ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

State-level Cyber Resilience: A Conceptual Framework

Geoffrey A. Hubbard | Bavarian School of Public Policy, Technical University of Munich, Germany, ORCID: 0000-0002-0771-292X

Abstract

There is currently a gap in our academic and practical understanding of the concept of resilience in cyber space at the level of the state, hampering research and policy-making due to the lack of a rigorously constructed, shared terminology. This article contributes to this area by providing a comprehensive capacities-based conceptualisation of state-level cyber resilience. After establishing that cyber resilience is necessary and that it should be developed at the state level, we perform a rigorous exploration of the concept of resilience as it pertains to the different areas involved in state-level cyber resilience. Seeking the most salient characteristics of each one, we identify from the general concept of resilience that it is a non-static process requiring an availability of assets; from state resilience, we identify that resilience capacities are harboured at multiple levels and across actors within the polity; and from cyber resilience, we identify that there is a plethora of different potential damages. Taking all this into consideration, our resulting concept of state-level cyber resilience is the following: the ability of a state, which (a) is made up of multiple layers, to (b) harness a set of key assets in order to (c) confront a particular type of damage to its cyber space, by (d) going through the stages of coping and eventually recovering to its normal state. Having constructed this conceptual framework, this work aids researchers and decision-makers by providing a common terminology and fostering a systematic, multidimensional approach to states' capacity for resilience in cyber-space.

Keywords

cybersecurity, cyberspace, national cyber resilience, critical infrastructure, national security, smart cities

Received: 08.05.2023

Accepted: 03.07.2023

Published: 09.08.2023

Cite this article as:
G.A. Hubbard, "State-level Cyber Resilience: A Conceptual Framework," ACIG, vol. 2, no. 1, 2023, DOI: 10.60097/ACIG/162859

Corresponding author:
Geoffrey A. Hubbard, Bavarian School of Public Policy, Technical University of Munich, Germany;
ORCID: 0000-0002-0771-292X,
E-MAIL: geoffrey.hubbard@tum.de

1. Introduction

We are currently experiencing a paradox: cyber technologies, which were partly created with the goal of making societies more resilient, now harbour threats that jeopardise this objective. Some of the technology that sustains cyber-space emerged from research intended to design communications able to withstand a nuclear attack [1]. Despite this background, cyber-space has inherent characteristics that nevertheless make it vulnerable. Humanity is in the midst of a technological revolution that "challenges all historical experience" [2] and our interconnectedness, for all its benefits, is rendering us ever more vulnerable to "radical... systemic shocks" [3]. As cyber technologies increasingly underpin the functioning of modern societies, states (also known colloquially as 'nations') find themselves in a position of growing dependence. For as long as cyber-space is operating normally, a state can reap its benefits and function as usual. But digital systems are inherently vulnerable, and when compromised, have the potential to severely affect a society's functioning. An example to illustrate the gravity of these vulnerabilities is the 2021 Colonial Pipeline ransomware attack, one of the largest cyber-attacks on American infrastructure and one of the most disruptive digital ransom operations on record.

The Colonial system, running 5,500 miles between Texas and New York, is the largest U.S. gasoline pipeline and transports 2.5 million barrels per day. It is the main source of fuel for the region, carrying nearly half of all fuel consumed on the East Coast [4]. The May 2021 attack compromised IT systems, locking down the victim's computers and demanding payment. A day earlier, the hackers had already stolen confidential industry data, which they threatened to leak if the payment was not made. To contain the attack, the company halted the pipeline's operations along the entire network, and in response to the double extortion attempt, decided to pay the ransom, worth 75 bitcoins. After receiving payment, the hackers granted the company access to its systems, but the recovery process was slow. The shutdown lasted six days, during which uncertainty and panic over fuel supply took hold across the East Coast [5, 6]. Gasoline prices spiked to a six-year high and gas stations continued running out of fuel, even days after the shutdown [7]. In order to best deal with such incidents, a state must have measures in place to improve its resilience. Unfortunately, the main focus in policy so far has been on cyber security (i.e. ensuring systems are fail-safe), and not on cyber resilience (i.e. ensuring systems are safe-to-fail). Furthermore, there remains a paucity of work in the social sciences regarding the intersection of resilience and cyber technologies, with different scholars asserting five years apart that this research topic remains in its infancy [8, 9].

A specific lacuna in our understanding hinders a shift in focus to improve resilience, namely, the fact that an integrated concept of state-level cyber resilience remains inchoate. Under these circumstances, policymakers are left struggling to implement strategies to improve this type of resilience. A consensus has emerged, particularly in Europe and the USA, that cyber-resilience considerations at the level of the state should be included in policy and regulation [10]. To accomplish this objective, further research is needed to better understand the phenomenon. The question that drives this research is therefore the following: how can we conceptualise the term state-level cyber resilience in a firmly grounded and comprehensive manner? This article addresses this gap in research by providing a capacities-based conceptual framework of state-level cyber resilience.

To fulfil its purpose, the article takes the following structure: after this introductory section and a brief note on terminology, we touch upon the theoretical background that supports the key assumptions in conducting this work. Next, we develop a conceptualisation of state-level cyber resilience. To this end, we conduct a conceptual examination of resilience from three points of view, namely the general, cyber, and state perspectives. With this knowledge we then proceed to positing a new concept of statelevel cyber resilience. In closing, we offer a final discussion of the advances made, reflect on future research paths, and share our concluding thoughts.

1.1. Terminology and theoretical assumptions

It is fundamental to have a good understanding of what cyber-space is to be able to study it. Over time there have been various approaches to the concept. Kuehl, for instance, identified fourteen different definitions [11]. For this work, cyberspace is defined as the "fusion of all communication networks, databases, and sources of information into a vast... blanket of electronic interchange" [12]. Importantly, cyber-space is a hybrid construction of physical and virtual layers [13]. As such, the result is a virtual interaction space enabled by new information technologies with physical grounding [14].

We are particularly interested in understanding how this "global synthetic substrate" relates to the functioning of societies [15]. A useful analogy to understand how societies interact with and in cyber-space is to view it as "a globally unfettered exchange space... like an enormous, ... moderately chaotic, annual medieval fair without adequate security from an overlord... and with all the human energy and pathologies possible in shared space" [15]. A plethora of risks fills this domain, varying by cause and including those arising from nefarious

intent, human error or due to environmental circumstances beyond human control. In this work, we collectively refer to the actualisation of these risks as adverse incidents in cyber-space.

This work has two main underlying assumptions, namely, (1) that developing resilience is desirable and necessary, and (2) that the state is an important unit of study related to resilience. Supporting the first assumption, we employ the theoretical background of a risk society. Developed most prominently by Ulrich Beck, he defined this idea as "a systematic way of dealing with hazards and insecurities induced and introduced by modernisation itself" [16]. He stated that dangerous threats to humanity have become an inherent part of industrial life, rather than a manageable by-product. These self-inflicted risks of modernisation are known as manufactured risks. In the same way that human actions are the key cause, humans can also (and must) do much to reduce the threat [17, 18]. Bearing this in mind helps us understand how modern developments that deeply disrupt human life become a double-edged sword. Our stance assumes that states have a resilience deficit regarding the manufactured risks of cyber-space, and that they need to act to improve their capacities for cyber resilience.

For our second assumption, we refer to the evolving role of the state and its ongoing primacy in organised human life. Over the last century, the reach of the state has grown with the development of welfare systems around the world. As such, states have generally taken on greater and more diverse responsibilities than they previously had. In the field of technology, it has been observed that states are highly reliant on the private sector for the development of cyber-capabilities, leading to the question of whether and to what extent the power of the state has been eroded in this area. Nevertheless, however much the power gap narrows between state and non-state actors, there are some key aspects where state power is nevertheless unrivalled – states still exercise the ultimate power of coercion and, unlike private actors, generally have social legitimacy, formal authority, and regulatory capability [14].

Returning to the analogy of cyber-space as a vast medieval fair, we see that despite all the dynamic power these fairs created for private citizens, ultimate control remained in the hands of the state – these markets did not substitute the institutions of feudal authority. We follow Nye's reasoning that cyber-space does not fundamentally challenge the governments of sovereign states, but like medieval markets, it will "coexist and greatly complicate what it means to be a sovereign state" [13]. By this reasoning we assume that states will remain the dominant

actors in cyber-space for the foreseeable future, and hold that state policy can have a substantial effect on cyber resilience capabilities.

2. Conceptual background

Resilience is a complex and multi-faceted phenomenon. As such it has been approached from different angles with variations in its manifestations. In this section we will explore the current understanding of the concept of resilience in different contexts, and develop a comprehensive conceptualisation of state-level cyber resilience. To this end, we first examine the concept of resilience in general, followed by a review of the concepts of state resilience and cyber resilience. Finally, we probe existing contributions in the direction of the joint concept of state-level cyber resilience, integrate the insights from the individual terms, and provide a new conceptualisation.

To lay the foundations for developing a sound conceptualisation of statelevel cyber resilience, it is necessary to start by understanding the background and existing applications of resilience in its general form. Deriving from the Latin resiliere, meaning to bounce back, the word resilience refers to an object's ability to return to its normal state following a disturbance. Over the decades, the concept of resilience has been used and developed to differing degrees in various fields, including materials science, engineering, psychology, ecology, and economics [19]. This co-development across disciplines means that the current understanding of resilience has diffuse roots. In the context of material sciences, resilience can be observed in its most tangible form, and its level is determined by how much stress or force a material can withstand before being permanently altered (e.g. breaking), and how quickly it can return to its previous state once the stress has been removed. The same fundamental logic is applied in the other disciplines, where the object of study is replaced by any other entity that can show a form of resilience construed in a broader sense, ranging from machines to humans and entire ecosystems [20]. As we would expect, the meaning of resilience becomes increasingly nuanced as we move beyond the study of materials into other domains. With its demonstrable permeability across disciplines, resilience is "a polysemous and malleable term" [19]. Despite variations, the fundamental concept outlined above remains the same across applications and there is an overlap of basic features across disciplines [21].

To determine whether an object is showing resilience it is necessary to understand what its normal state is. Therefore, having a clear

definition for the state of normalcy in question is a key consideration for the concept to be of any use. This normalcy can refer, e.g., to physical structure, in the case of materials, or to effective functioning – i.e., the delivery of expected results – in the case of a system. In this work we address resilience specifically as it is applied to human socio-technological systems, and this is the focus we shall take henceforth.

When observing a system, the layers at which resilience manifests itself are multiplied when compared to simpler objects. As a complex whole formed by an interconnected network of elements working together, a system is characterised by interdependence in order to achieve its function. As such, when looking at the resilience of a system, there are two simultaneous approaches [21]. First, it can be understood as the entire system's ability to maintain or resume its functions in spite of a disruption, in other words, how easily the system can run as it should normally when it has been disturbed. Second, it can also be viewed as a sum of multiple instances of resilience of the constituent elements and interconnections within the system. In this sense, one is looking at the maintenance of a sum of sub-functions, that keep the system running as a whole.

When dealing with human systems in particular, such as a company or a state, there is a further consideration, namely that the system and its components are not static at any point, including when disturbed. Human organisations are an example of adaptive systems, where resilience levels and response types vary depending on the characteristics of the component and of the adverse incident [20].

Resilience becomes manifest when an adverse incident occurs and the object of study has to cope with it. Resilience cannot be reduced to a single moment or state of being; rather, it is displayed as a process, involving preparation, detection and response, coping and/or adaptation, and recovery. As such, under normal conditions, resilience cannot be directly observed. Instead, what can be observed is an object's perceived capacity to perform at an acceptable level at each stage of the process of resilience in the event of an adverse incident. In other words, what can be observed in a state of normalcy is an object's perceived potential for resilience.

An important point to bear in mind is that a system's capacity for resilience will usually be influenced by the range of assets it has available. Possessing capacities solely sufficient for functioning in a state of normalcy may be detrimental during an adverse incident. Therefore, there must usually be latent resources that can be called

upon in case of emergency. Additionally, as mentioned above, resilience involves preparation as one of its stages, and this equates to an investment of resources in anticipation of disruptions. Systems resilience, therefore, entails clear costs. These, however, are significantly lower than the potential costs to an organisation that is not resilient. The higher an organisation's capacity for resilience, the lower the unforeseen costs deriving from adverse events. It is for this reason that investing in resilience capacities is described as a form of 'insurance' [20]. Here, an important decision must be made: pay the guaranteed costs of improving resilience, or wait to see the costs of an adverse incident, if it happens at all. Especially when budgets are constrained, it can be tempting to gamble by choosing the unknown costs.

2.1. Cyber resilience

Unlike other areas where resilience has been studied for longer, resilience in relation to the functioning of cyber technologies and its wider implications is relatively recent. Cyber resilience started to gain wide attention from 2012, with a World Economic Forum meeting focusing on the topic [9]. Since then, interest in cyber resilience has grown continuously [22]. The goal of cyber resilience has been described in terms very similar to the general concept of resilience. This concept can have different interpretations, including that of: (a) a purely technical system (e.g. a network) being resilient, or (b) an actor that uses cyber-space being resilient, or (c) a technical system's functions being resilient. Regarding the first approach, Linkov and Kott define it as "the ability of the system to prepare, absorb, recover, and adapt to adverse effects, especially those associated with cyber-attacks" [21]. As for the second approach, and serving as a bridge to the third, Hausken defines it as "the ability of an actor to resist, respond and recover from cyber incidents to ensure the actor's operational continuity" [23]. Continuity is indeed key and, when addressing socio-technological systems, we hold that it is more important to focus on the functions of cyber-space than on the technologies themselves. For Björck et al., cyber resilience refers to the ability to continuously deliver the system's intended outcomes, in spite of disturbances. The intended outcome refers to whatever it is that the technology is meant to deliver to the user. The starting point we take for cyber resilience is thus the use derived from the technology [9]. Bellini and Marrone share this thinking, asserting that cyber resilience seeks to guarantee acceptable levels of service by reducing variability and propagation of disruptions throughout the system [8]. Linkov and Kott also recognise the importance of this when they describe cyber resilience as "a bridge between sustaining operations of the system while ensuring mission execution" [21].

As with general resilience, cyber resilience is usually approached as a subset of (cyber) security [21]. The differences mentioned above are nevertheless evident, in particular when looking at their objectives. As Björck et al. succinctly put it, security seeks to protect IT systems with the intention of making them fail-safe. Resilience, in contrast, seeks to ensure "business delivery", regardless of any adverse events, ensuring the systems are safe-to-fail [9] within a specific time horizon. As Bellini and Marrone assert, developing resilience helps address the "remaining known, but unmitigated, risk as well as enhance the overall ability of the system to respond to unknown or emerging threats" [8].

As mentioned in the Introduction, there has been a multiplication of threats in cyber-space. An interview conducted by Radar Services of 105 security experts concluded that between 2018 and 2025, a 300% increase in cyber-attacks per year is expected [23]. Besides the increase in incidents, though, we must be aware of the enormous variety in the types of disruption they involve, and the real-world damage they can cause. This is important because the resilience response required in each case will be different. To exemplify this diversity, there are three incidents that stand out for their distinct kinds of impact: (1) the 2021 Colonial Pipeline ransomware attack, for instance, led to a six-day shutdown of one of the USA's most important energy infrastructure systems, affecting energy supply and markets; (2) the Stuxnet virus (uncovered in 2010) deployed in Iran altered the functioning of the centrifuges in the Natanz nuclear power plant, delaying the state's nuclear programme with diplomatic and geopolitical implications; and (3) the 2020 United States federal government data breach, sometimes known as the Solar Winds hack, was a major infringement on sensitive information as the result of cyber espionage exploiting software vulnerabilities. By virtue of such examples, it is evident that disruptions in cyber-space have numerous forms with multifarious impacts.

Indeed, instead of only being viewed as a technical affair, cyber resilience is increasingly also approached in a broader sense. In addition to the conventionally considered physical and information elements of cyber systems, Linkov and Kott also assert that human cognitive and social domains are equally interdependent in cyber systems. As such, cyber systems are increasingly viewed as "multi-genre" networks [21]. Further in this regard, Hausken describes cyber resilience as involving "most societal actors" including governments, organisations, individuals, and others, "at most levels of organization" [23]. In this respect, we see a recognition of cyber resilience as a phenomenon requiring multidisciplinary consideration.

2.2. State resilience

Returning to our theoretical background, we have observed states taking on an expanding goal of ensuring citizens' well-being. Whereas historically states prioritised conventional security, now many states seek to ensure broader well-being, including for instance health and economic growth. In its most basic form, the resilience of a state is manifested in the continued preservation of its functioning in spite of adverse incidents that affect its constituent parts (government, population, territory). In the context of governance, one of the predominant definitions of resilience is that of the National Academies of Science (NAS), which matches directly the general definition mentioned above [21]. In this case also, resilience is generally considered as a subset of the broader state security agenda [24]. Current conceptions of state or 'national' resilience are connected with the development of a risk society that serves as our theoretical background. Indeed, over recent years there has been a "resilience creep" into public discourse [25] due to widening security concerns. Certain key events have strengthened this trend, notably the September 11, 2001 attacks in the United States [19], as well as natural disasters and, most recently, the Covid-19 pandemic. In state resilience there are three aspects which are important to highlight: (1) the incorporation of new threats, (2) the multiple layers of the state involved in resilience, and (3) the importance of critical infrastructures. The rationale for selecting these three aspects is as follows: these three aspects constitute a three-part cycle which has to work properly for a modern state to have a robust capacity for resilience. Regarding the first aspect, with the aforementioned expanding role of the state in ensuring citizens' well-being, there are more ways in which the state can fail to deliver. This is exacerbated by the multiplication of manufactured risks as states become more technologically advanced (see theoretical background). This leads us to the second aspect – as was mentioned, states are highly reliant on private actors for their technological prowess. When analysing the complex functioning of a state, it would be unwise to approach it as a monolithic entity. Instead, it is important to view a state as a system with clearly defined parts working together. Finally, this connects with the third element, regarding critical infrastructures. Responsibility for these tends to be shared between private and public actors, and it is through this cooperation that a state can effectively continue to pursue its goals and face a diversity of threats (aspect 1), thus closing the cycle for understanding modern state resilience. In the following paragraphs we will go into more depth regarding each aspect.

With regards to the first aspect covering the multiplication of recognised threats, a researcher we take as our reference point is Fjäder, who emphasises the evolving role of the state as fundamental for

our current understanding of state-level resilience. He observes that states are faced with a broadening variety of threats linked to global interdependence and the rapid pace of change, and the fact that governments have decided to address a growing number of these threats. Indeed, security strategies around the world have increasingly opted for a new paradigm in which they attempt to cover 'all hazards' for 'all of society'. Given that security cannot fully cover such ambitions, developing resilience in tandem becomes key [20].

The expansion of the threats acknowledged by governments and included in security strategies entails a noteworthy shift in thinking. Given that these new risks are often considered unavoidable, in addition to prevention and conventional security efforts, there is an acceptance of managing the threat impact. This entails, in a sense, a change in the social contract between governments and citizens with regards to security, based on the common understanding that there is a partial shift from preventing to coping with adverse incidents [20].

Despite the increasing importance given to it, the concept of state resilience remains ambiguous, given that it must address multiple elements, including appropriate responses to security failures and emergencies, as well as critical infrastructure management. Because of this breadth, implementing resilience at a state level is not entirely straightforward [20]. Resilience is a necessary strategy with the potential of being highly effective, albeit whose implementation requires planning involving allocating responsibilities and defining their scope, designing methods for cooperation and coordination, as well as setting concrete goals.

Concerning the second aspect, the hurdles of implementing resilience at the state level are hardly surprising given the complexity of the state itself. A state can be understood as a system comprising multiple elements working together for a common goal, namely its preservation, and, in modern states, the well-being of its citizens. When viewing the state, we can employ a systems approach in which overall resilience is made up of multiple instances of resilience in its constituent parts. Several researchers have posited approaches along these lines. Darnell, for instance, holds that for a state to have resilience capacities, it must be resilient at multiple levels: individual, [federal] state, local, and federal [25]. Similarly, Walklate et al. propose a typology consisting of the individual, familial, communal, institutional, 'national', regional, and global levels. As such, a state's overall capacity for resilience is multilayered, and is the product of many interconnected "resiliences" [25].

Finally, regarding the third aspect, when we think of the functioning of a contemporary state (and its conditions of normalcy) it is clear that much of it depends on the running of critical infrastructures. These provide services essential to the social and economic well-being of citizens, to government functions and to public security. Among the sectors typically considered as critical infrastructure are: water services, food, energy, communications, transport, health, banking and finance, policing and defence-related assets. In addition, intangible assets such as supply chains are sometimes included [20, 25]. Finally, there is of course the growing importance of cyber-space as a special type of critical infrastructure often supporting the others (see the next section). Across all these different critical infrastructures, their importance lies in the services they deliver. Whereas before there was a greater focus on the protection of physical infrastructure, now there has been a shift to prioritising the infrastructure's function, i.e., the delivery of critical services. This recognition is manifest in a clear policy trend towards protecting critical services across different 'national' security agendas [10]. Indeed, resilience is closely linked to overall state power, generally described as the ability of a state to achieve its goals and influence other actors [26]. As such, Rowland et al. consider resilience to be one of the attributes of a state that is powerful in cyber-space [27].

What is considered a resilient state will vary between states and cultures, but in general terms it would mean a state that is able to cope with adverse incidents in a manner that is locally reasonable, and to adapt and recover to return to a state similar to the one that existed previously. To this end, critical services that enable the functioning of the state need to be maintained throughout the disruption, or at least rapidly reinstated. In the case of developed states, with a larger extent of critical services, the demands on the state are greater, as there are more services which must be guaranteed to operate.

3. Conceptualising state-level cyber resilience

Having covered the concepts of cyber resilience and state resilience, we can now proceed to an informed examination and subsequent construction of the concept of state-level cyber resilience. A couple of similarities between the previous concepts are apparent, specifically that cyber and state resilience both involve complex systems, and the fact that a resilience approach provides a necessary addition to conventional security measures given the latter's limitations. Beyond these similarities, there is a deep convergence. Specifically, state resilience is increasingly reliant on cyber resilience. Indeed, the latter

is becoming so important that contemporary state resilience can no longer be treated independently. The reason for this amalgamation lies in the increased role of cyber-space in the functioning of a state and its critical infrastructures. Digitalisation has meant that the work of governments and the economic activities of a society are on a trend towards reliance on cyber-space. This is not only apparent in terms of communication, but also in the 'smart' integration that is expanding to ever more economic and public sectors, including energy, transport, housing, and education, as well as across businesses and industries [10, 28].

It is surprising that state resilience is often discussed entirely separately from cyber resilience in the literature, given that cyber-space is emerging as the predominant critical service for a state. Fjäder [20], for instance, does not give cyber-space special emphasis amongst critical services; Walklate et al. [25] do not even mention cyber-space in the context of state resilience. Instead, the role of cyber-space is considered as part of broader communications, i.e., as one critical service among many. This, however, is patently changing. By updating our vision and embracing the notion that cyber-space is a ubiquitous substrate supporting ever more aspects of human existence, we realise that this is a special kind of infrastructure and needs to be accorded greater importance. If a state's use of cyber-space is compromised, then the multitude of other critical services that depend on it will also be compromised in a ripple effect. This is acknowledged by Bellini and Marrone, who observe that due to its "tight interdependency and pervasiveness, a fault on the cyber layer provokes a fault in several critical services…" [8]. This risk of "cascading and escalating failures" [29] across many dimensions of society is acknowledged in our theoretical background as one of the main traits of a contemporary risk society [18]. Rather than being one service among many, cyber technologies have become the critical infrastructure of critical infrastructures.

At this point we should highlight that in spite of the convergence of state resilience and cyber resilience, we do not propose a merging of the two concepts. When referring to the state, we must still distinguish between state-level cyber resilience and state resilience. The reason for this is that state resilience remains a broader concept. There are certain types of resilience that are largely independent of cyber-space, referring to ideational and political aspects, such as the resilience of state institutions, or the resilience of a sense of state belonging [27].

3.1. Existing contributions

Before we conceptualise state-level cyber resilience, we shall acknowledge a few existing contributions to this concept. As

we shall see, though valuable, these are altogether rather scant. There has been a growing interest in state-level cyber resilience due, specifically, to the growth of industry 4.0, the pioneering initiatives of some governments (e.g. the United Kingdom), and the proliferation of adverse incidents [28]. In the following section, we will briefly review two academic sources and one governmental policy paper that stand out as relevant. These have been selected from the extremely limited available material because they are the most representative of existing incipient approaches to the concept.

We begin with an article by Tiirmaa-Klaar, providing an overview of the notion of 'national cyber resilience' and what policymakers should consider in order to increase resilience levels. The author recognises that cyber technologies form a networked substrate for communications and all critical economic sectors across the world [10]. Amongst other points, Tiirmaa-Klaar mentions three basic policy areas that need to be covered to build 'national cyber resilience': protecting critical infrastructure, addressing crime in cyber-space, and developing sufficient state-level incident response capabilities. She also asserts that states need comprehensive cyber governance models, as well as ways of assessing and implementing varying policy goals and priorities [10]. Notwithstanding this, the author fails to provide a definition of "national cyber resilience".

Our second reference work is a systematic literature review of cyber resilience and incident response in smart cities by Ahmadi-Assalemi et al. Considering the manner in which the review is conducted, and the fact that parallels can be drawn between a smart city and a wider "cybered" state [15], we deem this work suitable for use as a proxy for our task. The authors conducted a review of primary studies related to the resilience of cyberphysical systems in smart cities and investigated how current cyber-physical systems address digital forensics and incident response [28]. They found that most of the reviewed literature focuses only on subsets of resilience and related concepts in incident response. Specifically, threat 'detection' had a very high incidence rank, along with 'security' and the broad concept of 'attacks'. In contrast, the term 'resilience' ranked low, with some of its constituent stages ranked very low, namely, 'response', and 'recovery' [28]. Furthermore, the review found that many of the papers focused only on particular sectors of a smart city (e.g. infrastructure, mobility), rather than on the cumulative whole [28]. This confirms that there is a dearth of scholarly work on cyber resilience and that the focus has instead been on more conventional security. The article provides only a generic definition for cyber resilience, without expressly connecting it to smart cities or states [28].

Our third and final reference is the United Kingdom's National Cyber Strategy 2022 [30]. This policy paper puts significant emphasis on cyber resilience as a state priority. The UK is one of the states at the forefront of research and policy concerning matters of cyber security. In 2016, the UK set up the National Cyber Security Centre (NCSC) with the task of protecting both the government and society in cyber-space [31]. In spite of actions such as this to improve the state's overall cyber security standing, the policy paper states that there is "growing evidence of gaps in our national resilience", with the number of incidents affecting government, businesses and individuals continuing to rise [30]. With its new strategy the government aims to work towards a vision of cyber-space "as a reliable and resilient place for people and business to flourish" as a fundamental part of building a "more resilient nation" [30]. This apparent level of concern and commitment is significant coming from one of the states considered to be most 'powerful' in cyber-space and highlights the ubiquitous perceived risks states face in cyber-space [32].

Unlike previous iterations, the 2022 strategy includes a definition of cyber resilience from the state's perspective which encompasses systems, organisations, and individuals [30]. Furthermore, the direction taken in this paper shows a maturation from a resilience perspective as it explicitly states the importance of aspects such as having a whole-of-society approach; differentiates between pre- and post-incident measures; stresses the need for collaboration with the private sector, as well as the proactivity of the latter; recognises the importance of (other) critical infrastructures; and highlights the need for government to provide direction and set an example.

With this brief review, we can see how state-level cyber resilience is gaining attention. This growing interest, though, has not yet produced significant theoretical advancements and the concept remains incipient. Indeed, something acknowledged in all three reference works is that further research is needed. The concept is still rudimentary and hardly goes beyond the generic definition of resilience. Without a sound and wellgrounded definition, we run the risk of state-level cyber resilience becoming a vague and misused concept, further clouding attempts for assessment and improvement. With this reasoning in mind, we now proceed to proposing a new, comprehensive concept.

3.2. Conceptual framework

In order to contribute a concept of state-level cyber resilience that can then be operationalised, it must be comprehensive

and concrete. At this point we can identify the elements we need for our conceptualisation. From the general concept of resilience, we know that it requires an availability of assets and an investment of resources, and we have understood that resilience is not static, but is manifested as a process; from state resilience, we know that resilience capacities are harboured at multiple levels and across actors within the polity; and from cyber resilience, we know that there is a wide variety of damage that can be inflicted, which would call for different resilience responses. Taking all this into consideration, our resulting concept is the following:

> state-level cyber resilience: the ability of a state, which (a) is made up of multiple layers, to (b) harness a set of key assets in order to (c) confront a particular type of damage to its cyber space, by (d) going through the stages of withstanding this damage and eventually recovering to its normal state.

The state of normalcy will vary between cases. Nevertheless, in abstract terms, we know that it will be the conditions in which the state finds itself capable of sustaining modern life in its typical day-to-day manner. This entails the provision of critical services, primarily the use of cyber-space, for the state to conduct its core functions. As for the adverse incidents that could occur which require a resilient response from the state, the threats are innumerable. Acknowledging the special trait of resilience as being applicable to unforeseen disturbances, we will consider these adverse incidents as being anything negatively affecting the use of cyber-space within the state, whether caused by humans or nature [9].

In order to operationalise the concept, we must first identify the variables involved. From the concept above, these can be isolated as follows:

- **a.** Layers;
- **b.** Assets;
- **c.** Damage;
- **d.** Stages.

These variables have component indicators that allow for their assessment. A deep exploration of these indicators is beyond the scope of this article, but we will briefly propose a set to illustrate the concept's operationalisation. These indicators have been selected with the intention of being comprehensive with respect to the key elements of each type of variable, whilst being succinct and

thus making assessment straightforward. In doing this we have heeded the recommendation that resilience metrics should be (1) broad enough to be used in diverse cases and (2) precise enough to measure specific system components [33]. Cyber resilience is "flexible by nature" [33] and as such, we reason that it is an adequate approach to provide the evaluator with a degree of autonomy within the framework.

Layers

Governments may be the directing actors within a state, but improving state cyber resilience requires multiple actors working together. Hausken, for instance, names eight state layers involved in cyber resilience [23]. We consider this selection inconsistent with our unit of analysis and therefore propose our own set of four layers where resilience is manifested, consisting of the government, as the directing and coalescing actor; private companies, as the main organised entities performing economic activity; communities, as the main organised entities performing non-economic activity, and the individual, as the smallest and most numerous unit within a state.

Assets

As discussed above, resilience has a cost, requiring an investment of resources in anticipation of disruptions. When this investment is effective, it means that the state in question can deploy or activate a number of assets to support its resilience response. From the existing literature, we will base our approach on the set of key resilience assets posited by Bellini and Marrone, consisting of human capital, involving the level of skills and preparedness of the people; technology, which includes the cyber technologies involved in the incident; organisation, referring to how well the states' layers can cooperate; and finance, referring to the capital at the state's disposal for confronting an adverse incident [8].

Damage

When it comes to distinguishing between types of damage, we suggest employing the CIA triad of cybersecurity, a common classification for the kind of damage inflicted in cyber-space. This acronym stands for the damage that can be suffered with regards to Confidentiality, Integrity, and Availability of data or systems. The impact of each type of damage would have to be assessed in relation to the state of normalcy of the state being studied, at a particular time [9, 24].

Table 1. State-level cyber resilience variables and their proposed component indicators.

Layers	Assets	Damage	Stages
Government	Human capital	Confidentiality	Preparation
Companies	Technology	Integrity	Response
Communities	Organisation	Availability	Recovery
Individuals	Finance		

Stages

As discussed earlier, when resilience is put into practice, it manifests itself as a process before, during and after an adverse incident. A common typology of stages is that employed by Bellini and Marrone [8], namely: prepare, withstand or absorb, recover and adapt. Although we find this typology to be insightful, we prefer a slightly condensed version consisting of three stages: Preparation, Response, and Recovery. Here we consider the Response stage to include both 'absorbing' a shock, as well as 'adapting' to it for its duration.

Much of the challenge in addressing the resilience this article has tackled stems from the fact that cyber resilience is typically understood pertaining to individual parts of the state system, and had not yet been conceptualised at the system level, incorporating the different constituent elements. This article explores and analyses the most important aspects of resilience, and subsequently distils them into an integrated and concise concept.

This framework will aid scholars and policymakers in identifying areas of strength and weakness in states' resilience, and the insights it provides will inform strategic decision-making and resource-allocation. In particular, it helps to avoid the potential quagmire of addressing resilience in a siloed manner. It simplifies approaching the issue by extracting the four most salient variables and describing how they interrelate to form a single concept. We provide a way of operationalising the concept by means of a set of indicators which serve as suggested guideposts for a comprehensive step-bystep assessment. With this four-pronged conceptual framework, the different elements of resilience can be approached simultaneously, allowing for research and policymaking that takes into consideration the full picture of state-level cyber resilience. This approach does not point at specific solutions. As Shimizu and Clark point out, "linear

and fixed decision-making approaches are of limited value" due to complexity and uncertainty [18]. Rather, our framework leaves the interested parties with the necessary flexibility and freedom to create their own strategies for improvement based on the specific insight that the assessment provides.

To illustrate the utility of this conceptual framework, we will return to the infamous case of the Colonial Pipeline ransomware attack. In the following table, we present the types of questions that could arise for each variable in this scenario.

Table 2. Illustrative application of the concept to a scenario based on the Colonial Pipeline attack

Variable	Indicators	Example questions for the case
Layers	Government Companies Communities Individuals	What are their responsibilities in this scenario? What are their strengths and weaknesses? How can these layers prepare to increase their capacity for resilience?
Assets	Human capital Technology Organisation Finance	How can the different layers of the state in question harness these assets in such a scenario? Do the layers have the necessary skills? What is the condition of the relevant technology? Are there mechanisms in place for effective cooperation within and across the relevant layers? What is the financial landscape and how would it respond to such a scenario?
Damage	Confidentiality Integrity Availability	What types of damage will the state suffer? Which of these would be most harmful? Which one is most likely and what measures are in place to deal with such damage?
Stages	Preparation Response Recovery	Given the previous questions and answers, what is the assessment of the state's overall preparation? Based on this, what is the perceived competence for a response and recovery to such an incident?

4. Conclusions

This work has taken on an ambitious challenge. In an increasingly important research field that is nevertheless in its infancy, we have proposed a comprehensive conceptual framework of state-level cyber resilience. To accomplish this, we have relied on an intensive cross-pollination of ideas and information provided by other scholars in related research areas. We do not claim to have achieved a definitive concept of state-level cyber resilience; rather, the accomplishments of this work are to aid researchers and policy-makers by providing a common terminology, fostering a systematic and multidimensional approach to states' capacity for resilience in cyber-space, and supplying a springboard for academic debate and further research.

A fascinating ensuing line of research would be to examine how the level of complexity of states aids or hinders their cyber resilience. Complexity has been observed to both strengthen and weaken resilience in systems [21], and states are no exception. Investigating the nature of this simultaneous scope for benefit and detriment would contribute greatly to this field's solidity.

Resilience as a strategy is not a panacea for state security challenges relating to cyber-space and beyond. It nevertheless provides a unique advantage by addressing unpreventable security challenges, whilst also being cheaper in the long term than conventional security. Total resilience cannot be guaranteed, even when adequate strategies are implemented, but a comprehensive understanding of state-level cyber resilience would nonetheless provide much-needed insight so that states can improve their resilience potential. The conceptual framework provided in this work is a step in this direction.

References

[1] J. Ryan, *A history of the Internet and the digital future*. London: Reaktion Books, 2010.

[2] H. Kissinger, *World order*. New York: Penguin Press, 2014.

[3] World Economic Forum, The Global Risks Report 2018, 2018. [Online]. Available: http://www3.weforum. org/docs/WEF_GRR18_Report.pdf. [Accessed: May 4, 2023].

[4] C. Bing, S. Kelly, "Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed," [Online]. Available: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/. [Accessed: Dec. 1, 2021].

[5] U.S. Government Accountability Office, "Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic)," U.S. GAO, May 18, 2021. [Online]. Available: https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic. [Accessed: May 4, 2023].

[6] U.S. Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," June 7, 2021. [Online]. Available: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside. [Accessed: May 4, 2023].

[7] C. Thorbecke, "Gas hits highest price in 6 years, fuel outages persist despite Colonial Pipeline restart," [Online]. Available: https://abcnews.go.com/US/gas-hits-highest-price-years-fuel-outagespersist/story?id=77735010. [Accessed: May 5, 2023].

[8] E. Bellini, S. Marrone, "Towards a novel conceptualization of Cyber Resilience," *2020 IEEE World Congress on Services (SERVICES)*, pp. 189–196, 2020, doi: 10.1109/SERVICES48979.2020.00048.

[9] F. Björck, M. Henkel, J. Stirna, J. Zdravkovic, "Cyber Resilience – Fundamentals for a Definition," in *New Contributions in Information Systems and Technologies*, vol. 353, A. Rocha, A. M. Correia, S. Costanzo, and L. P. Reis, Eds. Cham: Springer International Publishing, pp. 311–316, 2015, doi: 10.1007/978-3-319-16486-1_31.

[10] H. Tiirmaa-Klaar, "Building national cyber resilience and protecting critical information infrastructure," *Journal of Cyber Policy*, vol. 1, no. 1, pp. 94–106, 2016, doi: 10.1080/23738871.2016.1165716.

[11] D. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," in *Cyberpower and National Security*, F. D. Kramer, S. H. Starr, L. K. Wentz, Eds. 1st ed.Washington, DC: National Defense University Press, 2009, pp. 24–42.

[12] M. Dunn Cavelty, "Cyber-Security," in *Contemporary Security Studies*, A. Collins, Ed., Oxford: Oxford University Press, 2016, pp. 400–416.

[13] J. S. Nye, *The future of power*, 1st ed. New York: Public Affairs, 2011.

[14] N. Choucri, "Emerging Trends in Cyberspace: Dimensions & Dilemmas," in Cyberspace: Malevolent Actors, Criminal Opportunities and Strategic Competition, 2012, pp. 1–19. [Online]. Available: https://nchoucri.mit.edu/sites/default/files/documents/[Choucri]%202012%20Emerging%20Trends%20in%20CyberspaceDimensions%20%26%20Dilemmas.pdf. [Accessed: May 5, 2023].

[15] C. Demchak, "Cybered Conflict, Cyber Power, and Security Resilience as Strategy," in *Cyberspace and national security: threats, opportunities, and power in a virtual world*, D. S. Reveron, Ed., Washington, DC: Georgetown University Press, 2012, pp. 121–136.

[16] U. Beck, "Risk society: towards a new modernity," in *Theory, culture & society*. London, Newbury Park, New Delhi: Sage Publications, 1992.

[17] U. Beck, *World at risk*. Cambridge: Polity Press, 2009.

[18] M. Shimizu, A. L. Clark, *Nexus of Resilience and Public Policy in a Modern Risk Society*. Singapore: Springer Singapore, 2019. doi: 10.1007/978-981-10-7362-5.

[19] T. Prior, J. Hagmann, "Measuring resilience: methodological and political challenges of a trend security concept," *Journal of Risk Research*, vol. 17, no. 3, pp. 281–298, 2014, doi: 10.1080/13669877.2013.808686.

[20] C. Fjäder, "The nation-state, national security and resilience in the age of globalisation," Resilience, vol. 2, no. 2, pp. 114–129, 2014, doi: 10.1080/21693293.2014.914771.

[21] I. Linkov, A. Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks*, A. Kott, I. Linkov, Eds. Cham: Springer International Publishing, 2019, pp. 1–25. doi: 10.1007/978-3-319-77492-3_1.

[22] D. A. Sepúlveda Estay, R. Sahay, M. B. Barfod, C. D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Computers & Security*, vol. 97, 2020, doi: 10.1016/j.cose.2020.101996.

[23] K. Hausken, "Cyber resilience in firms, organizations and societies," *Internet of Things*, vol. 11, 2020, doi: 10.1016/j.iot.2020.100204.

[24] E. G. Carayannis, E. Grigoroudis, S. S. Rehman, N. Samarakoon, "Ambidextrous Cybersecurity: The Seven Pillars (7Ps) of Cyber Resilience," IEEE Trans. Eng. Manage., vol. 68, no. 1, pp. 223–234, 2021, doi: 10.1109/TEM.2019.2909909.

[25] S. Walklate, R. McGarry, G. Mythen, "Searching for Resilience: A Conceptual Excavation," *Armed Forces & Society*, vol. 40, no. 3, pp. 408–427, 2014, doi: 10.1177/0095327X12465419.

[26] A. F. K. Organski, *World politics*, 2nd ed. New York: Alfred A. Knopf, 1968.

[27] J. Rowland, M. Rice, S. Shenoi, "The anatomy of a cyber power," *International Journal of Critical Infrastructure Protection*, vol. 7, no. 1, pp. 3–11, 2014, doi: 10.1016/j.ijcip.2014.01.001.

[28] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, C. Maple, "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review," *Smart Cities*, vol. 3, no. 3, pp. 894–927, 2020, doi: 10.3390/ smartcities3030046.

[29] A. Vespignani, "The fragility of interdependency," *Nature*, vol. 464, no. 7291, pp. 984–985, 2010, doi: 10.1038/464984a.

[30] H.M. Government, "National Cyber Strategy 2022," [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1040805/National_Cyber_Strategy_-_FINAL_VERSION.pdf. [Accessed: May 5, 2023].

[31] M. Flournoy, M. Sulmeyer, "Battlefield Internet," *Foreign Affairs*, vol. 97, no. 5, pp. 40–46, 2018.

[32] J. Voo, I. Hemani, S. Jones, D. Winnona, D. Cassidy, et al., "National Cyber Power Index 2020," [Online]. Available: https://www.belfercenter.org/publication/national-cyber-power-index-2020. [Accessed: Dec. 10, 2021].

[33] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen, A. Kott, "Resilience metrics for cyber systems," *Environ Syst Decis*, vol. 33, no. 4, pp. 471–476, 2013, doi: 10.1007/s10669-013-9485-y.