CRITICAL CONNECTIONS, CONTINUITY AND SUPPLY

EU2019.FI

Assessing the security of European critical infrastructure and functions in a hybrid threat context

Report

On 6 November 2019, the European Union Institute for Security Studies (EUISS) and the Finnish Presidency of the Council of the European Union co-organised a conference in Brussels focusing on the security of European critical infrastructure and supply chains in a hybrid threat context. Hosted by the Finnish Permanent Representation to the EU, the event allowed participants to exchange views on strategic issues, assess the state of play and discuss the future ways in which the EU institutions, member states and private sector operators could reinforce European critical infrastructure protection. The conference brought together officials from EU member states, EU institutions and the North Atlantic Treaty Organisation (NATO) with representatives of the private sector and think tanks.

CRITICAL INFRASTRUCTURE: WHERE DIGITAL MEETS PHYSICAL

At the conference it was agreed that critical infrastructure – from energy, transport and telecommunications networks to water supply, waste management, healthcare and financial systems – is crucially important for the member states and the EU as a whole, as it is fundamental for the safety and stability of society. Moreover, a number of key themes were addressed, the combination of which has given rise to new challenges.

Societies have become used to dynamic 'just-in-time' global value chains, while disruptive digital technologies have emerged (e.g. 5G and Artificial Intelligence). Second, various critical infrastructures have become increasingly interconnected, with digital infrastructure both enabled by and linking together physical ones. As a result, threats in one sector can have cascading effects across the system. Moreover, the centrality of digital networks were emphasised, many of which in Europe are foreign-owned. In particular, data access and ownership are crucial security issues since data are used to identify and manage risks. In this regard, it was also noted that there is an inherent tension between privacy concerns and the 'need to know' for security purposes.

economic interdependence and integration in the EU have not been carried over to the security domain

At the same time, economic interdependence and integration have not carried over to the security domain. While most critical infrastructure across Europe is now in the hands of the profit-driven private sector, security and resilience is still the prerogative of sovereignty-minded governments. However, this division of labour is being challenged by the return of geopolitics and its attendant weaponisation of global interlinkages. The private sector mainly approaches critical infrastructure security from a business risk perspective and has neither the mandate nor the capacities to identify vulnerabilities and defend against threats coming from adversarial state or state-backed actors. In the context of hybrid threats, such actors may attempt to disrupt critical infrastructures in order to impede their target's stability and decision-making capabilities and gain a strategic competitive advantage.

In this context, several key elements for a European approach were raised during the conference. An important first step would be to identify and address European vulnerabilities before adversaries do, in order to mitigate potential threats and deny adversaries the opportunity to exploit these vulnerabilities. There was also agreement that perfect security across all forms of infrastructure is impossible. Therefore, setting priorities and working on bolstering the resilience of critical infrastructure is vital. In this regard, on several occasions it was underlined that the key objective is protecting the continuity of functions and services, rather than the physical infrastructures themselves, and that there is a need to employ an all-hazards and whole-of-government approach to risk management. In the context of hybrid threats, in particular, it is also crucial to focus on adversaries' goals, rather than risks themselves, and to protect the integrity of political decision-making. Another point underscored at the event was the value of exercises, particularly real-life simulations, as they allow for the assessment of vulnerabilities and enhanced preparedness.

data access and ownership are crucial security issues

Another view shared at the conference was that multi-stakeholder cooperation between the EU institutions, member states and the private sector was essential for achieving these objectives and effectively protecting Europe's critical infrastructure. Accordingly, it was important to develop a new paradigm for public-private cooperation, with a mutual understanding of both shared and diverging interests, and a clear division of labour, roles and responsibilities between the various stakeholders. Furthermore, while acknowledging diverging national priorities on several occasions during the event, the importance of identifying and designating pan-European critical infrastructure as a strategic asset was stressed. By doing so, this could contribute to deterring adversaries, especially in conjunction with increasing the visibility of the EU's mutual support and solidarity mechanisms, making use of, for example, the 2016 EU Cyber Diplomacy Toolbox and engaging in robust strategic communications.

a new paradigm for public-private cooperation on critical infrastructure is needed

RETHINKING THE EU APPROACH TO RESILIENCE AND PROTECTION

The conference also addressed the specific challenges associated with critical infrastructure protection in different sectors. Furthermore, it discussed concrete ways in which critical infrastructure management, supply resilience and the continuity of essential services to the Union's population could be enhanced. It was noted that cyber threats, in particular, were a common theme across sectors, exacerbated by outdated industrial control systems. Here, the importance of digital infrastructure security was underlined, especially given that 5G is expected to become a key component. This presented considerable challenges, however. The virtual, borderless nature of cyberspace hampers the identification of attackers. It is also difficult to predict the vulnerabilities of fast-developing technologies or to regulate them, particularly if owned by foreign-based private entities. What is more, these challenges are often exacerbated by the divergence of standards and regulations among the Member States.

it is difficult to predict the vulnerabilities of fast-developing technologies or to regulate them

Each sector faces unique challenges. Concerning the financial sector, regulation requires financial institutions to have highly advanced risk management frameworks in order to achieve acceptable levels of risk from a business continuity point of view. However, there are only limited capabilities for situational awareness and preparedness to cope with systemic low probability-high impact threats, which is important from the perspective of comprehensive security. Regarding the health sector, the absence of EU-level critical infrastructure or relevant legislation and the insufficient cooperation between member

states were identified as key challenges. Moreover, participants stressed the negative implications for security of supply resulting from the EU's considerable dependence on China and India for active pharmaceutical ingredients. In the energy sector, it was noted that the advent of digitalisation (e.g. smart metering, Internet of Things) and a greater reliance on renewable energy had introduced vulnerabilities to Europe's hitherto resilient electricity grid, which had prompted operational and regulatory measures at the European level in response. However, regulation may in some cases hamper resilience by creating additional barriers to the construction of new, more resilient infrastructure.

the multiplicity of sectoral processes has resulted in a weakness of policy coordination at the EU level

Despite these challenges, one of the conference conclusions was that the EU and its member states are generally capable and well-resourced to address critical infrastructure protection, provided that there is a sufficient awareness of the threats and vulnerabilities. Several tools and initiatives have been developed, including the Directive on Security of Network and Information Systems (NIS Directive) in 2016, the €3.8 billion Internal Security Fund, the EU Civil Protection Mechanism (UCPM), the Hybrid Fusion Cell, plus the EU's framework for foreign direct investment (FDI) screening. Such tools and initiatives complement the Directive on European Critical Infrastructures (CIP Directive) and the European Programme for Critical Infrastructure Protection (EPCIP). Nevertheless, it was acknowledged that the multiplicity of sectoral processes has also resulted in a weakness of policy coordination at the EU level. While the CIP Directive had raised awareness and spurred cooperation, it was too narrowly focused on specific sectors (energy and transportation) and insufficient for today's hybrid threat challenges.

As regards EU-NATO cooperation, it was noted that both organisations have a strong shared interest in fostering resilience and critical infrastructure protection. A number of potential avenues for cooperation were uncovered, including: shared critical infrastructure vulnerabilities assessments; collecting, analysing and exchanging open source intelligence; mainstreaming resilience in EU-NATO cooperation beyond hybrid threats; and, taking practical measures to enhance EU-NATO exercises. However, the need to maintain the autonomy of the two organisations, given their different mandates, priorities and approaches to critical infrastructure protection was stressed on a number of occasions.

the EU and NATO have a strong shared interest in fostering resilience and critical infrastructure protection

In terms of the next steps, the positive work done so far at the EU level was acknowledged and there was a call for member states to make better use of existing tools. However, there was scope for further action at the EU level especially with regard to addressing the seeming contradiction between 'security' and 'open markets', and here it was emphasised that there is a clear need to secure critical infrastructure and supply chains without resorting to protectionism or stifling industrial growth.