Flossbach von Storch
RESEARCH INSTITUTE

MACROECONOMICS 10/08/2023

“De-risking” critical infrastructures

AGNIESZKA GEHRINGER

Abstract

With intensifying authoritarian tendencies particularly in China, geopolitical risks have increased. A comprehensive and coherent framework is needed to address these risks. Especially in the European Union, a more active and systematic dialog is required to enhance the common understanding of critical infrastructures and their sectoral and transboundary interdependences. Failing to do so would turn the new mantra of “de-risking” relations with China into an empty phase.

Zusammenfassung

Mit der Verschärfung autoritärer Tendenzen, insbesondere in China, haben die geopolitischen Risiken zugenommen. Um diesen Risiken zu begegnen, ist ein umfassender und kohärenter Ansatz erforderlich. Insbesondere in der Europäischen Union ist ein aktiveres und systematischeres Vorgehen geboten, um das gemeinsame Verständnis für kritische Infrastrukturen und ihre sektoralen und grenzüberschreitenden Abhängigkeiten zu verbessern. Andernfalls würde das neue Mantra von der "De-Risking" der Beziehungen zu China zu einer leeren Phase werden.

1. Introduction

Due to a series of recent macroeconomic risk events, concerns about the critical infrastructure have increased among governments and experts worldwide. However, the perception of what is precisely deemed as critical infrastructure and what risks are involved especially when giving up control over it to foreign operators differs much across countries. This could be problematic since critical infrastructures are characterized by strong transboundary interdependences and require thus cross-border cooperation. Moreover, governmental strategies related to critical infrastructures may have important geopolitical consequences. This note summarizes the existing definitions and approaches to identify and protect critical infrastructure, by focusing on the major economies across the developed world.

2. What is a critical infrastructure?

Critical infrastructures play a pivotal role for economic and social well-being.

Despite a high degree of complexity surrounding the issue, there is a broad consensus in the scientific community, among experts and policymakers on the general definition of critical infrastructures. A **critical infrastructure** (CI) comprises a single or multiple assets or systems – physical, organizational or virtual – which are so vital for the society that any failure or degradation of their service would result in sustained supply shortages and/or a serious and undesirable impact on vital societal functions, including health, safety, security, economic or social well-being of people (OECD 2019, Alcaraz & Zeadally 2015). Accordingly, the focus is on the pivotal role that the functioning of CI plays for economic and social well-being.[1]

Typically, CI is identified in the national context, leading to the notion of the **national critical infrastructure** (NCI). In the context of the EU, **European critical infrastructures** (ECI) additionally accompany the framework. They "constitute those designated critical infrastructures which are of the highest importance for the Community and which if disrupted or destroyed would affect two or more MS [Member States], or a single Member State if the CI is located in another Member State" (EC 2006, p. 4).[2]

[1] There exist some other – often government-baked – definitions, which stress the importance of CI for the functioning of the state or national security (OECD 2019). Examples in question include former communist countries in Eastern Europe, namely, Czech Republic, Latvia, Slovak Republic, and Poland.

[2] Directive (EU) 2022/2557 slightly modifies this framework. Specifically, based on the list of 11 sectors, each Member State should identify critical entities therein. The Directive defines the term "critical infrastructure", as being "an asset, a facility, equipment, a network or a system, or a part of an asset, a facility, equipment, a network or a system, which is necessary for the provision of an essential service" but does not clarify the conceptual or practical link to the critical entity. However, from the reading of the Directive, critical entities are operators of one or more critical infrastructure (Art. 13(1b), Art. 21(1a)). Moreover, the Directive does not explicitly refer to ECIs, but requires cooperation between Member States in case their critical entities "use critical infrastructure which is physically connected between two or more

Critical infrastructures are characterized by manifold interdependences.

A distinguishing feature of critical infrastructures is the existence of **interdependences** between single infrastructures. They are evident in cross-sectoral dependences in the acquisition and implementation of products and services which are provided by one CI and are vital for a proper functioning of another CI (Laugé *et al*. 2015). Additionally, interdependences may be transboundary in nature if the functioning of a critical infrastructure in one country depends on another critical infrastructure located abroad.

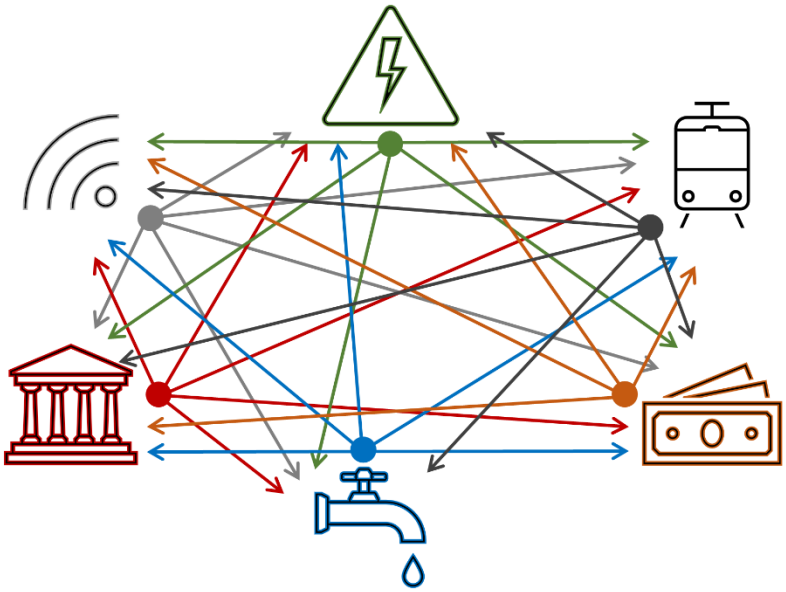
Beyond the sectoral feature, there exist four layers of interdependences between critical infrastructures (Rinaldi *et al*. 2001):

→ *physical*: the operation of one infrastructure depends on the material output(s) of the other;
→ *cyber*: dependency on information transmitted through the information infrastructure;
→ *geographic*: dependency on local environmental effects simultaneously affecting several infrastructures located in a certain area;
→ *logical*: any kind of dependency mechanism not characterised as physical, cyber or geographic layer, e.g. human decision-making and actions.

Since critical infrastructures are typically complex systems, multiple combinations of the four dimensions and thus multi-layer interdependences can occur between any bilateral set of CI at the same time. **Figure 1** breaks down the underlying complexity in a simplified framework for the core set of six critical infrastructures – energy, water, transport, information and communication, finance, and government. Each sectoral node is bi-directionally dependent on every other sectoral node. These interdependences are channeled through all the aforementioned layers. For instance, information and communication is a critical supplier of both material outputs (networks, hardware) and information (telephone and wireless services) to all the other critical infrastructures. Moreover, this interconnectedness often goes cross-border – if, for instance, energy providers from different countries exchange relevant information. Finally, since human interactions are an indispensable part of this communication, logical layer is obviously involved.

Member States" (Art. 11(1a)). Finally, the Directive identifies critical entities of particular European significance, as an entity that "provides the same or similar essential services to or in six or more Member States" (Art. 17(1b)).

Figure 1. Multi-dimensional interdependences between critical infrastructures



Source: Own elaboration Flossbach von Storch Research Institute, based on Rinaldi *et al*. (2001)

Accordingly, addressing interdependences requires viewing critical infrastructures in a systemic, multi-sector and multi-layer approach, in which all kinds of direct and indirect, physical, cyber, geographic and logical dependencies are accounted for. Finally, interdependences exist not only within national borders, but may have a strong international dimension. Accordingly, threats cannot be assessed in a purely national context. The interconnected nature of today's economy – e.g. ICT systems and financial infrastructures – and society means that external disruptions may have a serious impact on the domestic critical infrastructures – and vice versa.

Whereas the recognition and conceptualization of interdependences, interconnectedness and transboundary dimension are well-advanced and a common knowledge among experts, they have been much less reflected in practical applications across countries and regions so far (OECD 2019).

3. How are critical infrastructures classified?

Table 1 summarizes the existing sectoral classifications of the major developed economies. The US classification is taken as a reference for sectoral denominations, given that the US possesses the most developed and most comprehensive framework of critical infrastructures and their protection.

The US classification is not always perfectly compatible with other classifications and sectoral denominations sometimes differ. For instance, the US

classification treats separately communications and information technology, whereas in Germany, Canada, and Japan these two sectors are considered jointly as information and communication technologies.

Energy, transport, communications, information technology, food, health, water, finance, and government belong to a core set of critical instrastructures.

Despite these differences, there is at least a consensus regarding the core set of sectors/activities dubbed as CI. In all classifications, energy, transport, communications, information technology, food, health, water, finance, and government almost univocally emerge among critical infrastructures. Other sectors are more country-specific. This regards such seemingly important sectors as defense, chemical, commercial facilities, critical manufacturing, dams, emergency services, and nuclear sector.

In some countries, with the classification of critical infrastructure sectors, a specific agency or ministry is assigned the main responsibility. For instance, in the US, each sector falls under the responsibility of a designated Sector-Specific Agency (SSA), which is a federal department or another governmental entity. The most important institution in this sense is the Department of Homeland Security, responsible for 10 out of 16 critical infrastructures. In the EU, the recent Directive (EU) 2022/2557 requires from the Member States that they designate competent authorities for the correct application and enforcement of the rules set out in the Directive and single point of contact to ensure cross-border cooperation.

Also Australia has developed a transparent and detailed framework to deal with critical infrastructures. The country identifies not only the list of 11 critical infrastructure sectors but also an extensive list of 22 critical infrastructure assets as part of these CI sectors. This practice is not common in other analysed countries.

Until recently, the EU has not had any precise classification of critical infrastructure.[3] The only reference to concrete sectors was made in the Council Directive 2008/114/EC, by focusing on energy and transportation, with information and communication technology sector to be analysed and reviewed in the subsequent steps. With the Directive (EU) 2022/2557 of the European Parliament and of the Council, a classification with 11 sectors – as listed in **Table 1** – has been eventually elaborated. The Directive (EU) 2022/2557 is going to repeal the Council Directive 2008/114/EC from 18 October 2024.

[3] As a matter of facts, the European Commission has published in 2005 a green paper on a European Programme for Critical Infrastructure Protection with an indicative and detailed list of 11 critical infrastructure sectors (EC 2005). However, this classification was disregarded in the subsequent official documents on the subject.

Table 1. Overview of the existing classifications of critical infrastructures in the major economies worldwide

Critical infrastructure	USA	EU	Germany	France	Canada	UK	Australia	Japan
Chemical	+					+		+
Commercial facilities	+							+[5]
Communications	+	+[1]	+[2]	+	+[2]	+	+	+[2]
Critical manufacturing	+			+[4]	+			
Dams	+							
Emergency services	+				+	+		
Government facilities	+	+	+	+	+	+		+
Information technology	+	+[1]	+[2]	+	+[2]		+[3]	+[2]
Nuclear reactors, materials, and waste	+					+		
Transportation systems	+	+	+	+	+	+	+	+
Defense industry	+			+		+	+	
Energy	+	+	+	+	+	+	+	+[6]
Financial services	+	(+)	+	+	+	+	+	+
Food & agriculture	+	(+)	+	+	+	+	+	
Healthcare and public health	+	(+)	+	+	+	+	+	+
Water and wastewater systems	+	(+)	+	+	+	+	+	+
Disaster control & management			+					
National monuments & icons			+					
Media			+					
Space		(+)		+		+	+	
Higher education and research				+			+	

Source: USA – National Infrastructure Protection Plan 2013; EU – Council Directive 2008/114/EC, entries in brackets refer to sectors added with the Directive (EU) 2022/2557 that will repeal the Council Directive 2008/114/EC from 18 October 2024; Germany – FMI (2009); France - Arrêté du 3 juillet 2008 portant modification de l'arrêté du 2 juin 2006 fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desditssecteurs; Canada – National Strategy for Critical Infrastructure of 2010; UK – Public Summary of Sector Security and Resilience Plans of 2018; Australia – Security of Critical Infrastructure Act 2018; Japan – Fourth Action Plan for Information Security of Critical Infrastructure (重要インフラの情報セキュリティ対策に係る第４次行動計画（改定)).

[1] The sector is dubbed "digital infrastructure". [2] The reference is made jointly to information and communication technologies. [3] The sector is dubbed "data storage and processing". [4] The sector is dubbed "industry". [5] The sector is denominated "logistics services". [6] The classification distinguishes between three energy-related sectors, namely, "electric power supply services", "gas supply services", and "petroleum industries".

Due to transboundary interdependences between critical infrastructures and, accordingly, the need of cross-border cooperation, efforts to better align and harmonise approaches across countries is indispensable.

An important challenge within the EU for a functional coordination and effective protection of critical infrastructures is that countries differ much in defining, identifying, and managing critical infrastructures. An extreme example constitutes Italy where no CI strategy or programme exists nor is there any lead institution in charge of critical infrastructures (OECD 2019). Similarly, Portugal limits its CI policy coverage to two sectors – energy and transport – as identified in the Council Directive 2008/114/EC.

These differences in classifications and deficiencies in the underlying strategies often reflect national preferences and specific perceptions of priorities or the lack thereof. However, due to transboundary interdependences between critical infrastructures and, accordingly, the need of cross-border cooperation, efforts to better align and harmonise approaches across countries is an indispensable risk management strategy.

4. The blind spots in the recent CI policies

Two main problems in the past experience of CI protection can be identified. First, the negligence of transboundary interdependences between critical infrastructures results in a **weak cooperation** in setting a robust CI risk management framework. Second, industrial policy strategies of the major developed countries have been so far often inattentive in considering **geopolitical implications** of trade and cross-border investment strategies involving domestic critical infrastructures.

Regarding the cooperation issue, the strategies to date have been fragmented, limited to localized inter-governmental initiatives. The most institutionalized one is known as the Critical Five, established in 2012 by five developed economies, Australia, Canada, New Zealand, the UK and the US. The aim of the initiative was to enhance information sharing and work on issues of mutual interest. The efforts put so far have been of a conceptual nature, directed towards finding a common understanding of critical infrastructure (Critical Five 2014) and of the links between infrastructure investment, economic growth and prosperity in the framework of the Critical Five initiative (Critical Five 2015).

Within the EU, efforts have been made to strengthen both internal and external cooperation. A promising step to advance the internal cooperation is given by the Directive (EU) 2022/2557 that will shape the relevant framework from 18 October 2024. However, based on the past experiences with the adoption of the predecessor Directive 2008/114/EC, difficulties with establishing an effective cooperation practice cannot be excluded. This assumption is in so far realistic that the ultimate responsibility for national security is in the hands of single member states rather than at the EU level and the

incentives to cooperate have been often limited. Regarding the external cooperation, it has involved neighbouring countries of the EU and countries of the European Economic Area (Norway, Iceland, and Lichtenstein) as well as other countries in Europe and beyond. However, most of the initiatives involved mere informal cooperation, workshops and expert meetings with a vaguely specified exchange of best practices, as well as efforts – of Germany with Russia – that obviously failed due to misjudgement of risks related to pursuit of imperialist ambitions. An exception here regards the cooperation within NATO, which has recently led to a detailed scrutiny of current security challenges in critical infrastructures of energy, transport, digital infrastructure, and space (EU/NATO 2023). This notwithstanding, a much more far-reaching and outcome-oriented toolkit for cooperation is still lacking (Lazari & Mikac 2022).

Regarding the missing sensibility to geopolitical issues in the CI protection, it can be traced back to the past industrial policy strategies conducted in the global framework of liberalization of cross-border flows of goods, services and production inputs, including technological knowhow and information. The prevailing paradigm of free markets and open economies was unconditionally applied to a vast range of sectors, irrespective of their CI status. This often resulted in the foreign acquisition of assets also in CI sectors, with sometimes substantial shifts of ownership abroad. This process extensively happened in the EU, but also in other developed economies, the US included.

Among the major acquirers, Chinese investors were intensively involved in taking over CI entities. On the sectoral level, China strongly invested in port infrastructure worldwide, with important European port terminals now partially or fully owned by Chinese operators (Jüris 2023, Geinitz 2022). Also Chinese investment in US communication and information technologies proceeded inexorably during the 1990s and 2000s (Hillman, 2021). Finally, China is carving out a niche as the preferred provider of information and communications infrastructure to developing countries. Beijing currently intensifies efforts to sell communication satellites across the global South. The Chinese digital giant, Huawei, is currently active in more than 170 countries. Two other Chinese technology companies, Hikvision and Dahua, supply around 40% of surveillance cameras worldwide. Finally, Hengtong Group is among the four main global suppliers of submarine cables, which channels over 95% of international data transfer (Hillman 2021).

This process of intensifying FDIs and trade relations was for a long time perceived as an integral part of the democratization of non-democratic countries, ideologically motivated by change through trade as well as the liberating effect of communication technologies and open cyberspace (Gehringer 2023, Hillman 2021). However, with intensifying authoritarian tendencies

particularly evident in China's government style of Xi Jinping, geopolitical risks become non-negligible for countries giving up their control over critical infrastructures to Chinese entities. This is driven by the evidence that China's centralized and party-led political system blurs the distinction between commercial, political and military interests (Jüris 2023, Cristiani *et al*. 2021). The authoritarian lead of the China's Communist Party (CCP) explicitly regards the alignment of interest of the state and of private companies as a central strategy in the achievement of national strategic goals. The latter obviously involve domestic industrial policy targets, but, additionally, often expand beyond China's national borders (Gehringer 2023).[4] Accordingly, internationally oriented Chinese companies are instrumental in expanding the CCP influence abroad and – more precisely – in modernizing the People Liberation Army through technology transfer (Jüris 2023, Hillman 2021). This strategy is in so far enforceable that numerous companies in China are state-owned or – if allegedly private – under a strong influence of the CCP, via the CCP-affiliated management members. Moreover, internationally active companies are often financially incentivized and operationally supported to contribute to the achievement of China's strategic goals.

With the growing recognition of risks associated with unconditional liberalization of cross-border economic relations – baked by more frequent spying and cyberattacks incidents – governments, especially in developed countries, started revisiting their industrial policies and pursuing a de-risking approach, particularly if involving critical infrastructures and entities.

Among the first movers in this regard was Washington, with intelligence officials warning in a congressional report from 2012 that Chinese tech infrastructure could jeopardize the US networks.[5] In 2019, the Federal Communication Commission banned carries from device purchases from Huawei and ZTE.[6] The US warnings regarding the aforementioned risks are in the meantime well-perceived by other governments of Australia, Japan and several countries in Western Europe.

Despite a substantial delay, the EU has recently revisited its strategy towards China. In the "Strategic Outlook" Joint Communication from March 2019, the

---

[4] Such goals were formulated in different strategic CCP documents and national programmes, such as Belt and Road Initiative (BRI), Made in China 2025, China Standards 2035, or China's Military-Civil Fusion Strategy.

[5] "Investigative report on the U.S. national security issues posed by Chinese telecommunications companies Huawei and ZTE." U.S. House of Representatives. Available at: https://stacks.stanford.edu/file/druid:rm226yb7473/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

[6] "Protecting against national security threats to the communications supply chain through FCC programs." Federal Communications Commission. Available at: https://docs.fcc.gov/public/attachments/FCC-19-121A1.pdf.

EU declared to continue dealing with China simultaneously as a partner for cooperation and negotiation, an economic competitor in pursuing technological leadership and a systemic rival in promoting alternative governance models (EC 2019). Moreover, in the context of cross-border relations, the EU put a brake on undesirable transactions and investment practices. In spring 2019, the Community adopted a regulation establishing a new pan-EU investment screening framework for FDI review. Although the regulation is criticized for being a loose coordination and cooperation tool, with EU Member States being able to exchange relevant information on single foreign investments that may impact on their national security and public order, it marks a decisive step to increase awareness and catalyze the convergence of dispersed national FDI strategies (Hanemann *et al*. 2019). Moreover, similar measures are needed to screen other forms of direct and indirect involvement of foreign operators in critical infrastructures.

4. Conclusion

Foreign ownership of domestic critical infrastructures may bring about undesirable consequences to national security and public order. Especially China's footprint in critical infrastructures across the developed world poses a serious risk to strategic sovereignty of involved countries. The determination of the CCP to achieve strategic national goals often implies the direct engagement and contribution of Chinese CCP-loyal entities – at home and abroad.

Security loopholes in the CI-protection lead to further expansion of undesirable influences from China and more generally non-democratic systems.

The process of China's engagement in critical infrastructures abroad had begun in a regulatory and political vacuum, before governments of the leading developed countries started to raise concerns over national security issues. Although some counteractive answers have been given and strategies to protect critical infrastructure have been developed, the resulting framework is still underdeveloped and fragmented. As a consequence, security loopholes lead to further expansion of undesirable influences from China and more generally non-democratic systems.

A comprehensive and coherent framework is needed to address these risks. Regarding specifically the EU, a more active and systematic dialog is required to enhance the common understanding of critical infrastructures and their sectoral and transboundary interdependences. This should advance a framework for a regular exchange of relevant insights regarding particularly the ownership structure and other forms of risky foreign involvement in the operation of critical infrastructures. A unified EU approach on critical infrastructure might be challenging to arrive at but is a sure shield against adverse strategic rivalry.

References:

Critical Five (2015). Role of critical infrastructure in national prosperity. Available at: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-ci-national-prosperity-2015-508.pdf.

Critical Five (2014). Forging a common understanding for critical infrastructure. Available at: https://www.cisa.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf.

EC (European Commission) (2019). Joint Communication to the European Parliament, the European Council and the Council: EU-China – A strategic outlook. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0005.

EC (European Commission) (2006). Communicaton from the Commission on a European Programme for Critical Infrastructure Protection, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

EC (European Commission) (2005). Green paper on a European Programme for Critical Infrastructure Protection, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576

EU/NATO (2023). EU-NATO task force on the resilience of critical infrastructure. Final Assessment Report. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/6/pdf/EU-NATO_Final_Assessment_Report_Digital.pdf.

European Council (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union, L 345/75, available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF.

FMI (Federal Ministry of the Interrior of Germany) (2009). National strategy for critical infrastructure protection (CIP strategy), available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=2.

Geinitz, C. (2022). Chinas Greif nach dem Westen. Wie sich Peking in unsere Wirtschaft einkauft. C.H. Beck: München.

Gehringer, A. (2023). Calibrating the EU's trade dependence. *Survival* 65(1), 81-96.

Hanemann, T., Huotari, M., Kratz, A. (2019). Chinese FDI in Europe: 2018 trends and impact of new screening policies. Rhodium Group and the Mercator Institute for China Studies (MERICS).

Hillman, J.E. (2021). Chinas digitale Seidenstrasse. Der globale Kamp um die Herrschaft über die Daten. Plassen Verlag: Kulmbach.

Jüris, F. (2023). Security implications of China-owned critical infrastructure in the European Union. European Parliament, Directorate-General for External Policies. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf.

Laugé, A. Hernantes, J. Sarriegi, J. (2013). Disasterimpact assessment: aholisticframework. In: Proceedings of the Tenth International Conference on Information Systems for Crisis Response and Management, pp. 730–734.

Lazari, A., Mikac, R. (2022). The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation. CRC Press.

OECD (2019). Good Governance for Critical Infrastructure Resilience. OECD Publishing, Paris.

Cristiani, D., Ohlberg, M., Parello-Plesner, J., Small, A. (2021). The security implications of Chinese infrastructure investment in Europe. The German Marshall Fund of the United States. Available at: https://www.gmfus.org/sites/default/files/2022-01/Cristiani%20et%20al%20-%20report%20(1)%20Updated.pdf.

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, p. 11-25.

LEGAL NOTICE

SITE INFORMATION

Publisher: Flossbach von Storch AG, Research Institute, Ottoplatz 1, 50679 Cologne, Germany; Phone +49 221 33 88-291, research@fvsag.com Directors: Dr. Bert Flossbach, Kurt von Storch, Dirk von Velsen; *Registration*: No. 30 768 in the Commercial and Companies Register held at Cologne District Court; *VAT-No.* DE200075205; **Supervisory authority**: German Federal Financial Services Supervisory Authority, Marie-Curie-Straße 24 – 28, 60439 Frankfurt / Graurheindorfer Straße 108, 53117 Bonn, www.bafin.de; *Author*: Prof. Dr. Agnieszka Gehringer; *Editorial deadline:* 9th of August 2023