has contributed to several national and international research projects and published articles on her research topics. Her recent work has addressed issues such as Russia's hybrid influence strategies in Europe, the online mobilisation of Russian anti-war activism, and the geopolitical significance of Russia's Arctic natural resources. She is currently a researcher in the project "Managing sustainability amidst geopolitical turbulence" (MANU), funded by the Foundation for Economic Education, which examines how firms can manage and advance their sustainability in a rapidly changing global security environment.

Abstract

The resurgence of great power competition has intensified Chinese and Russian espionage activities in Europe, posing significant threats to security and stability. China seeks technological dominance through legal and covert means, while Russia, driven by its confrontation with the West and the war in Ukraine, engages in aggressive intelligence operations to bypass sanctions and destabilize societies. Both actors employ a blend of traditional human intelligence (HUMINT), sophisticated cyber operations, economic coercion, and influence campaigns targeting critical infrastructure and democratic institutions. This report analyses their goals, methods, and recent cases of political, military, technological, and cyber espionage, compares their strategies, and explores implications for European security, offering recommendations to strengthen resilience against these growing threats.

Key words: great power competition, geopolitical tensions, technological sovereignty, Chinese espionage, Russian espionage, European security, human intelligence, cyber operations, influence campaigns

Disclaimer: The opinions expressed in this report represent those of the authors and do not represent the opinion of the Centrum Balticum Foundation, and thus, the Centrum Balticum Foundation does not bear any responsibility for the opinions expressed in the report.

Contents

1. Introduction

Along with the resurgence of great power competition, both China and Russia have intensified their intelligence activities in Europe, driven by strategic ambitions and geopolitical tensions. China's rapid technological rise and its aspiration to dominate strategic and emerging industries have led to widespread efforts to acquire advanced know-how through legal and covert means (Säpo 2025). Meanwhile, Russia's confrontation with the West, exacerbated by its war in Ukraine, has pushed it toward aggressive intelligence operations aimed at circumventing sanctions, gathering military and political intelligence, and destabilising European societies (Mäkinen & Liuhto 2025; Supo 2025). These developments underscore the growing complexity of espionage threats, which combine traditional human intelligence (HUMINT) with cyber operations, economic and political coercion, and influence campaigns targeting democratic institutions and critical infrastructure.

Europe faces growing threats from Chinese and Russian espionage, which pose significant risks to its security and stability. These threats target critical infrastructure, political institutions, and technological sovereignty, aiming to undermine democratic governance, disrupt essential services, and erode Europe's strategic autonomy. Covert HUMINT and influence campaigns, combined with increasingly sophisticated cyber operations, challenge European nations to safeguard their national interests and maintain resilience against foreign interference.

This report examines Chinese and Russian espionage in Europe, focusing on HUMINT and cyber operations. It analyses the goals and methods of Chinese and Russian espionage, and explores recent cases of their political, military and technological espionage and cyber operations targeting Europe. As a conclusion, it presents a comparison of Chinese and Russian espionage strategies, and discusses the implications of Chinese and Russian espionage for European security and ways to strengthen resilience against these growing threats.

2. The goals and methods of Chinese and Russian espionage

2.1 China: Technology-driven, long-term strategy

China's intelligence targets are influenced by intensifying great power competition between the USA and China, increasing Western criticism towards and export restrictions imposed on China, and China's own internal dynamics (Supo 2025). China seeks to acquire know-how and technology that will benefit its long-term strategic goal to become the world's leading economy and technological superpower, and further, to reshape the world order (Säpo 2024; Säpo 2025). However, the USA has restricted the export of semiconductor technology to China in order to limit China's access to these critical components. Semiconductors form the foundation of nearly all modern electronic devices and are of crucial importance for both civil and military technologies. Hence, the restrictions have had a significant impact on China's technological development (Shivakumar et al. 2024) and its goal to establish global high-tech dominance.

Chinese espionage targets a wide range of sectors, focusing on industries supporting its economic and technological development, such as microelectronics, artificial intelligence (AI), quantum technology, and military and dual use technologies. China seeks to modernise its industries by acquiring know-how and technology from abroad (Säpo 2024) and uses espionage as a key method to gain competitive advantage (Microsoft 2025a). It also aims to achieve self-sufficiency in terms of critical technology, such as semiconductors and AI, and rather make other countries, particularly the USA, dependent on China (Allen 2023). In addition, key areas of interest for Chinese intelligence include foreign and security policy decision-making, groups viewed as threat by the Chinese government, and critical infrastructure. Furthermore, as a part of its aspiration to succeed in great power competition, China seeks to acquire Arctic know-how and technology to strengthen its presence in the region. (Supo 2025)

China's methods in acquiring technology and know-how range from overt and legal methods, such as research and business collaborations, to covert and illegal methods, such as HUMINT and cyber espionage (Dragonfly Intelligence 2023; Säpo 2024). As regards overt methods, Chinese are well established in international business networks and skilled at utilising business contacts for various purposes.

Various legal channels, such as investments and acquisitions, are used to gain access to intellectual property (IP) and technologies abroad (Dragonfly Intelligence 2023). China's access to data through and control of Chinese communication technologies, software and Internet-connected devices also provide it potential tools for espionage, influencing and even cyberattacks and physical sabotage. The dependence on Chinese technology has raised significant concerns in both Europe and the USA, leading them to consider and impose restrictions on Chinese information and communication technology (ICT) and software, such as the social media platform TikTok and telecommunication infrastructure providers Huawei and ZTE. (Harrell 2025)

China is active in academia and has gained a firm foothold in universities worldwide, allowing it to gather information through university partnerships, academic exchanges and research collaborations. China also seeks to boost its scientific and technological capabilities with talent plans – recruitment programmes to attract top scientific and technological expertise from abroad to China by offering them significant financial and professional incentives. Talent recruitment programmes have raised concerns for instance among the US government about trade secret and IP theft. (FBI 2025) Technologies and knowhow applicable for military purposes also interest China, and because several Chinese universities are linked to the country's armed forces, academic cooperation is used to acquire the related expertise as well (Supo 2025).

When it comes to covert methods, China's civilian intelligence service, the Ministry of State Security (MSS), performs intelligence and counterintelligence operations, including HUMINT and cyber operations abroad. There are also other state organisations in China that specialise in intelligence and influencing, including the Chinese Military Intelligence Directorate (MID), the Chinese Ministry of Public Security (MPS), the International Department of the Communist Party of China (IDCPC), and the United Front Work Department (UFWD). (Supo 2025) These state agencies also collaborate with public universities and private companies to support China's espionage goals. There is no clear boundary between the public and private sectors in China (Dragonfly Intelligence 2023) and traditional espionage and corporate espionage are intertwined (Lassila 2024).

Chinese intelligence services perform traditional espionage under diplomatic cover as well as under various other cover identities, such as businesspeople and academics. Working as a journalist is one of the typical covers for Chinese intelligence officers (Skön 2024a). They also recruit HUMINT sources which often takes place through academic or professional channels and among people that have some connections to China (Dragonfly Intelligence 2023). Chinese nationals abroad are often targeted for intelligence gathering and recruitment – they can be easy targets for pressure if they intend to return to China or have family ties there (CSIS 2023). Chinese legislation also requires Chinese citizens and organisations to support and cooperate with national intelligence efforts (CNA 2023). In addition, China actively uses social media platforms, particularly LinkedIn, for intelligence gathering and recruitment. Social media provides a cheap and easy way to look for and contact suitable targets. Hiding the involvement of Chinese intelligence services is also easier in social media than in face-to-face contacts (Supo 2025).

Nevertheless, cyber operations are the primary form of espionage in China – for instance, according to the CSIS survey of Chinese espionage in the USA since 2000, almost half of the cases of Chinese espionage directed at the USA involved cyber espionage, usually by state-linked actors (CSIS 2023). Achieving cyber superpower status is an essential part of China's technological development and China's cyber resources are in a class of their own compared to most Western countries. China's extensive cyber capabilities pose significant security challenges for the West, as China can exploit them to achieve its political, economic and military goals. (Supo 2025) Chinese state-sponsored advanced persistent threat (APT)[1] groups are actively targeting global critical infrastructure networks, including telecommunications, transport, government and military infrastructure (Cybersecurity Advisory 2025), which creates possibilities for cyber influencing (Supo 2025). Chinese state-affiliated cyber actors use a wide range of sophisticated methods, which they adapt as information security evolves, and are able to quicky exploit the vulnerabilities they find (Microsoft 2025a). They actively exploit Internet-connected consumer devices that are poorly protected and also cooperate with Chinese public and non-governmental organisations and private IT companies in their operations, for instance in vulnerability research, malware creation and systemic intrusion into consumer devices (Microsoft 2025a; Supo 2025).

[1] According to Microsoft, "An advanced persistent threat is a long-term, targeted cyberattack designed to infiltrate an organization and remain hidden for as long as possible". APT groups are well-funded, skilled and motivated, and often connected to nation states or criminal networks. (Microsoft 2025b)

China also performs cyber operations and covert influencing that target political decision-making and public opinion, trying to undermine democratic institutions, influence matters and regions that are important for China's interests, and steer the discussion in a favourable direction. China also spies on and tries to control and pressurise Chinese citizens living abroad, in particular people it considers a threat, such as dissidents. (Gorera 2025; Microsoft 2025a; Supo 2025) In addition to covert influencing, China uses political and economic coercion, such as import bans for countries that have taken actions that are seen to conflict with China's interests (Säpo 2024). For instance, after the 2010 Nobel Peace Prize was awarded to Chinese dissident Liu Xiaobo, China imposed restrictions on Norwegian salmon imports (Lewis 2011). Following the opening of the representation of Taiwan in Vilnius, Lithuania, in 2021, China first imposed a customs block on Lithuanian exports. After it had proven ineffective, China imposed informal secondary sanctions on Lithuania, warning companies buying goods from Lithuania that they could face problems in their commercial relations with China. (Reynolds & Goodman 2022) China's influence operations also reflect its long-term strategy aimed at reshaping the global order, enhancing China's geopolitical position, and diminishing Western influence (Microsoft 2025a).

2.2 Russia: Politically-driven, opportunistic strategy

Russia's espionage supports its geopolitical and strategic objectives, such as succeeding in its war of aggression against Ukraine, strengthening its own great power position and influence, weakening the West, and preventing NATO expansion. Russia's full-scale invasion of Ukraine has had a significant impact on Russian espionage. The Western sanctions and export restrictions imposed on Russia have limited Russia's access to advanced products, technologies and know-how. At the same time, it urgently needs them to maintain and develop its military and civil industrial capabilities (Säpo 2024).

Russia's ability to influence Europe through overt and conventional channels has also been significantly reduced by the deterioration of their relations due to the war in Ukraine (Supo 2025). Business collaborations have largely been suspended, which limits Russia's possibilities to gather information and acquire technology and know-how through legal, commercial methods. Unlike China, Russia also engages less in overt academic partnerships, particularly since many Western universities have cut off academic cooperation with Russia due to the war in Ukraine, and instead, aims to infiltrate universities and research institutions to gather information.

Key targets of Russian intelligence are the sectors that are subject to Western sanctions, such as defence, aerospace and microelectronics. Russia seeks to acquire the needed products, technologies and knowhow by evading sanctions and export restrictions, and by espionage. As regards circumventing sanctions and export restrictions, Russia seeks to conceal supply chains by increasing the number of intermediaries ranging from the EU internal market to third countries, leaving the actual end user unknown (Supo 2025). Russia has succeeded in establishing networks in third countries that it uses to procure advanced technology and equipment. Russian defence industry procurement networks have been operating for instance in China, India, and Türkiye, in which they have also included companies linked to Russia's intelligence services. (Jensen 2024; U.S. Department of the Treasury 2024) The EU's exports to Central Asian and Caucasian countries have been growing after Russia invaded Ukraine, which at least partly reflects the use of these countries to disguise exports actually going to Russia. For instance, the growth in Finland's exports to Central Asia has mainly consisted of goods the export of which to Russia is subject to sanctions. (Lindholm 2024)

Russia's covert operations in the West are primarily conducted by state intelligence agencies operating under direct guidance from the Kremlin, especially the military intelligence agency GRU. The foreign intelligence agency SRV, the Federal Security Service (FSB) and the Main Directorate for Deep Sea Research (GUGI), operating under the Russian Ministry of Defence, are also involved in covert operations. Russian intelligence agencies are carrying out espionage, cyber operations, sabotage and influence operations in the West. (Jones 2025) They are also involved in the procurement of sanctioned Western equipment and technologies (Roslund & Hänninen 2024).

Russian HUMINT in Europe has become increasingly difficult since the war in Ukraine. Russian intelligence officers have mainly been operating under diplomatic cover in Europe, but the expulsion of hundreds of them from Europe since 2022 has significantly reduced Russia's espionage capability. This has forced Russia to resort to other means of operation, such as recruiting intermediaries for intelligence and sabotage activities. (Edwards & Seidenstein 2025; Supo 2025) These intermediaries include criminals but also individuals that are motivated by ideology or simply just by money (Jones 2025). Besides that, Russian intelligence services recruit HUMINT sources, such as officials or politicians, that are rewarded for gathering information, or may use coercion to get for instance Russians living abroad to cooperate with them (Mac Dougall & Reid 2023). They also deploy illegals – deep-cover agents living under false identities – abroad that infiltrate companies, public organisations and research institutions, often posing as professionals or academics (see e.g. Cecco 2022; Sabbagh 2022).

At the same time, Russia has shifted towards cyber-enabled espionage and influencing in the West (Joint Cybersecurity Advisory 2025; Supo 2025). Russia has developed its cyber capabilities extensively in various areas: invested in cybersecurity expertise and the information, communications and technology sector, and amended legislation to better enable the use of information held by private sector actors for intelligence and influence. State-controlled media and national communication platforms enable the spread of propaganda and control of information flows, thus supporting Russian cyber influence. (Supo 2025) Russian cyber operations are conducted by both GRU and SVR cyber units, in particular GRU Unit 26165 (APT28, known as Fancy Bear), GRU Unit 74455 (APT44, known as Sandworm) and SVR unit Cozy Bear/Nobelium (APT29, also known as the Dukes and Midnight Blizzard). (Jones 2025) In addition to groups operating under GRU and SRV, there are also cybercriminal and hacktivist groups that are not directly state-sponsored but more or less approved by the Russian state (Supo 2025), such as the pro-Russian cybercriminal group NoName057(16) (Europol 2025). Proxies, such as individuals who support Russia ideologically, are also used in cyber operations. Besides cyber operations aiming at intelligence gathering, Russian cyberattacks have targeted government agencies, financial services, healthcare sector, media, and critical infrastructure to cause disruption (Jones 2025; Mäkinen & Liuhto 2025).

Russian espionage is also part of Russia's broader hybrid warfare doctrine, which includes disinformation campaigns, political influence operations, economic, political and diplomatic coercion, cyberattacks and sabotage. It aims to weaken adversaries without direct military confrontation by causing insecurity, confusion and discord[2]. The GRU leads sabotage campaigns against governmental, industrial, infrastructure and transportation targets in Europe, and it has also been linked to several assassinations and their attempts in Europe (Jones 2025). Proxies, such as criminals or 'gig workers' recruited in social media, are often used in carrying out sabotage operations (Richterova et al. 2024; O'Carroll 2025). In addition, Russian espionage is often paired with information influencing, such as disinformation campaigns particularly in social media, public opinion manipulation, election interference, and political destabilisation efforts, through which it seeks to boost pro-Russian candidates in elections, increase polarisation, divide the EU and NATO, and undermine support for Ukraine (Mäkinen & Liuhto 2025).

3. Recent cases of Chinese espionage in Europe

3.1 Political and military intelligence gathering

Chinese political and military espionage targets both technologies and knowhow applicable for military purposes, and sensitive information. A recent case of about how Chinese intelligence had succeeded in infiltrating the European Parliament via the right-wing party Alternative for Germany (AfD) raised concerns about Chinese espionage in the EU. In 2025, a former aide of a German AfD politician – who is also under investigation for taking bribes from China – was convicted to nearly five years in prison for working with Chinese intelligence. The German politician was a member of the European Parliament (MEP) at the time of the espionage. According to the court, his former aide had gathered information, transferred sensitive documents to Chinese authorities and monitored Chinese dissidents living in Europe. In connection to the same case, a former employee of a German aviation logistics firm was given suspended sentence. She had provided the former MEP aide with information about aircraft, passengers and cargo, including shipments of weapons and movements of troops, that was also passed to China. (Connor & Moore 2025; Kirby & Bell 2025)

[2] Russia's hybrid warfare in Europe is not discussed in this report, as we have examined it in more detail in our previous study. Please see Mäkinen & Liuhto (2025) for further information.

The methods of Chinese political and military espionage consist of both cyber operations and HUMINT. In 2024, the Dutch intelligence agencies revealed that a Chinese state-sponsored cyber espionage group had infiltrated a Dutch military network the previous year and placed malware in it (Euractiv 2024). In Estonia, in turn, a marine scientist from the Tallinn University of Technology was convicted to three years in prison for spying for China in 2021 (BNS 2021). In connection to the same case, an Estonian entrepreneur received a prison sentence of eight and half years in 2022. She had been charged with cooperating with China's military intelligence for several years, her task being to gather information about maritime, environmental and cyber security issues concerning Estonia and the Baltic Sea and the Arctic regions. (ERR 2023) According to the verdict, she was, for instance, passing information about Helsinki-Tallinn tunnel to China (Skön 2024b). The court stated that she had acted as an intermediary for the Chinese military intelligence in its broader goal to gain access to classified NATO information (ERR 2023).

In 2024, Germany's Federal Prosecutor's Office arrested three German nationals for working for the Chinese intelligence service. Two of them owned a company in Germany through which they had been in contact with several German universities and established a cooperation agreement with one of them, Chemnitz University of Technology. Their aim was to transfer knowledge on maritime and dual use technologies to China. The case drew attention to how foreign intelligence services can exploit academic freedom in Germany and prompted German officials to urge universities to reassess the risks and benefits of their collaborations with China. (Der Generalbundesanwalt 2024; Weisskopf 2024)

3.2 Technological espionage: focus on semiconductor technology

The USA has imposed strict restrictions on the export of semiconductor chips, technology, expertise and manufacturing equipment to China, significantly limiting China's ability to access these crucial components for its technological development. This has fuelled China's motivation to reduce its dependence on foreign technology, especially American, and develop its own semiconductor industry. Besides the efforts to boost its own chip manufacturing capabilities with massive state support and investments, China has also been circumventing export controls and acquiring semiconductor companies, purchasing technology, and recruiting expertise abroad. In addition, it has been acquiring foreign technology through espionage – both by cyber espionage and by recruiting people to spy for China. (Allen 2023; Shivakumar et al. 2024)

Although Europe is not the key region of the semiconductor industry, it has state-of-the-art expertise of semiconductor manufacturing and research that has been of interest for the Chinese intelligence. In Europe, Chinese espionage has particularly targeted Dutch semiconductor companies ASML and NXP. (O'Connor 2024) Between 2017 and 2020, a Chinese hacking group Chimera infiltrated the networks of NXP and was able to steal IP, such as chip designs, from the Dutch company. The data breach remained unnoticed for two and half years until a similar attack was uncovered in a Dutch airline company. (Shilov 2023) ASML, in turn, has been facing thousands of security incidents every year and has therefore been forced to invest significantly in developing its cyber security and IP protection. According to the company's CEO, the US export restrictions and China's attempts to boost its own semiconductor industry have increased the risk of IP theft in the company. In 2023, ASML also reported an incident where its employee in China had stolen technological information from the company. (Gross & Bradshaw 2023)

In addition, research institutes focusing on semiconductor technology have been of interest for Chinese intelligence. As a result, the Belgian university KU Leuven, hosting the Imec research institute, a global leader in microelectronics research, has prohibited research collaboration with Chinese universities that have ties to the country's military and restricted Chinese researchers' access to research projects it considers to have military applicability. (Haeck 2024) Earlier, a Chinese researcher working at Imec was also deported suspected of spying by the Belgian authorities (O'Connor 2024).

In an exceptional espionage case in Finland, a retired engineer from Meyer shipyard was charged with corporate espionage. He had copied very valuable trade secrets while working at the shipyard and later while working as a consultant for the Royal Caribbean shipping company, and allegedly used them in his consulting work with a Chinese shipyard. According to the district court's decision in 2023, his actions constituted infringement of copyright and trade secrets, and corporate espionage. However, his criminal liability was not investigated because he died during the legal process. Instead, his estate and his company were ordered to pay Meyer compensation of five million euros. (Laine 2023; Lehtola 2023)

3.3 Cyber operations: intelligence gathering, influence and control

China uses its cyber capabilities not only for information gathering, but also for political and economic influence and control both at home and abroad. For example, attacks on Western critical infrastructure provide opportunities for Chinese cyber influence. (Supo 2025) According to Microsoft, the main targets of Chinese cyber operations include the ICT sector, government agencies, military and defence sector, think tanks and NGOs. Geographically, the main focus has been on the USA, the Far East, and Southeast Asia. (Microsoft 2025a) Taiwan, in particular, has been a regular target of China's cyberattacks, which it uses as a tool for economic and political pressure (Lee 2025).

Although Europe is not the main target of Chinese cyber operations, attacks are also constantly directed there. For instance, in 2022, an US-based cyber security company Cybereason revealed that a Chinese state-sponsored cyber espionage group Winnti, also known as APT41, had carried out a massive, years-long cyber espionage campaign against multinational companies in North America, Europe, and Asia. In addition to stealing IP and sensitive data from technology and manufacturing companies in defence, energy and pharmaceutical sectors, Winnti hackers gathered information that could be used in future cyberattacks. (Cybereason Nocturnus 2022; Sganga 2022)

Chinese cyber operations also target governmental agencies and aim to gather intelligence on elections and influence their outcomes. Chinese cyber operations and influence campaigns aim to weaken democratic institutions, create divisions, and advance narratives that legitimize its governance model. (Microsoft 2025a) For instance, a cyberattack against the UK Electoral Commission in 2021, allowing the attackers to gain access to electoral registers and, hence, personal details of millions of voters in the UK, has been linked to China (Gregory & Watson 2024). In 2025, the Czech government accused the Chinese APT31 of a cyberattack targeting one of the unclassified networks of the Czech Ministry of Foreign Affairs since 2022 (Ministry of Foreign Affairs of the Czech Republic 2025). In 2020, APT31 tried to intrude into the IT systems of the Finnish parliament (Supo 2021). APT31, associated with the Chinese MSS, has been linked to thousands of cyberattacks against government agencies, strategically important companies, and influential people criticizing China and supporting Chinese political dissidents around the world (Yerushalmy 2024).

4 Recent cases of Russian espionage in Europe

4.1 Gathering political and military information

During the recent years, there have been several espionage cases in Europe involving illegal gathering of political and military information for Russia. Some of them have also led to long prison sentences. In Estonia, a Russian professor working at the University of Tartu was arrested for espionage in 2024. He had been gathering intelligence on Estonia and passing it to Russian intelligence services. (Meduza 2024) According to the prosecutor of the case, he had been cooperating with the GRU for a long time, and had been instructed to collect political, security and defence information about Estonia. He was found guilty for activities against Estonia on behalf of a foreign security service, and sentenced to more than six years in prison. (Kapo 2024)

In Sweden, in turn, two Iran-born brothers were arrested in 2021 for transmitting classified information to the GRU for 10 years. One of the brothers had previously worked for Swedish Security Service (Säpo) and Swedish Military Intelligence and Security Service (MUST), and, according to the court, the intelligence gathering had taken place during these employments. Both brothers were convicted of aggravated espionage in 2023, one of them receiving life sentence and the other almost 10 years in prison. (SVT 2023)

Russia has also used illegals in gathering political and military intelligence. In 2022, the Norwegian domestic security agency exposed a Russian GRU officer who had worked as a researcher at the Arctic University of Norway in Tromsø with a false Brazilian identity. Before moving to Norway, he had spent years in Canada, likely building up his cover story. (Cecco 2022) At the University of Tromsø, he had worked with issues related to security, such as hybrid threats (Eklund 2022). He received charges of gathering intelligence on behalf of Russia in Norway but was released to Russia in a prisoner swap in 2024 (Murphy & Khalil 2024).

In 2022, another Russian GRU officer, also with a Brazilian identity, tried to infiltrate International Criminal Court (ICC) in the Hague, the Netherlands. When he arrived to the Netherlands to take his position as an intern in ICC, he was detained by the Dutch immigration officials and expelled to Brazil. At that time, ICC had started to investigate Russian war crimes in Ukraine, and infiltration attempt was likely aimed at gathering and possibly destroying information related to the investigation. (Sabbagh 2022) Following his exposure, the US Federal Police was able to discover and dismantle a whole network of Russian illegals in Brazil (Pinto 2025).

4.2 Technological espionage to support Russian military capabilities

Russia's technological espionage is also connected to its political and military goals, as it often seeks to gain access to products and technologies needed to support its war machine. For instance, in Germany in 2022, a Russian-born researcher working at the Institute for Materials Research was charged for cooperating with the SVR and passing it information about aerospace research, in particular rocket technology (von Hein 2022). He received a one-year suspended sentence for espionage (The Associated Press 2022).

As regards evading sanctions to acquire products and technologies, investigative journalists have exposed several companies operating in Finland, owned by individuals that have Russian background, that have either directly exported products classified as critical war supplies to Russia or acted as a forwarding agency between a foreign seller and a Russian buyer in the procurement of these supplies. In addition, it has been revealed that some of the customers of these companies have had connections to Russia's military complex and intelligence agencies FSB and GRU. A few of these companies are also currently under criminal investigation in Finland. (Roslund & Hänninen 2024) In 2024, a CEO of two companies received suspended prison sentence for violating sanctions. However, most of the charges against him – for instance regarding the export of 3500 drones to Russia – were dismissed. The prosecutor has appealed the verdict. (Rautio & Salumäki 2024)

In Sweden, a Russian-born businessman was arrested in 2022 for unlawful intelligence activities against Sweden and the USA (AP 2023). He was accused of running a business to acquire sensitive technology for the Russian military complex and the GRU for nearly a decade (AFP 2023). According to the charges, advanced technology subject to export regulations and sanctions, mainly electronic equipment suitable for nuclear weapons research, was delivered to the Russian military. In 2023, the Stockholm district court ruled that while it was proven that the defendant had acquired technology from the West and illicitly exported it to Russia, his actions did not meet the legal definition of espionage, i.e., that the purpose would have been to collect sensitive information with high security value concerning Sweden and the USA. The district court's verdict has been appealed. (AFP 2023; Säpo 2024)

Besides being targeted by Chinese espionage, the Dutch semiconductor industry has been at the focus of Russian intelligence efforts because semiconductors are critical for modern military technology. In 2020, the Dutch officials uncovered an espionage network targeting Dutch companies specialising in AI, semiconductors and nanotechnology. As a result, two Russian spies acting under diplomatic cover were expelled from the Netherlands. (BBC 2020) In 2025, a Russian national was sentenced to a jail term of three years for violating sanctions. He had delivered sensitive information concerning ASML – namely know-how of how to set up a microchip production line – to Russia. (Kelly 2025)

4.3 Cyber operations: intelligence gathering and disruption

Russia has increased its cyber operations against the West during the war in Ukraine (Joint Cybersecurity Advisory 2025). According to the Microsoft Digital Defense Report 2025, besides Ukraine that remains the main target of cyber operations conducted by Russian state-linked actors, the countries most affected by Russian cyber operations are the NATO member states the USA, the UK, Germany, and Belgium. According to Microsoft, Russian cyber actors mainly target organisations in NATO countries that have intelligence value – government organisations, think thanks and NGOs – but cyberattacks against smaller businesses in countries supporting Ukraine have also slightly increased. (Microsoft 2025a) It seems that Russia has shifted towards cyber operations, especially after setbacks in traditional HUMINT due to diplomatic expulsions and consulate closures since the war in Ukraine, but also due to the growing need for intelligence from NATO member states amid the war.

Cyber espionage groups that are directly linked to the Russian state, such as the GRU unit Fancy Bear, have increased their espionage, destruction, and influence activities against the West since the start of the war in Ukraine to support Russia's military objectives and disturb the aid to Ukraine. In 2025, eleven Western countries released a statement about how Fancy Bear had carried out over two-year-long cyber espionage campaign against European and American companies and organisations in defence, logistics and IT sectors involved in assisting Ukraine. Besides acquiring sensitive information by, for instance, phishing and malware attacks, the group has been gaining access to public and private Internet-connected cameras near Ukrainian border crossings to keep track of aid shipments. (Joint Cybersecurity Advisory 2025)

Besides cyber espionage, Russian hacker groups also carry out cyberattacks, such as denial-of-service (DoS) attacks that aim to bring down websites by flooding them with internet traffic. Russia has long enabled cybercrime that targets outside the country and is consistent with its national interests and foreign policy goals. DoS attacks targeting Western countries by Russian cybercriminal groups and hacktivists have increased due to the war in Ukraine and heightened geopolitical tensions. (Supo 2025)

For instance, a pro-Russian cybercrime network NoName057(16) has targeted government agencies, authorities, public services, banks, media outlets, and private companies around Europe with DoS attacks during the recent years (Yle News 2023; Europol 2025). According to Europol, the unorganised NoName network includes several thousands of supporters that are involved in DoS attacks and motivated by pro-Russian ideology and money. The main target of NoName has been Ukraine but they have also been attacking countries involved in countering Russian aggression against Ukraine. (Europol 2025) A large international operation by European and American authorities aimed to disrupt the group's activities in the summer of 2025, but NoName has continued cyberattacks against Ukraine and its supporters also after that (Sillanpää 2025). These cyberattacks have often been temporally linked to certain occasions, such as targeting Finland when it was completing its NATO accession process in 2023 (Yle News 2023), Switzerland during the Peace Summit for Ukraine in 2024, and the Netherlands during the NATO summit in 2025 (Eurojust 2025). They are part of Russia's hybrid warfare tactics aiming to cause political, social and economic disruption in countries Russia considers unfriendly or hostile, and thus supporting its broader political and strategic goals (Mäkinen & Liuhto 2025).

5. Conclusions

5.1 Comparison of Chinese and Russian espionage strategies

China and Russia employ espionage as a strategic tool to advance their national interests, but their approaches differ. China focuses on a long-term, technology-driven strategy aimed at achieving global technological and economic dominance, while Russia pursues a politically driven, opportunistic approach designed to secure short-term geopolitical leverage and destabilise adversaries.

China's espionage strategy is deeply rooted in its ambition to become the world's leading economy and technological superpower. It targets advanced technologies to accelerate industrial modernization and self-sufficiency, and to evade export restrictions imposed on it. To achieve these objectives, China employs both overt and covert methods. Overt channels include business partnerships, acquisitions, academic exchanges, and talent recruitment programs, while covert operations involve HUMINT and extensive cyber espionage. China's cyber capabilities are among the most advanced globally, enabling large-scale intrusions into critical infrastructure and facilitating influence campaigns. In addition to technological acquisition, China uses political and economic coercion and covert influence operations to diminish Western influence and strengthen its global position. Its centrally-led intelligence apparatus, including the MSS and other agencies, works closely with universities and private companies, blurring the line between state and corporate espionage.

Russia's espionage strategy is primarily shaped by its geopolitical objectives, such as supporting its war in Ukraine, weakening Western unity, and preventing NATO expansion. Unlike China, Russia has limited access to overt channels due to sanctions and diplomatic isolation, forcing it to rely heavily on covert operations. These include HUMINT, covert procurement networks, sabotage, and cyber-enabled espionage conducted by agencies such as the GRU, SVR, and FSB. Russian cyber units and hacktivist groups play a central role in intelligence gathering and disruptive operations. Espionage is integrated into Russia's broader hybrid warfare doctrine to destabilise adversaries and advance its strategic interests. Despite facing operational challenges in Europe due to the expulsion of diplomats, Russia continues to exploit intermediaries, criminal networks, and ideological proxies to maintain its espionage capabilities. The comparison of Chinese and Russian espionage is summarized in the following table.

Table 1. Comparison of Chinese and Russian espionage

Dimension	China	Russia
Strategic goal	• Global technological and economic dominance • Reshape world order	• Support geopolitical objectives • Weaken and divide the West
Primary focus	• Technology acquisition	• Sanctioned sectors and political influence
Overt methods	• Business and academia	• Severely limited post-Ukraine war
Covert methods	• MSS-led HUMINT • Cyber operations • Economic and political influence and coercion • Pressure on nationals abroad	• GRU, SVR, and FSB-led HUMINT • Use of proxies • Cyber operations • Covert procurement networks • Disinformation and sabotage
Key strengths	• Global technological reach • Cyber capabilities • Integration of state and private sectors	• Hybrid warfare expertise • Sabotage operations • Disinformation campaigns for polarisation
Key weaknesses	• Vulnerable to export restrictions and technology bans	• Reduced overt and covert channels due to sanctions and expulsions

5.2 Implications of Chinese and Russian espionage for European security

European countries face growing threats from Chinese and Russian espionage. Both China and Russia target sectors essential for national security – such as critical infrastructure and defence. China's focus on acquiring advanced technologies undermines Europe's ability to maintain leadership in strategic industries and its strive for global technological dominance threatens the EU's goal to achieve strategic autonomy. Meanwhile, Russia's goal to advance its geopolitical interests by integrating espionage and hybrid warfare tactics challenges European unity and its support for Ukraine. Russia's sanctions evasion networks and China's covert acquisitions expose Europe to risks of technology leakage, and IP theft and infiltration of research institutions may weaken innovation and competitiveness.

Both states utilise cyber operations and deploy APT groups capable of long-term infiltration into public and private systems. These cyber operations not only steal data but also create opportunities for sabotage. China also uses economic leverage—such as trade restrictions and informal sanctions—to punish countries that oppose its interests, which creates pressure on states to align with Chinese policies. Russian hybrid warfare, in turn, combines espionage and cyber operations with disinformation campaigns, election interference, and sabotage, threatening to destabilise and polarise European societies and weaken EU and NATO cohesion.

Hence, Chinese and Russian espionage requires a comprehensive and coordinated response from Europe. To mitigate these risks, governments and organisations should adopt a comprehensive strategy that combines political, societal, technological, and legal measures. Strengthening cybersecurity in both public and private sectors, enhancing counterintelligence capabilities, securing supply chains, limiting opportunities to evade sanctions and export restrictions, and promoting international cooperation and information sharing are key priorities. Increasing public awareness on espionage and foreign influence, and strengthening media literacy and digital skills improve citizens' abilities to identify disinformation and combat information influence. Developing legal frameworks to address emerging espionage and hybrid threats will further reduce vulnerabilities and improve resilience.

References

AFP (2023) Swedish Court Acquits Alleged Russian 'Agent'. The Moscow Times, October 26. https://www.themoscowtimes.com/2023/10/26/swedish-court-acquits-alleged-russian-agent-a82894. Accessed: November 26, 2025.

Allen, G. C. (2023) China's New Strategy for Waging the Microchip Tech War. Center for Strategic & International Studies, May 3. https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war. Accessed November 26, 2025.

AP (2023) Swedish Court Acquits Russian-Born Businessman Of Spying For Moscow. Radio Free Europe/ Radio Liberty, September 29. https://www.rferl.org/a/prosecutors-prison-russian-swede-spying-acquitted/32615788.html. Accessed November 26, 2025.

The Associated Press (2022) Russian convicted of spying in Germany, gets suspended term. Toronto City News, April 13. https://toronto.citynews.ca/2022/04/13/russian-convicted-of-spying-in-germany-gets-suspended-term/. Accessed November 26, 2025.

BBC (2020) Netherlands expels two Russians after uncovering 'espionage network'. December 10. https://www.bbc.com/news/world-europe-55258790. Accessed November 26, 2025.

BNS (2021) Court sentences well-known marine scientist to prison for spying for China. Postimees, March 19. https://news.postimees.ee/7205290/court-sentences-well-known-marine-scientist-to-prison-for-spying-for-china. Accessed November 26, 2025.

Cecco, L. (2022) Suspected Russian spy arrested in Norway spent years studying in Canada. The Guardian, October 28. https://www.theguardian.com/world/2022/oct/28/russian-spy-norway-canada-brazil-academic. Accessed November 26, 2025.

Connor, R. & Moore, M. (2025) Germany: Ex-AfD aide convicted of spying for China. DW, September 30. https://www.dw.com/en/germany-ex-afd-aide-convicted-of-spying-for-china/a-74183401. Accessed November 26, 2025.

CSIS (2023) Survey of Chinese Espionage in the United States Since 2000. Center for Strategic & International Studies. https://www.csis.org/programs/strategic-technologies-program/survey-chinese-espionage-united-states-2000. Accessed November 26, 2025.

Cybereason Nocturnus (2022) Operation CuckooBees: Cybereason Uncovers Massive Chinese Intellectual Property Theft Operation. https://www.cybereason.com/blog/operation-cuckoobees-cybereason-uncovers-massive-chinese-intellectual-property-theft-operation. Accessed November 26, 2025.

Cybersecurity Advisory (2025) Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System. America's Cyber Defense Agency, September 3. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a?utm_source=SaltTyphoon&utm_medium=AlertAdvisory. Accessed November 26, 2025.

Der Generalbundesanwalt (2024) Festnahmen wegen mutmaßlicher geheimdienstlicher Agententätigkeit. Der Generalbundesanwalt beim Bundesgerichtshof, April 22. https://www.generalbundesanwalt.de/SharedDocs/Pressemitteilungen/DE/2024/Pressemitteilung-vom-22-04-2024.html?nn=478184. Accessed November 26, 2025.

Dragonfly Intelligence (2023) Global | Assessment of Chinese industrial espionage risks. Dragonfly, March 31. https://dragonflyintelligence.com/news/global-assessment-of-chinese-industrial-espionage-risks/. Accessed November 26, 2025.

Eklund, V. (2022) Venäläisvakooja soluttautui Norjassa tutkimaan hybridiuhkia – saman yliopiston suomalaisprofessori: "Ihmiset kokevat tulleensa huijatuiksi". MTV Uutiset, October 29. https://www.mtvuutiset.fi/artikkeli/venalaisvakooja-soluttautui-norjassa-tutkimaan-hybridiuhkia-saman-yliopiston-suomalaisprofessori-ihmiset-kokevat-tulleensa-huijatuiksi/8559256#gs.ie2pez. Accessed November 26, 2025.

ERR (2023) Supreme Court part-annuls Gerli Mutso China spying conviction. June 17. https://news.err.ee/1609010261/supreme-court-part-annuls-gerli-mutso-china-spying-conviction. Accessed November 26, 2025.

Euractiv (2024) Chinese spies hacked Dutch defence network last year - intelligence agencies. February 7, last updated September 30. https://www.euractiv.com/news/chinese-spies-hacked-dutch-defence-network-last-year-intelligence-agencies/. Accessed November 26, 2025.

Eurojust (2025) Hacktivist group responsible for cyberattacks on critical infrastructure in Europe taken down. European Union Agency for Criminal Justice Cooperation, July 16. https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down. Accessed November 26, 2025.

Europol (2025) Global operation targets NoName057(16) pro-Russian cybercrime network. https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network. Accessed November 26, 2025.

FBI (2025) The China Threat. https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans. Accessed November 26, 2025.

Gorera, G. (2025) How China really spies on the UK. BBC, October 30. https://www.bbc.com/news/articles/cgr4xpyrkdqo. Accessed November 26, 2025.

Gregory, J. & Watson, I. (2024) China linked to UK cyber-attacks on voter data, Dowden to say. BBC, March 25. https://www.bbc.com/news/uk-politics-68652374. Accessed November 26, 2025.

Gross, A. & Bradshaw, T. (2023) ASML chief warns of IP theft risks amid chip sanctions. The Financial Times, March 8. https://www.ft.com/content/dfef74a7-bcc0-441b-95a5-380e212d9854. Accessed November 26, 2025.

Haeck, P. (2024) Belgian research powerhouse turns hawkish on China. Politico, April, 4. https://www.politico.eu/article/belgium-university-town-leuven-reposition-protectionist-world-trade-technology-council/. Accessed November 26, 2025.

Harrell, P. (2025) Managing the Risks of China's Access to U.S. Data and Control of Software and Connected Technology. Carnegie Endowment for International Peace, January 30. https://carnegieendowment.org/research/2025/01/managing-the-risks-of-chinas-access-to-us-data-and-control-of-software-and-connected-technology?lang=en. Accessed November 26, 2025.

Jensen, B. (2024) Silicon Surrender: How Ending Russian Electronics Imports Supports Negotiations. Center for Strategic & International Studies, December 9. https://www.csis.org/analysis/silicon-surrender-how-ending-russian-electronics-imports-supports-negotiations. Accessed November 26, 2025.

Joint Cybersecurity Advisory (2025) Russian GRU Targeting Western Logistics Entities and Technology Companies. https://media.defense.gov/2025/May/21/2003719846/-1/-1/0/CSA_RUSSIAN_GRU_TARGET_LOGISTICS.PDF. Accessed November 26, 2025.

Jones, S. G. (2025) Russia's Shadow War Against the West. Center for Strategic & International Studies, March 18. https://www.csis.org/analysis/russias-shadow-war-against-west. Accessed November 26, 2025.

Kapo (2024) The court convicted Viatcheslav Morozov of intelligence activity. Press release, June 18. https://kapo.ee/en/content/court-convicted-viatcheslav-morozov-intelligence-activity/. Accessed November 27, 2025.

Kelly, B. (2025) Russian breached sanctions sharing Dutch tech giant's know-how. European Interest, July 11. https://www.europeaninterest.eu/russian-breached-sanctions-sharing-dutch-tech-giants-know-how/. Accessed November 27, 2025.

Kirby, P. & Bell, B. (2025) Former aide to far-right German politician jailed for spying for China. BBC, September 30. https://www.bbc.com/news/articles/c99g52y7k1xo. Accessed November 27, 2025.

Laine, L. (2023) Insinööri kopioi telakan yrityssalaisuuksia ja kuoli – Oikeus tuomitsi miljoonakorvaukset. Helsingin Sanomat, October 16. https://www.hs.fi/kotimaa/turku/art-2000009926006.html. Accessed November 27, 2025.

Lassila, A. (2024) Yritysvakoilun suurvalta. Helsingin Sanomat, April 14. https://www.hs.fi/talous/art-2000010345440.html. Accessed November 27, 2025.

Lee, Y. (2025) Taiwan flags rise in Chinese cyberattacks, warns of 'online troll army'. Reuters, October 14. https://www.reuters.com/world/asia-pacific/taiwan-flags-rise-chinese-cyberattacks-warns-online-troll-army-2025-10-14/. Accessed November 27, 2025.

Lehtola, J. (2023) Oikeus lätkäisi miljoonahyvitykset yritysvakoilutapauksessa Meyer-telakalle. Yle, Ocotber 16. https://yle.fi/a/74-20055482. Accessed November 27, 2025.

Lewis, M. (2011) Norway's salmon rot as China takes revenge for dissident's Nobel Prize. Independent, October 6. https://www.independent.co.uk/news/world/europe/norway-s-salmon-rot-as-china-takes-revenge-for-dissident-s-nobel-prize-2366167.html. Accessed November 27, 2025.

Lindholm, P. (2024) Venäjä-pakotteita kierretään Keski-Aasian kautta – Suomen vienti alueelle on kasvanut poikkeuksellisen paljon. Yle, October 14. https://yle.fi/a/74-20114461. Accessed November 27, 2025.

Mac Dougall, D. & Reid, S. (2023) Spies like us: How does Russia's intelligence network operate across Europe? Euronews, August 18. https://www.euronews.com/2023/08/18/spies-like-us-how-does-russias-intelligence-network-operate-across-europe. Accessed November 27, 2025.

Meduza (2024) Estonia sentences Russian professor Viacheslav Morozov to six years in prison for espionage. June 18. https://meduza.io/en/news/2024/06/18/russian-professor-viacheslav-morozov-sentenced-to-six-years-in-prison-for-espionage. Accessed November 27, 2025.

Microsoft (2025a) Microsoft Digital Defense Report 2025. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/. Accessed November 27, 2025.

Microsoft (2025b) What is an advanced persistent threat (APT)?. https://www.microsoft.com/en-us/security/business/security-101/what-is-advanced-persistent-threat-apt. Accessed November 27, 2025.

Ministry of Foreign Affairs of the Czech Republic (2025) Statement by the Government of the Czech Republic. May 28. https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.html. Accessed November 27, 2025.

Murphy, M. & Khalil, H. (2024) Who are the prisoners in the Russia-West swap? BBC, August 2. https://www.bbc.com/news/articles/cjjwexqj11xo. Accessed November 27, 2025.

Mäkinen, H. & Liuhto, K. (2025) Russia's shadow war: The media coverage of Russia's hybrid war against the EU in the 21st century. In Russia's war against Ukraine (Ed. Pentti Forsström). Series 2: Research Reports. The Department of Warfare. Helsinki: National Defence University. https://www.doria.fi/handle/10024/193284.

O'Carroll, L. (2025) Russia using criminal networks to drive increase in sabotage acts, says Europol. The Guardian, March 18. https://www.theguardian.com/technology/2025/mar/18/russia-criminal-networks-drive-increase-sabotage-europol. Accessed November 27, 2025.

O'Connor, I. (2024) Watch Out Europe: China is Stealing Your Chip Secrets. Center for European Policy Analysis, July 9. https://cepa.org/article/watch-out-europe-china-is-stealing-your-chip-secrets/. Accessed November 27, 2025.

Pinto, N. T. (2025) A perfect 'legend' for the 'illegals': How a Russian spy couple became Portuguese citizens. Euronews, May 31. https://www.euronews.com/my-europe/2025/05/31/a-perfect-legend-for-he-illegals-how-a-russian-spy-couple-became-portuguese-citizens. Accessed November 27, 2025.

Rautio, M. & Salumäki, T. (2024) Venäjä-pakotteita rikkonut yrittäjä tuomittiin ehdolliseen vankeuteen – tuhansien droonien ei näytetty päätyneen Venäjälle. Yle, March 7. https://yle.fi/a/74-20077859. Accessed November 27, 2025.

Reynolds, M. & Goodman, M. (2022) China's Economic Coercion: Lessons from Lithuania. Center for Strategic & International Studies, May 6. https://www.csis.org/analysis/chinas-economic-coercion-lessons-lithuania. Accessed November 27, 2025.

Richterova, D., Grossfeld, E., Long, M., & Bury, P. (2024) Russian Sabotage in the Gig-Economy Era. The RUSI Journal, 169(5), 10–21. https://doi.org/10.1080/03071847.2024.2401232.

Roslund, R. & Hänninen, J. (2024) Huomaamattomissa peltihalleissa toimii yrityksiä, jotka ovat vieneet Suomesta Venäjälle suuria määriä sotatavaraa. Yle, January 15. https://yle.fi/a/74-20068825. Accessed November 27, 2025.

Sabbagh, D. (2022) Russian spy caught trying to infiltrate war crimes court, says Netherlands. The Guardian, June 16. https://www.theguardian.com/law/2022/jun/16/russian-spy-caught-trying-to-infiltrate-war-crimes-court-says-netherlands. Accessed November 27, 2025.

Sganga, N. (2022) Chinese hackers took trillions in intellectual property from about 30 multinational companies. CBS News, May 4. https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/. Accessed November 27, 2025.

Shilov, A. (2023) Chinese hackers steal chip designs from major Dutch semiconductor company — perps lurked for over two years to steal NXP's chipmaking IP: Report. Tom's Hardware, November 25. https://www.tomshardware.com/news/chinese-hackers-steal-chip-designs-from-major-dutch-semiconductor-company. Accessed November 27, 2025.

Shivakumar, S., Wessner, C. & Howell, T. (2024) Balancing the Ledger: Export Controls on U.S. Chip Technology to China. Center for Strategic & International Studies, February 21. https://www.csis.org/analysis/balancing-ledger-export-controls-us-chip-technology-china. Accessed November 27, 2025.

Sillanpää, S. (2025) Venäläinen hakkeriryhmä jatkaa hyökkäyksiä Euroopassa – HS esittelee etsintäkuulutetut johtajat. Helsingin Sanomat, November 21. https://www.hs.fi/tutkiva/art-2000011634124.html. Accessed November 27, 2025.

Skön, K. (2024a) Naapurit muistavat kiinalaismiehen mukavana seuramiehenä – itähelsinkiläisen asunnon isäntä oli todellisuudessa vakooja. Yle, November 19. https://yle.fi/a/74-20122549. Accessed November 27, 2025.

Skön, K. (2024b) Vankeuteen tuomittu virolaisnainen kertoo, miten suomalainen liikemies esitteli hänet Kiinan sotilastiedustelulle. Yle, November 20. https://yle.fi/a/74-20125803. Accessed November 27, 2025.

Supo (2021) Supo identified the cyber espionage operation against the parliament as APT31. Press release, March 18. https://supo.fi/en/-/supo-identified-the-cyber-espionage-operation-against-the-parliament-as-apt31. Accessed November 27, 2025.

Supo (2025) Kansallisen turvallisuuden katsaus 2025. https://katsaus.supo.fi/etusivu. Accessed November 27, 2025.

SVT (2023) Bröder döms för grovt spioneri. January 19. https://www.svt.se/nyheter/inrikes/broder-doms-for-grovt-spioneri. Accessed November 27, 2025.

Säpo (2024) The Swedish Security Service 2023–2024. https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/swedish-security-services-annual-assesments.html. Accessed November 27, 2025.

Säpo (2025) The Swedish Security Service 2024–2025. https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/swedish-security-services-annual-assesments.html. Accessed November 27, 2025.

U.S. Department of the Treasury (2024) Treasury Takes Aim at Third-Country Sanctions Evaders and Russian Producers Supporting Russia's Military Industrial Base. Press releases, October 30. https://home.treasury.gov/news/press-releases/jy2700. Accessed November 27, 2025.

Weisskopf, M. (2024) Chinese scientific espionage in Germany: what next? Science|Business, May 2. https://sciencebusiness.net/universities/chinese-scientific-espionage-germany-what-next. Accessed November 27, 2025.

von Hein, M. (2022) Russian scientist stands trial for espionage in Germany. DW, February 17. https://www.dw.com/en/russian-scientist-stands-trial-for-espionage-in-germany/a-60804917. Accessed November 27, 2025.

Yerushalmy, J. (2024) China cyber-attacks explained: who is behind the hacking operation against the US and UK? The Guardian, March 26. https://www.theguardian.com/technology/2024/mar/26/china-cyber-attack-uk-us-explained-hack-apt-31. Accessed November 27, 2025.

Yle News (2023) Pro-Russia hacker group suspected of targeting Finnish parliament, Sanna Marin websites with DoS attack. April 4. https://yle.fi/a/74-20025824. Accessed November 27, 2025.

Earlier publications in the BSR Policy Briefing series by Centrum Balticum Foundation

BSR Policy Briefing 8/2025: "The Northwestern Federal District of Russia: Economic Dynamics and Regional Asymmetries after 2022" by Sergei Gladkov

BSR Policy Briefing 7/2025: “Changes in Russian Investments Abroad Since the Start of the Full Scale War in Ukraine" by Sergei Gladkov

BSR Policy Briefing 6/2025: “Economies of St Petersburg and Leningrad Oblast by 2025: Present-day Picture” by Nikita Lisitsyn

BSR Policy Briefing 5/2025: “Kaliningrad’s Economy: Vulnerabilities and Performance” by Artur Usanov

BSR Policy Briefing 4/2025: “Scenarios for Ukraine. A Theory of Victory and Peace” by Andrés Pastrana, Greg Mills and Juan-Carlos Pinzon

BSR Policy Briefing 3/2025: “Solutions for media to achieve financially sustainable journalism online and in print” by Kimmo Lundén

BSR Policy Briefing 2/2025: “Changes in economic cooperation between Russia and China since the start of the full-scale war in Ukraine” by Sergei Gladkov

BSR Policy Briefing 1/2025: “Recent trends in international trade and investments of the Baltic states” by Alari Purju

BSR Policy Briefing 9/2024: “Russia’s War in Ukraine: What should this conflict teach us?” by Greg Mills and David Kilcullen

BSR Policy Briefing 8/2024: “Impact of the war in Ukraine on nuclear waste management in arctic Russia” by Sergei Gladkov

BSR Policy Briefing 7/2024: “Belarus and its future development: What does it mean for the Baltic Sea region?” by Andrei Sannikov

BSR Policy Briefing 6/2024: “Demographic challenges of the Kaliningrad region in the new geopolitical reality: Trends, risks and prospects” by Salavat Abylkalikov

BSR Policy Briefing 5/2024: “The competitiveness of Finnish firms in the changing business landscape” by Anna Karhu, Eini Haaja & Hanna Mäkinen

BSR Policy Briefing 4/2024: “Economy of St. Petersburg two years after the beginning of the conflict in Ukraine” by Nikita Lisitsyn

BSR Policy Briefing 3/2024: “Arctic Europe and its Future” by Markku Heikkilä

BSR Policy Briefing 2/2024: “Germany’s economic structure in times of multiple shocks” by Michael Grömling

BSR Policy Briefing 1/2024: “China’s influence in Northern Europe” by Oscar Shao

BSR Policy Briefing 8/2023: “The wicked problem of eutrophication - next steps in the process towards sustainable agriculture in Finland” by Anna Törnroos-Remes

BSR Policy Briefing 7/2023: “A literature review on the main environmental challenges in the Baltic Sea region in the 21st century” by Sergei Gladkov and Léo Pignol

BSR Policy Briefing 6/2023: “Developing the economic competence in Åland: Recommendations and key learning points for policymakers” by Anna Lundgren and Jukka Teräs

BSR Policy Briefing 5/2023: “The green transformation of the European maritime sector: Six tricks to support sustainable cruise shipbuilding” by Elisa Aro and Eini Haaja

BSR Policy Briefing 4/2023: “Iron curtain on Belarus’ western border: Does the crisis in Minsk’s relations with its Baltic neighbors threaten Belarusian independence?” by Kamil Kłysiński

BSR Policy Briefing 3/2023: “The economic interaction between the USA and the littoral states of the Baltic Sea” by Alari Purju

BSR Policy Briefing 2/2023: “The Resource Balanced Economy to meet the twin challenges of phasing out fossil fuel energy and self-sufficient supply of raw materials” by Simon P. Michaux

BSR Policy Briefing 1/2023: “Baltic Sea region security of supply after Russia’s invasion on Ukraine: The past is just a prologue” by Anna Mikulska and Luke Min

BSR Policy Briefing 11/2022: “Sanctions against Russia, their effectiveness and impacts on Finland” by Hanna Mäkinen

BSR Policy Briefing 10/2022: “The Baltic Sea islands and their impact on the regional security” by Zdzislaw Sliwa, Hans Helseth and Viljar Veebel

BSR Policy Briefing 9/2022: “Willingness to fight for Ukraine: Lessons to the Baltic States” by Jānis Bērziņš and Victoria Vdovychenko

BSR Policy Briefing 8/2022: “Chinese investment in the Baltic Sea region: Main characteristics and policy challenges” by Kálmán Kalotay and Ágnes Szunomár

BSR Policy Briefing 7/2022: “NATO and security in the Baltic Sea region” by Klaus Wittmann

BSR Policy Briefing 6/2022: “The Ostrovets Nuclear Power Plant: Energy independence on paper – isolation in practice” by Justinas Juozaitis

BSR Policy Briefing 5/2022: “Aspects of blue economy in the Baltic Sea region” by Riitta Pöntynen

BSR Policy Briefing 4/2022: “Leveraging bioeconomy development for climate change mitigation and adaptation in the Baltic Sea Region” by Alisher Mirzabaev

BSR Policy Briefing 3/2022: “Russia’s renewable energy sector: Policy recommendations” by Liliana Proskuryakova

BSR Policy Briefing 2/2022: “The circular economy in St. Petersburg” by Yury Nurulin, Olga Kalchenko and Inga Skvortsova

BSR Policy Briefing 1/2022: “Energy dimension of green growth in Kaliningrad” by Artur Usanov

BSR Policy Briefing 11/2021: “Mortality in Russia during the pandemic in 2020 and in the first half of 2021” by Marina Lifshits

BSR Policy Briefing 10/2021: “Building security in the Baltic Sea region: Military perspective and NATO approach” by Andrzej Fałkowski

BSR Policy Briefing 9/2021: “The “Swedish model” in the COVID-19 pandemic” by Torbjörn Becker, Jesper Roine, and Svante Strömberg

BSR Policy Briefing 8/2021: “Lithuania’s response to the COVID-19: Two stages, mixed results” by Linas Kojala

BSR Policy Briefing 7/2021: “The Kaliningrad Region and COVID-19” by Vitaly Petrovich Zhdanov

BSR Policy Briefing 6/2021: “Polish struggle against COVID-19” by Bartosz Arłukowicz

BSR Policy Briefing 5/2021: “COVID-19 and Finland: Not good news for fiscal sustainability” by Jouko Vilmunen

BSR Policy Briefing 4/2021: “Latvia and COVID-19: Preliminary impressions” by Dzintars Mozgis and Normunds Vaivads

BSR Policy Briefing 3/2021: “The German economy and the Corona shock – An acceleration of structural changes?” by Michael Grömling

BSR Policy Briefing 2/2021: “Contemporary trends and future scenarios for the Greater St. Petersburg region” by Nikita Lisitsyn

BSR Policy Briefing 1/2021: “The COVID-19 in Estonia: Governance of the Health Care System, spread of the disease, regulations and impact on economy” by Alari Purju

BSR Policy Briefing 6/2020: “Leadership in Turbulent Times: Germany and the Future of Europe” by Kimmo Elo

BSR Policy Briefing 5/2020: “Denmark and COVID-19” by Marin A. Marinov

BSR Policy Briefing 4/2020: “Lithuania and Belarus: Will Lithuania become Belarus’ “Iceland”?” by Ruslanas Iržikevičius

BSR Policy Briefing 3/2020: “The corona pandemic and its impact on the economic development of the Baltic Sea region in 2020” by Kari Liuhto

BSR Policy Briefing 2/2020: “Increasing Eco-efficiency via Digitalisation in Maritime Industry in The Baltic Sea Region: Policy Support through Carrots or Sticks?” by Milla Harju

BSR Policy Briefing 1/2020: “The forest industry around the Baltic Sea region: Future challenges and opportunities” edited by Kari Liuhto

BSR Policy Briefing 9/2019: “The Baltic states and security in the Baltic Sea region: Dark clouds in blue sky” by Kristi Raik

BSR Policy Briefing 8/2019: “Creation of regional gas market in the Baltic States and Finland: Challenges and opportunities” by Tadas Jakstas

BSR Policy Briefing 7/2019: “US FDI in the Baltic Sea region: The state of American investment and selected challenges” by Kalman Kalotay

BSR Policy Briefing 6/2019: “Germany and the Baltic Sea region: political and security interests” by Tobias Etzold

BSR Policy Briefing 5/2019: “Government support for the Russian shipbuilding industry: Policy priorities and budgetary allocations” by Elena Efimova and Sergei Sutyrin

BSR Policy Briefing 4/2019: “Finnish tonnage as the implementer for security of seaborne supply in maritime transport” by Bo Österlund

BSR Policy Briefing 3/2019: “The Estonian-Finnish economic cooperation” by Alari Purju

BSR Policy Briefing 2/2019: “Bioeconomy Policies in the BSR” by Torfi Jóhannesson

BSR Policy Briefing 1/2019: “Cooperation between Saint-Petersburg and Finland” by Stanislav Tkachenko

BSR Policy Briefing 10/2018: “The sanctions against Russia. Are there winners and losers around the Baltic Sea?” by Susanne Oxenstierna

BSR Policy Briefing 9/2018: “Future of Public Sector Governance and Digitalization” by Meelis Kitsing

BSR Policy Briefing 8/2018: “American Policy Towards the Baltic States” by Stephen Blank

BSR Policy Briefing 7/2018: “Russian direct and indirect investment in the Baltic Sea region” by Alexey Kuznetsov

BSR Policy Briefing 6/2018: “Foreign economic relations of the Kaliningrad region” by Vitaliy Zhdanov, Vladimir Kuzin and Mikhail Pliukhin

BSR Policy Briefing 5/2018: “Why is Russia seeking to ignite a civil war in the European Union and how to stop it?” by Ruslanas Iržikevičius

BSR Policy Briefing 4/2018: ”On the paradoxes of foreign expansion: the experience of Polish firms” by Piotr Trąpczyński and Krystian Barłożewski

BSR Policy Briefing 3/2018: ”The bioeconomy in the Baltic Sea region” by Anna Berlina

BSR Policy Briefing 2/2018: ”Russia vis-à-vis Ukraine: On Some Economic Costs” by Sergey Kulik

BSR Policy Briefing 1/2018: ”Chinese Direct Investment in the Baltic Sea Region” by Jean-Marc F. Blanchard

BSR Policy Briefing 5/2017: ”The economic impact of China on the Baltic Sea region” by Jean-Paul Larçon

BSR Policy Briefing 4/2017: ”National innovation and smart specialisation governance in the Baltic Sea region” edited by Zane Šime

BSR Policy Briefing 3/2017: ”The economic state of the Baltic Sea region” edited by Kari Liuhto

BSR Policy Briefing 2/2017: ”Russia’s foreign relations and the Baltic Sea region” by Sergey Kulik

BSR Policy Briefing 1/2017: ”Russia and the security in the Baltic Sea region” by Justyna Gotkowska & Piotr Szymański

BSR Policy Briefing 2/2016: ”The EU-Russia relations and their reflections in the Baltic Sea region” Stanislav L. Tkachenko

BSR Policy Briefing 1/2016: ”The maritime cluster in the Baltic Sea region and beyond” edited by Kari Liuhto

BSR Policy Briefing 1/2015: ”Natural gas revolution and the Baltic Sea region” edited by Kari Liuhto

BSR Policy Briefing 4/2014: ”A Russian Sudden Stop or Just a Slippery Oil Slope to Stagnation?” by Torbjörn Becker

BSR Policy Briefing 3/2014: ”Poland and Russia in the Baltic Sea Region: doomed for the confrontation?” by Adam Balcer

BSR Policy Briefing 2/2014: ”Energy security in Kaliningrad and geopolitics” by Artur Usanov and Alexander Kharin

BSR Policy Briefing 1/2014: ”The Baltic Sea region 2014: Ten policy-oriented articles from scholars of the university of Turku” edited by Kari Liuhto

BSR Policy Briefing 4/2013: ”The Kaliningrad nuclear power plant project and its regional ramifications” by Leszek Jesien and Łukasz Tolak

BSR Policy Briefing 3/2013: ”Renewable Energy Sources in Finland and Russia - a review” by Irina Kirpichnikova and Pekka Sulamaa

BSR Policy Briefing 2/2013: ”Russia’s accesion to the WTO: possible impact on competitiveness of domestic companies” by Sergey Sutyrin and Olga Trofimenko

BSR Policy Briefing 1/2013: ”Mare Nostrum from Mare Clausum via Mare Sovieticum to Mare Liberum - The process of security policy in the Baltic” by Bo Österlund

BSR Policy Briefing series 1/2026

CENTRUM BALTICUM

www.centrumbalticum.org/en