The Hague **Security Delta**

HSD Issue Brief 3/2014

Building Cyber Resilient Cities

From New York to New Delhi – modern cities are built on a dense jungle of wires and cables that form the indispensable infrastructures of our city life. Information and Communication Technology (ICT) forms the artery system that helps fuel economic growth and makes cities more 'smart' and livable. But this has also created new vulnerabilities. Hackers attacking critical infrastructures. Natural disasters like Hurricane Sandy leading to ICT failures with large scale cascading effects. Eliminating such threats is impossible. We can, however, develop strategies aimed at rapidly bouncing back when risks materialize. This Issue Brief looks at how cyber resilience strategies can help cities deal with risks in a hyper-connected world.

Hyper-connected cities

All corners of our cities have become reliant on ICT systems, and for many of us laptops, tablets, mobile phones, WiFi hotspots, and 'the cloud' have become indispensable assets in our daily urban lives. Innovations and the rapid spread of information and communication systems throughout our economy and society have led to tremendous advantages. One report estimates that ICT developments have generated around a third of all economic growth from 1995-2007 in EU-27 countries.[1]

Spurred by such innovations, our cities have become increasingly 'smart', using ICT to make urban areas more livable, sustainable, and vital. Cities are using cyber technologies to create growth and find solutions to challenges, for example using innovative technologies to ease traffic congestion, or developing more efficient electricity provision systems. Such 'smart cities' are built on different layers (see Figure 1). The cyber infrastructure is about more than just wires and cables, or the 'physical infrastructure'. It is as much about software, big data collection, and other 'logical network components', as well as the people that operate and use these (i.e., the 'social layer'). Smart cities are built on these three layers, using functions based on a complex web of physical and social relations.

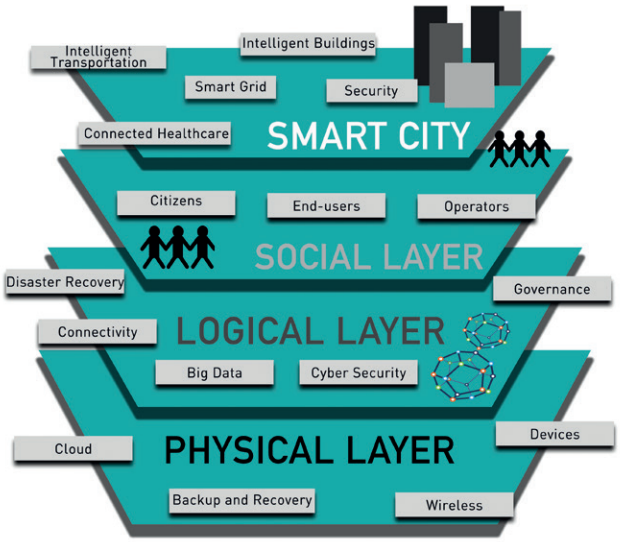

Figure 1 Smart City infrastructure (HSD)

Interdependence and hyper-risks

The proliferation of ICT innovations has allowed for a plethora of smart solutions to urban problems. But it has also led to new risks. If our communication systems break down, services which

we deem indispensable, such as emergency services or health care systems, may no longer be available. In fact, we have become so reliant on ICT that it has been dubbed a 'critical infrastructure' in itself: an asset that is essential for the normal functioning of our societies. Risks are particularly high because ICT is also an integral part of almost all other critical infrastructures. Our hospitals, water provision, and sewage systems all depend on ICT to run properly.

Such interdependencies are particularly present in our increasingly smart cities, with densely packed and overlapping critical infrastructures. Interconnections and interdependencies create huge cascading risks (see Figure 2). ICT failure can lead to massive ripple effects, causing a crisis in one sector to lead to problems in another.[2] For example, when hackers broke into the Honk Kong stock exchange's website in August 2011, trading of almost 20 percent of all stocks was suspended.[3] The fact that ICT systems depend in turn on other infrastructures, most notably energy provision, increases this vulnerability even further. More and more, we are dealing with 'hyper-risks', where a small change in one system may have extreme repercussions in another.[4]

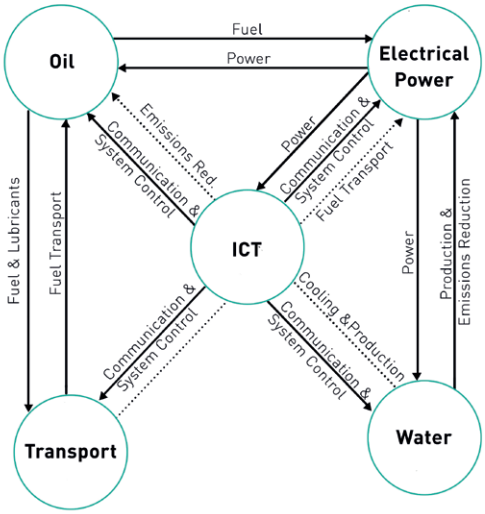

Figure 2 An example of the interdependent nature of infrastructure systems[5]

Failure of our ICT systems can be triggered by natural disasters like Hurricane Sandy, which caused ICT failures throughout New York. But they may also result from attacks by malign actors, as in the example of hackers attacking the Hong Kong stock exchange. A major security flaw in the websites of 50 cities in the Netherlands that was exposed in October 2011, which could have enabled hackers to seize privacy-sensitive information.[6]

Crises can also be triggered by unintentional events resulting from technical failures or negligence. Many Supervisory Control And Data Acquisition (SCADA) systems used to monitor and control related operations are outdated and ill-protected. And operational technology such as switches in traffic lights or sensors in sewage systems are often not designed or intended to be nodes in an expanding network of connections, forming weak links and easy targets in the network. This became painfully apparent in 2003, after a massive blackout hit the American Northeast after the alarm system failed due to a bug in the control systems. A cascade of failures rippled through a whole range of cities across the Northeast of the United States and into Canada. Eventually, 50 million people were cut off from power for up to two days. Eleven people died as a consequence, and economic losses were estimated to be around $6 billion.[7]

Cyber resilient cities

Our smart cities make use of extremely complex webs of interconnected infrastructures. In fact, there is no such thing as a comprehensive overview of all nodes, relations, and weaknesses in cyberspace. Fool-proof systems aimed at protecting cities against all threats are an illusion. As a result, strategies are shifting away from risk mitigation towards resilience.[8] The term resilience refers to "the capacity of a social system (e.g. an organization, city, or society) to proactively adapt to, and recover from, disturbances that are perceived within the system to fall outside the range of the normal and expected."[9] Applied to cities and ICT systems, cyber resilient cities can be said to limit the effects of ICT failure and have the ability to rapidly 'bounce back' after a crisis.

A resilient city would be able to contain and prevent cascade effects, for example during a major blackout. And it would limit the time needed to recover to either the pre-disaster state of the system, or to another desirable system state. In the case of a blackout this could mean restoring electricity delivery, or even creating a more efficient energy delivery system.[10] And more specifically, cyber resilience relates to both the availability, confidentiality, and integrity of (information) systems and digital information, in order to maintain continuity and effectiveness of services.[11] Cyber resilient cities ensure that ICT systems as well as their content remains available and unaltered, and that unauthorized actors will not have access.

Building a strategy

Although risks are becoming more global and interconnected, cities play an increasingly important role in protecting against these risks. As noted earlier, cities form a network of densely packed critical infrastructures, from cables and roads to sewage systems. And city authorities often own, oversee, or maintain critical infrastructures, such as local transport or sewage systems. Second, cities may be susceptible to particular threats with specific consequences. Port cities like Singapore and Rotterdam are vulnerable to floods in a way that Berlin is not. Whereas the impact of a communication systems failure in Silicon Valley would be mainly economic, in Washington DC the same failure could threaten government functions. Finally, responding adequately will also require involving local actors, from businesses to emergency responders.

Cities can thus play an important role in building cyber resilience. Good examples in recent years are cities like New York and (city-state) Singapore, that have taken the lead in developing more detailed cyber resilience strategies. These strategies aim at improving four specific resilience properties:[12]

- **Robustness:** the ability to withstand a given level of stress or demand without suffering degradation or loss of function, for example by improving physical protection against flooding.

- **Redundancy:** being able to substitute critical functions in case of a crisis. Creating buffer capacity in a system may help increase system resilience.[13] Examples include emergency power generators at important cyber nodes or better communication systems that can maintain functionality independently.
- **Resourcefulness:** the capacity to identify problems, establish priorities, and mobilize resources. This involves technical competence of cyber infrastructure as well as adequate governance and accessible social capital.
- **Rapidity:** the ability to quickly meet priorities and achieve goals. The advent and development of crises are unpredictable, making timely improvisation during crises critical to avoiding cascade effects.[14]

According to Rutger Gerritz, Director Solutions, KPN Critical Communications, **"the dependency and risks related to critical infrastructures have rapidly increased. To reduce the chance of unavailability of ICT systems and limiting potential impact, preventing system failure is key. Redundancy can be achieved by the design of the system or removing single point of failures (SPOF). Alternatively, back-up systems that run in parallel to the primary system and ensures a safe fallback level are essential. And finally, limitation of system size can help to establish upper bounds to the possible scale of disaster."**

To devise and reinforce these elements of a resilient strategy, several building blocks can be identified.

Create a multi-stakeholder platform

Cities are increasingly important in combating cyber threats. Due to increasingly global, interconnected, and complex threats, any effective resilience strategy will require a multi-level and multi-stakeholder approach. Local authorities are well placed to provide a platform to bring together key stakeholders in the functioning and restoration of cyberspace. City authorities have the political and public mandate to devise crisis strategies and they maintain extensive relations with companies, NGOs, citizens, and other levels of government.

Public-private cooperation is key, since much of our critical infrastructure has been privatized. And many critical infrastructures do not stop at the city border. Electricity grids, for example, generally span multiple countries, and sometimes even continents. Particularly in the cyber domain, boundaries are near non-existent. Creating resilience of cities will thus often mean involving actors in other cities, regions, and countries. A good example is the Multi-state Information Sharing and Analysis Centre (MS-ISAC) in the US, which bundles monitoring, early warning, and crisis response advice at different levels.[15]

To respond to threats in a resilient way may sometimes require early and aggressive action. The only defense against an attempt to attack the cyber infrastructure of a city by highly capable actors, such as large-scale terrorist organizations or foreign states, may be to disrupt enemy capabilities.[16] Such highly complex security threats can only be addressed if integrated resilience-security policies exist at different levels of government.

Assess vulnerabilities

A forum such as a multi-stakeholder platform can serve to assess vulnerabilities. This entails both the identification of city specific cyber critical infrastructure and effective assessment of the risks and means of disruption. Such an exercise could help to identify what could go wrong, and assess both likelihood and consequences.[17] Addressing these questions involves defining what elements of infrastructures and connected services are critical for the city. In other words: what functions need to be maintained during a crisis? Risk assessments are presently most common at the national level. The Dutch government, for example, provides annual national risk assessments, which also measure the impact of crises on critical infrastructure.[18] Since 2010, it regularly also performs regional risk assessments. As the impact of these risks often play out at the local level, developing city-specific risk assessments provides important insight into vulnerabilities. Due to the speed of ICT developments, such an exercise would have to be updated regularly.

Determine level of resilience

Based on a vulnerability assessment, a resilience strategy can be devised for city-specific vulnerabilities and responsibilities. This will entail trade-offs between risks and investments. What measures can be afforded, and which risks can be taken, will differ from actor to actor, and city to city. Assessing the level of upfront investment needed to balance against future risks is a notoriously difficult process, but devising a resilience strategy will require a fair assessment of investment and potential yields. For example, following hurricane Sandy, the New York City Council commissioned Siemens to perform a study on the costs involved in developing more resilient electricity grids in the long term.[19]

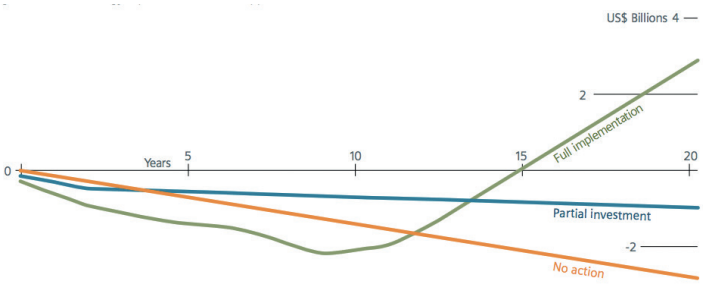

Figure 3 An economic analysis by Siemens of investments to make New York electrical grids more resilient[20]

Identify responsibilities

Drafting a resilience strategy involves asking the question: who owns the risks? Because of the multitude of stakeholders, the responsibilities of various actors need to be identified so that strategies can be implemented effectively. Here, cities can help to facilitate this discussion, and stimulate actors to take responsibility. In "A stronger, More Resilient New York", for example, the City Council drafted four recommendations to increase the resilience of the city's telecommunications infrastructure.[21] The plan includes measures to increase accountability by sharing business continuity plans, to be administered by a dedicated resilience office. In Singapore meanwhile, internet service providers are required by law to adopt cyber security measures. Also, city authorities can take

the lead in administering critical infrastructures, such as sewage and traffic systems; set standards for cyber resilience; and exercise best-practices.

Ida Haisma, Director of the Hague Security Delta (HSD), stresses that **"resilience is about much more than technology alone. Cyber resilient cities will need to focus on the human factor and procedural elements too. This requires extending research on the role of the citizen as both consumers and providers of resilience. In addition, the different roles of companies, NGOs, and cities in providing cyber resilience need to be looked at in a more systematic manner and with a perspective of long term developments."**

Putting a strategy into practice

Writing plans and devising strategies is one thing, putting these into practice is quite another. Resilience is much more than plans and technology. It requires expertise, practice, and training. Singapore's Master Plan, for example, details measures to strengthen communication during crises, and to stimulate growth of security expertise.[22] It also includes plans for new cross-sector exercises to improve the overall resilience of infrastructure and services. Such efforts are a 'sine qua non' for any effective resilience strategy.

Fill in the blind spots

Cyber resilience literature and policies remain patchy. In concluding this Issue Brief, we list some considerations that can help to fill in the 'blind spots' and make cyber resilience strategies stronger:

- **Focus on all layers of cyberspace.** Cyber resilience encompasses both the physical, logical, and social layers (see Figure 1). To weather a large scale cyber crisis, it is as important to maintain public confidence and devise effective governance systems (i.e., societal resilience) as it is to develop back-up capacity (i.e., physical resilience).
- **Involve a broad spectrum of stakeholders.** Aim for a triple helix approach, involving citizens, private, and public parties. Furthermore, involve players at different levels, from strategic to operational.
- **Involve citizens both as consumers and providers of security.**
- Integrate policies at different levels: regional, national, and international.
- **Develop open-ended and dynamic strategies.** The triggers and development of crises are notoriously hard to predict. An effective response will require agility and adaptability to deal with unforeseen circumstances.

Footnotes

1 Desirée van Welsum, Willem Overmeer, and Bart van Ark, *Unlocking the ICT Growth Potential in Europe: Enabling People and Businesses* (European Commission, 2014), 6.
2 Louise K. Comfort, Arjen Boin, and Chris Demchak, eds., *Designing Resilience: Preparing for Extreme Events* (Pittsburgh, PA: University of Pittsburgh Press, 2010), 6.
3 Vikram Subhedar and Alison Leung, "Hong Kong Exchange Trading Disrupted as Hackers Target Website," *Reuters*, August 10, 2011.
4 Dirk Helbing, "Globally Networked Risks and How to Respond," *Nature*, May 1, 2013, 51.
5 Based on Steven M. Rinaldi, James P. Peerenboom, and Terrence K. Kelly, "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies," *IEEE Control Systems Magazine*, December 2001.
6 *Cybersecuritybeeld Nederland CSBN-2* (The Hague: Nationaal Cyber Security Centrum, June 2012), 23.
7 JR Minkel, "The 2003 Northeast Blackout--Five Years Later," *Scientific American,* August 13, 2008.
8 Arjen Boin and Allan McConnell, "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience," *Journal of Contingencies and Crisis Management* 15, no. 1 (March 2007).
9 Comfort, Boin, and Demchak, *Designing Resilience: Preparing for Extreme Events,* 9.
10 *Risk and Responsibility in a Hyperconnected World* (World Economic Forum, June 2012).
11 *Cybersecuritybeeld Nederland CSBN-2, 10.*
12 Fran H. Norris, "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness," *American Journal of Community Psychology* 41 (2008); Stephen E. Flynn, "America the Resilient," *Foreign Affairs*, March/April 2008.
13 C.S. Holling, "Resilience and Stability of Ecological Systems," *Annual Review of Ecology and Systematics* 4, no. 1 (November 1973): 1–23.
14 Arjen Boin and Michel J.G. van Eeten, "The Resilient Organization," *Public Management Review* 15, no. 3 (2013).
15 See for instance the Multi-State Information Sharing and Analysis Center, http://msisac.cisecurity.org/.
16 For example, see Chris C. Demchak, ed., *Securing Cyberspace: A New Domain for National Security (*Washington, D.C.: Aspen Institute, 2012).
17 Stanley Kaplan and B. John Garrick, "On The Quantitative Definition of Risk," *Risk Analysis* 1, no. 1 (March 1981): 11–27.
18 See for instance http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/11/08/nationale-risicobeoordeling-2012.html
19 Arup, RPA, and Siemens, *Toolkit for Resilient Cities: Executive Summary* (San Francisco: California Academy of Sciences, 2013).
20 Ibid.
21 New York City Council, *A Stronger, More Resilient New York* (New York City Economic Development Corporation, 2013), chap. 9 – Telecommunications.
22 "Singapore Continues to Enhance Cyber Security with a Five-Year National Cyber Security Masterplan 2018" (Infocomm Development Authority of Singapore, July 24, 2013).

HSD Issue Brief 3/2014
Maarten Gehem, Willem Auping, Willem Oosterveld (HCSS)

The Hague Security Delta HSD Campus, Wilhelmina van Pruisenweg 104, 2595 AN The Hague, The Netherlands,
T +31 (0)70-3028180, info@thehaguesecuritydelta.com, www.thehaguesecuritydelta.com, @HSD_NL