Question time: Protecting critical infrastructure in the EU and countering hybrid attacks

The escalation of Russia’s war on Ukraine, and recent incidents – such as the Nord Stream pipeline sabotage – highlight the urgent need to protect the EU’s key infrastructure against physical and digital threats, including hybrid attacks. The European Parliament will use its powers of oversight in the revived ‘question time’, during the October II plenary session, to question the European Commission on the issue.

Context
On 26 September 2022, four large explosions hit the Nord Stream gas pipelines connecting Russia to Germany and led to the largest methane leak in history, releasing up to 300,000 tonnes of a fuel that is 84 times more potent than carbon in terms of its greenhouse gas emissions over a 20 year timeframe. At the time, the Nord Stream pipelines were not being used to transport gas supplies to Europe, due to the geopolitical tensions between Russia and the EU. Western officials and commentators have tended to blame Russia for the sabotage of its own pipelines, although its precise motivations for doing so remain unclear. In any case, the closure of the Nord Stream pipelines marks a further rupture in energy relations between the EU and Russia, and emphasises the importance of building alternative infrastructure for gas supplies to Europe, including new liquefied natural gas (LNG) import terminals and smaller floating storage and regasification units (FSRUs). On 8 October, train services in north-west Germany were halted for 3 hours after critical cables for the communication system between the trains and the railway operators were sabotaged.

These latest incidents exemplify the vulnerability of the EU’s critical infrastructure – ‘the new frontier of warfare’, as the Commission President, Ursula von der Leyen, put it recently, pointing to the need to protect physical infrastructure such as pipelines and underwater cables. She also outlined possible action to enhance preparedness, including stress-testing critical infrastructure, using the EU’s satellite surveillance capacity more effectively, and triggering the EU civil protection mechanism in the event of disruption.

Malicious cyber-activities by state and non-state actors are yet another form of threat and are being used increasingly to target critical infrastructure (such as the healthcare, transport and energy sectors) and even EU institutions. Cyber-attacks are part of Russia’s hybrid approach to warfare, and have been used against the EU, not only to disrupt essential services but also to undermine democracy and spread disinformation. The EU’s growing exposure to hybrid threats requires it to increase its resilience and strategic autonomy.

EU action
Enhancing the resilience of critical entities and network and information security
The EU’s efforts to enhance critical infrastructure protection date back to 2006 with the setting up of the European Programme for Critical Infrastructure Protection (EPCIP) and the subsequent adoption of the Directive on European Critical Infrastructure in 2008. However, the 2008 directive has a limited scope, applying only to the energy and transport sectors. To take into account the evolving security landscape, the EU is currently updating these rules. The new directive on the resilience of critical entities (CER) will expand the scope of the 2008 one to cover 11 sectors – energy, transport, banking, financial market infrastructure, health, drinking water, waste water, digital infrastructure, public administration, space and food. It aims to create an all-hazards framework to support Member States in ensuring that critical entities are able to prevent, resist, absorb and recover from disruptive incidents, whether they are caused by natural disasters, accidents, terrorism, insider threats or public health emergencies.

While the legislation on protecting critical infrastructure deals with ‘physical’ security, a separate set of rules aims to ensure ‘digital’ security. The Network and Information Security Directive (NIS1) – currently under review – was the first piece of EU-wide legislation on cybersecurity. The new NIS2 will strengthen security...
EPRS Question time: Protecting critical infrastructure in the EU and countering hybrid attacks

requirements, address supply chain security, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. It will also have a broader scope, imposing the obligation to take risk management measures on more entities and sectors, such as providers of public electronic communications services, social media operators, manufacturers of critical products (e.g. medical devices), postal and courier services, and public administrations. To ensure alignment between the two instruments, all critical entities identified under the CER directive will be subject to cyber-resilience obligations under NIS2. Entities carrying out activities in areas such as defence, national security or public security, and law enforcement agencies, the judiciary, parliaments and central banks, are excluded from the scope of both directives.

The co-legislators reached provisional agreements on the NIS2 and CER directives on 13 May and 28 June 2022 respectively. The final votes by the European Parliament are scheduled for November 2022. Once adopted, both directives should be transposed into national law by 2024 (within 21 months of their entry into force).

Countering hybrid and cyber-threats

The Strategic Compass for Security and Defence adopted on 24 March 2022 identifies countering hybrid threats and protecting critical infrastructure as key areas where the EU needs to bolster its security. EU leaders committed in the Compass to boosting the EU’s intelligence analysis capacities, and to developing a ‘hybrid toolbox’ – bringing together instruments to tackle hybrid threats – and hybrid response teams – to help Member States, partners and CSDP missions and operations tackle hybrid threats. They have also agreed to develop a foreign information manipulation and interference (FIMI) toolbox and to improve cyber-resilience. The Compass calls for the EU’s cyber-defence policy to be strengthened and for a new European cyber-resilience act. There are also plans to shore up the cyber-diplomacy toolbox – a framework for a joint diplomatic response from the EU to malicious cyber-activities – and the Joint Cyber Unit (JCU) – a platform that strengthens cooperation between EU institutions and Member States’ authorities – and to boost cyber-defence capabilities. EU Member States have meanwhile committed to work together with the Commission in 2023 to review the risk to critical infrastructure supply chains, not least in the digital domain.

Substantial progress has already been made in this field. In recent months, the Council has issued conclusions on the EU’s cyber posture, on a framework for a ‘coordinated EU response to hybrid campaigns’, and on FIMI. On 15 September 2022, the Commission proposed an EU cyber-resilience act to ensure more secure hardware and software products. A proposal for an EU cyber-defence policy is expected on 9 November 2022. Important steps have been taken to bolster cyber-resilience through permanent structured cooperation (PESCO) – a framework for defence cooperation between EU Member States. Ten PESCO projects currently focus on the cyber domain.

Sectoral initiatives

On 23 May 2022, the Commission adopted a contingency plan for transport. Part of the sustainable and smart mobility package and aiming to improve the response to crises following the COVID-19 pandemic, the plan lists a number of initiatives, drawing also on experience from the start of the war in Ukraine. It proposes measures to increase the transport sector’s crisis preparedness and its ability to respond to disruption that could be caused by natural disasters, pandemics, terrorist attacks, cyber-attacks, military conflicts, infrastructure failure or power outages. The Commission also intends to review EU transport laws to assess whether they could be amended to cope better with crises and how to ensure minimum connectivity. It is proposing contingency tests to assess crisis preparedness, to feed into contingency measures for the transport industry and authorities. It also wants to step up cybersecurity cooperation with the EU’s transport agencies. In September 2022, the Commission proposed the single market emergency instrument to respond quickly to emergencies and crises that threaten the functioning of the single market. In November 2022, Parliament will vote on new rules to boost financial sector resilience (DORA regulation).

European Parliament position

In March 2022, the European Parliament expressed the need for an EU strategy against foreign interference, covering, for instance, critical infrastructure, strategic sectors and resilience against cyber-attacks. It recommended extending the list of critical entities to digital election infrastructure and education systems.
It also recommended urgent implementation, under the Strategic Compass, of a strengthened toolbox to tackle hybrid and cyber-threats and to fight disinformation, while reinforcing cyber-defence capacities.