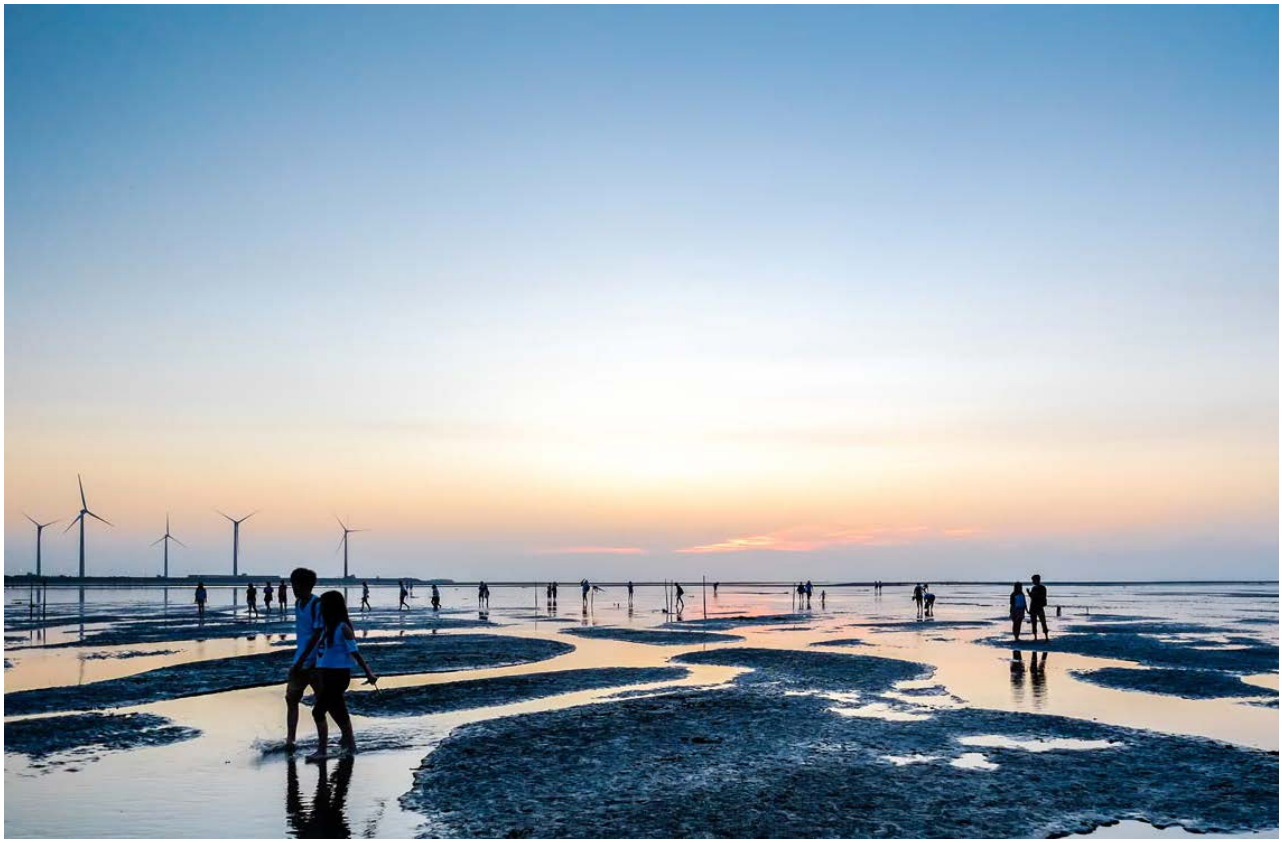
THE RESILIENCE SHIFT

Engineering Resilient Urban Cyber Landscapes

Agenda Setting Scoping Studies Summary Report



Drafted by Martijn Neef, Hanneke Duijnhoven, Anna Herder, Tom van Schie

15/06/2017

Table of contents

Project Approach

The purpose of this project is to arrive at a set of guiding principles for further research into the development of urban cyber resilience. In the 12 weeks of this projects, the project has gone through three development cycles: a **foundational** phase**,** an **elaboration phase,** and a **finalisation** phase.

The first research phase was aimed at establishing the basic foundation of the exploration. Desk research in this phase was aimed at obtained a core understanding of the 'urban cyber landscape', and what is means to build *resilience* in this landscape.

Secondly, we explored the concept of *resilience* as it applies to the urban cyber landscape. We delved deeper into the details of urban cyber resilience. This was done through interviews and a workshop with a panel of topic experts that brought expertise from a wide field of disciplines.

In the workshop, the group explored the urban cyber landscape and discussed key aspects such as governance, technological developments, well- and lesser known dependencies among infrastructures, and societal developments that were catalysed by technology and connectivity. These topics were discussed through the lens of resilience engineering, and key building blocks for resilience in the urban cyber domain where formulated.

In the final phase of the project, expert views and results from case- and desk-research were compiled to create this report.

Setting the scene

Technological transition: the emergence of the urban cyber society

Our world is changing. For decades, we have anticipated the advent of the true digital society. It is hard to deny that it has arrived. Our personal and professional lives are infused with digital services, and digital services empower many societal functions. From our phones to our homes, from our work to our leisure – everything is connected, digitised, online and everywhere. It is now hard to imagine a world without digital networks, online services and other 'cyber' facilities – even more so if we consider the digital networks that are invisible to most, but critical to the functioning of the urban landscape, in particular when it comes to critical infrastructures: financial systems, government systems, industrial control systems, health information systems and so on. The increasing reliance on digital networks is part of an irreversible transformation: 'cyber systems' are no longer a mere auxiliary ingredient, but rather an extra fundamental layer in the complex foundation of our cities. With this extra layer, the urban cyber society is now a fact, and we need to learn to take advantage of its immense potential, and harness its vulnerabilities.

In this report, we adopt a 'sociology of technology' perspective (cf. Geels, 2002. From this perspective, societal functionalities are achieved by so-called socio-technological configurations of interlinked physical artefacts, organisations, natural resources, scientific elements and legislative artefacts (Geels, 2002). Technological transitions, then, consist of the replacement of a sociotechnical configuration by a new configuration. The emergence of the urban cyber society can be seen as such a reconfiguration. However, this process of reconfiguration has not occurred overnight. Processes of digitization and automation are developments that have been taking place for many decades. Since the age of industrialization, cities have been built up by continuously adding new systems onto existing infrastructures, and by increasingly automating and digitizing the control of such infrastructures. The result is an amalgamation of tangled layered networks (cf. Woods) consisting of interwoven and mutually dependent systems that are difficult to manage and make resilient. Without a clear frame of reference, it is difficult to sense what is going on, and respond effectively.

If we want to increase resilience in urban cyber landscapes we need to recognize that this is a wicked problem, with a broad array of stakeholders and interests involved, and intricate linkages between human agency, physical elements, technology, digital systems, institutional and legal arrangements, multiple interests and organisations, etc. It does not suffice to focus on one of those elements alone when thinking about (re)engineering resilience into the system.

Cyber in the urban context

To fully grasp the fundamental changes of the emergence of the digital society it is important to highlight some of the main technological developments that make up this urban cyber landscape:

- Increasingly, critical infrastructures rely on the correct and undisturbed functioning of **Industrial Control Systems** (ICS); the control systems that are in place to monitor and control physical processes. ICS have gradually transformed into open, networked and publicly connected systems (Luiijf & Te Paske, 2015). This transformation introduces a wide array of benefits for CI operators but at the same time, there are significant cybersecurity risks involved. ICS and the processes they monitor and control are increasingly vulnerable for cyber threats such as malware, hacking, or other deliberate network disruptions (Luiijf & Te Paske, 2015).

- The internet is increasingly becoming a core foundation of our everyday lives. Without realising it, ICT have permeated our daily lives. **The Internet of Things** (IoT) has a significant influence on how we live today and how we will live tomorrow. Generally, "IoT refers to the networked interconnection of everyday objects which are often equipped with ubiquitous intelligence" (Xia, et al. 2012: 1101). Because we are generally unaware of how much we use such technology, we do not anticipate or cope well with its failure. It is striking how quickly people have unlearnt how to live without mobile communication or other smart devices.

- The Internet of Things does not just operate consumer smart devices, but is also linked to what is broadly referred to as **'smart city'** innovations. Through (real-time) monitoring sensors, surveillance cameras, actuators, vehicles and other devices, data is generated that support increasing efficiency of services in a wide variety of domains such as, energy management, water management, traffic management, healthcare, home automation industrial automation and much more (Zanella et al., 2014). Technology aside, the label 'smart city' reflects a paradigm in urban development in which values such as economic growth, sustainability, liveability, safety and security are paramount. The pursuit of these values is clearly supported by technological innovation, but it also requires social innovation.

- With ever-increasing computational power, data-storage capacity and networking capabilities, computer systems are acquiring new functionalities at an enormous pace. We are seeing computer systems performing new responsibilities, with more autonomy and proficiency than ever before. In the urban realm, there are many instances of **autonomous systems**. Examples are autonomous traffic-systems, smart energy grids, sensor networks for pollution monitoring, noise monitoring, camera surveillance and crowd sensing. Even more futuristic developments, such as autonomous vehicles and robotic companions are now within reach and will impact the urban environment.

- Another major transition that ride the waves of digitalisation is the widespread rise of 'electronic governance', or **e-governance** for short (Palvia & Sharma, 2007). E-governance

refers to application of digital systems to implement government services. The widespread availability of the internet has enabled new e-governance functionalities, such as personalised communication, online voting and community counsel appeals and open urban data dissemination. Such developments have not only facilitated and accelerated government functions, but have had an influence on governance itself. E-governance systems make it easier for citizen and businesses to engage with city agencies and provide direct feedback on initiatives and events and can be seen as an important stepping stone towards more direct democracy and shared responsibility.

On resilience

For this scoping study we have reviewed resilience conceptualisations and approaches in scientific literature as well as practical and policy documents. Our starting point has been literature that specifically addresses ‘cyber resilience’ and ‘critical infrastructure resilience’. In addition, we reviewed academic literature on ‘resilience engineering’. In this section we will highlight the main findings of this literature review.

Cybersecurity and resilience

Cyber is a growing field of interest both in research and in business and government. The realisation that cyber is everywhere and that cyber threats are quickly evolving and difficult to manage leads to a broad body of publications about cybersecurity and increasingly also about cyber resilience. Although still dominated by technically-oriented approaches, the field is adopting more and more holistic views on cybersecurity and resilience that include human and organisational aspects as well. This reflects the recognition that cyber is more than the technical ICT systems or data flows.

When looking at approaches to cyber resilience as developed in the business community or within (national) cybersecurity strategies and policy, it becomes clear that they are not very (theoretically) advanced. What these approaches have in common is that they mainly aim to create awareness among business organisations across the globe about the importance of building cyber capabilities from a holistic management perspective. Looking at the operationalisation of resilience in such approaches, it becomes clear that what these publications are generally proposing is a dedicated cyber risk management or business continuity management approach (including company-wide awareness and leadership uptake). Although there is much to say for advanced risk management, in particular when it comes to cyber challenges, these approaches do not offer much concrete insights or suggestions when it comes to ‘engineering’ resilient cyber infrastructures.

Cyber resilience within the field of cybersecurity research

Although the field of cybersecurity research is growing fast and it addresses a wide variety of topics, the focus on cyber resilience as a research interest is still in its infancy (Björck et al., 2015). Reviewing several approaches it becomes clear that each of them offers relevant aspects with regard to the operationalization of cyber resilience. Nevertheless, almost all of these approaches are designed from the perspective of a single system or organization. Even when they address the importance of multilevel approaches to the problem of cybersecurity and resilience, there is little direction how to operationalize this. Therefore, it will take effort to adopt these approaches for an urban cyber context in which cyber resilience is analysed at the system-of-systems level.

Björck et al. (2015) present fundamental ingredients for a useful definition of cyber resilience. According to them, cyber resilience refers to “the ability to continuously deliver the intended outcome despite adverse cyber events” (Björck et al., 2015: 312). The definition also emphasizes that the aim of resilience is the *continuous* delivery of intended outcomes, regardless whether this is achieved through recovery or adaptation of functions. By this, the conceptualization moves away from a traditional cybersecurity perspective that aims for systems to be fail-safe, towards an approach whereby systems are designed to be ‘safe-to-fail’ (Björck et al., 2015: 313).

Bodeau & Grobart (2011) combine a risk management approach with a decision-support system that provides insights into relevant engineering trade-offs. According to the authors, cyber resiliency engineering “considers (i) the ways in which an evolving set of architectural resilience practices contribute to the resilience of a set of cyber resources in light of the cyber threat, and (ii) the engineering trade-offs associated with those practices” (Bodeau & Grobart, 2011:1). The focus on engineering trade-offs helps to weigh the costs and benefits of different approaches or strategies by focusing not only on the actual costs from a measure and the improved resilience, but also weighing in other costs or benefits in terms of management, accountability, efficiency, etc. The framework maps the practices and objectives, supporting decision-makers (ranging from mission operators, cyber defenders, system engineers) to select and perform key resilience-related activities.

DiMase et al., (2015) argue that approaching cyber physical system security through the lens of resilience will overcome some of the limitations that traditional cybersecurity or risk management approaches have. Whereas traditional risk assessment focuses on the combination of threat, likelihood and consequences, this approach falls short when applied to cyber risks because it is difficult to clearly identify threats, assess vulnerabilities or quantifying consequences (DiMase, 2015: 292). The authors present a Cyber Physical Systems Security framework (CPSS) that emphasizes the objective of continued functionality of critical services that are provided by cyber infrastructure. The CPSS is provided as a scorecard tool that facilitates analysis and decision-support at the level of an a cyber-physical system.

Linkov et al. (2013) observe that federal/government agencies fail to produce useful cyber metrics and propose to apply a resilience matrix framework developed in the context of critical infrastructures to cyber systems. The matrix combines four phases (plan/prepare for; absorb; recover from; adapt to) with four areas (physical, information, cognitive, social) and suggests a direction for generating metrics. There are no generic metrics due to the diversity of systems. For each of the cells in the matrix, technical experts and stakeholders associated with the specific system need to develop and generate specific measures (either quantitative or qualitative).

(Cyber) Supply chain resilience and cyber-physical systems

Another area of interest that has emerged in relation to cyber resilience is the study of supply chain resilience. It is increasingly recognized that there is value in approaching cybersecurity or resilience

as a supply chain problem (recognizing the ICT dependencies between different partners and the vulnerability of the weakest link) (e.g. Boyes, 2015; Khan & Sepúlveda Estay, 2015). The partners (elements/links) in a chain are dependent upon one another and they share a common “dominant chain problem” (Grijpink 2010). None of the chain partners is able to solve the problem on its own and only by effectively cooperating can the chain partners prevent systematic failure in their own organisation or the entire chain. In the cyber domain supply chains can be characterized as complex chains that have a nodal or networked structure. Increasing digitisation causes production/business processes and information services to become more and more interlinked and it is not uncommon for multiple information chains to be required to effectively operate a single supply or value chain (Van Ruijven & Keijser, 2017). The complexity and variety of cyber supply chains limit the options for a uniform approach towards cyber supply chain resilience. Measures and good practices are not easily duplicated but need to be translated for each specific case.

Critical infrastructure resilience

Critical Infrastructures are generally defined as those products, services and underlying processes that, should they fail, have the potential of causing serious societal disruptions. Due to their networked character and mutual dependencies failures in one part of the network of critical infrastructures can cause problems in other parts of the network, potentially causing cascading impact across society that is difficult to predict. Although in most countries, critical infrastructures are defined at the national level, they have a great significance for urban areas or cities as well since that is the level where most of the impact – should they fail – is experienced.

When it comes to the field of Critical Infrastructure research, it has traditionally focused on the protection and reliability of infrastructure systems in light of different causes of disturbances (threats). Recently, a shift can be observed from a focus on the protection of critical infrastructures towards a focus on critical infrastructure resilience (Alsubaie et al., 2015).

Definitions of critical infrastructure resilience vary and are usually inspired by the use of the term resilience in other disciplines (Alsubaie et al., 2015; Bach, et al., 2013). Precise definitions aside, the actual conceptualization of resilience is generally related to the reliability and robustness of the system.

When it comes to resilience analysis, several distinguishing approaches can be identified across the domain of critical infrastructures. Alsubaie et al. (2015) present a literature review of 19 approaches towards CI resilience. They distinguish between structural, performance-based and hybrid approaches (Alsubaie et al, 2015:45). In similar vein, Vugrin (2016) distinguishes between two broad categories of instruments for critical infrastructure resilience assessment: attribute-based approaches and performance-based approaches.

Attribute-based approaches

Attribute-based approaches aim to identify key properties or core characteristics of a system that contribute to its resilience. There is no widely accepted list of resilience attributes, but they often include attributes such as robustness, redundancy, resourcefulness, adaptability. These attribute-based approaches usually involve a qualitative (or semi-quantitative) assessment of the degree to which the system demonstrates such attributes. According to Vugrin (2016), the benefit of this type of approach is that it is less time- or resource intensive. These approaches, however cannot really predict how resilient the system will be for future (unknown) disruptions and rely heavily on qualitative, subjective assessments. Often, these approaches have a practical orientation and are meant to be used by infrastructure operators and governmental agents to assess the resilience of the systems under their responsibility.

Performance-based approaches

Performance-based approaches generally aim to quantitatively measure the degree of resilience of a system by measuring the performance level of the system in case of a specified disruption (Vugrin, 2016). Resilience is then presented as a “time dependent ratio of recovery over loss” (Barker et al., 2013) or a slightly different but similar equation. A benefit of such approaches is that they are more useful for comparative analyses (bench-marks) because they rely less on qualitative, subjective assessment (Vurgin, 2016). Limitations are that such approaches usually require a vast amount of data and complex (computational) modelling which is generally more time- and resource intensive. More importantly, the outcome of this type of resilience assessment does not offer much explanatory information about why the system is more or less resilient. These complex models require a lot of knowledge about a system, but the actual calculation of resilience is a black box that does not contribute to a better *understanding* of resilience. The scientific orientation and high requirements in terms of data and expertise generally makes these approaches less suitable for practical application in an operational context.

Resilience engineering

In the previous sections, it becomes clear that there are many approaches towards cyber resilience or critical infrastructure resilience that offer interesting ideas and relevant insights. Yet most of these approaches do not fully meet the challenge of engineering resilience in urban cyber landscapes (representing a complex, multilevel, multi-stakeholder context). The conceptualizations of resilience as developed within the Resilience Engineering (RE) community (based on the work Woods (2015; 2016) and Hollnagel (2012), among others) may offer part of the solution to address these limitations because this field is specifically concerned with opening up the ‘black-box’ of complex systems and understanding where its boundaries are and what the adaptive capacity constitutes (thereby having the potential to provide concrete insights to decision-makers about how to enhance resilience). In particular, the conceptualisation of ‘resilience as graceful extensibility’ as developed within the RE community offers relevant (conceptual insights).

Resilience as graceful extensibility

This perspective focuses on “how a system extends performance, or brings extra adaptive capacity to bear, when surprise events challenge its boundaries” (Woods, 2015; 2016). The main idea behind this conceptualization is that every system has a finite amount of resources and is faced with the inherent variability of its environment and thereby has a limited ‘envelope of performance’ or capacity under normal (albeit dynamic) circumstances. The precise location of boundaries of the system are dynamic due to the continuous adaptation to the dynamic context in which the system operates. When the system reaches the boundaries of performance due to surprise events (or when the adaptive capacity saturates) the system is in danger of collapsing.

Graceful extensibility, according to Woods, is found in the “capabilities to anticipate bottlenecks ahead, to learn about the changing shape of disturbances/challenges prior to acute events, and possess the readiness-to-respond to meet new challenges” (Woods, 2016). Systems with low graceful extensibility sooner reach the limits of their ability to respond and adapt to challenges, leading to cascade of disturbances. As such, a system with high graceful extensibility has the possibility to activate and mobilize additional resources or modify how the adaptive capacity is used and can extend performance across the boundaries by entering a new ‘regime of performance’ (Woods, 2016). With low graceful extensibility, systems exhaust their ability to respond as challenges grow and cascade. As the ability to continue to respond declines in the face of growing demands, systems with low graceful extensibility risk a sudden collapse in performance. Resilience management in this conceptualization aims to build, sustain, and adjust graceful extensibility. It aims to identify what specific architectural properties contribute to the capacity of systems to continue adapting to surprises under dynamic and evolving conditions (i.e. to graceful extensibility).

Conclusions

The dominant approaches to cyber resilience and critical infrastructure resilience have a rather narrow interpretation of resilience, for instance as the ratio of loss and recovery in the face of a disturbance or as a variation on traditional risk management. The performance-based approaches do not provide pointers for governance of resilience. Other approaches provide lists of attributes of resilience that can give direction as to what type of capacities a system should strive for, but these are rather subjective and do not guarantee that it constitutes sustainable capacity in changing circumstances. What is more, most of these approaches are targeting single organizations or infrastructure systems, while it is important to address resilience at the level of the network (system of systems) and even at the city (societal) level. We argue that some of the limitations may be addressed by embracing some of the insights from the theoretically advanced field of Resilience Engineering, in particular with regard to the conceptualization of resilience. This field specifically aims to gain an understanding of how socio-technical systems function and aim to identify how to achieve sustained adaptability. However, the literature in the Resilience Engineering community tends to focus on relatively closed systems and it does not explicitly address resilience of networks of systems at a society or intersectoral level. The application of a resilience engineering perspective on a fuzzy

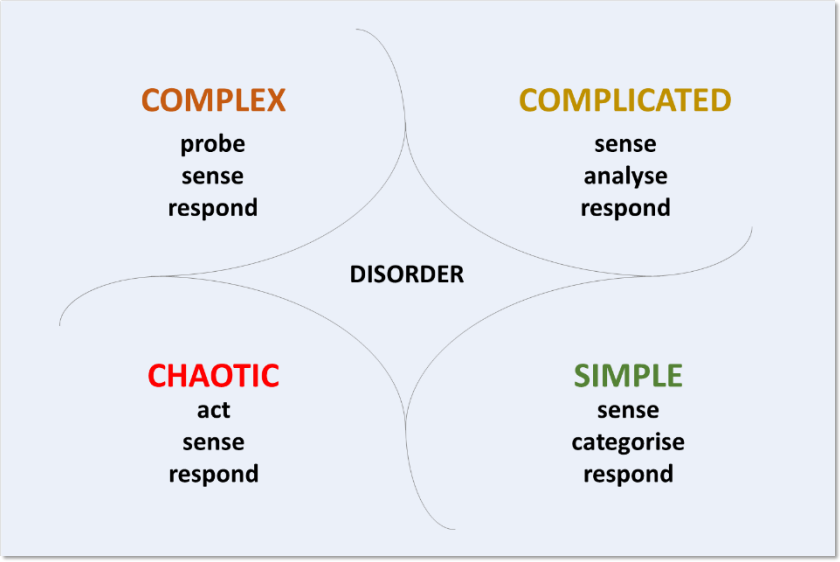
system such as a city is relatively new and poses a range of challenges related to the scope and demarcation of what the adaptive capacity of ‘a system’ means. However, this seems to be a logical and necessary step if we want to contribute to the resilience enhancement of urban landscapes.

From theory to practice

Disentangling a complex decision-making landscape

A major recurring theme in this field is the fact that the ongoing digitalisation adds to the already complex nature of our societies. We might perceive that novel digital services simplify our life, but from an infrastructure and governance perspective, the ubiquitous permeation of digital networks and services make it even harder to understand how urban environments function. Digital networks create new communication pathways, enable new societal functions, change information ownership and control paradigms, and so forth.

Looking at the 'Cynefin framework' (Snowden & Boone, 2007), it can be concluded that the cyber landscape is complex. To be precise*: the landscape is complex from a decision-making perspective*. Decision-making in this domain is explorative and not well-grounded in established practices. The outcomes of actions are often unknown or ill-understood, and there is a badly defined decision-making context that lacks substantial evidence about future events. The many 'unknowns' make it difficult to make decisions, or even build a common view among stakeholder communities.



There are two major pathways for decision-makers to take: 1) Embrace the complexity of the urban cyber landscape and build the competence to make sensible decisions under such circumstances, 2) Obtain a better decision making position by removing complexity, and effectively moving from the 'complex' to the 'complicated' state where more traditional decision making rules apply.

Resilience Engineering literature offers four key areas of capability development that would contribute here (Hollnagel, 2015): **Anticipation**, **Monitoring**, **Response**, and **Learning**. It is important that these capabilities are developed in tandem, be intrinsically linked and jointly constitute a foundation upon which decision-makers obtain a better-informed position. This requires a strong, sustainable and widely support **strategy**. Capabilities in this area ensure leadership, resources, responsibility and explicit objectives. The '**linking'** provides for the necessary feed-forward and feed-backward loops that are characteristic of systems that are resilient.

Subsequent research programs on this topic should further delve into effective capacity development for urban cyber resilience, and should aim to build up practical knowledge by which cities can develop their own, fitting set of capacities.

Urban cyber resilience in practice

Cities across the world exchange knowledge and practices about increasing resilience in the face of a multitude of challenges. However, the digital transformations are – as of yet – underemphasized. This is due to a widespread lack of understanding about the vulnerabilities of a digitally-reliant city, and, consequently, an under-appreciation of this topic. Cities are struggling to take steps when it comes to their cyber resilience. Cyber is often not considered a ‘city’ issue, but rather a business or national issue. However the impact of cyber vulnerabilities can be extensive at the level of a city and therefore it should be considered as part of urban resilience enhancement strategies.

An illustration – Rotterdam cyber resilience strategy

The city of Rotterdam participates in the Rockefeller 100 Resilient Cities programme and is one of the few cities to explicitly address cyber resilience in her strategy. The strategy emphasizes important topics that require attention if Rotterdam wants to transform to a true digital city. These topics include awareness and education, cyber resilience in the city and port and the need to assess and strengthen the resilience of its critical infrastructures.

The implementation of the Rotterdam Resilient strategy is a year underway. Many of the current activities are bottom-up collaborations between active citizens, small business and the resilience strategy team at the city council. However, to truly embed the resilience thinking within the city management and beyond remains a difficult challenge. When it comes to resilience in the context of a city, there are many stakeholders with different interests and goals and these do not necessarily require the same actions. In fact, what is ‘resilient’ in terms of sustainability against climate change, may interfere with ‘resilience’ in economic sense. Similarly, a measure that increases the adaptive capacity of the energy infrastructure does not necessarily correspond with increased adaptivity of financial or transportation services. Therefore, the governance of resilience is a crucial element to bring a strategy into practice.

Governance of the urban cyber landscape

Urban Resilience is generally approached as a responsibility of the government (national or city). This makes sense because they are in charge of organizing and regulating how we live. However, when it comes to cybersecurity and resilience, the government may be an important stakeholder to stimulate awareness and to a certain extent develop appropriate regulation. But there are so many more parties that have a crucial role (ICT businesses, operators, users, etc.). Given all the above, it becomes clear

that no single stakeholder is capable of addressing cyber resilience by itself. This is an issue that surpasses the level of nation states, which requires the collaboration of many organisations and institutions across the globe.

Conclusions

Ten observations

This project has rendered a myriad of observations concerning the typical urban cyber landscape. We highlight ten observation of which we feel that they need to be recognised in future work in this domain.

1. The urban landscape is more digital and connected in nature than most stakeholders realise
2. The current way of thinking about cyber resilience is very narrow in scope.
3. There are fundamental barriers for a resilience shift in the urban cyber landscape
4. There is a prevalence of sectoral approaches in ‘resilience’
5. There are little established practices for comprehensive cyber resilience creation, especially for the urban domain
6. There is a deep lack of understanding of the cyber domain by those in charge
7. There is a lacking incentive to collaborate on cross-sectoral or societal cyber resilience
8. Developments in the cyber landscape move faster than control measures can absorb
9. New emerging self-organising infrastructures that are by definition uncontrollable
10. Shifting perception on digital norms, privacy and freedom of information, especially in urban hubs

Directions for research and engineering

The greater goal of this report is to arrive at elements of interest for further research and application in engineering.

True urban cyber resilience requires a new foundation

It might be time to accept that old risk management paradigms are not sufficient anymore, and that we need to adopt novel perspectives for building resilient cities. What is needed, is a strong ‘urban cyber resilience foundation’: a thorough understanding of the implications of ‘cyber developments’ in the urban domain (e.g. opportunities, threats, trends and interactions with other domains), and a strong grasp on how societal capabilities can be directed towards a more ‘cyber resilient’ society. This foundation needs to be built upon two major avenues of research:

- Gaining a deep understanding of the urban cyber society: Phenomena, practices, trends, dependencies, vulnerabilities in the urban environment.
- Exploring ways of 'resilience building' for urban environments: Dealing with uncertainty, investing in adaptive capacity build-up, the use of evidence-based policies and interventions.

To underpin these two avenues of research, we reiterate the key conclusions from the chapters in this report.

A deep, comprehensive understanding of the domain. The increasingly complex urban landscape lacks a clear instruction or game-plan, simply because it has never been designed but it has emerged out of decades of urban development and technological progress. There is not a single actor who has a complete picture, let alone or is responsible for the system. In addition, cyber resilience is a multilevel and multi-stakeholder challenge. It is not just about the technological aspects of digitization, but it is related to the social, organizational, environmental, physical and digital realms of urban life. So, any approach to enhance urban cyber resilience should address and include all those aspects.

Cyber resilience engineering must be distinguished from common cyber-security measure development. The concept of cyber resilience receives wide attention within the business community and policy domain. These approaches generally are based on a risk management paradigm and are meant to increase awareness and create a sense of urgency among businesses and politics to focus attention on cybersecurity issues. Their value lies in the agenda-setting approach and the heightened attention for cybersecurity measures. In terms of resilience engineering, these approaches do not offer many new insights.

Focus on practical multi-level operationalisation of cyber resilience. Different approaches offer relevant definitions and methods to operationalize cyber resilience. It becomes clear that almost all of these approaches are designed from the perspective of a single system or organization. Even when they address the importance of multilevel approaches to the problem of cybersecurity and resilience, there is little direction how to operationalize this.

Emphasize the important of collaboration building across sectors and communities. Digitisation leads to the interweaving of physical production processes and information systems, creating what is called cyber-physical systems consisting of many mutually dependent processes or units. Such systems are very complex and therefore it is difficult to identify a uniform set of measures or approaches to tackle the cyber resilience challenge. Steps towards collaboration between partners is a viable starting point towards building resilience.

Understand the fundamental differences in the existing dominant types of resilience approaches. Current (dominant) approaches in the domain of critical infrastructure resilience are useful for specific purposes, but do not fully embrace the potential of a resilience perspective. Attribute-based approaches are valuable to increase awareness among stakeholders and offer organisations a means to assess their resilience activities in a qualitative manner. The downside is that the results are subjective and hard to relate to actual performance in the face of a crisis.

Performance-based approaches offer a quantitative measure for resilience that is comparable. Yet, these approaches are black-box calculations that require a lot of data and offer little actionable insights.

Operationalise graceful extensibility as a key capability in resilience engineering. Despite their conceptual and theoretical maturity, the Resilience Engineering approach to resilience is strongly embedded within organizational resilience and safety management. However, the practical application of these methods is quite limited. Furthermore, it has not yet been applied empirically to other, more complex systems or contexts. An interesting next step would be to operationalize the conceptualization of graceful extensibility in the context of dependent networks of a range of different critical infrastructures, with multiple stakeholders and often different or even competing interests.

Resilience Engineering should aim to reduce decision-making complexity. Resilience is built upon the capacity of a society to prepare, monitor, respond and learn, but requires that these capabilities are developed and exploited in tandem, clearly linked and explicitly bring decision-makers in the stakeholder community in a better-informed position. There should be an ongoing endeavour to reduce the complexity of the decision-making landscape, and effectively move decision-making to a ‘complicated’, not complex state.

In conclusion: It is important to recognise that urban resilience is not a neutral endeavour. It is important to decide and agree across stakeholders what the objectives are (whether they be sustainability, liveability, economic prosperity, security) in order to select and prioritize areas of action. Governance is a key factor, even more so than the assessment and enhancement of cyber resilience of critical infrastructures.

References

1. Alsubaie, A., Alutaibi, K., & Martí, J. (2015). Resilience Assessment of Interdependent Critical Infrastructure. In *International Conference on Critical Information Infrastructures Security* (pp. 43–55). Springer.

2. Bach, C., Bouchon, S., Fekete, A., Birkmann, J., & Serre, D. (2013). Adding value to critical infrastructure research and disaster risk management: the resilience concept. *SAPI EN.S.Surveys and Perspectives Integrating Environment and Society*, (6.1).

3. Barker, K., Ramirez-Marquez, J. E., & Rocco, C. M. (2013). Resilience-based network component importance measures. *Reliability* Engineering & System Safety, 117, 89–97. https://doi.org/http://dx.doi.org/10.1016/j.ress.2013.03.012

4. Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience–Fundamentals for a Definition. In *New Contributions in Information Systems and Technologies* (pp. 311-316). Springer International Publishing.

5. Bodeau, D., & Graubart, R. (2011). Cyber resiliency engineering framework. *MTR110237, MITRE Corporation*.

6. Boyes, H. (2015). Cybersecurity and Cyber-Resilient Supply Chains. *Technology Innovation Management Review*, *5*(4), 28.

7. DiMase, D., Collier, Z. A., Heffner, K., & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, *35*(2), 291-300.

8. Geels, F.W. (2002) Technological transitions as evolutionary reconfiguration processes: a multi-level perspective and a case-study. *Research Policy,* 31(2002): 1257-1274*.*

9. Grijpink, J.H.A.M. (2010) Chain Analysis for Large-scale Communication Systems: A Methodology for Information Exchange in Chains. *Journal of Chain-computerisation Information Exchange for Chain Co-operation,* 1(1): 1-32*.*

10. Hollnagel, E. (2012). *FRAM – The Functional Resonance Analysis Method*. Farnham, UK: Ashgate.

11. Hollnagel, E. (2015). *Introduction to the Resilience Analysis Grid (*RAG). A Technical Note. http://erikhollnagel.com/onewebmedia/RAG%20Outline%20V2.pdf

12. Khan, O., & Sepúlveda Estay, D. A. (2015). Supply Chain Cyber-Resilience: Creating an Agenda for Future Research. *Technology Innovation Management Review*, 5(4): 6‑12.

13. Luiijf, H. A. M., & Te Paske, B. J. (2015). *Cyber Security of Industrial Control Systems*. Den Haag: TNO. https://www.tno.nl/ics-security/

14. Palvia, S. C. J., & Sharma, S. S. (2007, June). E-government and e-governance: definitions/domain framework and status around the world. In *International Conference on E-governance* (pp. 1-12).

15. Snowden, D. J., & Boone, M. E. (2007). A leader's framework for decision making. *Harvard business review*, 85 (11): 68.

16. Van Ruijven, T. & Keijser, B. (2017) *Ketenweerbaarheid tegen cyberdreigingen. Uitganspunten, Good Practices en een stappenplan voor het vergroten van cyber-ketenweerbaarheid*. Whitepaper, februari 2017. Den Haag: TNO.

17. Vugrin, E. D. (2016). Critical Infrastructure Resilience. In IRGC (Ed.) (v. 29-07-20). Lausanne: EPFL International Risk Governance Center.

18. Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reli*ability Engineering & System Safety, 141, 5-9. doi:http://dx.doi.org/10.1016/j.ress.2015.03.018

19. Woods, D.D. (2016) Resilience as Graceful Extensibility to Overcome Brittleness. In: IRGC. *Resource Guide on Resilience* (v29-07-2016). Lausanne: EPFL International Risk Governance Center. https://www.irgc.org/wp-content/uploads/2016/04/Woods-Resilience-as-Graceful-Extensibility-to-Overcome-Brittleness-1.pdf

20. Xia, F., Yang, L. T., Wang, L., & Vinel, A. (2012). Internet of things. *International Journal of Communication Systems*, *25* (9): 1101-1102.

21. Zanella, A., Bui, N., Castellani, A., Vangelista, L. & Zorzi, M. (2014). Internet of Things for Smart Cities. *IEEE Internet of Things Journal,* 1(1): 22-32.