A HYPERCONNECTED WORLD:

EYE ON THE PAST, THE PRESENT AND THE FUTURE

Keynote Speech CRITIS 2013

Henk Geveke, managing director Defence, Safety and Security TNO

Introduction

Good afternoon. Imagine the spot where you are right now, 'het IJ'. Any idea where you would stand, on a grey Monday morning 400 years ago. Let's say in September 1613, the year that the famous Amsterdam canals were built? Any idea?

Well, probably you would stand on deck of one of those beautiful tall ships, barks and clippers that sailed across the oceans, part of the largest merchant fleet at the time. Could have been a ship with names like the 'Bruynvisch' or the 'Groene Draeck', or a war ship named 'De Zeven Provinciën' or de 'Maecht van Enkhuyzen'. Across the water you would see shipyards, warehouses, wholesale dealers, and brokerage houses. Actually, the Central Railway station is on top of the old mooring berths.

In the 17th century this was one of the wealthiest places on earth. It was a period of rapid economic growth for the Netherlands and led to a boost in physics, health and other sciences, but also in art and literature. That's why we call it the 'Gouden eeuw' – the Golden Age. The Netherlands became the centre of world trade and we were a real superpower.

Amsterdam played a central role in the worlds trade because all information, goods and services where available in a relatively small space. The city was the gravity point of political power, growth and prosperity.

The secret of the success of the city were the sea-lanes. "Connectivity" of the 17th century was this: a busy network in the city and sea-lanes that formed the main lines through which information and goods travelled to and from the rest of the world. They were critical for the

functioning of society and they were well protected by the war ships of the Dutch Republic, de Staatse vloot.

Nowadays, we have replaced our sea-lanes with critical information infrastructures. The analogy, the similarity between the city then and the city now, between its critical infrastructures then and now, and the necessity of protection of the critical infrastructure then and now, is striking. When our cities are becoming smart cities, then they also have to be safe and secure cities. Without security, connectivity is mere illusion. Actually that is the topic of my speech.

Welcome

But first let me also welcome you at CRITIS 2013 on behalf of the host organisation TNO, the Netherlands Organisation for Applied Scientific Research.

Secondly, I would like to take the opportunity to congratulate the City of Amsterdam with the new Institute of Advanced Metropolitan Solutions -Ton Jonker was telling you about- that will be here soon, and I congratulate the TU Delft, Wageningen UR en MIT for winning the design contest for this institute. Of course I am also happy and proud to say TNO is also partner in the winning proposal.

Today I want to say a few words about the past, the present and the future. The past, in telling you about 12,5 years in modern Dutch Critical Infrastructure Protection research. The present by looking at the hyperconnected world of today, including M2M, 'the internet of things'. And I will peek into the future: what are the R&D challenges that are coming towards us.

The past: 12,5 years of modern CIP and CIIP

Let me take you back in time again, not to the 17th century but just some 12,5 years ago. Based on a TNO study, the Netherlands government was the first nation in the world that designated the Internet as a critical infrastructure. In 2002, TNO performed a quick-scan on

critical infrastructure for the Dutch government. Twelve critical sectors and over thirty critical products and services were identified. Besides their identification, a cobweb was created which showed their dependencies.

Over the years, data about critical infrastructure failures and disruptions is systematically collected in a database. This database now holds almost 9000 serious critical infrastructure disruptions, domino – and common-mode failure effects from 150 countries, space and cyberspace. The information from the database is used in developing realistic scenarios for (inter)national exercises and our National Risk Assessment.

Insight into incidents helps us better understand dependencies and the impact of critical infrastructure disruptions. Analysis shows that at the most three to four critical sectors in a chain are affected. That's the good news. The bad news, however, is that disruptions in critical infrastructure can lead to serious consequences for the society. Luckily insight from the database also help us to identify the weak spots - where more resilience has to be created.

The present, a hyperconnected world

Which leads me to the present day. The news is full of cyber-attacks which cause hindrance, damage and undermine the trust, of people, consumers, the electronic payment systems, in the government, and in the credibility of information.

The scale is gigantic: on www.Sicherheits-Tacho.EU you can see a real-time map of 150 to 450 thousand DDoS attacks each day. And that is an underestimation. Money is an important driver for criminal behaviour on the internet. Serious money can be made by hacking data. The trade in electronically stolen credit card data is estimated to be billions of dollars. Prices for hacking services circulate on the web. Rent a hacker? 30 to 70 dollar per hour. Email spam? 10 dollar for 1 million emails.

There even seems a cyberwar going on. In the news we read about the Chinese Unit 61398, which is led by prof Zhang, a retired general of the Peoples' Liberation Army, better known with his nickname "Ugly Gorilla". From this unit, networks and accounts were hacked and sometimes tracked for years, especially in the defence and security sector. And of course Snowden-gate revealed the monstrous cyber-program of the US National Security Agency, also led by a general, Keith Alexander. I don't know his nickname but in Foreign Policy Magazine this week he was portrayed as "the Cowboy of the NSA". Gorilla's and cowboys or not, disclosure of Chines activities and NSA-documents shed light on the enormous scale and sophistication of internet surveillance.

And it is not only the internet. Our physical world is full of ICT. ICT is everywhere. The Next Web Magazine expects that in 2015 there will be 6 billion objects connected to the internet. From sewage installations, to traffic lights, to insulin pumps and pacemakers in the human body. "Resistance is futile" I would almost say.

Most of the current innovations are ICT driven and happen at a very, very quick pace. ICT brings people and, public and private organisations together in networks. Networks that create efficiency, increase productivity, and bring new business and new jobs. And we live this, we enjoy this; new milk is ordered when your fridge is empty; your car automatically calls 1-1-2 when you have a serious collision. But it has a shadow side because it leads to dependencies, vulnerabilities and new risk. Cyber security and cyber resilience are essential enablers for digitally driven innovations and for prosperity in our networked society. But, if we accept that everything gets digitally connected, then we better make sure we do it safely and secure, and that fall-back options are at hand and do work.

The future

This leads me to the future. What challenges are we facing and what actions need to be taken?

In 2050 70 % of the world population is living in cities. It could be a threat, but it is also a promise. Cities as smart cities. With smart governments, smart businesses, smart people.

Working together to achieve economic growth and a high quality of life. Thus making the city attractive, competitive and sustainable. Real-time. Online. Networked. Connected. Hyperconnected. That counts for this city Amsterdam: Smart City Amsterdam - AmSMARTerdam. Again it aims to be the gravity point of power, growth and prosperity.

But this will only be, if we take into account proper arrangements for safety and security, for protection and resilience the vital infrastructure. Smart cities are, in fact, dynamic ecosystems. That ecosystems build upon complex environments of which the underlying critical information infrastructure is not owned by a single actor, such as the government. Public and private infrastructures are connected on many places.

New technology is inserted in a continuous rhythm. Is there anybody who still has an overall view? Are we still able to identify critical hubs and spokes in our inter-dependent infrastructures? Do we know where vulnerabilities are, and where those with malicious intent can hurt us the most? The simple answer is no, no one has the overview, now one has the possibility of intervention, one has the kill and resume switch.

Part of the solution is in creating resilience at the social level. Regulation, securing privacy of citizens and economic interests of companies, and assuring business continuity of the critical infrastructure is not the only answer. We have to create trusted, public-private and good functioning communities. Continuity of critical infrastructure services is not the sole responsibility of a single organisation. It is a shared responsibility. Cooperation is key. Cooperation that matches the pace of technological developments. Cooperation that is agile and flexible.

In a hyperconnected world bi-lateral cooperation and service level agreements do no longer satisfy our security needs.
Long term projects and blueprints won't do anymore. We need to be able to learn on a daily basis. Learning by doing, from concept to implementation, in open innovative ways of working. Government, industry and science working together. Be curious about the other's perspective, accept differences but formulate a common goal and show visible commitment.

This calls for new kind of leadership. Leadership that will look beyond the boundaries of the own organisation, that will share responsibilities and take the right actions across end-to-end chains.

Our society is complex. We must dare to admit that we are not all-knowing. We must dare to experiment and to say “let us find new ways”. Combine developing and trying out new technology with the daily operations of critical infrastructure. Collect and share data methodically in the trusted community. Use that data to adjust operations, services, standards, laws and regulations.

The introduction of smart grids is a good example. The convergence of energy and telecom networks leads to a manifold of new questions. How do we monitor these networks? Under which circumstances do we intervene? What will cause alarms? How to guarantee privacy? How do we achieve quality control? Who supervises the grid? Etc. Let us start today with answering these questions, develop new technology and solutions, experiment and implement during daily operations. Gather data, analyse, determine effects, develop predictive capabilities, refine, adjust direction, and plot new courses of action. So, it is not only public-private cooperation that is important. Knowledge and science play an essential role and are needed to provide a guidance and direction that is evidence based. In order to support this we need to have scientific, international programs that help bind together the Triple Helix: the government, industry and academia, universities and institutes for applied sciences. Soon, somewhere here in the city the new Institute for Advanced Metropolitan Solutions will arise as an excellent example of this triple helix cooperation.

Concluding

I come to a conclusion. I talked about the past, the present and the future. Our modern society evolves fast, ICT-driven innovations push us forward and we rely heavily on ICT for everyday’ s wellbeing. These developments started in the past, created what we face today, and will determine our future. The costs and trouble of discontinuity and disruptions in our critical information infrastructure can be huge. We must be prepared to take new directions to protect them.

One last look at the location where we are today. I started out by talking about the Dutch Golden Age, and the central role Amsterdam and “het IJ” played. Sea-lanes were our main lines through which information and goods travelled to the rest of the world. Securing those lines was key for the success of yesterday’s city. Likewise securing todays critical infrastructures will be key to the bright promise of the smart city of the future.

I wish you all an inspiring conference!