Independent Review on European Security and Defence

Volume N°46

The European

Security and Defence Union

Cybersecurity and global politics

How to protect our vulnerable societies in unpredictable times

60 years after the Elysée Treaty – putting the French-German relations back on track

Interview with

François Delattre,
Ambassador of France to
Germany, Berlin

Dr Hans Dieter Lucas,
Ambassador of Germany to
France, Paris

www.magazine-the-european.com

Edition 1/2023

Protecting critical infrastructure

Lessons for Europe to learn from recent hybrid and cyber-attacks

by Prof Dr Angelika Niebler MEP, European Parliament, Brussels/Strasbourg

Do you remember the attacks in September 2022 on the Nord Stream gas pipelines that connect Germany and Russia? The four explosions that hit the pipelines were immediately suspected to have been carried out by Russia, as there were already major political tensions after the Russian invasion and ongoing war against Ukraine, as well as its consequences for the European Union (EU). Until today, there is no clear evidence on who attacked the gas infrastructure. The Nord Stream attack is not the only example of attacks on critical infrastructure in recent years. Another well-known incident happened in October 2022, when foreign hackers destroyed communication cables of the German railway Deutsche Bahn: public transport services were interrupted for several hours in northern Germany. Another particularly striking example is the ransomware attack on Irish hospitals in 2021 that paralysed hospitals for a whole week. Aggressors in cyberspace have increasingly been focussing on damaging critical infrastructure.

There are three lessons to be learned from cyber-attacks on critical infrastructure.

1. Cyber-attacks have become more dangerous.

For years, hybrid war has been an issue. However, the number of attacks on critical infrastructure is consistently increasing, thus exposing new vulnerabilities, as they can have a detrimental effect on society. In the digital age, our societal and economic ecosystems are closely connected to citizens: healthcare, transport networks, energy supply. Imagine if all the medical devices in a hospital could not be used anymore. No X-ray, no access to disease progression data, no medical analysis. During the ransomware attack in Ireland, doctors had to send their cancer patients home because they could not treat them. Without an adequate cybersecurity response, attackers can even disrupt supply chains that are of the utmost importance to the everyday life of citizens.

2. The EU plays an important role in coordinating national efforts towards protecting critical infrastructure.

In the European internal market, nearly all grids and networks are connected, be it in energy, telecommunications, transport or aviation. For that reason, there is a risk that the disruption of infrastructure in one Member State can affect the

photo: Martin Lahousse

Prof Dr Angelika Niebler

has been a Member of the European Parliament (EP) since 1999. She chairs the CSU Group in the EP and is co-chair of the CDU/CSU Group. Holding a doctorate in law, she is a member of the Committee on Industry, Research and Energy, (ITRE), a substitute member of the Legal Affairs Committee (JURI) and of the Special Committee on the COVID-19 pandemic: lessons learned and recommendations for the future (COVI). She is also a member of the EP's Delegation to the US. Angelika Niebler has been deputy party chair of the CSU since 2015 and was elected president of the Union Economic Advisory Council in 2018. Since 1991, she has worked for various law firms in Munich. Besides her work as a lawyer, she is a professor for Business Administration/Applied Business Innovation at the University of Applied Sciences in Munich.

→ *Continued on page 28*

> “The EU plays an important role in coordinating the Member States’ efforts towards more cybersecurity.”

whole European-wide network. Thus, we need high cybersecurity standards throughout the EU to protect our connected infrastructures. The EU plays an important role in coordinating the Member States’ efforts towards more cybersecurity. For instance, the **European Union Agency for Cybersecurity** (ENISA) engages in sharing the Member States’ knowledge, building capacity and raising awareness in the field of cybersecurity. Coordination is important so that Member States can learn from each other and be alerted swiftly in case of an emergency.

3. Adapting to emerging threats is key.

Adapting to the threats that are emerging with hybrid and cybersecurity attacks on critical infrastructure is key. The EU is in fact already doing so. In 2016, the **Directive on security of Network and Information Systems** (NIS1 Directive) entered into force, which obliged Member States to build up national capacities for cybersecurity. According to this directive, any attack on critical infrastructure has to be notified to the competent authority immediately. With the **Directive on measures for a high common level of cybersecurity across the Union** (NIS2 Directive), the EU modernised these cybersecurity measures for critical infrastructures. The new legislation entered into force in January 2023. What is new: new sectors and entities, such as cloud computing service providers, data centre service providers and operators of ground space infrastructure, are now also within the scope of the existing cybersecurity rules. Further, every Member State is required to set up a “Computer Security Incident Response Team” to respond in emergency cases. A new “Cooperation Group” will facilitate the exchange of information between the EU Member States. The NIS2 Directive also introduces more detailed reporting obligations for cyber-attacks. Attacked companies are obliged to send an early warning. This update of the EU cybersecurity measures was the right step towards protecting our critical infrastructure.

Further to the NIS2 Directive, the EU is also making efforts to better protect the infrastructure of its own public institutions. To this end, in March 2022, the EU Commission proposed a **Regulation laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union**, which is currently under consultation in Council and Parliament.

However, despite all efforts to counter cyber-attacks, it should always be clear that you cannot prevent them, you can only minimise the risk and arrange for immediate response.

documentation

The new EU Cybersecurity Directive (NIS2)

Illustration: ESDU/KanawatTH, stock.adobe.com

(Ed/nc, Paris) The 2016 Network and Information Security (NIS) Directive was the first piece of a EU-wide legislation aimed at increasing Member States' cybersecurity capabilities. To respond to the growing threats posed with digitalisation, the existing legal framework was updated by the **Directive on measures for a high common level of cybersecurity across the Union** (NIS2 Directive) that came into force on 16 January 2023. The scope of the cybersecurity rules was expanded to new sectors and entities that are obliged to take security measures. The aim is to further improve the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

The NIS2 Directive will:

Strengthen Member States' preparedness, by requiring them to be appropriately equipped, e.g., with a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority.

Foster the cooperation among all the Member States by setting up a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States.

Build a culture of security across sectors that are vital for the economy and society, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

web **https://bit.ly/3Ifrmxf**