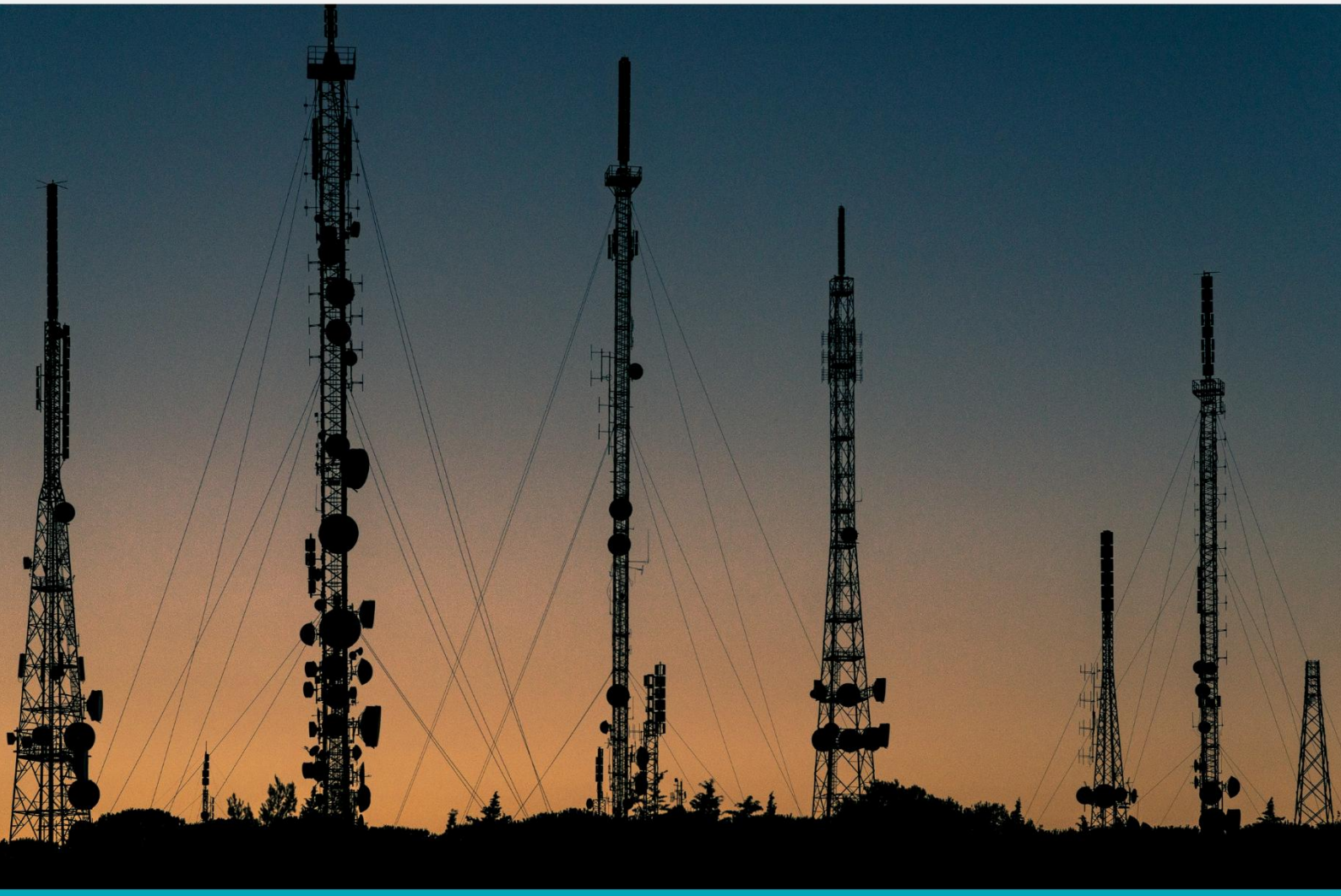
IDR
Romanian Diplomatic Institute



POLICY PAPER no. 43/2025

TYPHOONS, BEARS, AND PANDAS. LATEST MAJOR CYBER ESPIONAGE CAMPAIGNS

Claudiu Codreanu

MINISTERUL AFACERILOR EXTERNE

Typhoons, bears, and pandas. Latest major cyber espionage campaigns*[1]

Claudiu Codreanu[2]

Researcher

Romanian Diplomatic Institute

ABSTRACT: Cyber espionage remains among the most common forms of interstate cyber operations worldwide. Most states spy on each other, and this practice is not unusual in international affairs. However, the exploitation of cyberspace for espionage amplifies the potential for collecting sensitive data and entails the risk of generating security breaches that can later be exploited by other actors. China and Russia represent the main actors conducting such actions against Euro-Atlantic states, although their objectives and methods of operation remain largely distinct. This study analyses two major cyber campaigns carried out by China – Volt Typhoon and Salt Typhoon – highlighting Beijing's transition from conventional espionage to the strategic infiltration of Western critical infrastructure. In parallel, the research also examines Russia's cyber espionage activities, focusing on campaigns related to the war of aggression against Ukraine. The role of commercial spyware, such as Pegasus, used for repressive purposes against journalists, activists, and political opposition, is also assessed. Finally, the study proposes a series of public policy recommendations, including the public attribution of campaigns, the imposition of sanctions, as well as strengthening cybersecurity and regulating the export and usage of commercial spyware.

KEYWORDS: cyber espionage, Volt Typhoon, Salt Typhoon, Russia, commercial spyware.

* The present text is the English translation of the article originally published in Romanian in July 2025.

[1] This publication draws exclusively on open-source materials. The opinions expressed herein are solely those of the author and do not necessarily reflect those of the institution.

[2] claudiu.codreanu@idr.ro

INTRODUCTION

Espionage – understood as a set of activities aimed at understanding and anticipating the actions of others – does not by itself provide control, but it can enable control through the systematic accumulation of information (Zilincik, Myklin & Kovanda 2019). **China, Iran, Russia, the United States, and most other states engage in various forms of cyber espionage.** Similarly, North Korea conducts cyber espionage campaigns, even though Pyongyang's state-sponsored hackers are better known for ransomware operations than financial theft (Iyengar 2023). More recently – and arguably more troubling than traditional espionage activities – the role of commercial spyware has become increasingly visible. These digital tools allow governments and other actors to target not only foreign officials, but also journalists, anti-governmental activists, and members of the political opposition.

Hacker groups, often referred to by pseudonyms coined by cybersecurity companies and experts, have been at the forefront of such operations. Russian groups such as *Fancy Bear* and *Cozy Bear*, or Chinese groups like *Evasive Panda* and *Volt*/*Salt Typhoon*, were later attributed to military or intelligence units of the two countries. They are the main actors behind campaigns targeting Euro-Atlantic states. **Russia has tended to employ a hybrid approach, combining cyber espionage focused on military and security information with political influence operations, cyberattacks, and disinformation campaigns. Beijing, by contrast, has historically emphasized commercial espionage**. China is widely regarded as the leading global actor in large-scale cyber espionage (Gilli & Gilli 2019). Between 2007 and 2011, Chinese cyber campaigns succeeded in extracting vast amounts of sensitive data from the Pentagon, including the design of the F-22 and F-35 fighter jets (Gilli & Gilli 2019, 180). In December 2024, the United States accused China of conducting a cyber intrusion against the Treasury Department in a cyber espionage campaign (Agence France-Presse 2024). Just three months earlier, the US Department of Justice announced that it had dismantled a network of 200,000 devices worldwide, alleging it was operated by Chinese state-sponsored hackers for cyber operations (Agence France-Presse 2024).

Two additional Chinese hacking campaigns were publicly disclosed in 2023-2024. **Salt Typhoon** involved cyber intrusions into dozens of telecommunications companies as part of a broader espionage campaign, while **Volt Typhoon** exploited vulnerabilities across US critical infrastructure (Davidson 2024; Montgomery 2024). The evolution to Volt Typhoon suggested a shift beyond routine espionage, raising signals of preparations for potentially disruptive cyberattacks in the event of international escalation. This indicates that China is seeking to pre-position itself within critical US networks in order to enable destructive or disruptive cyber operations against vital infrastructure during a major crisis or potential conflict with the United States (Davidson 2024).

In parallel, in April 2024, six individuals were arrested in the United Kingdom and Germany on charges of spying for China, amid mounting opposition to Beijing's influence campaigns in European politics and trade (Higgins & Schuetze 2024). Authorities in Berlin and London accused the Chinese state of attempting to influence democratic processes, marking an intensification of espionage activities from primarily economic to overtly political ones, mirroring longstanding Russian practices (Higgins & Schuetze 2024). These events illustrate both a shift in China's espionage priorities and a reduced tolerance among European governments for Chinese influence operations.

This study therefore examines the most recent developments in major interstate cyber espionage campaigns, with a particular focus on China's *Volt Typhoon* and *Salt Typhoon*, alongside similar Russian activities. It also assesses the use of commercial spyware and the targeting of dissidents. The paper begins by offering conceptual clarifications and a brief historical overview, then turns to China and Russia's operations, as well as the case of the Pegasus spyware. Finally, it places these campaigns in context and concludes with a set of policy recommendations.

CYBER ESPIONAGE – DEFINITIONS AND CONTEXT

The concept of cyber espionage

Brandon Valeriano and Ryan C Maness define cyber espionage as "the use of dangerous and offensive intelligence measures to steal, corrupt, or erase information in the cybersphere of interactions" (2015, 49). It refers to the **theft of government or commercial secrets, the**

appropriation of intellectual property rights, or the extraction of sensitive information from strategic sectors (ENISA 2020).

Cyber espionage falls under what the specialised literature classifies as subversive or sabotage activities (Maschmeyer 2023). Such operations are generally conducted at low intensity, remaining well below the threshold of war, yet they can have consequences that extend far beyond their initial objectives. Interstate cyber espionage is one of the most common forms of cyber operations globally (Valeriano & Maness 2015, 9). Its primary aim is the accumulation of intelligence – namely, the extraction of sensitive information from other actors' systems (Rid 2012). **Espionage thus functions less as a means of shaping the world directly and more as a tool to facilitate its understanding** (Zilincik, Myklin & Kovanda 2019, 5; Rid 2012).

Most state and non-state actors that conduct frequent, large-scale, and sophisticated cyber espionage campaigns are classified as APTs (advanced persistent threats). **APTs are actors with exceptional capabilities who use cyber operations to pursue specific objectives over extended periods of time** (Dunn Cavelty & Egloff 2019, 44). Intelligence agencies rank among the most important actors in the strategic use of cyberspace (Dunn Cavelty & Egloff 2019, 47). The exploit vulnerabilities in widely used software to position themselves across the internet's infrastructure or gain access to targeted systems (Dunn Cavelty & Egloff 2019, 47). States refrain from deploying their full cyber capabilities in espionage operations, opting instead for targeted, precise actions (Valeriano & Maness 2015, 49). **The vast majority of cyber espionage operations take place at a relatively low level of intensity, below the threshold of war, with objectives ranging from data extraction and harassment of other states to demonstrating penetration capabilities** (Valeriano & Maness 2015, 68).

Historical background

One of the most significant developments that shed light on the modus operandi of intelligence agencies in cyberspace was the data leak orchestrated by **Edward Snowden**, a former contractor for the US National Security Agency (NSA). From his position inside the agency, Snowden extracted and published a substantial volume of classified files detailing NSA cyber intelligence activities (Devanny, Martin & Stevens 2021, 434). **His disclosures revealed**

both the scope of the United States' global intelligence efforts and the methods, techniques, and software used (Devanny, Martin & Stevens 2021, 435).

China, however, stands out as the state most deeply engaged in interstate cyber espionage (Gilli & Gilli, 2019). **Beijing has a long record of targeting government institutions in Europe and the United States**. Between 2007 and 2011, Chinese state hackers infiltrated Pentagon servers, gaining access to large volumes of sensitive data, including blueprints and designs for US stealth fighter aircraft (Gilli & Gilli, 2019). Nearly a decade later, the US Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) accused China of having penetrated US oil and gas pipeline networks between 2011 and 2013 (Greenberg & Newman 2023).

In 2014, Chinese state hackers carried out an unprecedented intrusion into the US Office of Personnel Management (OPM), stealing the personal data of more than 22 million individuals (Devanny, Martin & Stevens 2021, 436). These actions allowed Beijing not only to deepen its understanding of the US federal workforce, but also to identify potential targets for future targeted cyberattacks, blackmail, or phishing campaigns (Devanny, Martin & Stevens 2021, 437). Following this breach, China, and the United States signed a bilateral cybersecurity agreement aimed at curbing commercial cyber espionage, which succeeded in temporarily reducing the intensity of Chinese operations (Martin 2025).

More recently, in 2020-2021, the United States revealed another major Chinese cyber espionage campaign targeting federal agencies as well as private companies (Devanny, Martin & Stevens 2021, 439). Notably, the campaign was marked by a certain degree of recklessness, especially when compared to Russia's meticulous operation in the same period. Chinese hackers exploited a vulnerability in Microsoft Exchange software, leaving victims exposed to subsequent cyberattacks by other actors whose objectives went beyond espionage to include disruption (Devanny, Martin & Stevens 2021, 441).

In 2023, US officials claimed that China was planning to establish espionage facilities in Cuba to monitor electronic communications in the southeastern United States (Reuters 2023). Beijing's Ministry of Foreign Affairs rejected the allegations, instead accusing Washington of being "the world's largest hacker empire" and denying any intent to develop surveillance installations against the US on Cuban territory (Reuters 2023). Nonetheless, hackers linked to China's Ministry of State Security have gone beyond simple espionage in

Southeast Asia, launching destructive cyberattacks, including one that targeted Taiwan's state-owned oil company (Greenberg & Newman 2023).

By contrast, **Russian state and state-affiliated hackers have conducted a wide array of cyber espionage campaigns. These have ranged from intrusions into government systems for the purpose of commercial espionage or election interference, to more sophisticated operations such as the hijacking of satellite internet connections** (Mueller et al. 2023; Maschmeyer & Dunn Cavelty 2022). Russian operations typically combine advanced espionage campaigns with the deployment of malware (Mueller et al. 2023). In 2018, Washington accused Russia of infiltrating multiple sectors of US critical infrastructure, including nuclear facilities, energy, aviation, and even water supply networks (Lonergan & Poznansky 2025). So far, however, Russia has not exploited these footholds to launch direct cyberattacks on the US – though the risks have grown significantly since the war of aggression against Ukraine (Lonergan & Poznansky 2025).

One of the most notable examples was the **SolarWinds** cyber espionage campaign, in which Russia managed to infect thousands of public and private organisations in the US by compromising a widely used software product deployed across dozens of federal agencies and departments (Devanny, Martin & Stevens 2021, 438). The hacker group *Cozy Bear* (APT 29), identified as part of Russia's military intelligence agency (GRU), exploited a vulnerability in SolarWinds software to extract sensitive data (Mueller et al. 2023). Russian intelligence operatives injected malicious code into SolarWinds' Orion software in 2021, gaining access to US federal networks as well as major private companies (Sanger & Barnes 2024). At the same time, the potential employment of independent hacker groups against Euro-Atlantic states has become more visible. In 2021, a cybercrime group suspected of receiving Russian government backing launched a ransomware attack against Colonial Pipeline – the largest fuel distributor on the US East Coast – disrupting fuel supplies across the region (Sanger & Barnes 2024; Mueller et al. 2023).

RECENT MAJOR INTERSTATE ESPIONAGE CAMPAIGNS

China – Salt Typhoon

In November-December 2024, the United States exposed a large-scale Chinese cyber espionage campaign, dubbed **Salt Typhoon** by Microsoft. The hacker group had previously been accused of operations against government targets in Saudi Arabia, Brazil, Burkina Faso, Canada, Israel, and Guatemala (Montgomery 2024). In this campaign, nine major US mobile carriers were targeted, allowing real-time access to call and text-message data (Greenberg 2025a). Overall, **the operation compromised the systems of more than 80 US companies, including internet providers and major telecommunications firms such as Verizon, AT&T, and T-Mobile** (Tait 2024). The hackers gained access not only to call records and text-message metadata but also to the messages' content (Montgomery 2024).

Although communications of US government officials in Washington, DC were intercepted, the range of targets was broad, and access was extensive (Montgomery 2024). Hackers affiliated with China's Ministry of State Security successfully penetrated telecom networks to spy on the voice calls and text messages of prominent officials and politicians, including Donald Trump, JD Vance, and the campaign of Democratic candidate Kamala Harris (Volz 2025; Sanger & Barnes 2024). **Even the US government's lawful intercept program was breached, with hackers extracting official call recordings** (Montgomery 2024).

However, the attackers could not intercept communications conducted over end-to-end encrypted apps such as WhatsApp or Signal. Their access was limited to unencrypted SMS messages and standard voice calls – the very communications the US government itself can only monitor under judicial warrant (Sanger & Barnes 2024). In response, US authorities urged public-sector employees to avoid traditional SMS and instead use encrypted messaging services (Montgomery 2024).

According to anonymous US officials cited by *The Wall Street Journal*, Chinese representatives indirectly acknowledged Beijing's role in Salt Typhoon during a secret US-China meeting in Geneva in December 2024 (Volz 2025). At the same time, *The Guardian* reported that US officials considered the operation's motivation to be intelligence collection rather than preparation for an attack on critical infrastructure (Tait 2024).

Following the exposure of the Salt Typhoon operation, the hackers appear to have suspended their intrusion to prevent the full mechanism of the hack from being uncovered, but this does not necessarily mean that they no longer have access to US networks (Sanger & Barnes 2024). In February 2025, the cybersecurity company *Recorded Future* reported that Salt Typhoon had continued its intrusions during December 2024 – January 2025, identifying the presence of hackers in five additional mobile and internet companies worldwide, as well as in more than ten universities in the United States, Vietnam, and other areas (Greenberg 2025a).

The Volt Typhoon case – more than simple espionage

Volt Typhoon is the name given to a Chinese cyber operation through which thousands of internet-connected devices were compromised (Davidson 2024). US authorities have stated that the operation is part of a broader Chinese campaign to infiltrate the critical infrastructure networks of Western states, including those of the energy sector, telecommunications, internet service providers, and maritime ports (Davidson 2024).

In 2023, Microsoft and US authorities detected malicious code in telecommunications systems in Guam – a US territory in Micronesia – as well as in other parts of the United States (Sanger 2023). Microsoft noted that a group of Chinese government hackers had injected the code, raising concerns since the Pacific island hosts several ports and a significant US air base, both critical for any potential American military response to a Chinese escalation against Taiwan (Sanger 2023). The operation was conducted great precision and secrecy, at times by exploiting household network routers and other internet-connected devices to avoid detection and tracking (Sanger 2023). The NSA, together with counterpart agencies from the United Kingdom, Canada, Australia, and New Zealand, issued a joint report referencing Microsoft's findings and China's activities (Sanger 2023).

In May 2023, Microsoft announced that it had identified a hacker group considered to be linked to the Chinese government (Greenberg & Newman 2023). **This group, named Volt Typhoon, carried out a large-scale cyber campaign targeting critical infrastructure in the United States and Guam, including communications networks**. By pre-positioning themselves in these systems, the hackers could exploit vulnerabilities to conduct disruptive cyberattacks in the event of a military or diplomatic conflict between Washington and Beijing. According to Microsoft's investigation, Volt Typhoon had been active since mid-2021, with

the company claiming that by targeting US infrastructure in Guam and elsewhere, the campaign aimed to build capabilities to disrupt communications between the United States and Asia in the context of potential future crises (Davidson 2024). The Volt Typhoon operation was carried out by exploiting vulnerabilities and security flaws in outdated routers and other devices that no longer received security updates (Davidson 2024).

In May 2023, NSA, CISA, and the Department of Justice, along with key intelligence agencies from Canada, the United Kingdom, and Australia, released a joint statement exposing the operation (Greenberg & Newman 2023). Since the late 2000s, China has been accused of infiltrating US energy infrastructure networks with the aim of exploiting those intrusions in the event of a conflict (Greenberg & Newman 2023). Washington emphasized that the method of operation and chosen targets did not fit the pattern of a traditional cyber espionage campaign (Davidson 2024). US authorities warned that the malware found within US infrastructure appeared to be prepared for use in the event that Washington intervened militarily to support Taiwan amid a potential escalation (Sanger & Landler 2024). **Unlike other Chinese operations, the United States and its allies argued that the goal was not the extraction of data for conventional espionage but rather the pre-positioning in key points of critical infrastructure to prepare for possible future acts of sabotage** (Davidson 2024). Lin Jian, the spokesperson for the Chinese Ministry of Foreign Affairs, rejected the allegations, dismissing them as disinformation (Sanger & Landler 2024).

All eyes on the war of aggression against Ukraine. Russia's latest campaigns

On May 21, 2025, CISA issued a joint statement with several counterpart agencies from the United States and other Euro-Atlantic states, revealing a Russian cyber espionage campaign targeting technology companies and logistics networks across the Western space (CISA 2025). The statement was co-signed by agencies in Australia, Canada, the Czech Republic, Denmark, Estonia, France, Germany, the Netherlands, Poland, and the United Kingdom. The Russian campaign targeted entities involved in coordinating, delivering, and transporting aid to Ukraine, with a particular focus on surveillance camera systems along the borders of several Euro-Atlantic states (CISA 2025). Attempts to gain access to these camera systems were reported in Bulgaria, the Czech Republic, France, Germany, Greece, Italy, the Netherlands, Poland, Slovakia, the United States, Ukraine, **as well as Romania and the Republic of**

Moldova (CISA 2025). CISA attributed the campaign to the APT28 group, also known as Fancy Bear, previously identified as Unit 26165 within the GRU.

Since 2022, following Russia's full-scale invasion of Ukraine, Russian government-backed hackers have begun targeting countries providing security assistance to Ukraine, focusing on entities in the government, financial, energy, healthcare, and transportation sectors (CISA 2024). Their cyber campaigns have included website defacement, data exfiltration, vulnerability scanning of critical systems, and data leak operations (CISA 2024). In addition to publishing stolen data online, GRU hackers have also sold the exfiltrated information on the black market (CISA 2024).

According to US government officials cited in American media, on April 4, 2024, CISA issued an emergency directive concerning a cyber intrusion by a group of hackers affiliated with the SVR into Microsoft's networks (Heilweil et al. 2024). The group, known as APT29 (or Cozy Bear), is also responsible for the 2015-2016 hacks against the Democratic National Committee and the SolarWinds espionage campaign in 2020. In March 2024, Microsoft announced that Russian hackers had succeeded in accessing the source code of several of its software products (Heilweil et al. 2024).

In September 2024, the FBI, CISA, and NSA issued a joint statement publicly attributing a series of cyber operations to a unit of Russia's military intelligence agency (GRU), which was found responsible for operations worldwide involving sabotage, espionage, and reputational damage (CISA 2024). The objectives of GRU Unit 29155's cyber operations include intelligence collection, hack-and-leak operations involving sensitive information (also known as *kompromat*), and systemic sabotage through data destruction (CISA 2024). **Unit 29155 has targeted Ukraine with the WhisperGate malware, as well as NATO member states and other countries across Europe, Latin America, and Central Asia** (CISA 2024).

In February 2025, Microsoft disclosed a cyber intrusion campaign conducted by the **Sandworm** group (identified by US authorities as part of the GRU) against targets in the United States, the United Kingdom, Australia, and Canada (Greenberg 2025b). More specifically, Microsoft researchers identified a new group called **BadPilot**, which carried out the initial intrusions to establish footholds in targeted networks before Sandworm operatives took over (Greenberg 2025b). Whereas in 2022 Sandworm had focused exclusively on Ukraine, by 2023 it has expanded its cyber operations globally (Greenberg 2025b). According to Microsoft,

targets included government networks as well as the energy, telecommunications, maritime transport, and defence industries (Greenberg 2025b).

GOVERNMENT ESPIONAGE AGAINST DISSENT. THE ISSUE OF COMMERCIAL SPYWARE

In 2021, a series of media outlets, including *The Guardian*, *Haaretz*, and *The Washington Post*, published an investigation into the abusive use of spyware developed by the Israeli company NSO Group. **Pegasus was used to infiltrate phones via a WhatsApp vulnerability, extracting text messages, location data, app usage information, and intercepting phone calls** (European Parliament 2023). Pegasus belongs to the category of commercial spyware – monitoring software developed by private companies and sold primarily to governments. Greece, Poland, and Hungary were embroiled in scandals concerning its abusive deployment of the spyware tool against journalists and opposition figures (Deibert 2022). According to a *AccessNow* report, cited by *The Guardian*, at least seven journalists and activists critical of the Kremlin were targeted by a state actor using Pegasus while located within the EU (Kirchgaessner 2024).

In May 2025, a US federal court ordered NSO Group to pay nearly 170 million dollars in compensation to WhatsApp and Meta due to cyber intrusions that compromised at least 1,400 accounts in 2019 by exploiting the video call system to infect phones with malware (Miller 2025).

The European Parliament also established a special committee to investigate spyware use across EU member states (Miller 2025). In March 2023, the committee adopted a report on Pegasus and drafted recommendations condemning the abusive use of spyware by EU governments (European Parliament 2023). The list of Pegasus targets includes journalists, activists, civil society members, politicians, diplomats, businesspeople, and others (European Parliament 2023).

In 2024, following elections in Poland that brought a new government to power, authorities revealed that more than 600 people had been spied on by the former conservative government using Pegasus (Smalley 2024b). After an 18-month Senate investigation, one conclusion was that the 2019 elections had been influenced due to cyber intrusions targeting the then-opposition leader (Smalley 2024b). Poland is not an isolated case: similar Pegasus

abuse scandals have surfaced in Greece, Spain, and Hungary (Smalley 2024b). **Investigative journalists revealed that Greece, Spain, Poland, and Hungary all deployed Pegasus, targeting journalists, opposition politicians, and civil society leaders across Europe** (Smalley 2024a). For instance, even the President of the European Parliament, Roberta Metsola, was targeted with the Predator spyware in 2023 (Smalley 2024a). Likewise, in Spain, the High Court opened an inquiry into the potential spying on Prime Minister Pedro Sánchez and other politicians, alongside an investigation into the alleged surveillance of Catalan independence activists (Smalley 2024b). Journalistic investigations further revealed that Pegasus targets in Spain included every Catalan member of the European Parliament who supported independence, as well as every Catalan president between 2010 and 2020 (Deibert 2022).

At the same time, Pegasus was used against government critics in the United Arab Emirates, Thailand, and Saudi Arabia (Deibert 2022). Both authoritarian states and democracies such as the US, Spain, Mexico, and Hungary have used Pegasus spyware in ways that violate public accountability and human rights norms (Deibert 2022) The NSO Group company stated repeatedly that the software was intended only for use in police investigations and intelligence operations, claiming that Pegasus had been used to capture major criminals such as drug trafficker Joaquin Guzman Loera (El Chapo) (Smalley 2024b).

In 2024, the Biden Administration, together with other countries, pledged to use spyware responsibly, and even the Trump Administration in 2025 supported an international effort to establish a code of conduct for the use of such software (Miller 2025). In 2023, the United States, the United Kingdom, and nine other states signed a statement on the dangers posed by the global proliferation and abuse of commercial spyware (GOV.UK 2024). Later, six more states joined, with the full list including Australia, France, Japan, Poland, and South Korea, among others (GOV.UK 2024). **In 2021, the US Department of Commerce added NSO Group to the list of entities responsible for malicious cyber activities**, restricting the company's ability to do business with American firms and making it more difficult to sell its software globally (Miller 2025).

ANALYSIS. INTERSTATE CYBER ESPIONAGE AND OFFENSIVE CYBER OPERATIONS

The fact that states spy on each other is not remarkable in international affairs. For instance, following HUMINT (human intelligence) operations, states impose costs intended to damage the other actor's reputation and disrupt their operations, such as declaring embassy personnel *personae non gratae* and expelling them – but such actions tend to be proportional and temporary (Devanny, Martin & Stevens 2021, 431). However, a recent study showed that **destructive or disruptive cyber operations generate more news and media coverage compared to cyber espionage activities, thereby attracting greater public attention** (Makridis, Maschmeyer & Smeets, 2024).

Nevertheless, recent research has shown that cyber operations are often too weak, slow, or volatile to become effective tools in military campaigns, offering only limited strategic value even in hybrid conditions (Maschmeyer & Dunn Cavelty, 2022). Moreover, **cyber espionage could even reinforce strategic stability, as long as the affected states recognise it as such and refrain from escalating situations** (Devanny, Martin & Stevens, 2021). Cyber espionage, including activities carried out by Russia or China, is common and routine in international affairs. Therefore, measures should be taken to hinder the operations of other states, but this does not necessarily mean that such activities constitute novel developments warranting particularly severe responses. The exception here is negligent cyber espionage campaigns that create exploitable breaches for other potential actors, or that seriously disrupt the proper functioning of targeted systems.

If Salt Typhoon represents a traditional espionage campaign (albeit an exceptional one), in the case of Volt Typhoon the initial purpose of information-gathering was exceeded, involving intrusions aimed at securing strategic pre-positioning in critical infrastructure. Volt Typhoon more closely resembles Russian cyber campaigns, in which hackers attempt to scan or test vulnerabilities and breaches in the IT networks of various critical sectors. The ultimate goal of these **pre-positioning** actions, or of implanting malware into networks, is the activation (or "detonation") of such tools in the context of major escalations in relations between the two states – whether in the event of a conflict in Taiwan or an escalation of the Russo-Ukrainian war.

According to an analysis by Ciaran Martin (2025) for RUSI, in the last two years China has undergone a transition in its cyber capabilities and objectives – from economic to political goals, from opportunistic actions to strategic operations, and from a passive to an active approach. Thus, **China has shifted from simple cyber espionage campaigns and data theft to operations that could lay the groundwork for massive cyberattacks against the critical infrastructure of Western states (Martin 2025)**.

Salt Typhoon represents a traditional cyber-espionage operation, even if it had a significant scale (Lonergan & Poznansky 2025). It was carried out by China's Ministry of State Security (the main intelligence service) and involved successful infiltrations into US telecommunications systems (Martin 2025). By contrast, Volt Typhoon represents a cyber operation with political and potentially military strategic objectives, conducted by the Chinese army's cyber unit, which inserted malware into American critical infrastructure (Martin 2025). According to the Biden Administration, the areas targeted by Volt Typhoon included energy, transportation, construction, education, government, and the IT sector (Martin 2025).

Although it is sometimes used to prepare for cyberattacks and involves offensive actions, espionage is not inherently offensive, but rather aims at a better understanding of international affairs. Both cyber operations aimed at disruption and cyber espionage campaigns involve offensive activities (such as intrusions and illegal access to data or networks), but what matters is the ultimate goal of these activities. Nevertheless, it is becoming increasingly difficult to distinguish between simple acts of espionage and intrusions with offensive purposes, such as pre-positioning for future attacks.

Volt Typhoon represents a pre-positioning action for potential future cyberattacks, its objective being to gain access and infiltrate different points of networks in order to exploit them in the event of a conflict (Lonergan & Poznansky 2025). **In the case of a conflict, China could launch destructive or disruptive cyberattacks against the critical infrastructure of the US or its partners, either to discourage involvement in the conflict or to hinder military and civilian capabilities in the vent of a crisis or war** (Lonergan & Poznansky 2025). A joint statement issued by the Five Eyes countries (United States, United Kingdom, Australia, Canada, New Zealand) noted that malware implants constitute strategic assets that could be activated in the event of a crisis or major conflict between China and the West (Martin 2025). At the same time, Erica Lonergan and Michael Poznansky (2025) argue that Volt Typhoon is part of a broader set of tools prepared by China for a potential conflict with the US

and its partners, which means Washington will have to deter a war with China in order to deter the activation of the implanted malware.

China does not have a strong record of launching destructive cyberattacks (Martin 2025). While China's cyber capabilities have been developed largely to pursue economic goals, Russia's have always been aimed at political objectives (Martin 2025). In recent years, cybercrime groups originating in Russia (and likely tolerated or supported by the Russian government) have caused significant disruptions in critical sectors such as energy or healthcare through ransomware operations (Martin 2025). By contrast, state actors have not carried out substantial cyberattacks. **Russia has not managed to cause significant disruptions or secure strategic victories even in cyber operations against Ukraine and its allies following the full-scale invasion in 2022** (Martin 2022).

Beyond simple espionage campaigns, **Russia** has also focused on cyber operations aimed at disrupting the state, society, and economy, as well as undermining citizens' trust in public institutions. **Pre-positioning efforts by Russian government hackers in sensitive sectors of US critical infrastructure – similar to the Volt Typhoon campaign – have been identified over the past seven years, but they have not (yet) been exploited**. The reasons for this range from Russia or China's potential restraint from escalating tensions through cyberattacks, to fears of cyber or other type of retaliation, to the strengthening of cyber defences in Euro-Atlantic states, as well as the fact that tensions between the two blocs have not crossed certain red lines considered by them. In recent years, most of Russia's cyber and information operations in the Western space have been tied to the war of aggression against Ukraine.

In addition, Myriam Dunn Cavelty argues that actions undertaken by different state actors to increase security can in fact reduce overall security, both in cyberspace and in the physical world (Dunn Cavelty 2014, 702). Thus, **intelligence services may create a less secure cyberspace in their attempts to gain access to as much data as possible** (Dunn Cavelty 2014, 710). Edward Snowden's revelations showed that the NSA identified and exploited zero-day vulnerabilities while also injecting its own malware into various parts of internet infrastructure (Dunn Cavelty 2014, 710). In this way, covert access points (backdoors) were created, which could be activated at any time for activities ranging from monitoring and espionage to destructive attacks (Dunn Cavelty 2014, 710). However, such vulnerabilities can also be exploited by cybercriminal groups or hackers from other states – thus creating threats even for the state that maintains them (Dunn Cavelty 2014, 710).

Alongside the worrying developments regarding interstate cyber espionage, **commercial spyware** represents another potentially equally dangerous factor for democracies, as it is used to spy on the opposition, civil society, and journalists. **Recent incidents have highlighted the need for substantial international regulation, as well as the imposition of sanctions** when certain companies or states allow their software to be abused by others, or when they choose to export such programs to authoritarian regimes known for repressing democratic opposition and with a history of abusing such software. However, taking serious measures in this regard is a difficult effort, given that the export of commercial spyware provides strategic advantages for the states delivering these tools. For example, a *New York Times* investigation revealed that sales made by NSO helped the Israeli government led by Benjamin Netanyahu conclude the Abraham Accords with Bahrain, Morocco, and the United Arab Emirates, given that the Israeli government approves export licenses for the company's sales (Deibert 2022).

Responses taken by Western states against cyber espionage

Devanny, Martin & Stevens (2021) argue that responses of states to cyber operations targeting them depends substantially on the strategic and bilateral context in which such incidents occur. In general, the United States refers to the idea of **"imposing costs"** following cyber espionage campaigns against it, which may include launching its own cyber operations (Devanny, Martin & Stevens 2021, 431).

For example, in April 2021, the United States imposed economic sanctions following the SolarWinds campaign, expelled several members of Russia's diplomatic mission in Washington, and launched its own cyber operations against Russian intelligence agencies (Devanny, Martin & Stevens 2021, 439). However, it is unclear whether the American response to the SolarWinds campaign – **public attribution, economic sanctions, and indictments** – played any role in deterring Russia from conducting further cyber espionage operations (Lonergan & Poznansky 2025).

Similarly, in March 2024, the United States and the United Kingdom announced sanctions against hackers accused of a cyber espionage campaign dating back to the 2010s, run through a front company of the APT31 group (Zirconium or Judgement Panda), associated with the Chinese government (Robins-Early 2024). Washington and London accused China's

Ministry of State Security of conducting the campaign for 14 years, in an effort to inject malware into US critical infrastructure (Sanger & Landler 2024). The campaign lasted about 14 years and targeted not only companies, public officials, and critics of Beijing, but also intrusions into US critical infrastructure sectors such as defence and energy (Robins-Early 2024). At the same time, British authorities accused the campaign of compromising data from tens of millions of voters at the UK Electoral Commission, and in other cases of targeting members of Parliament known for raising concerns about the issue of threats coming from China (Robins-Early 2024).

Other measures have also been taken, such as banning companies from bidding on contracts (e.g., Huawei) or restricting the products of other firms. For example, in June 2024, Washington banned the Russian cybersecurity company Kaspersky in the United States for both companies and individuals – revoking its authorisation to sell products or even to send updates to systems that already had its antivirus software installed (Stahie 2024). The reason given by US authorities was a lack of confidence that, if Russia decided to weaponize the data collected by the antivirus, the company would be able to resist government pressure (Stahie 2024). In fact, Kaspersky had already been banned from US federal government systems since 2017, accused of ties to Russian intelligence agencies and of illegally extracting data from companies (Stahie 2024). In 2022, Germany, Italy, and Romania also banned Kaspersky in the public sector (Stahie 2024).

CONCLUSIONS AND RECOMMENDATIONS

Cyber espionage becomes a significant problem when certain limits are exceeded, such as campaigns that result in the extraction of highly sensitive data. The same is true of campaigns that create security breaches – vulnerabilities that can then be exploited by other malicious actors – endangering end-users. **Concerning developments have not only emerged from interstate cyber espionage, but also from governments spying on their own citizens, other states, NGOs, companies, and other governments through the use of commercial spyware**. Unlike black-market practices where such software is auctioned off, these companies must comply with national and international regulations (Perlroth 2021).

Regardless of the measures that can be taken, **low-intensity** disruptive operations will continue to affect Western states, such as **ransomware** attacks (Maschmeyer & Dunn Cavelty

2022). Campaigns such as **Salt Typhoon** will likely continue in the coming period, but the greatest risk lies in the continuation of **Volt Typhoon**-type operations and the potential use of destructive or seriously disruptive attacks against economic or governmental activity. Moreover, cyber intrusions and access obtained for **espionage** purposes can just as easily be repurposed for launching **disruptive or destructive operations** (Devanny, Martin & Stevens, 2021). At the same time, cyber influence operations designed to deepen social polarization, as well as espionage campaigns, are likely to intensify in the coming years, given growing tensions among major international actors (Maschmeyer & Dunn Cavelty, 2022).

Cyber espionage is a normal activity so long as it does not negatively affect critical infrastructure. In the case of **Russia**, Euro-Atlantic states already have experience and can anticipate that Moscow's cyber espionage operations are often followed by disinformation campaigns and/or data leaks, or in fact disguise pre-positioning or data-wiping cyberattacks. **China**, however, has focused over the past 20 years on espionage rather than on disruptive or destructive operations. For this reason, a Volt Typhoon-type campaign may catch decision makers by surprise.

Recommendations

The main measures to manage the impact of an operation like Salt Typhoon are: identifying the scale of the operation, stopping its spread, eliminating intrusions from networks, and updating or replacing telecommunications equipment to make it less vulnerable to future operations (Lonergan & Poznansky 2025).

Western states must continue the policy of naming and shaming in response to such cyber campaigns – **public attribution of the state responsible for the operation and issuing joint statements with as many states as possible**. Another important measure is **indicting those found responsible and describing the hackers' exact methods of operation** – steps that can help identify patterns in the future and deter similar operations against other states. At the same time, **international initiatives to reduce interstate tensions in cyberspace** should also include states outside the "like-minded" circle of Western space democracies, to ensure greater international legitimacy.

Publicly communicating that a state targeted by such operations is willing to use any means to defend itself is also a form of deterrence. The United States and its allies must

continue to send a clear and public message to China that disruptions of US or allied critical services are unacceptable and will result in serious consequences (Martin 2025).

In addition, **traditional espionage can be countered through better data security for critical infrastructure servers and networks closely tied to national security**. Likewise, reducing the intensity of foreign cyber operations and lowering the risk of destructive attacks can also be achieved by **improving diplomatic and trade relations and by easing international tensions**.

However, **countering and punishing interstate cyber espionage must also be accompanied by precise measures to limit the use of commercial spyware**, available to a wide range of actors, even if the most sophisticated versions remain limited to governments. The measures should include **export controls and sanctions for both companies and states** that allow such software to be abused, as well as sanctions against states that use them abusively.

BIBLIOGRAPHY

Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, *15*(1), 35–57.

CISA. (2024, September 5). *Russian Military Cyber Actors Target US and Global Critical Infrastructure*. CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a

CISA. (2025, May 21). *Russian GRU Targeting Western Logistics Entities and Technology Companies*. CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a

Davidson, H. (2024, February 13). Explainer: What is Volt Typhoon and why is it the 'defining threat of our generation'? *The Guardian*. https://www.theguardian.com/technology/2024/feb/13/volt-typhoon-what-is-it-how-does-it-work-chinese-cyber-operation-china-hackers-explainer

Deibert, R. J. (2022). The Autocrat in Your iPhone: How Mercenary Spyware Threatens Democracy. *Foreign Affairs*. https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert

Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. *Journal of Cyber Policy*, *6*(3), 429–450. https://doi.org/10.1080/23738871.2021.2000628

Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, *20*(3), 701–715. https://doi.org/10.1007/s11948-014-9551-y

ENISA. (2020). *Cyber Espionage* (ENISA Threat Landscape). ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-cyber-espionage

European Parliament. (2023). *Investigation of the use of Pegasus and equivalent surveillance spyware*. European Parliament. https://www.europarl.europa.eu/RegData/etudes/ATAG/2023/747923/EPRS_ATA(2023)747923_EN.pdf

France-Presse, A. (2024, December 31). Beijing denies involvement in US treasury cyber-attack. *The Guardian*. https://www.theguardian.com/technology/2024/dec/31/beijing-denies-involvement-in-us-treasury-cyber-attack

Gilli, A., & Gilli, M. (2019). Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage. *International Security*, *43*(3), 141–189. https://doi.org/10.1162/isec_a_00337

GOV.UK. (2024, March 28). *Efforts to counter the proliferation and misuse of commercial spyware: Joint statement*. GOV.UK. https://www.gov.uk/government/news/efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware-joint-statement

Greenberg, A. (2025a). A Hacker Group Within Russia's Notorious Sandworm Unit Is Breaching Western Networks. *Wired*. https://www.wired.com/story/russia-sandworm-badpilot-cyberattacks-western-countries/

Greenberg, A. (2025b). China's Salt Typhoon Spies Are Still Hacking Telecoms—Now by Exploiting Cisco Routers. *Wired*. https://www.wired.com/story/chinas-salt-typhoon-spies-are-still-hacking-telecoms-now-by-exploiting-cisco-routers/

Greenberg, A., & Newman, L. H. (2023). China Hacks US Critical Networks in Guam, Raising Cyberwar Fears. *Wired*. https://www.wired.com/story/china-volt-typhoon-hack-us-critical-infrastructure/

Heilweil, R., Starks, T., Vicens, A., & Groll, E. (2024). Federal government affected by Russian breach of Microsoft. *CyberScoop*. https://cyberscoop.com/federal-government-russian-breach-microsoft/

Higgins, A., & Scheutze, C. F. (2024). Suddenly, Chinese Spies Seem to Be Popping Up All Over Europe. *The New York Times*. https://www.nytimes.com/2024/04/27/world/europe/china-spies.html

Iyengar, R. (2023). North Korea's Hackers Prioritize Espionage Over Cryptocurrency. *Foreign Policy*. https://foreignpolicy.com/2023/06/23/north-korea-cyber-espionage-cryptocurrency-theft/

Kirchgaessner, S. (2024, May 30). Critics of Putin and his allies targeted with spyware inside the EU. *The Guardian*. https://www.theguardian.com/technology/article/2024/may/30/critics-of-putin-and-his-allies-targeted-with-spyware-inside-the-eu

Lonergan, E., & Poznansky, M. (2025, February 25). A Tale of Two Typhoons: Properly Diagnosing Chinese Cyber Threats. *War on the Rocks*. https://warontherocks.com/2025/02/a-tale-of-two-typhoons-properly-diagnosing-chinese-cyber-threats/

Makridis, C., Maschmeyer, L., & Smeets, M. (2024). If it bleeps it leads? Media coverage on cyber conflict and misperception. *Journal of Peace Research*, *61*(1), 72–86. https://doi.org/10.1177/00223433231220264

Martin, M., Ciaran. (2025). Typhoons in Cyberspace. *RUSI*. https://www.rusi.org/explore-our-research/publications/commentary/typhoons-cyberspace

Maschmeyer, L. (2023). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, *46*(3), 570–594. https://doi.org/10.1080/01402390.2022.2104253

Maschmeyer, L., & Dunn Cavelty, M. (2022). Goodbye Cyberwar: Ukraine as Reality Check. *Policy Perspectives*, *10*(3). https://doi.org/10.3929/ETHZ-B-000549252

Miller, M. (2025, May 6). Israeli spyware giant NSO Group ordered to pay nearly $170M to WhatsApp for hacking accounts. *POLITICO*.

https://www.politico.com/news/2025/05/06/nso-group-pegasus-whatsapp-hack-170-million-damages-00332155

Montgomery, B. (2024, December 12). Why did China hack the world's phone networks? *The Guardian*. https://www.theguardian.com/technology/2024/dec/09/why-did-china-hack-the-worlds-phone-networks

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). Cyber Operations during the Russo-Ukrainian War. *CSIS*. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

Perlroth, N. (2021). *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*. Bloomsbury.

Reuters. (2023, June 9). China: 'Hacker empire' US is 'spreading rumours' with talk of Cuba spy station. *Reuters*. https://www.reuters.com/world/china-hacker-empire-us-is-spreading-rumours-with-talk-cuba-spy-station-2023-06-09/

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Robins-Early, N. (2024, March 26). US and UK unveil sanctions against Chinese state-backed hackers over alleged 'malicious' attacks. *The Guardian*. https://www.theguardian.com/technology/2024/mar/25/us-sanctions-chinese-hackers

Sanger, D. E. (2023). *Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target?* https://www.nytimes.com/2023/05/24/us/politics/china-guam-malware-cyber-microsoft.html

Sanger, D. E., & Barnes, J. E. (2024). China's Hacking Reached Deep Into U.S. Telecoms. *The New York Times*. https://www.nytimes.com/2024/11/21/us/politics/china-hacking-telecommunications.html

Sanger, D. E., & Landler, M. (2024). U.S. and Britain Accuse China of Cyberespionage Campaign. *The New York Times*. https://www.nytimes.com/2024/03/25/us/politics/china-hacking-us-sanctions.html

Smalley, S. (2024). *How Italy became an unexpected spyware hub*. https://therecord.media/how-italy-became-an-unexpected-spyware-hub

Smalley, Suzanne. (2024). *Polish Parliament strips official of immunity, clearing path for prosecution in spyware scandal*. https://therecord.media/polish-parliament-strips-official-of-immunity-pegasus-spyware

Stahie, S. (2024). *US Bans Kaspersky Software for Users and Companies; Customers Advised to Seek Trusted Alternatives*. Bitdefender. https://www.bitdefender.com/en-us/blog/hotforsecurity/us-bans-kaspersky

Tait, R. (2024, December 14). Democrats and Republicans condemn espionage-driven Chinese hack. *The Guardian*. https://www.theguardian.com/world/2024/dec/13/democrats-republicans-condemn-salt-typhoon-hack

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

Volz, D. (2025). In Secret Meeting, China Acknowledged Role in U.S. Infrastructure. *The Wall Street Journal*. https://www.wsj.com/politics/national-security/in-secret-meeting-china-acknowledged-role-in-u-s-infrastructure-hacks-c5ab37cb

Zilincik, S., Myklin, M., & Kovanda, P. (2019). Cyber power and control: A perspective from strategic theory. *Journal of Cyber Policy*, *4*(2), 290–301. https://doi.org/10.1080/23738871.2019.1635177

Our mission. The Romanian Diplomatic Institute (RDI) has the mission to make a substantial contribution to increasing the quality of Romanian diplomacy through training, further education, research, the development of critical and strategic thinking and international networking. A good foreign policy serves as a beneficial domestic policy.

Guiding principles: human resource development, professionalism, respect and dialogue, and responsibility for the community.

Based on the founding legal attributions of the RDI, the further development of the Institute is carried out, according to the needs identified in the MFA, along the following four directions:

- Training and further education of diplomats and other trainees;
- Deepening the research and expertise dimension on regional and functional issues;
- Operating the RDI as a think-tank of the MFA;
- Integration of the RDI into an international network of similar relevant institutes.

Author: Claudiu Codreanu (PhD) is a researcher at the Romanian Diplomatic Institute – Department of Expert Analysis.

RDI Policy Paper series
ISSN 2285-8938
ISSN-L 2285-8938

Cover photo: https://unsplash.com/photos/black-towers-during-sunset-0C9VmZUqcT8

The Romanian Diplomatic Institute
https://www.idr.ro/en/ | secretariat@idr.ro
Primăverii 17, sector 1, Bucharest, 011972