ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Redefining Systemic Cybersecurity Risk in Interconnected Environments

Giacomo Assenza | Complex Systems & Security Lab, University Campus Bio-medico (UCBM) of Rome, Italy; the World Bank Group, US | ORCID: 0009-0007-4909-5775

Alessandro Ortalda | Brussels Privacy Hub, Vrije Universiteit Brussel (VUB), Faculty of Law and Criminology, Brussels, Belgium | ORCID: 0000-0001-9414-9938

Roberto Setola | Complex Systems & Security Lab, University Campus Bio-medico (UCBM) of Rome, Italy | ORCID: 0000-0002-8792-2520

Abstract

While the different entities that compose any socio-economic environment have always had a certain degree of interconnection, the evolving dynamics of cyberspace are intensifying their interdependence and shared reliance on the digital realm. This is giving rise to increasingly possible origins of systemic cybersecurity risk, potentially leading to scenarios where supply chains and essential services experience the rapid and widespread propagation of cascade events at unprecedented levels and velocities. If this interdependence is widely recognised and accepted (Section 2), the concept of systemic cybersecurity risk is still subjective and functional to the core mission of single components of a system (Sections 3 and 4), and this lack of common terminology prevents the community from adopting a shared posture to manage these risks. In this paper, we propose a workable and inclusive definition of systemic cybersecurity risk (Section 5). We then review relevant cybersecurity events arguing that while catastrophic episodes are still unseen, there are incidents that highlight systemic dynamics (Section 6). Finally, we review relevant diagnostic tools that have been developed to address systemic cybersecurity risks and

Received: 01.05.2024

Accepted: 07.08.2024

Published: 29.08.2024

Cite this article as:
G. Assenza, A. Ortalda, R. Setola "Redefining systemic cybersecurity risk in interconnected environments," ACIG, vol. 4, no. 2, 2024, DOI: 10.60097/ACIG/192119

Corresponding author:
Giacomo Assenza, Complex Systems & Security Lab, University Campus Bio-medico (UCBM) Rome, Italy; the World Bank Group, US; E-mail: giacomoassenza@gmail.com
0009-0007-4909-5775

discuss their limitation as well as opportunities for future research (Section 7). We conclude by highlighting that systemic cybersecurity risk is, by definition, a shared risk, thus developing a common understanding is the starting point to endorse coordinated mitigations at system level.

Keywords

risk assessment, risk management, cybersecurity, systemic cybersecurity risk

1. Introduction

Ongoing evolutions of cyberspace dynamics have amplified the attention around systemic cybersecurity risks. The rapid integration of Information and Communication Technology (ICT) into societal functions has come together with a market concentration of products and services which has made the different entities constituting the socio-economic environment increasingly interconnected and dependent on shared infrastructure and common providers. In such a context, there is a growing concern that even single failures can spread across a system, leading to scenarios where supply chains and essential services could experience rapid and widespread cascading events at unprecedented scales. While most cybersecurity events traditionally have a narrowly defined set of victims [1], recent studies provide empirical evidence of an increased prevalence, scale, and impact of cyber-related incidents [2, 3]. Furthermore, recent episodes have demonstrated how failures can affect multiple entities simultaneously. For example, in May 2023 the exploitation of a vulnerability in the firewall system recommended by the industry body and adopted by most energy operators in Denmark led to 22 companies being compromised, with several of them forced to go into island mode operation [4]. In the report analysing the incident, it is highlighted that Denmark has a highly decentralised energy system composed of many small companies, which makes the sector fairly resilient in case of a single disruption. However, a situation of 'systemic vulnerability – where the same vulnerability is exploited across companies' can create a potentially critical situation [5]. This event is just one of the last of a series of episodes, such as WannaCry, NotPetya, SolarWind, and Log4J (and more recent ones like the Crowdstrike incident), which have demonstrated how failures can propagate across complex supply chains, emphasising how their reliance on shared infrastructure products and services, concentrates risk into an unknown number of critical nodes.

Despite the growing concern surrounding systemic cybersecurity risk, the underlying problems and potential solutions seem to remain unseizable and poorly understood. The concept of systemic cybersecurity risks results subjective and ambiguous in both literature and the community of cybersecurity practitioners, and so are the existing tools and methodologies for identifying and measuring sources of this type of risk. Currently, there is no shared terminology, and there is little agreement not only on what constitutes a systemic cybersecurity risk but also on the granularity at which a system can be defined (operator, sector, countries, or supra-national level), with existing definitions being functional to the mission of the entity defining them. This has so far hindered the development of a unified approach to managing these risks. The identification of what can be defined as a systemic cybersecurity risk is not just an academic exercise but it is seminal to understand how systemic dynamics affect cyberspace and consequently devise appropriate risk mitigation policies and incident response procedures. Systemic cybersecurity risk is, by definition, a shared risk, thus developing a common understanding is the starting point to endorse coordinated actions at the system level, both in terms of policies and operational capacities.

In this article, we first explore the broader concept of systemic risk and its roots in the financial sector (Section 2). Then, we turn to the existing approaches to defining and dealing with systemic cybersecurity risk, highlighting how these result in ad hoc and uncoordinated strategies. In particular, we briefly outline the existing interpretations, and argue that (i) currently systemic cybersecurity risk is a 'contextual' concept, with its definition heavily influenced by the specific mandate of the involved entities; (ii) existing approaches consider the systematicity of cybersecurity risk primarily on the impact that they may have, with limited attention given to the underlying dynamics that give rise to such risks (Sections 3 and 4). We then propose a comprehensive and flexible definition of systemic cybersecurity risk that can be applied at different levels of granularity, providing a common foundation for understanding and addressing the issue (Section 5). Subsequently, we apply our definition to review relevant case studies, arguing that while catastrophic cybersecurity incidents are still unseen, several cybersecurity events highlight systemic dynamics (Section 6). Finally, we review some of the diagnostic tools and methodological frameworks that have been developed, discussing how these efforts are undermined by a general lack of data, a partial and uneven application of methodologies, and a general resistance from operators to share information (Section 7).

2. The Emergence and Evolution of 'Systemic Risk' as a Concept

The concept of systemic risk emerged in the field of finance and economics, with some of the earliest references dating back to the aftermath of the Great Depression in the 1930s [6] when economists and policymakers began to recognise how the failure of individual entities, such as banks and financial institutions, could affect the entire economic and financial system. However, within the literature, more structured definitions of systemic risks started to appear only in the 1990s. The concept gained even further prominence during the 2007–2008 global financial crisis, when the collapse of major financial institutions and interconnectedness of financial markets highlighted the potential for shocks to cause far-reaching financial and economic downturns [7, p. 315, 8].

Definitions adopted between 1988 and 2014 by academics and banking institutions [9][1] identify the following features of systemic risks: (i) *scale of the phenomenon*: systemic risks affect a large part of a system; (ii) *contagion effect*: due to the interdependencies and interconnectedness among its components, systemic risks have the potential to trigger a cascading series of adverse events spreading across the entire system; and (iii) *system failure*: systemic risks have the potential to impair the functioning of the system itself.

Overtime, the understanding of systemic risk has evolved, and its application expanded from the economic and financial perspectives of the early days to other disciplines and areas of study. Scholars and practitioners begun to approach the issue with the goal of understanding the dynamics of complex and cross-sector supply chains and the potential for widespread disruptions as a consequence of the interconnectedness and interdependence of infrastructures, processes, and services across the globe [10–14]. In particular, the exposure of society to systemic risks has been amplified by what is known as the information revolution [15]. Already in 1997, the US Presidential Commission on Critical Infrastructure Protection (PCCIP) concluded that the country was so reliant on ICT infrastructure that the government had to frame it within the broader 'national security focus' to address the impacts that would result for the entire nation in case of its disruptions [16]. Since then, hyperconnectivity, digitalisation, widespread deployment of Internet of Things, adoption of readily available cloud technologies, and, more broadly, the pace and reach of technological innovation have contributed to shaping a quickly evolving and interdependent environment. This environment makes it more difficult for

1——In Smaga (2014) [9], systemic risks are defined as 'the risk that a shock will result in such a significant materialisation of (e.g. macro-financial) imbalances that it will spread on a scale that impairs the functioning of the financial system and to the extent that it adversely affects the real economy (e.g. economic growth)'.

operators to pursue business continuity, because they often have to rely on goods or services provided by other parties [17].

While this rapid innovation is bringing benefits in terms of efficiency and reach of operations, it is also introducing structural aspects that magnify the potential for risks. First, the interdependencies in the ICT ecosystem are growing in number and complexity, with related risks going beyond the mere technical aspect [18, 19]. As a result, both policy-makers and operators struggle with understanding the 'intricate and interlocking dependencies' [20], both upstream and downstream [21]. This often translates into inadequate risk management practices [22]. Second, the market concentration of digital services, where stakeholders often rely on similar – when not the same – technologies, infrastructures, services, and providers, implies that when these fail, the impact may affect a large number of assets and organisations [23]. Third, the growth of hacking capabilities and their availability through models, such as the Hacking-as-a-Service one, makes it easier and cheaper for malicious actors to operate [24]. Especially the large number of potential targets that can be hit with a single capability – see the above-mentioned feature (ii) of systemic risks – makes it appealing to attackers from a cost-benefits perspective.

These rapid developments have been largely acknowledged by the security community, which has increasingly focused on the structural vulnerabilities of societal functions [25–28] and has started to formulate the concept of 'systemic cybersecurity risk'. However, there is little agreement on what these risks are, how to manage them, and even if they have ever materialised.

3. Systemic Cybersecurity Risk is a Contextual Concept

When it comes to systemic cybersecurity risks, most of the academics and practitioners have kept the economic and financial perspective [29–32]. They refer to these risks as a subset of systemic financial risks where a cybersecurity event on systemic entities may lead to spillover effects. For example, the European Systemic Risk Board (ESRB) defines systemic cyber-related incidents as those occurring 'in the financial sector' and which could cause 'serious negative consequences for the internal market and the real economy' [33]. Similarly, the European Central Bank provides an understanding of systemic cyber risks within the broader context of macro-financial perspectives. Accordingly, systemic risks should be assessed by looking at the following two dimensions: (i) the cross-sectional dimension, which relates to how the risk propagates within the financial system;

and (ii) the time-related dimension, which looks at the dynamic evolution of financial stability risks over time and consider the procyclical build-ups of financial fragility [34]. On the other hand, other authors and practitioners have developed more comprehensive conceptualisations of systemic cybersecurity risks, which include aspects such as safety and security. These broader approaches are not limited to the financial sector, but apply to all sectors [1, 35]. For example, according to the World Economic Forum (WEF), systemic cybersecurity risk is 'the risk that a cyber event at an individual component of a critical infrastructure ecosystem will cause significant delay, denial, breakdown, disruption, or loss, such that services are impacted not only in the originating component but consequences also cascade into related (logically and/or geographically) ecosystem components, resulting in significant adverse effects to public health or safety, economic security, or national security' [36]. This approach entails a more inclusive concept that considers the goals of societal (and not only economic) wellbeing, and which therefore is extended to all the critical functions of society.

Another point of view that can be adopted to look at systemic cybersecurity risk concerns the level of granularity at which a 'system' is perceived. A system can be defined as a collection of interrelated and interconnected elements or components that work together to achieve a common purpose or goal[2] [37, 38]. Building on this definition, transnational processes, countries, sectors, societal functions, single operators, or even circumscribed sections of a corporate ICT landscape can all be characterised as systems [1]. Therefore, under this assumption, the adjective 'systemic' can assume different meanings depending on the point of view. For instance, while the WEF definition takes an international perspective, the 2021 Systemic Cyber Risk Reduction Venture – established by the US Cybersecurity and Infrastructure Security Agency (CISA) – adopts a national perspective, focusing on understanding how 'cyber risks or incidents in individual pieces or components of National Critical Functions (NCF) could create far-reaching cascading impacts, leading to system-wide functional degradation or failure' [39]. CISA's understanding of 'system' corresponds to the United States as a country, and therefore its point of view on systematicity is nationally centred. In fact, it includes the risks that might affect the recognised NCFs[3] (e.g., the provision of medical care, distribution of electricity, etc.), but it disregards the impacts that can manifest at the international level or be suffered by other countries. The 2023 US National Cybersecurity Strategy further emphasises this nation-centric view, highlighting the importance of addressing systemic risks to make the US digital ecosystem – clearly spelled out as 'our digital

2——These elements can be tangible entities, such as physical objects or processes, as well as intangible entities, such as concepts or information flows. The interactions and relationships between the components of a system lead to emergent properties or behaviours that may not be evident when considering each component in isolation.

3——A list of 55 NCFs is available here: https://www.cisa.gov/topics/risk-management/national-critical-functions

ecosystem' – resilient [40]. Going further down the abstraction scale, there is a well-established perspective that frames systemic cybersecurity risks within the context of enterprise risk management. In 2019, the Digital Director Network (DDN) released the DiRECTOR™ risk framework to help corporate boards and management teams to manage systemic risks in 'complex digital business systems' [41]. This framework defines systemic risk as the risk that a component's failure in a corporate digital system propagates and escalates, putting the entire organisation at stake [42].

These definitions present significant differences but share the idea that systemic cybersecurity risks materialise after cybersecurity events that produce digital and physical damages, and create cascading effects across the system, with potentially significant disruptions. This perspective is rooted in the interdependence of functions and the importance that ICT has in modern systems. It looks at how widespread the impact of the cybersecurity risks is and considers this as the determinant variable to categorise a cybersecurity risk as 'systemic'. However, this approach does little to determine the dynamics producing them. In other words, any cybersecurity risk with 'far reaching cascading impacts' [39] or 'cascade into related (logically and/or geographically) ecosystem components' [36] would be considered systemic. This blurs the different categorisations, on the one hand, between systemic cybersecurity risks and high-impact cybersecurity risks, and, on the other hand, between systemic cybersecurity risks and systemic risks more broadly. In fact, the widespread cascades of a cybersecurity event might be caused by physical or logical interdependencies, rather than digital or cyber ones, which entail that effective risk management measures are not necessarily driven by cybersecurity considerations.

A different and relatively new approach to typify systemic cybersecurity risk comes from the insurance industry. In recent years, insurance companies have been increasingly vocal about systemic cybersecurity risks, claiming that these challenge the sector's capacity to provide adequate insurance coverage [43]. From their perspective, risks are systemic when they become uninsurable due to the massive losses that would arise from the interconnections among clients, sectors, and locations, as well as the difficulties of modelling and hedging [1]. For instance, the insurance company AIG defines as 'systemic' those risks that are 'capable of impacting many companies at the same time' [44]. Under this interpretation, insurers adopt a different definition of 'system': not anymore a group of elements working together towards a goal, but simply the group of entities that would be eligible to receive compensation in

case of cyber events. The apprehension pertains to the conceivable scalability, wherein a solitary incident could concurrently impact numerous companies, resulting in substantial interconnected liabilities for insurers. For instance, in the case of damages affecting cloud computing platforms employed by a large number of clients, the insurer would be compelled to settle claims for all its policyholders concurrently with evident economic losses [45]. For insurers, a particular type of systemic cyber risk relates to the so-called 'cyberwar' or, more generally, state-sponsored hacks, which, due to their high potential costs, most insurers are deciding not to cover [46]. For instance, Lloyd's of London requires insurance policies to have an explicit exemption for state-backed computer network operations [47]. This approach could undermine trust and reliance on insurance instruments, as it creates uncertainty about the possibility of getting coverage where it is needed the most. In fact, not only is attributing a cyberattack, let alone identifying one as an act of war, a complex, multilayered, and ultimately political exercise [48, 49], but it is also well beyond the scope of insurers. Despite these complexities, insurers are trying to pursue this interpretation in practice, as shown by NotPetya and the consequent dispute between the US food company Mondelez and the Swiss insurance company Zurich (further analysed in Section 6).

Finally, a minoritarian interpretation of systemic cybersecurity risk examines it from the perspective of technological standardisation and adoption. In a sense, this is similar to the issue arising from the interconnectedness that characterises today's systems that have been referred above. However, this conceptualisation does not focus on the cascading effect that an event might have. Rather, it looks at the fact that incidents involving certain technologies that are widely shared have near-instantaneous effects on a large surface, making traditional redundancy measures ineffective [50]. In a conventional non-cyber system, redundancy serves as a risk-reduction strategy. This is built on the assumption that not all systems fail simultaneously. However, in the realm of cybersecurity, this assumption does not necessarily hold true, as vulnerabilities, if exploited, might simultaneously affect all replicas. The SolarWinds episode (further analysed in Section 5), as well as the event in the Danish power sector, serve as prominent examples of this dynamic [50, 51].

4. Have Systemic Cybersecurity Events Occurred?

In Section 3, we presented different definitions of systemic cybersecurity risk, highlighting how these are highly context-related

and how they can be driven by subjective considerations. These aspects add complexity to the ongoing efforts to establish shared terminology for this evolving concept. Similarly, the lack of a common understanding prevents the community from organically identifying when and if systemic cyber risk has ever materialised. Many agree that while systemic cybersecurity risks are concrete, one of the main challenges related to understanding and managing them is the lack of data and case studies. For example, in 2019, the EastWest Institute asserted that no cybersecurity incidents had ever qualified as systemic [52]. To date, catastrophic cybersecurity events, which are likely to be unanimously labelled as systemic are still unseen [1], but the existing unclarity in the terminology and definitions creates substantial challenges in identifying if and how potential systemic dynamics have accompanied less evident, but still significant events.

For example, the 2021 Colonial Pipeline hack had a significant impact, but concentrated in the US energy sector. The incident forced the Colonial Pipeline, a crucial fuel transport system, to suspend operations for a week. This disruption led to widespread fuel shortages and price spikes along the East Coast, affecting numerous states and prompting panic buying. The Colonial Pipeline moves approximately 45% of the fuel supply for the East Coast, which made its shutdown particularly impactful. The incident resulted in an estimated 5500 gas stations running out of fuel, and the national average gas price saw an increase of around 8 cents per gallon in just 1 week [53]. According to some of the definitions analysed above, this episode could be seen as presenting systemic characteristics. It did have an impact in terms of price reaction and destabilised volatility [54], and it did disrupt one of the so-called NFCs categorised as systemic [1]. However, services were restored relatively quickly, the long-term impacts of this episode were limited, as well as its cascades on other sectors and countries, which would in turn undermine the categorisation of this incident as systemic under certain definitions of it, like the one from the WEF.

Similarly, classifying an event as systemic depends on the level of granularity at which a system is defined. WannaCry, for instance, was a 2017 ransomware that affected over 200,000 computers across 150 countries, with a specific concentration in the UK National Health Service (NHS). Within the NHS, it severely impacted 81 out of 236 NHS trusts, resulting in the cancellation of approximately 19,000 medical appointments. Also, the financial toll was significant, with the NHS estimated to have spent around £92 million in direct costs and lost revenue due to the hack [55]. Yet the impact

was significantly concentrated within the UK healthcare supply, with limited consequences on the delivery of the service globally. If analysed through a national/sectoral security-based framework, WannaCry is likely to be categorised as a systemic event, but the same label would be more difficult to apply from global or regional perspectives. Also, despite the significant loss of revenues and recovery costs, the event was far from resulting in economic or financial instability, which entails that financially focused definitions would disregard this incident as systemic.

On the other hand, the impacts from other episodes were severe enough to be considered systemic but distributed enough to elude this categorisation from national security-based framework. The 2017, NotPetya ransomware, which the White House stated to be the 'most destructive and costly cyber-attack in history' [56], had a substantial impact on various organisations across countries. The incident's total cost to businesses worldwide has been estimated to be in the range of $10 billion [57] and is reported to have affected countless machines around the world, from hospitals in Pennsylvania to a chocolate factory in Tasmania, affecting multinational companies, including FedEx's European subsidiary TNT Express, the pharmaceutical giant Merck, French construction company Saint-Gobain, food producer Mondelēz, and manufacturer Reckitt Benckiser, inflicting nine-figure costs in each case. One of the hardest-hit industries was shipping, with Maersk, a global shipping company, forced to suspend operations in 17 terminals around the globe [58], reporting losses of around $300 million. The NotPetya incident also affected the insurance market. For instance, the refusal of Zurich Insurance Group to pay a $100 million claim from food company Mondelēz arguing that the stipulated policy was not liable to cover 'warlike actions' [59], led to a dispute between the Swiss and American companies. Eventually, the insurance company covered most of the damages created by NotPetya, but this created a precedent which resulted in industry-wide effort to update insurance policies with war exclusion clauses [47]. While from an international, sectoral, and corporate standpoints, the systemic element of NotPetya is difficult to deny, its impacts were distributed across many stakeholders globally to the extent that, except for Ukraine, where the effects were particularly manifest [57], in no countries the damages were so significant to be considered a national security issue, thus a systemic event from a national standpoint.

Existing impact-oriented definitions of systemic cybersecurity risks are functional, which means that the identification of this type of risk is largely subjective and dependent on the mission or

perception of entities at play. This creates challenges in studying, understanding, and addressing this phenomenon.

5. An Inclusive Definition

As described in the previous section, systemic cybersecurity risk is a highly contextual concept. This makes it difficult for the community of stakeholders to collaborate and effectively manage it. To address this challenge, a shared terminology or, at the very least, a mutual understanding must be developed. In this section we propose a definition of systemic cybersecurity risk, which tries to create common ground among different stakeholders. Following is the proposed definition:

> A risk is to be considered as systemic cybersecurity risk when, within the context of the system under analysis, has the potential to initiate a cybersecurity event (trigger) that can spread over a number of other ICT parts or functionalities of the system (circuit) that is sufficient to create changes to the system (impact).

This definition takes an inclusive approach. The *trigger* refers to all the events that might lead to losses of confidentiality, integrity, or availability of information, data, or information (or control) systems [60, 61]. This includes events occurring through digital (such as malwares, ransomwares, distributed denial-of-services [DDoS], software failures, etc.) and physical (such as destruction or impairment of hardware, natural disaster) mean.

The *circuit* refers to the systems or networks of ICT assets, components, or infrastructures through which an initial trigger propagates. This is irrespective of the extension or surface of the system, meaning that the concept of circuit can be applied at different scales, as a system can comprise from a single entity to multiple entities distributed across sectors, countries, and regions. In order to differentiate systemic cybersecurity risks from broader systemic risks, the circuit relates to cyberspace only. This excludes physical or logic cascades that extend beyond the perimeter of ICT systems (e.g., a slowdown in the supply of healthcare services due to a shortage of goods due to a cybersecurity event in the provider of these goods). In fact, these types of cascades, while extremely relevant in a context of great interdependency between assets, do not necessarily require cybersecurity mitigations, which position them beyond the scope of this definition and related policy measures. It is also important to differentiate the circuit from the supply–chain

and related risks, the latter being a narrower concept referring to the people, processes, and technologies associated with the delivery of services from one entity to another [62].

Finally, *the impact* is intended as all the disruptions that may introduce changes to the system. This language suggests first that the impact implies a broader perspective than the mere economic–financial one suggested by some definitions adopted by experts (see Section 2). In fact, if it is likely that a catastrophic cyber-related event can affect the financial environment, this is not an essential condition for systematicity because, as we have established, systematicity is not a measure of the extensions but a measure of the perimeter within which a risk exists and materialises its impact. Second, while this definition recognises that the effect of a systemic cybersecurity risk is larger with respect to the generating trigger, it does not tie the idea of systematicity to high-impact events. Even if rare, there might be scenarios of cybersecurity events presenting systemic dynamics, which nonetheless did not affect aspects, such as national economy or security, and did not result in catastrophic or severe incidents. For instance, the Stuxnet malware self-replicated, infecting thousands of machines worldwide regardless of their operating system version, but it was designed to release its payload only in the nuclear power plant in Natanz [63, 64]. This means that, while the circuit in which the malware spread was extensive, the actual impact was circumscribed to a single operator with effects that resulted to be far from catastrophic.

6. Dynamics of Systemic Cyber Risks

The lack of an agreed upon definition translates into a lack of common taxonomies to categorise systemic cybersecurity risks and related events. This is exacerbated by a paucity of case studies. In this section, we adopt our definition outlined above to review relevant events and highlight how, even though none of them resulted in catastrophic effects, they still show systemic dynamics that can be helpful to understand, thus address, systemic cybersecurity risks. Systemic cybersecurity risk manifests in various forms and can be classified in multiple ways. In the following paragraphs, we analyse three different dynamics in which a trigger spreads across a circuit causing impacts. In particular, we identify *top-down*, *distributed*, and *independent* dynamics [1].

In a *top-down dynamics*, even a single event disrupting a critical component within a system has the potential to trigger a chain reaction that progressively influences a widening array of interdependent

entities. For example, if a critical asset of the Internet infrastructure fails, such as a submarine fibre optic communication cable (SCC), an Internet Exchange Point (IXP), or Domain Name Service (DNS), businesses and services operating over the Internet would be affected by the disruption and might be unable to deliver their services in a far-reaching domino effect. For example, SCCs handle 98% of the global traffic, and despite redundancies being available for most countries, there are episodes showing significant impacts of potential disruptions [65]. In 2015, in the archipelago of the Northern Marianas, the only available submarine cable was severed, cutting off the island from broadband traffic for days [66]. Impacts included a loss of access to the Internet and the collapse of communications, with disruptions in critical services (health, tourism, education, etc.), with estimated damages amounting to US$21 million [67]. Similarly, data shows significant impacts triggered even where countries have redundancy systems and multiple alternative cables [68]. Other examples show the top-down dynamic that damages in the Internet infrastructure might cause. In 2016 Dyn, a major DNS provider in the United States, fell victim of a massive DDoS campaign launched by the Mirari Botnet that overwhelmed its servers with an unprecedented amount of traffic [69]. While the incident did not take down the Internet, caused catastrophic impacts, or affected the real economy, it did result in substantial disruptions and emphasised the 'systemic role' that single pieces of the Internet infrastructure play in maintaining the stability and availability of online services. The Dyn disruption resulted in a 'massive East Coast Internet outage' [70], and service disruptions for many major websites and online services that relied on Dyn's DNS services. Popular services (like Twitter, Netflix, Reddit, Spotify, Airbnb, GitHub, Paypal, and more) were affected, either experiencing slow load times or becoming completely inaccessible for users not only in the United States but also in Europe and different parts of the world. Systemic cyber risks might also materialise following physical triggers; for instance, in 2019, a malicious fire in an Italian rail transformer room caused the unavailability of train data and information, which eventually caused significant delays and service suspensions [71]; or as part of broader systemic events, such as when the extreme weather caused a power outage in Gambia, which, in turn, caused disruption of the nodal IXP in the region as well as all the online activities depending on it [72].

In a *distributed dynamic*, a single event disrupts simultaneously similar components scattered across a system. In this case, the systematicity is not given by a vertical chain reaction, where a disruption leads to another, but rather from structural vulnerabilities

that simultaneously affect various assets. Distributed dynamics are particularly relevant when many entities from different sectors rely on the same landscape of providers, products, and services, or in other words, share the same vulnerabilities. This trend concentrates cybersecurity risks into critical nodes, potentially magnifying the impact of events. Recently, there has been a notable surge in events that triggered distributed dynamics, highlighting how failures have the potential to escalate into systemic incidents. For instance, in November 2021, a group of researchers disclosed a critical vulnerability in the Apache Log4j software library. Log4j is a piece of open-source software which provides logging capabilities for Java applications, and that is embedded in billions of devices and systems worldwide. Exploiting this vulnerability gave the possibility to execute remote code on affected systems, leaving an open door to all sorts of malicious activities [73]. The vulnerability has triggered widespread concern and a massive effort to release patches, which is still ongoing. Further, organisations are encountering difficulties in implementing these patches. Insights from experts suggest that a complete resolution of the problem could span years, which leaves a vast number of stakeholders exposed until this issue is comprehensively addressed. Currently, there have been no reported instances of exploiting this vulnerability. However, experts agree that this can potentially trigger distributed dynamics and lead to systemic events [74].

A similar distributed dynamic led to the 2020 SolarWinds incident. SolarWinds is a software vendor which provides IT management and monitoring solutions to many clients in different industries. Hackers managed to infiltrate its software development process, injecting malicious code into their Orion platform updates. The malware was then spread across the client ecosystem as part of a legitimate software update [50]. Using SolarWinds as a vector, the malicious actors compromised more than 18,000 operators, including relevant government agencies and sensitive targets (such as the Treasury Department and Los Alamos National Laboratory, which designs nuclear weapons for the US government) as well as major ICT providers, such as Microsoft, Cisco, and FireEye [75]. While the specific details remain undisclosed, the fact that threat actors potentially accessed highly sensitive governmental information or that they could leverage the same exploit to release wipes or other destructive tools raises concern about the security around software supply chain, especially when it comes to critical operators [51].

Some authors identify a third type of systemic dynamic, the simultaneous occurrence of *independent cyber failures.* They see it as the

result of cybersecurity incidents exploiting independent vulnerabilities in single operators [76]. In theory, numerous individual cyber incidents could happen simultaneously to create a systemic event, but practically this type of event seems unlikely. For this reason, this paper focuses on top-down and distributed dynamics as the main drivers of systemic cybersecurity risk. These two scenarios are ideal types to understand how systemic cascades spread across a given environment. In concrete applications, systemic events are likely to materialise in a 'hybrid way' [1] with multiple, simultaneous, and interconnected top-down and horizontal dynamics.

In the analysed cases, the systematicity seems to stem from a confluence of factors, such as risk concentration, scale, and increased complexity of supply chains. The consolidation of cyberspace around shared assets, technologies, products, and third-party providers has created concentrated dependency on a limited set of critical nodes facilitating the establishment of shared vulnerabilities and single points of failure [77]. Moreover, the increasing complexity of computer networks and associated operational and human systems, as well as the intricate web of technical, contractual, and financial linkages on the Internet, introduces hidden levels of mutual dependence. This complexity prevents stakeholders from fully stocktaking the support that system components provide to their processes, reducing their visibility over potentially critical vulnerabilities [1].

Given the shared ownership of systemic cybersecurity risks, it is critical that all the stakeholders involved share a common understanding of the phenomenon in order to put in place meaningful and concerted mitigations. To this goal, in addition to a common definition, and analysis of systemic dynamics, practitioners need to explore new and shared approaches for identifying systemic cybersecurity risks, gaps, and vulnerabilities to enhance their capacity to address them.

7. A Review of Diagnostic Tools

It is often said that 'if you cannot measure it, you cannot manage it' [78]. Efforts to address systemic cybersecurity risks should therefore starts with some sort of capacity to quantify the likelihood and severity of events as well as to identify system gaps and vulnerabilities where remediations can be applied. In this section we review some of the diagnostic tools and methodological frameworks that have been developed, and we discuss that these

efforts are undermined by a general lack of data, a partial and uneven application of methodologies as well as by a general resistance from operators to share information [79].

Given the increasing complexity, interdependency, and opacity of cyberspace, it is challenging to develop even a shared grasp of systemic cybersecurity risk, let alone efficient and consistent assessment methodologies to capture the phenomenon. Also, building this common understanding seems to be a necessary and preparatory step to develop clear regulatory frameworks for operators to manage these risks. Several efforts have been made to assess systemic cybersecurity risks. While some studies attempt to assess the individual state vulnerability to Internet infrastructure failures (such as SCC) in global comparison [67], a prevalent approach has been to leverage methods from traditional risks analysis to measure the economic impacts of cascades propagating across different linkages of a system following cybersecurity incidents. While all these studies point at the similar conclusion that direct costs associated with 'normal' cybersecurity incidents are significantly lower in comparison to those associated with systemic cyber events [29, 80], they also uncover concrete uncertainties in their models' outputs. For example, a model which simulates a cybersecurity incident in a major cloud provider that disrupts service to its users estimates total losses between US$5 and 15 billion [81]. Similarly, a recent tool to gauge the aggregated economic impact of cyber incidents in more than 60 countries through supply chain connections across various sectors estimated potential annual costs comprehended between hundreds of billions and trillions of dollars [80]. An even more emblematic example is a 2021 model to estimate the potential economic damage associated with a given cyber incident considering its cascading failures. The authors applied this model to Maersk's NotPetya infection and found that the total economic cost may have been as little as US$3 billion or as much as US$57 billion [29]. These examples show significant intervals in their estimates, which in turn entail uncertainties in attempting to manage the effects on systemic cybersecurity events. The same uncertainties are highlighted in the insurance world, where catastrophe modelling is often applied to understand systemic cybersecurity risk [82], and partnerships are being endorsed to build shared datasets [83]. In fact, many authors argue that one of the main challenges that has prevented the development of approaches capable of modelling the costs and consequences of systemic failures has been the lack of data on production networks at firms' levels, which prevents a clear understanding of interdependencies among operators [84].

A different typology of diagnostics focuses on maturity, rather than risk. These tools define a set of indicators to explore how proficiently stakeholders at different levels (from single operators to sub-sectors, sectors, and countries) implement cybersecurity measures. While these frameworks are not specifically designed to target systemic cybersecurity risks, they include measures and controls that are relevant for addressing sources of risk systematicity. More broadly, they aim to support stakeholders in building cyber robustness and resilience, which, according to recent studies, is one of the largest factors for addressing cybersecurity systemic risks [29]. Lately, most methodological frameworks have deepened their focus on systemic aspects of cybersecurity risk. At corporate levels, in 2021, the National Institute for Standards and Technology (NIST) published the 'Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations', with guidance for operators to reduce the risks associated with an enterprise's decreased visibility into and understanding of how the technology they acquire is developed, integrated, and deployed or the processes, procedures, standards, and practices used to ensure the security, resilience, reliability, safety, integrity, and quality of the products and services [85]. The Cyber Resilience Framework (CRF) and related Cyber Resilience Index (CRI) published in 2022 [86] has an even stronger focus on securing interdependencies among organisations, ecosystems, and supply chains. The CRF identifies 'systemic resilience and collaboration' as one of the six key principles that stakeholders should keep in mind while securing their assets, which entails the following 'practices': understanding the interdependencies within each ecosystem, engaging with the other relevant stakeholders and fulfilling its role in maintaining ecosystem resilience [86]. Building on the CRF, the CRI aggregates results from individual organisations and establishes an index of cyber resilience performance for sub-sectors, sectors, and supply chains. While this tool might provide a precious overview to practitioners and policymakers, its insightfulness largely depends on how broadly it is adopted by the operators forming the system as well as on the quality and accuracy of the information that is shared. This might be a significant obstacle, as organisations are often hesitant to reveal sensitive information regarding their dependencies to external parties, including government authorities. Their concerns may include the risk of losing competitive edges, attracting regulatory and legal scrutiny, or inadvertently offering a blueprint for potential adversaries to exploit. This is particularly true for large technology providers who tend to closely protect their technical architectures as a trade secret [1].

At a less granular level, the Sectoral Cybersecurity Maturity Model (SCMM) [87] and the Cybersecurity Capacity Maturity Model for

Nations (CMM) [88] aim at measuring the general cybersecurity maturity of a sector and country, respectively, and they both include relevant indicators for systemic cybersecurity risks. The SCMM builds upon the contemporary research on system science showing that an increase in resilience of individual components within a system does not necessarily result in a proportional improvement in the resilience of the system as a whole [89]. Rather, system resilience is intricately linked to the interactions among its components and is not simply the sum of the individual capacity of its constituent parts. The SCMM tries to take an approach which looks at a sector 'as a system' focusing not only on the maturity of individual components (such as critical operators) but also emphasising interdependencies and interactions among various stakeholders that constitute the sector (e.g., supervisory authorities, individual organisations, etc.) and with relevant external entities that may influence or impact the cybersecurity, capabilities, and resilience of the sector, such as Ministries, Departments, and Agencies (MDAs), national competent authorities for cybersecurity, and ICT/operational technology (OT) service providers [87]. To this end, it analyses a sector adopting, among others, indicators that look at how sector interdependencies are mapped, how information are shared among stakeholders, and how minimum levels of security are guaranteed by supply chain providers. Similarly, the CMM employs analogous indicators to assess capacity at the national level. This methodology, in addition to assessing general cybersecurity risk management and critical infrastructure protection (CIP) practices, includes specific indicators on how a country supports the resilience of Internet services and security ICT supply chain, which is particularly relevant to reducing systemic cybersecurity risks [29]. While both methodological frameworks have the potential to help countries build better security at both sectoral and national levels, including practices to target systemic cybersecurity risks, their focus on capacity, or in other words, what measures are implemented, says little about the adequacy of these measures in relation to the risk. In fact, systems are heterogeneous with different levels of digitalisation and interconnection, thus facing different risk profiles. Therefore, any capacity assessment should be contextualised and focused not primarily on what capacities are in place but rather on the process that led stakeholders to build these capacities. In particular, implementing cybersecurity measures should follow an information-driven approach. Especially for cybersecurity systemic risks, due to the increased complexity and opacity, how decision-makers identify gaps and prioritise remediation is an aspect that future research should emphasise more vigorously.

8. Conclusions

The trends and events outlined in this paper serve as a signal that systemic dynamics within cyberspace are concrete, with the potential for related risks to materialise. Nonetheless, different interpretations make it more difficult to unite stakeholders in concerted actions. Given the shared ownership of systemic cybersecurity risks, and that effective solutions demand extensive collaboration across stakeholders, establishing a common terminology and comprehension is crucial. In fact, single entities hardly have sufficient data and information, mitigations, tools, and, more broadly, capacity, to manage systemic cybersecurity risks on their own. Rather, the necessary capacity seems spread across a variety of public and private actors. Building a successful partnership among these disparate stakeholders requires not only a mutual understanding of different contextual interests and interpretations of systemic cybersecurity risk but, most importantly, a workable definition of the phenomenon itself, which, in turn, positively affects the proficiency with which stakeholders protect their assets. This is particularly relevant, as national and regional governments have started producing regulations that include requirements for operators to address systemic cybersecurity risks. For instance, the European Union Digital Operational Resilience Act (DORA) sets rules on ICT third-party risk monitoring and mitigation that highlight the need for a clearer discussion of where supply chain risk ends and where systemic cybersecurity risk begins. At the same time, the revised European Union (EU) Network and Information System Directive (NIS2) requires member states to address cybersecurity in the supply chain as part of their national cybersecurity strategies.

In this paper, we first explored existing approaches to dealing with systemic cybersecurity risk, highlighting how efforts to define and manage it result in ad hoc and uncoordinated strategies. We then proposed a comprehensive and flexible definition of systemic cybersecurity risk that could be applied at different levels of granularity, providing a common foundation for understanding and addressing the issue. Subsequently, we applied our definition to review relevant case studies, arguing that while catastrophic cybersecurity incidents are still unseen, several cybersecurity events highlight systemic dynamics. Finally, we concluded by reviewing some of the diagnostic tools and methodological frameworks that have been developed, discussing how these efforts are undermined by a general lack of data, a partial and uneven application of methodologies, and a general resistance from operators to share information.

Given the breadth and complexity of the underlying problem, new policy approaches are needed. Future research should focus on how policymakers can enhance the ability to identify and measure systemic cybersecurity risk on the one hand, and mitigate, externalise, or even eliminate it on the other. Inclusive mechanisms need to be established to involve a diversity of stakeholders: private actors, such as technology providers, cybersecurity firms, critical infrastructure operators, and reinsurers, as well as public actors, including regulators and national security agencies. International cooperation is also essential because systemic cybersecurity risk is inherently global.

References

[1] D. Forscey, J. Bateman, N. Beecroft, B. Woods. *Systemic cyber risk: A primer*. Washington, DC: Carnegie Endowment for International Peace, 2022.

[2] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity*, vol. 2, no. 2, pp. 121–135, 2016, doi: 10.1093/cybsec/tyw001.

[3] I. Aldasoro, L. Gambacorta, P. Giudici, T. Leach, "The drivers of cyber risk," *Journal of Financial Stability*, vol. 60, pp. 100989, 2022, doi: 10.1016/j.jfs.2022.100989.

[4] H. Labus. (Nov. 14, 2023). *Danish energy sector hit by a wave of coordinated cyberattacks* [Online]. Available: https://www.helpnetsecurity.com/2023/11/14/danish-energy-sector-cyberattack/ [Accessed: Nov. 15, 2023].

[5] SektorCERT. (Nov. 2023). *The attack against Danish, critical infrastructure*, SektorCERT [Online]. Available: https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf [Accessed: Feb. 12, 2024].

[6] S.R. Das, K.J. Mitchener, A. Vossmeyer. (2018). *Systemic risk and the great depression* [Online]. Available: https://www.econstor.eu/handle/10419/198785 [Accessed: Aug. 12, 2023].

[7] S. Eijffinger, "Defining and measuring systemic risk," in *Handbook of central banking, financial regulation and supervision: After the financial crisis*, 2011, doi: 10.4337/9781849805766.00018.

[8] G. Galati, R. Moessner, "Macroprudential policy – A literature review," *Journal of Economic Surveys*, vol. 27, no. 5, pp. 846–878, 2013, doi: 10.1111/j.1467-6419.2012.00729.x.

[9] P. Smaga. (Aug. 2014). *The concept of systemic risk* [Online]. Available: https://papers.ssrn.com/abstract=2477928 [Accessed: Aug. 12, 2023].

[10] P. Pederson, D. Dudenhoeffer, S. Hartley, M. Permann, "Critical infrastructure interdependency modeling: A survey of US and international research," *Idaho National Laboratory*, vol. 25, pp. 27, 2006.

[11] M. Ouyang, "Review on modeling and simulation of interdependent critical infrastructure systems," *Reliability Engineering & System Safety*, vol. 121, pp. 43–60, 2014, doi: 10.1016/j.ress.2013.06.040.

[12] S.M. Rinaldi, J.P. Peerenboom, T.K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems Magazine*, vol. 21, no. 6, pp. 11–25, 2001, doi: 10.1109/37.969131.

[13] V. Rosato, L. Issacharoff, F. Tiriticco, S. Meloni, S. Porcellinis, R. Setola, "Modelling interdependent infrastructures using interacting dynamical models," *International Journal of Critical Infrastructures*, vol. 4, no. 1–2, pp. 63–79, 2008, doi: 10.1504/IJCIS.2008.016092.

[14] E. Luiijf, M. Klaver, "Analysis and lessons identified on critical infrastructures and dependencies from an empirical data set," *International Journal of Critical Infrastructure Protection*, vol. 35, p. 100471, 2021, doi: 10.1016/j.ijcip.2021.100471.

[15] D. W. Jorgenson, K.M. Vu, "The ICT revolution, world economic growth, and policy issues," *Telecommunications Policy*, vol. 40, no. 5, pp. 383–397, 2016, doi: 10.1016/j.telpol.2016.01.002.

[16] PCCIP. (Jan. 1998). *Critical foundations: Protecting America's infrastructures* [Online]. Available: http://www.tandfonline.com/doi/abs/10.1080/1097198X.1998.10856225 [Accessed: Aug. 14, 2023].

[17] A. Azadegan, M.M. Parast, L. Lucianetti, R. Nishant, J. Blackhurst, "Supply chain disruptions and business continuity: An empirical assessment," *Decision Sciences*, vol. 51, no. 1, pp. 38–73, 2020, doi: 10.1111/deci.12395.

[18] G. Strupczewski, "Defining cyber risk," *Safety Science*, vol. 135, p. 105143, 2021, doi: 10.1016/j.ssci.2020.105143.

[19] R. Böhme, S. Laube, M. Riek, "A fundamental approach to cyber risk analysis," *Variance*, vol. 12, no. 2, pp. 161–185, 2019.

[20] E.M. Brunner and M. Suter, *International CIIP handbook 2008/2009: An inventory of 25 national and 7 international critical information infrastructure protection policies.* ETH Zürich: Center for Security Studies (CSS), 2008.

[21] World Economic Forum (WEF). *Systemic cybersecurity risk and role of the global community: Managing the unmanageable*. Cologny, Geneva: WEF, 2022.

[22] T. Macaulay (2019). *The danger of critical infrastructure interdependency* [Online]. Available: https://www.cigionline.org/articles/danger-critical-infrastructure-interdependency/ [Accessed: Aug. 24, 2023].

[23] D. Geer, E. Jardine, E. Leverett. (Feb. 2020) "On market concentration and cybersecurity risk," *Journal of Cyber Policy*, vol. 5, no. 1, pp. 9-29, doi: 10.1080/23738871.2020.1728355.

[24] M. Lehto, "Cyber-attacks against critical infrastructure," in *Cyber security*. Cham: Springer, 2022, pp. 3–42, doi: 10.1007/978-3-030-91293-2_1.

[25] M. Klaver, E. Luiijf, "Analyzing the cyber risk in critical infrastructures," in *Issues on risk analysis for critical infrastructure protection*. IntechOpen, 2021, doi: 10.5772/intechopen.94917.

[26] E. Luiijf, M. Klaver, *Resilience approach to critical information infrastructures.* Cham: Springer, 2019, doi: 10.1007/978-3-030-05849-4.

[27] R. Setola, "How to measure the degree of interdependencies among critical infrastructures," *International Journal of System of Systems Engineering*, vol. 2, no. 1, pp. 38–59, 2010, doi: 10.1504/IJSSE.2010.035380.

[28] D. Clemente, *Cyber security and global interdependence: what is critical?* London: Chatham House, Royal Institute of International Affairs, 2013.

[29] J.W. Welburn, A.M. Strong, "Systemic cyber risk and aggregate impacts," *Risk Analysis*, vol. 42, no. 8, pp. 1606–1622, 2022, doi: 10.1111/risa.13715.

[30] D.J. Bodeau, C.D. McCollum. (2018) *System-of-systems threat model* [Online]. Available: https://apps.dtic.mil/sti/citations/AD1108059 [Accessed: Aug. 15, 2023].

[31] Office of Financial Research (OFR). "Cybersecurity and financial stability: Risks and resilience," *OFR Viewpoint*, 17-01, Feb. 2017.

[32] P. Sommer, I. Brown, *Reducing systemic cybersecurity risk*. Organisation for Economic Cooperation and Development (OECD), Working Paper No. IFP/WKP/FGS, vol. 3. Paris: OECD, 2011.

[33] European Systemic Risk Board (ESRB). (2020). *Systemic cyber risk* [Online]. Available: https://data.europa.eu/doi/10.2849/566567 [Accessed: Aug. 15, 2023].

[34] J. Fell, N. de Vette, S. Gardó, B. Klaus, J. Wendelborn. (Nov 2022). "Towards a framework for assessing systemic cyber risk," *Financial Stability Review* [Online]. Available: https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html [Accessed: Aug. 18, 2023].

[35] A. Masys, "Examining systemic risk in the cyber landscape," in *The great power competition,* vol. 3, *Cyberspace: The fifth domain.* Cham: Springer, pp. 69–82, 2022, doi: 10.1007/978-3-031-04586-8_4.

[36] World Economic Forum (WEF). *Understanding systemic cyber risk*. White Paper. Cologny, Geneva: WEF, Oct. 2016

[37] R.D. Arnold, J.P. Wade, "A definition of systems thinking: A systems approach," *Procedia Computer Science*, vol. 44, pp. 669–678, 2015, doi: 10.1016/j.procs.2015.03.050.

[38] A. Kossiakoff, S.M. Biemer, S.J. Seymour, D.A. Flanigan, *Systems engineering principles and practice*. Hoboken, NJ: John Wiley, 2020, doi: 10.1002/9781119516699.

[39] US Cybersecurity and Infrastructure Security Agency (CISA). (2021). *Systemic cyber risk reduction venture* [Online]. Available: https://www.cisa.gov/sites/default/files/2023-02/fs_systemic-cyber-risk-reduction_508.pdf [Accessed Feb. 12, 2024].

[40] White House. (Mar. 2023). *National cybersecurity strategy* [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [Accessed Feb. 12, 2024].

[41] Digital Director Network (DDN). (Dec. 08, 2019). *DDN releases DiRECTOR the only systemic risk framework focused on complex digital systems*. [Online]. Available: https://www.digitaldirectors.network:443/blogs/ddn-releases-director-the-only-systemic-risk-framework-focused-on-complex-digital-systems [Accessed: Dec. 08, 2023].

[42] B. Zukis. (Dec. 09, 2019). *Digital directors network releases DiRECTOR™ the only systemic risk framework focused on complex digital systems* [Online]. Available: https://www.einpresswire.com/article/504281736/digital-directors-network-releases-director-the-only-systemic-risk-framework-focused-on-complex-digital-systems [Accessed: Aug. 21, 2023].

[43] I. Smith. (Aug. 18, 2023). "Cyber attacks set to become 'uninsurable', says Zurich chief," *Financial Times* [Online]. Available: https://www.ft.com/content/63ea94fa-c6fc-449f-b2b8-ea29cc83637d [Accessed: Dec. 26, 2026].

[44] AIG. (2017). *Is cyber risk systemic* [Online]. Available: https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/may2017/cs2017_0167.pdf [Accessed Feb. 12, 2024]

[45] A. Granato, A. Polacek. (2019). *The growth and challenges of cyber insurance – Federal Reserve Bank of Chicago*, Chicago Fed Letter No. 426 [Online]. Available: https://www.chicagofed.org/publications/chicago-fed-letter/2019/426 [Accessed: Aug. 18, 2023], doi: 10.21033/cfl-2019-426.

[46] S. Scalfane. (2021). *Writing cyber is key to survival, Munich Re Exec says* [Online]. Available: https://www.carriermanagement.com/news/2021/09/13/226172.htm [Accessed: Aug. 18, 2023].

[47] I. Smith, "Lloyd's of London defends cyber insurance exclusion for state-backed attacks," *Financial Times*, Sep. 05, 2022.

[48] T. Rid, B. Buchanan, "Attributing cyber attacks," *Journal of Strategic Studies*, vol. 38, no. 1–2, pp. 4–37, 2015, doi: 10.1080/01402390.2014.977382.

[49] M. Mueller, K. Grindal, B. Kuerbis, F. Badiei, "Cyber attribution," *Cyber Defense Review*, vol. 4, no. 1, pp. 107–122, 2019.

[50] R. Alkhadra, J. Abuzaid, M. AlShammari, N. Mohammad. (2021). "Solar winds hack: In-depth analysis and countermeasures," in *2021 12th International conference on computing communication and networking technologies (ICCCNT)*, IEEE, pp. 1–7, doi: 10.1109/ICCCNT51525.2021.9579611.

[51] W. Growley, L. Gruden, W. Canter, "Navigating the solar winds supply chain attack," vol. 56, no. 2, 2021.

[52] EWI. (2019). *Cyber insurance and systemic market risk.* EastWest Institute [Online]. Available: https://www.eastwest.ngo/cyberinsurance [Accessed: Aug. 16, 2023].

[53] S. Smith, *Out of gas: A deep dive into the colonial pipeline cyberattack.* SAGE Business Cases Originals. Thousand Oaks, CA: SAGE, 2022, doi: 10.4135/9781529605679.

[54] J.W. Goodell, S. Corbet, "Commodity market exposure to energy-firm distress: Evidence from the Colonial pipeline ransomware attack," *Finance Research Letters*, vol. 51, pp. 103329, 2023, doi: 10.1016/j.frl.2022.103329.

[55] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi, P. Aylin, "A retrospective impact analysis of the WannaCry cyberattack on the NHS," *NPJ Digital Medicine*, vol. 2, no. 1, pp. 1–7, 2019, doi: 10.1038/s41746-019-0161-6.

[56] White House. (2018). *Statement from the Press Secretary – The White House* [Online]. Available: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/ [Accessed: Aug. 17, 2023].

[57] C. Nast (Aug. 21, 2018). *The untold story of NotPetya, the most devastating cyberattack in history* [Online]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed: Aug. 17, 2023].

[58] A. Jones, O. Khan, "Surviving NotPetya: Global supply chains in the era of the cyber weapon," in *Cyber security and supply chain management: Risks, challenges, and solutions*, pp. 133–146, 2021, doi: 10.1142/9789811233128_0006.

[59] A. Satariano, N. Perlroth (Apr. 15, 2019). "Big companies thought insurance covered a cyberattack. They may be wrong," *The New York Times* [Online]. Available: https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html [Accessed: Aug. 18, 2023].

[60] ISO. (2016). *ISO guide 73: 2009* [Online]. Available: https://www.iso.org/standard/44651.html [Accessed: Aug. 22, 2023].

[61] K. Stine, R. Kissel, W.C. Barker, J. Fahlsing, J. Gulick, *Guide for mapping types of information and information systems to security categories*, vol. 1. 2008, doi: 10.6028/NIST.SP.800-60v1r1.

[62] M.H. Hugos. *Essentials of supply chain management.* New York, NY: John Wiley, 2024.

[63] F. Rieger. (Jan. 17, 2019). *Stuxnet: targeting the Iranian enrichment centrifuges in Natanz? Knowledge brings fear* [Online]. Available: https://frank.geekheim.de/?p=1189 [Accessed: Nov. 08, 2023].

[64] J.R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies*, vol. 22, no. 3, pp. 365–404, 2013, doi: 10.1080/09636412.2013.816122.

[65] NATO CCDCOE. (2019). *Strategic importance of, and dependence on, undersea cables* [Online]. Available: https://ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf [Accessed: Aug. 22, 2023].

[66] ESCAP, "Broadband Connectivity in Pacific Island Countries," 2018

[67] J. Franken, T. Reinhold, L. Reichert, C. Reuter, "The digital divide in state vulnerability to submarine communications cable failure," *International Journal of Critical Infrastructure Protection*, vol. 38, p. 100522, 2022, doi: 10.1016/j.ijcip.2022.100522.

[68] G. Aceto, A. Botta, P. Marchetta, V. Persico, A. Pescapé, "A comprehensive survey on Internet outages," *Journal of Network and Computer Applications*, vol. 113, pp. 36–63, 2018, doi: 10.1016/j.jnca.2018.03.026.

[69] G.M. Graff. (Dec. 13, 2017). *How a dorm room "Minecraft" scam brought down the Internet* [Online]. Available: https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/ [Accessed: Aug. 23, 2023].

[70] L.H. Newman. (Oct. 21, 2016). *What we know about Friday's massive East Coast Internet outage* Online]. Available: https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/ [Accessed: Aug. 23, 2023].

[71] L. Chadwick. (Jul. 22, 2019). *Italy hit by four-hour train delays after suspected arson fire* [Online]. Available: https://www.euronews.com/2019/07/22/italy-hit-by-four-hour-train-delays-after-suspected-arson-fire-outside-florence [Accessed: Aug. 23, 2023].

[72] M. Faye. (Mar. 14, 2023). *When mother nature strikes: Lessons learned from an IXP crash* [Online]. Available: https://www.linkedin.com/pulse/when-mother-nature-strikes-lessons-learned-from-ixp-crash-faye [Accessed: Aug. 23, 2023].

[73] P. Ferreira, F. Caldeira, P. Martins, M. Abbasi, "Log4j vulnerability," in: *Information technology and systems.* Cham: Springer, 2023, pp. 375–385, doi: 10.1007/978-3-031-33261-6_32.

[74] J. Marks. (Jan. 11, 2022). *Analysis: One month in, there aren't any huge, known log4j hacks* [Online]. Available: https://www.washingtonpost.com/politics/2022/01/11/one-month-there-arent-any-huge-log4j-hacks/ [Accessed: Aug. 25, 2023].

[75] K. Zetter. (May 02, 2023). *The untold story of the boldest supply-chain hack ever* [Online]. Available: https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/ [Accessed: Nov. 15, 2023].

[76] E.D. Peet, M.J. Vermeer. (2020). *Securing communications in the quantum computing age*: *Managing the risks to encryption* [Online]. Available: https://policycommons.net/artifacts/4835890/securing-communications-in-the-quantum-computing-age/5672600/ [Accessed: Nov. 11, 2023].

[77] J.E. Scheuermann, "Cyber risks, systemic risks, and cyber insurance symposium," *Penn State Law Review*, vol. 122, no. 3, pp. 613–644, 2017.

[78] J. Drucker. (Dec. 04, 2018). *Council post: You are what you measure* [Online]. Available: https://www.forbes.com/sites/theyec/2018/12/04/you-are-what-you-measure/ [Accessed: Nov. 10, 2023].

[79] F. Cremer et al. "Cyber risk and cybersecurity: A systematic review of data availability," *The Geneva Papers on Risk and Insurance – Issues and Practice*, vol. 47, no. 3, pp. 698–736, 2022, doi: 10.1057/s41288-022-00266-6.

[80] P. Dreyer et al. (2018). *Estimating the global cost of cyber risk.* Research Reports RR-2299-WFHF. Rand Corporation [Online]. Available: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2299/RAND_RR2299.pdf [Accessed: Nov. 11, 2023].

[81] Lloyd's. (2018). *Cloud down impacts on the US economy* [Online]. Available: https://assets.lloyds.com/assets/pdf-air-cyber-lloyds-public-2018-final/1/pdf-air-cyber-lloyds-public-2018-final.pdf [Accessed: Aug. 22, 2023].

[82] Gallagher Re. (Jan. 2019). *Evaluation of cyber models* [Online]. Available: https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/evaluating-cyber-models-report.pdf [Accessed: Aug. 22, 2023].

[83] C. Shi. (Sep. 28, 2022). *CFC spearheads cyber cat-declaration initiative to tackle systemic risk* [Online]. Available: https://www.insuranceinsider.com/article/2aoh41qs3atr6x3jpj75s/reinsurers-section/cfc-spearheads-cyber-cat-declaration-initiative-to-tackle-systemic-risk [Accessed: Apr. 18, 2024].

[84] V.M. Carvalho, A. Tahbaz-Salehi, "Production networks: A primer," *Annual Review of Economics*, vol. 11, no. 1, pp. 635–663, 2019, doi: 10.1146/annurev-economics-080218-030212.

[85] J. Boyens, A. Smith, N. Bartol, K. Winkler, A. Holbrook, et al., "Cybersecurity supply chain risk management practices for systems and organizations," Oct. 2021, doi: 10.6028/NIST.SP.800-161r1-draft2.

[86] World Economic Forum (WEF) and Accenture. (Jul. 2022). *The cyber resilience index: Advancing organizational cyber resilience* [Online]. Available: https://www.weforum.org/publications/the-cyber-resilience-index-advancing-organizational-cyber-resilience/ [Accessed: Nov. 11, 2023].

[87] The World Bank Group. (2023). *Sectoral cybersecurity maturity model* [Online]. Available: https://documents1.worldbank.org/curated/en/099062623085028392/pdf/P17263707c36b702309f7303dbb7266e1cf.pdf [Accessed: Feb. 12, 2024].

[88] *Global Cyber Security Capacity Centre (*GCSCC). (2021). *Cybersecurity capacity maturity model for nations* [Online]. Available: https://gcscc.ox.ac.uk/the-cmm [Accessed: Nov. 12, 2023], doi: 10.2139/ssrn.3822153.

[89] L. D. Valdez et al. "Cascading failures in complex networks," *Journal of Complex Networks*, vol. 8, no. 2, p. cnaa013, 2020, doi: 10.1093/comnet/cnaa013.