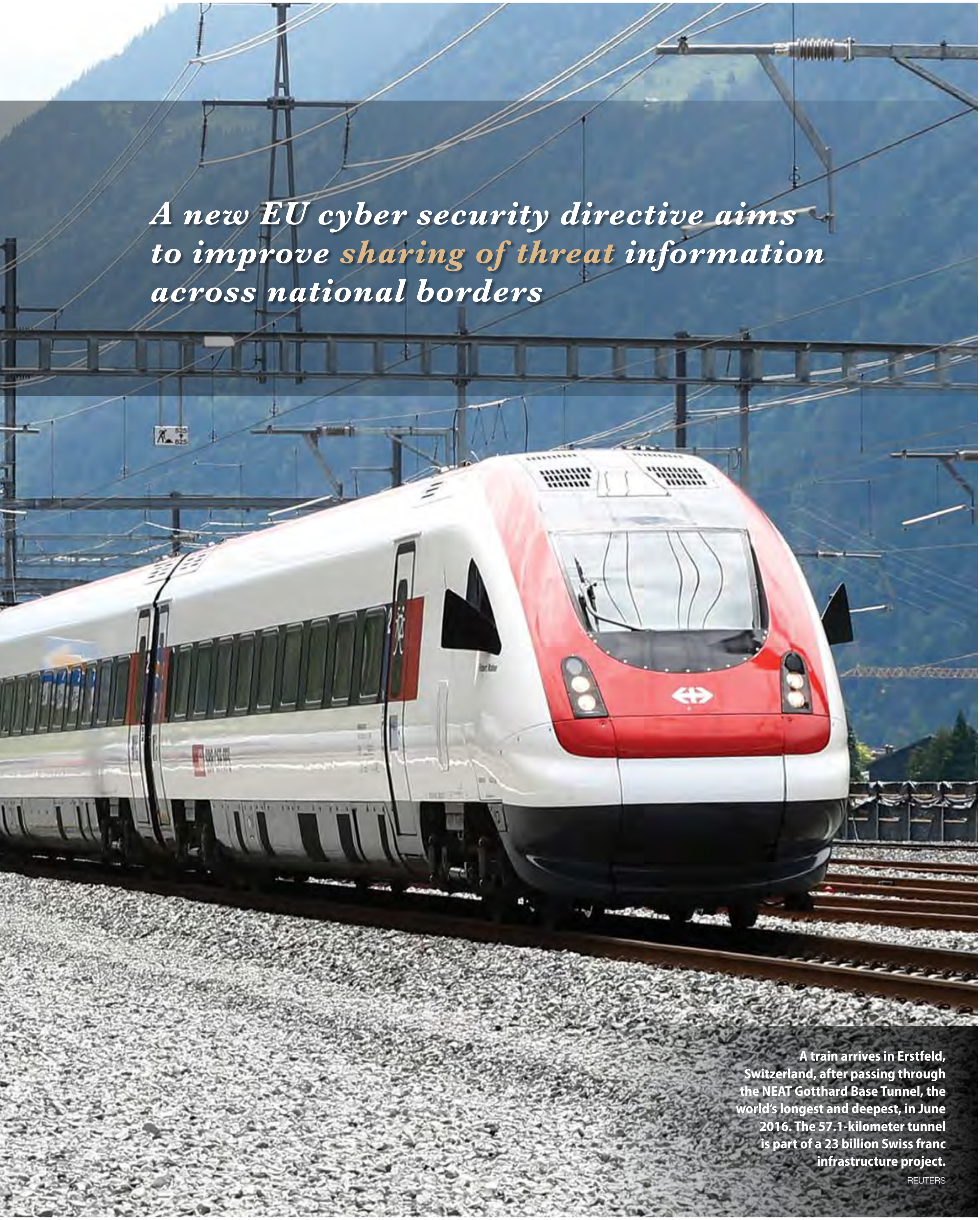
PROTECTING *EUROPE'S CRITICAL* INFRASTRUCTURE

By Benedikt Hopfner



A new EU cyber security directive aims to improve sharing of threat information across national borders

A train arrives in Erstfeld, Switzerland, after passing through the NEAT Gotthard Base Tunnel, the world's longest and deepest, in June 2016. The 57.1-kilometer tunnel is part of a 23 billion Swiss franc infrastructure project.

REUTERS

This article is based on a paper I wrote trying to identify the effects of a European Union legislative proposal. I am an engineer, not a lawyer with any affiliation to EU legislation, so this may have been a bold undertaking. But nourishing discussions sometimes require a little boldness.

In December 2015, the European Parliament and the European Council made the first proposal for an agreement on the first EU-wide legislation on cyber security and finally released it in July 2016. This Network and Information Security (NIS) Directive could lay the foundation for a future framework of cooperation and multilateral regulation within Europe regarding information and communications technology (ICT). The new legislation requires every country to establish a national NIS strategy. It also postulates the formation of a "Cooperation Group" to foster trust and the exchange of information among participating nations, as well as best practices and the creation of a network of national Computer Security Incident Response Teams (CSIRTs) to improve coordinated incident response.

Further, the NIS Directive mandates reporting for significant disruption of "essential services." A look at those essential services shows a remarkable overlap with sectors that are regarded as critical infrastructure, as shown in Table 1. Implementation of this new directive will affect existing regulations regarding critical infrastructure.

To protect potentially critical infrastructure, the EU has established a framework of directives and regulations. But according to a 2014 *Contemporary Security Policy* article by Krzysztof Sliwinski, due to the sensitivity to national security issues and questions of sovereignty, there has always been a reserved attitude toward more than minimalistic EU regulation. Nevertheless, it has been commonly accepted that the closer economic ties in Europe make it necessary to protect critical infrastructure on an EU level. Therefore, the EU needs a suitable overarching national critical infrastructure protection (CIP) system, as can be concluded from Javier Argomaniz' paper in 2015 for the journal *Intelligence and National Security*.

By changing the rules of information distribution, ICT has permeated virtually every facet of modern life. This new paradigm has also led to increasing cross-border interdependencies, and critical infrastructure is not excluded. To the contrary, there is an apparent "digitalization" of critical infrastructure through the use of modern information and control systems and tightening interrelations among different entities, resulting in growing complexity and the possibility of cascading disruptions. Without a supporting policy framework that helps unify various perspectives on ICT and critical infrastructure, it will be difficult to develop resilience against future threats in the cyber-physical domain. The regulation of critical infrastructure, the field of cyber security and the related field of critical information infrastructure have been regulated separately until now.

The growing interrelation of critical infrastructure in the digital environment and the interdependence of European countries' infrastructures have created a need to harmonize these two sectors to enhance security and ensure European competitiveness. The new NIS Directive could be an important starting point for a harmonized CIP program and support the governance of critical infrastructure in an EU environment.

Overlap of EU critical infrastructure sectors and essential services

Table 1

Critical Infrastructure	Essential services
Energy	Energy
Information and communication technologies	Digital infrastructure
Water	Drinking water supply and distribution
Food	
Health	Health sector
Financial	Banking/financial market infrastructures
Public & legal order and safety	
Civil administration	
Transport	Transport
Chemical and nuclear industry	
Space and research	

Sources: Commission of the European Communities and Council of the European Union

Initiatives in the new directive are helpful to a certain point, but are not sufficient to establish an effective framework to ensure critical infrastructure resilience. The NIS Directive does not emphasize a holistic enough view, including the private sector. We must examine the directive's potential benefits and shortcomings in light of these challenges.

Defining CIP and critical infrastructure framework

The abstract idea and understanding of critical infrastructure and how it is defined are very similar in most countries; it can be reduced to infrastructure that ensures the continuity of society. However, national points of views diverge when it comes to defining which infrastructure is critical. In 2005, the EU published a list of 11 indicative sectors of critical infrastructure. As seen in Table 2, there is only partial agreement within the EU as to what constitutes critical infrastructure. The list contains only 17 EU member states and Switzerland, because the relevant information was made available in the English language to the European Union Agency for Network and Information Security (ENISA) only for these states.

Out of 11 sectors, only energy and transportation are uniformly regarded as "European Critical Infrastructure" by the Council Directive 2008/114/EC that defines the European Program on Critical Infrastructure Protection (EPCIP). These

The energy sector is among Europe's most critical infrastructure.

REUTERS

are the only transnational infrastructure sectors that are considered to fulfill the criteria for "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States," as defined by the Council of the European Union. Further, ICT is not even regarded as critical infrastructure in Luxembourg and Italy, although it is explicitly mentioned in the directive as a potential European critical infrastructure sector.

This means that only the energy and transportation sectors are regulated through the EU. To facilitate further exchange on potential threats and establish an optional cross-sectional information sharing and coordination network, the Critical Infrastructure Warning Network was established. But according to Raphael Bossong, in his 2014 article in the journal *European Security*, thanks to the lack of mandatory information provisions, this network has lagged behind expectations in supporting situational awareness. In their 2015 article for the *European Journal of Risk Regulation*, Marjolein van Asselt, Ellen Vos and Isabelle Wildhaber point out that potential participants are concerned with the confidentiality of provided information, and this is a major problem facing this network.

The European Reference Network for CIP was founded to provide scientific support for EPCIP and to improve the standardization and harmonization of technology. But this network lacks influence and exchange with private industry, which Bossong says is crucial to the effective establishment of operational security governance. ICT is not included in the existing critical infrastructure frameworks, so parallel structures have been established within the EU to support the advance of critical information infrastructure.

ENISA, which according to its website "was set up to enhance the capability of the European Union, the EU Member States and the business community to prevent, address and respond to network and information security problems," and is an independent European community agency. Neil Robinson states in the book *Cybersecurity: Public Sector Threats and Responses* that ENISA provides expertise and advice to the European Commission and EU member states regarding information technology (IT) security and risk management and supports public-private partnerships. ENISA is essentially seen "as a hub for exchange of information, best practices and knowledge in the field of information security," according to Sliwinski, and does not have any real directive power apart from advising the European Council. Bossong contends that there is still no leading agency that has the capability to coordinate and influence policy in support of CIP. Nevertheless, in its independent role ENISA recognizes the problem of the growing convergence between industrial control systems, IT and their functional elements. Therefore, it has put forward several recommendations and guidelines for mitigating the problem on technical and practical levels, but there is no legal obligation for member states to follow those recommendations.

The European Union Public Private Partnership for Resilience was focused on the telecommunications sector but was closed down in April 2014. Robinson explains that the goal of this public-private partnership was to provide a platform for information sharing and exchange of best practices between public officials and industry and to establish mutual comprehension of priorities and objectives. Its effectiveness was considered only partially satisfactory, and therefore it shall be succeeded by a new Public Private Partnership on Cybersecurity. The European Union Computer Emergency Response Team (CERT-EU) was established in 2012. CERT-EU says it "cooperates closely with other CERTs in the Member States and beyond as well as with specialized IT security companies." (The terms CERT and Computer Security

The requirement that each state establish a national NIS strategy is fundamental to future collaboration between states, as it demands "measures relating to preparedness, response and recovery."

and Incident Response Team [CSIRT] are used synonymously in the literature; the NIS Directive uses the term CSIRT).

Previously, success in establishing a coordinated approach to protect critical infrastructure from emerging threats has been limited.

The NIS Directive — changes to CIP

Because the European Commission narrowly defines critical infrastructure to include only the energy and transportation sectors and defines "essential services" broadly, the NIS Directive can have a more extensive impact on EU-wide CIP than the EPCIP, if only from a cyber security aspect.

Critical Infrastructure sectors as identified by EU countries Table 2

Sectors	Energy	ICT	Water	Food	Health	Financial	Public & Legal Order	Civil Admin.	Transport	Chemical & Nuclear Industry	Space & Research	Other
AT	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	
BE	✓	✓				✓			✓			
CZ	✓	✓	✓	✓		✓		✓	✓			Emergency services
DK	✓	✓		✓	✓				✓			
EE	✓	✓	✓	✓	✓	✓	✓	✓	✓			Rescue services
FI	✓	✓	✓	✓	✓	✓	✓		✓			
FR	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	Industry
DE	✓	✓	✓	✓	✓	✓	✓		✓			Media & Culture
EL	✓								✓			
HU	✓	✓	✓	✓	✓	✓	✓		✓			Industry
IT	✓								✓			
MT	✓	✓			✓	✓			✓			
NL	✓	✓	✓	✓		✓	✓		✓	✓		
PL	✓	✓	✓	✓	✓	✓			✓	✓		Rescue system
SK	✓	✓	✓		✓				✓			Industry/Postal
ES	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	
UK	✓	✓	✓	✓	✓	✓		✓	✓			Emergency services

Source: ENISA 2014

The identification of operators of essential services (OES) is defined by each member state, although the Council of the European Union recommends that the "definition of operator of essential services should be coherently applied by all Member States." Friction over the definition can be expected, as was already seen regarding the definition of European critical infrastructure. But, as all OESs have to report security incidents to their national CSIRTs, the individual states and the companies within these states will have sufficient interest to form a common baseline defining essential services and relevant incidents for all. Mandatory incident reporting for all OES, will encourage private firms to improve their cyber security capabilities and comply with basic technical security standards, although it should be guaranteed that the notification shall not necessarily expose the notifying party. The legal obligation to publicly admit security flaws, even if anonymously, will raise risk awareness.

The requirement that each state establish a national NIS strategy is fundamental to future collaboration between states, as it demands "measures relating to preparedness, response and recovery." The U.S. National Institute of Standards and Technology's 2014 Framework for Improving Critical Infrastructure Cybersecurity provides a similar, more detailed approach toward CIP: "The Framework Core consists of five concurrent and continuous Functions - Identify, Protect, Detect, Respond, Recover." These functions correspond to the CIP life cycle, as described by Bernard Hämmerli and Andrea Renda in their 2010 report for the Centre for European Policy Studies. The effective and coherent establishment of such frameworks across Europe should raise awareness and improve overall performance in countering cyber threats to critical infrastructure.

However, the effectiveness of NIS strategy implementation may vary from state to state without formal corrective support from the EU. A formal strategy that is too static would be counterproductive regarding a highly dynamic digital environment. And while essential services must be identified and reported within a certain timeframe, there is no explicit time limit for the implementation of the NIS strategy.

These factors can obstruct effective implementation, because without the beneficial exchange of practices and information for all parties there will be little incentive to participate above the minimum required. This is especially true when taking into account the different starting points regarding capabilities and the significance of this problem in different nations. Collaboration between states, as well as with private industry, is essential, but can be effective only if all participants benefit.

Although the importance of cooperation with the private sector is explicitly stated in the NIS Directive, it does not address how this should take place or which institutions should be responsible at the EU level. This could be a lost opportunity, because ENISA recommended in its closing report on the European Public Private Partnership for Resilience initiative that simple but formal rules of governance be defined at the earliest stage of future public-private partnerships. There is seemingly no platform to exchange information among member states and with the private sector apart from reports to the national CSIRTs. It is dangerous that no formal cooperation organ or forum for information exchange for private entities, such as the Information Sharing and Analysis Centers (ISACs) established in the United States, is actively promoted on a European level, considering how much critical infrastructure is privately owned.

The NIS Directive states that a supportive framework for fostering risk management could be initiated by providing a clear mandate for national CSIRTs to cover essential services and establishing a CSIRT network for "the development of confidence and trust between the Member States and to promote swift and effective operational cooperation." Cooperation within such frameworks can also foster progress toward common understanding and standards. This is necessary for effective operations regarding CIP, as Hämmerli and Renda determined. Sharing of incident reports can certainly help improve overall situational awareness of advanced threats within the EU, though herein lies a potential problem, as these incidents are shared only voluntarily. If no real, trustful cooperation is established between sharing CSIRTs, the threat picture won't be valuable. However, it is not clear how big this group will be, because each state defines which national CSIRTs will participate in the network and, therefore, how trustful the environment will be. The question of how to integrate the private sector into the process also remains. There is no mention of the process by which the OES will profit from this information sharing and, therefore, improve resilience.

The directive also lacks differentiated coordination among the various critical infrastructure sectors. The specified tasks assigned to the cooperation group seem to imply a "one size fits all" strategy, implying that this group will be the focal point of information and best practices. This design cannot keep up with demand, because the variety of essential services is enormous. Banking and financial services have much different agendas and needs than water utilities; there is no general option for effective risk management. A risk information overload could result from a lack of information exchange capabilities on a more horizontal level, between sectors.

It is useful to have a high-level institution to achieve a unified, overarching vision of potential risk, but there is no formal provision to ensure the demanded effectiveness in the implementation of this vision, nor does it prioritize risks. It is questionable that the needs for information exchange, experience and risk-management approaches among different stakeholders can be assured within this cooperation group. Further, the situational picture will miss important pieces without the direct insight of the mainly private OESs. Of course, it is not productive to integrate single companies into such a group — such an unwieldy expanded group membership would destroy trust. However, there is a clear need for direct input from a panel representing the different sectors of critical infrastructure in the private sector.

Conclusion

The EU has a clear need to consolidate its approach to protect different critical infrastructure sectors, but it's been lacking so far. Evolving technology and rapid information transmission beyond national borders has caused the fusion of critical infrastructure and ICT, even though the original requirements of these two sectors were different.

The approach of the NIS Directive to merge major aspects of critical infrastructure and ensure visibility by requiring national regulations across the entire EU will certainly help raise awareness of the issue and is a major capstone for consolidation. The establishment of national NIS strategies as well as mandatory reporting of disruptive incidents can help countries focus on improvements, but this won't be enough to achieve effective long-term protection.

To meet the challenge of managing the emerging complexity, the EU needs a culture of threat awareness and flexible adaptation. And with the transnational interconnection of critical infrastructure, information must be shared across borders to manage risk effectively. The CSIRT cooperation network will support information sharing, but will not ensure a complete information picture or effectively support an overall risk management strategy for critical infrastructure sectors on an EU level. The cooperation group has similar handicaps. To ensure successful information sharing and risk management, the private sector needs to be included in the process.

Here, the new NIS Directive has shortcomings. It creates no formal interfaces with the cooperation group or the CSIRTs. The creation of a representative construct for individual critical infrastructure sectors and its integration into the NIS Directive would help ensure that insights on potential risks and industry influence on future policies are formally channeled into a cooperative framework. This could be addressed as part of the still-to-be-defined Public-Private Partnership on Cybersecurity, but nothing regarding cooperation between the private and public sectors, on the EU level, is mentioned in the NIS Directive apart from its importance and necessity.

The innovations of the new NIS Directive represent a positive step toward establishing a common understanding and laying the groundwork for future collaboration, but they are insufficient to meet the challenges ahead. The lack of close and integrated collaboration between individual states within the EU or with the private sector reduces the ability of stakeholders to synergize efforts to protect European critical infrastructure. □