# Insufficient Situational Awareness about Critical Infrastructures by Emergency Management

**Eric Luiijf and Marieke Klaver**
TNO Defence, Security and Safety
P.O. Box 96864, 2509 JG The Hague
The Netherlands

{eric.luiijf, marieke.klaver}@tno.nl

## ABSTRACT

*This paper discusses critical infrastructures (CI) and their dependencies, with as central theme the hypothesis that a lack of CI situational awareness and protection in emergency management operations results in unnecessary amplification of the consequences. This paper discusses the hypothesis and findings along some well-known international emergencies analysed from the perspective of the hypothesis.*

*Societies are increasingly dependent on a set of products and services which comprise the Critical Infrastructures (CI). CI are those assets and parts thereof which are essential for the well-functioning of critical societal functions, including the supply chain, health, safety, security, economy or social well-being of people (European Commission, 2008). Failing CI may have serious consequences to citizens and society as a whole. One would expect that emergency management functions have full situational awareness of the state of CI during a major incident and of the responsibilities to protect them. CI (public and private) are important to emergency management and disaster response in three ways: for one's own operations inside the incident area including one's own C3I structure as well as for one's static command infrastructure, for the population in the incident area, and for critical infrastructure services to the area around the incident area.*

*Empirical evidence from reports about emergencies and disasters in various regions in the world shows that situational awareness and caretaking for CI is a weak spot in emergency management unless the disruption of a CI is the emergency itself. This causes unwanted extensions of the duration and size of emergencies with more casualties, more suffering, and more damage than needed. If, however, emergency management has a proper situational awareness and takes proper care of the protection of CI, it may even help to decrease the consequences and speed up recovery. Apart from awareness-building, this paper presents several recommendations for Emergency Management.*

## 1.0 INTRODUCTION

Modern societies are increasingly dependent on a set of products and services which comprise Critical Infrastructures (CI). According to [1], a CI is defined as "*an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions*". Most nations concerned about their CI use a definition for CI which is close to this one (see e.g., [2]).

It will be clear that disrupted and destroyed CI have serious consequences to citizens and the society as a whole. Based upon their national definition, a number of nations determined what their national CI is and the critical services it delivers [2]. A common set of these critical services comprises: energy (power, gas, oil), transport (road, rail, air, shipping, pipelines, main ports), water (drinking water, sewerage), food, health services, telecommunications (fixed lines, mobile, broadcasting, internet, satellite, navigation, postal services), and financial services. Another subset of such critical functions is often clustered and organised differently per nation because of, e.g., historical and cultural reasons. These critical services include emergency response services, police, law enforcement, justice (courts, jails), and armed forces (especially when they have a homeland security or disaster response task). Some CI services are very peculiar to a nation, like e.g. water management in the Netherlands, and the defence industry and key cultural heritage objects in some other nations.

For ages, the protection and resilience of CI has been important to society, think for instance about the Roman road system and the Venetian shipping lanes. The reason that the protection of CI is now high at the political agenda of many governments is because of several paradigm shifts in CI. First of all, one can recognise the increased just-in-time stacking of critical societal services on top of each other, and the chains of linked critical services. This paradigm shift is often caused by the use of information and communication technologies (ICT). Secondly, deregulation, unbundling, and privatisation cause the majority of CI being operated by private operators with a mindset of creating revenue. Governments, if at all, have now no or only limited control over the way CI are operated, while citizens hold their government responsible for the slow recovery of CI. The latter is certainly the case during and after emergency and disaster situations. The reactions by the public after the Katrina and Rita hurricanes are a case in point.

## 2.0 CRITICAL INFRASTRUCTURE DEPENDENCIES

One of the main, not yet fully understood, risk factors to CI is the dependency of a CI on one or often more other CI or on the supply of base materials. A *dependency* is the relationship between two products or services in which one product or service is required for the generation of the other product or service. *Interdependency* is the mutual dependency of products or services [3].

Many people consider a CI dependency as an availability issue: the resource stream one critically depends on is either available or not available. As [3] outlines, dependencies are more complex. First of all, they shall be regarded as a set of qualities. When one or more qualities are outside a certain expected level, one experiences a critical dependency. For instance, when the power outlet in one’s house delivers 40 Hz, 80V AC, power is still delivered. Unfortunately, most people cannot use it. Drinking water may come out of the tap, but when biologically or chemically contaminated, it has limited use for people.

Secondly, as [3] shows the resulting effect of one or more dependencies on the delivery of the critical product or service is a complex function of the qualities. Many effects may cause the delivery of a critical product or service to be below acceptable level. On the other hand, both physical effects and measures taken, may cause a CI to be more resilient to disturbances in its dependencies than one would expect. For example: when the pumps in a drinking water distribution system fail, most customers hardly notice that for a while, as the pressure decay in the system depends on the water pressure in the system before the failure, the amount of water that is used by all customers, and the floor one is living. In case recovery is in time, many customers may have noticed only a less powerful flow of water. However, when the pressure drops below one bar, the never fully leak-free drinking water pipeline joints may have an influx of ground water. This may cause a biological and chemical contamination of the drinking water. The local administration in collaboration with the drinking water operator has to issue warnings that customers have to boil the water for some minutes before use.

Thirdly, [3] recognises that the set of CI dependencies changes with the mode of operation (see Figure 1). For instance, when an organisation enters a stressed mode of operations, e.g. due to the failure of a CI, a complete different set of CI dependencies can be recognised. Empirical evidence (e.g., from [4]) shows that CI operators and emergency management (EM) planning mostly understand and plan mitigations for disruptions of a CI one is depending upon during *normal operations*. However, it is much harder to understand and prepare for CI dependencies which occur in the non-normal modes of operations. An example is the shift in critical dependencies when the provision of electric power fails. That a back-up generator requires a fuel refill after a while, which in its turn requires a means to transport fuel which in turn requires unhampered fuel pumping services at a depot location (which in turn …), is often some levels of dependency analysis too deep for most public and private sectors to plan for.

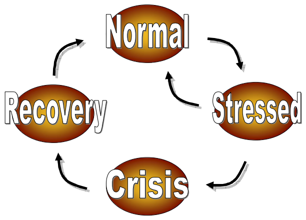

**Figure 1: Modes of CI operation**

The two aspects related to dependencies which are feared most by governments are the cascading or domino effect, and interdependencies. The first aspect is due to the potential of hurting the population and society in a hard way. The second because of the risk that CI ‘A’ in a way brings down the services provided by CI ‘B’. This in turn is required by CI ‘A’. The worry is that one is unable to recover both CI without major efforts. Empirical evidence from press reports and other public sources [5] shows that the extent of serious CI cascading is often limited to three to four layers of critical services. Moreover, the number of CI interdependencies reported in the press and publically available reports is almost non-existing.

## 3.0 EMERGENCY MANAGEMENT AND CRITICAL INFRASTRUCTURES

Without any doubt, it will be obvious that EM and disaster response functions depend on CI. EM should deal with the protection and fast recovery of the large set of CI for the following reasons:

1. sustaining and supporting the ‘static’ EM operation, by supporting e.g. command centre(s) and operational centres like police, fire-fighter, ambulance, and other emergency rescue services stations,
2. sustaining and supporting the EM operations deployed to the incident area in order to handle the emergency or disaster at hand, by e.g. delivering mobile communication services and water supply to fire fighters,
3. supporting the not (yet) evacuated population in the incident area, with essential services as e.g. drinking water, and
4. the continuation of critical services to the area that is neighbouring the incident area, for instance a power generation station in the incident area that supports an neighbouring area.

### 3.1 Hypothesis

As we track CI outages in many nations on a daily basis and collect serious information about such CI disruptions in a database [4], our empirical findings led to the formulation of the following hypothesis: ‘The effects of emergencies and disasters may have become larger than required by lack of understanding of CI, causing more suffering and damages to citizens. This is caused by emergency planning and response functions lacking sufficient awareness and understanding of CI and their dependencies. Where such awareness and understanding exists, the number of victims, suffering by population and damages may decrease.‘

## 3.2 Case studies and incidents

In [6] we discussed our initial finding about this hypothesis. That study comprised inter alia the following: the 2001 train derailment in the Baltimore tunnel, the 11/09 events and disaster response in New York, the 2002 Elbe flood response efforts, the 2005 tsunami disaster in Asia, and some local and regional emergency plans in the Netherlands and United Kingdom. A short summary of some incidents:

- In July 2001, train wagons containing chloride acid derailed in a downtown tunnel in Baltimore. Fire fighters decided to let the train burn. Unknown was that a high-pressure water mains, a set of glass fibres and a power transmission cable were routed through the same tunnel. Due to the fire the water mains burst. As a result over 70 million gallons of water flooded downtown streets and houses; the drinking water supply failed, and the fire fighters lost their water supply. The glass fibres melted and caused a noticeable world-wide slowdown on the internet and local and international telephony outages. Over 1200 buildings lost power.
- The New York World Trade Centre was a vital co-location of a multitude of CI. Amongst others, it comprised the Port Authority Emergency Management centre, the Office of Emergency Management Operations Center, electrical power substations, steam and gas distribution, metro stations, and was a key location for a number of financial institutions. After the 09/11 attacks, the emergency response actions were analysed in detail and a number of lessons were identified. The lessons identified partially lack a clear understanding of the emergency response CI dependencies, and the need for CI protection and fast recovery in future operations. For instance, the Verizon building 140 West St., contained 306.000 telephony and over 55.000 data lines from 30 operators and provided services to 34.000 customers in Lower Manhattan. A set of these lines was connected to antennas for first responders and mobile telephony at the roof of the towers and adjacent buildings. The communication capacity for the first responders was almost immediately lost due the fire and subsequent collapse of the WTC towers. Data and telephony services failed as the Verizon building became damaged by falling debris. Lines were cut and backup power was lost due to the flooding of batteries. Many of the communication back-up lines for first responders and agencies involved in disaster management were co-located with the primary circuits and failed. The remaining fixed and wireless communication for emergency response failed as police did not allow Verizon to refill the fuel tanks for their back-up power generators at two other, still operating, communication switch locations. During the recovery phase, police did not allow crews of all co-located operators to enter the closed-off area; only crews of Verizon as an obvious CI landlord were allowed.

  A second lesson was that the NYC emergency preparedness plans did not account for total neighbourhood and facility disasters including the outage of telephony of their own command centres. The emergency plans and back-up tapes with databases were inaccessible as a result of the collapse of the two WTC towers [7]. The Emergency Operations Center at WTC 7 was destroyed and had to be relocated three times during the emergency operations, something the centre was not prepared for [8].
- In August 2002, the river Elbe in Germany flooded. Failures of the EM operations were analysed in [9]. CI specific lessons were not fully understood. Some examples: emergency plans had not pre-planned that the dispatch of emergency support to the other side of the river depended on bridges that are closed for all traffic. Situational awareness of the disaster became unclear as the fixed telephony broke down due to the flooding and emergency operations relied on public communication means and overloaded – often flooded – single-point-of-failure emergency communication centres. No help was given to safeguard a power generator of a hospital from flooding. The result was the need to evacuate 300 patients somewhat later. Lacking plans for using public radio, emergency operations could only dispatch police cars to warn people.

Since that paper, we studied recent Dutch flooding and power disruption emergencies, the US emergency response to the 2006 Katrina and Rita hurricanes, and the 2007 flooding in the UK. We also studied news articles on CI disruption incidents all over the world as have been recorded in TNO’s CI outage database

[4]. Analysis showed that in many cases emergency planning and response authorities do not understand the nature of CI, their complexity and dependencies. One does not understand that certain CI in an emergency area needs protection in order to safeguard the CI supply to many just outside the area of emergency. A good example is the Walham power substation in the UK National Grid on July 23, 2007. The whole area in Gloucestershire became flooded and no authority cared for the protection of the substation until it was almost too late. The local power distribution company had no feeds from the substation and obviously had other priorities to care for. However, if the substation had failed or had to be disconnected due to the flooding, an estimated number of 500.000 customers would have lost power. This would have increased the load on EM operations, extended the duration of suffering of the population, and extended the time required for recovery even without taking into account the cascading effects to other CI (e.g., [10]).

And last, we investigated how emergency response and planning authorities in the Netherlands are aware of CI, how they prepare for CI disruptions, and how they protect CI during emergencies [11]. The results were revealing:

- Are you planning for disruption of your own CI? Reaction: “As there is a risk of flooding, our emergency response centre [for an area of over 1 million people] is located at the n$^{th}$ floor. We have emergency generators and a backup location.” … “Our generators and fuel storage is in the basement… The communication lines at our primary site need to be intact for the operation of the backup centre…”.
- “We discovered the existence of a high pressure gas pipeline when a leak was reported” …
- “Our emergency response staff is alerted by mobile phone.” Overload of the infrastructure? “A good point! We need to consider that in future.”
- “As mayor of this town I am responsible for the protection of CI. However, I do not know what CI exists in my town or passes through my area of responsibility. Can you help me?”.
- “We use Google Earth instead of the old maps. Internet was designed for resisting a nuclear attack…” (disregarding access nodes, cables and other single-point-of-failures; overloading; etc.).

Personal discussions with EM operators in other nations learned that such a lack of CI awareness occurs in other nations as well. All these national and international findings confirmed our hypothesis that emergency planning and response still need to make a big step in understanding CI and their dependencies as well as in collaborating with CI operators.

As outlined in [6], a proper understanding of CI, its dependencies and its potentials by emergency planning and response can save lives and reduce the time to recover CI in benefit of the emergency response itself and the affected population.

## 3.3 Emergency response and CI - a model

Emergency planning in most nations creates plans for a unary CI outage such as an outage of the power grid or the failing of drinking water supply. Preparation for such disruptions is even exercised. However, multiple CI disturbances and disruptions may occur due to a common mode failure (e.g., earthquake, hurricane) or due to cascading effects via dependencies. That CI may play a large role in emergency operations hardly comes to the mindset of the emergency response decision takers at the strategic, tactical and operational levels. As discussed at the start of this section, there are four main reasons why EM should take care of the protection and fast recovery of all CI during emergencies covering the whole incident response cycle (pro-action, prevention, preparation, response and recovery). We recognise nine types of dependencies (see Figure 2):

1. CI services required by the EM command and coordination centre for their operations. The required CI services include energy, fixed, mobile and internet communications, transport (personnel) and other logistics (food, drinking water).
2. CI services required by the base stations of first responders and disaster response agencies in their support of the emergency operations. The required CI services include energy, fixed, mobile and internet communications, transport (personnel), medical supplies and other logistics (food, drinking water).
3. Still operating CI services in the emergency area that are of high value for the forward emergency operations. These include drinking water, food supplies, transport, fuels, communications, and water management (e.g. pumps).
4. CI services in the emergency area itself which support non-evacuated people or people assembled in emergency shelters. These include drinking water, food and medical supplies, transport, fuels, financial infrastructure (e.g., availability of cash), law and order, and fixed, mobile and internet communications, sewage, water management (e.g. pumps).
5. CI services provided from within the neighbouring -not yet much affected- area which support the forward emergency operations and people in the disaster/emergency area, e.g., communication nodes and still operating communication base stations, hospitals, supplies, and heavy equipment.
6. CI services provided directly from the outside which are required in support of the forward emergency operations and the people in the disaster/emergency area as well as in support of recovery operations.
7. CI services provided from within the emergency area to the outside world. These include for instance generation or production nodes of power, gas, drinking water, medicines and isotopes.
8. CI nodes with a footprint within the disaster or neighbouring areas which do not directly supply services to these areas. This may include high voltage power lines and substations, gas pipelines, and communication backbones.
9. CI services provided from the outside to the neighbouring area given that some supply may be affected or disrupted due to the emergency. Failing such supply will enlarge the emergency area.

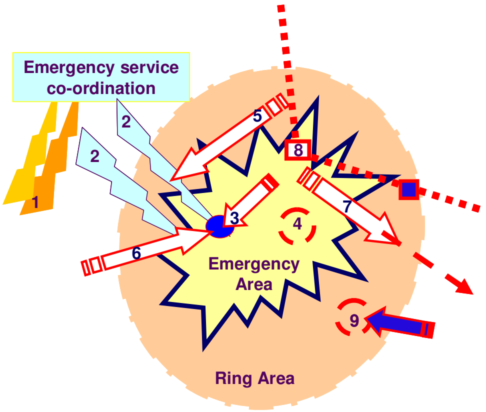

**Figure 2: CI dependencies to be considered by emergency management**

## 3.4 Pitfalls

Analysis of emergency response planning and operations in various nations -as outlined in paragraph 3.2- shows a number of pitfalls in the understanding of CI and their dependencies by EM:

- EM at various levels of response (e.g., municipal, regional) does not plan for emergencies and disasters which extend beyond one's own imagination. The command centre, and the operational coordination and back-up centres are often located at a close distance of each other. However, in case of a larger affected area, e.g. due to a common mode failure, the command and coordination centres become part of the emergency area. Optimistically, the EM response starts at these locations without a fast assessment of the reliability of required CI (dependency 1 above blurs with dependencies 3, 5 and 6). If at a later stage CI required for one's operations become unreliable, one has to relocate in the midst of the EM response phase. That will seriously hamper the effectiveness of the EM operations as the WTC and Elbe emergencies have shown [7, 8, 9]. Moreover, when the command centre is in the middle of the emergency area, there does not seem the need to deploy the operational organisation to another location. This may become a cause for conflicts, for instance about CI recovery priorities, as the strategic, tactical and operational decision-taking becomes mingled as all actors are at the same location [7, 12].
- We found that often CI for EM coordination and response centres should have at least two independent sets of communication links and power. In practice, one either forgot at all about this requirement –especially when it concerns the backup location– or over time primary and backup infrastructures became routed through the same ducts and nodes introducing a single-point-of-failure [6, 7, 11].
- EM planning for a unary CI disruption does not understand and therefore does not plan for the effects of other CI being dependent, especially when regarding their non-normal mode operations (see Figure 1). For example, CI still operating in the emergency area after may depend on power back-up generators which at regular time intervals require fuel reloads. Lack of CI awareness by emergency response operations may cause fuel transports not being organised, or -when organised by a CI operator- not being admitted to the emergency area [7] (dependencies 5, 6, 9). As a result, the deployed emergency operations may experience the breakdown of critical services and non-evacuated citizens may have to become evacuated due to the subsequent failure of critical services.
- EM often cordon off an emergency area and evacuate all people that survived the emergency. There is a need, however, to admit repair crews of CI operators. Police or military forces often block such repair crews as they lack the appropriate sticker, are of a co-located CI operator at premises of a well-known main CI operator, or are not recognised being a CI operator at all. The split of CI operators in generation companies, distribution and transport/transmission services companies does not help either. As the local forces are inflexible and communications of CI operators and EM decision layers is often not pre-arranged, an impasse may occur delaying the restore of the needed CI services [7, 8, 9, 11].
- EM operations increasingly depend on critical ICT means and information sources. For example, emergency command centres have switched to 'Google Earth' and inquire databases via Internet to find the owner of a property of e.g. hardware like earth moving equipment; and at the operations level, one often sees the use of personal cell phones. The dependence upon fixed and mobile telecommunication and internet services has become high. The lack of fully understanding ICT dependencies and the lack of training with situations where the use of the new ICT means fails may cause hampered emergency response operations [9, 11].
- EM often does not know the local nodes of national CI. In case of an emergency, one will not protect such nodes as the potential consequences are not known. National grid operators often cannot easily get access to the local EM decision-makers resulting in the risk of enlargement of the emergency at hand. The result may be an enlargement of the emergency at hand causing longer and more suffering of the population and hampering of the emergency operations. The Walham case discussed above is a case in point (dependencies 8 and 9).

- EM planning needs to understand the basics with respect to the operation of a CI and the current CI state (e.g., using a classification like normal, hampered, at disruption risk, disrupted, recovery) especially where one is not able to evacuate all people from the emergency area (dependency 4). The EM operations during the Katrina hurricane are a case in point showing what the lack of water and food supplies, sewerage, law and order may lead to.

## 4.0 CONCLUSIONS AND RECOMMENDATIONS

As outlined in this paper, our hypothesis about the lack of understanding of CI and their dependencies by EM planning and response has been confirmed by our study of various EM operations in The Netherlands and abroad, as well as by studying and discussing various EM plans with the responsible authorities.

Therefore, we recommend that EM authorities:

- Start understanding the full set of CI and their dependencies along the full incident response cycle. One approach may be to reread analysis reports of earlier disaster/emergency response operations with their mindset (triggered by this paper) focussed on the protection and fast recovery of CI. One easily identifies a set of new lessons which were overlooked or not fully understood before (e.g., we found 11 of such observed but not identified lessons in [12]). The model in Figure 2 may help to understand one's operational CI dependencies.
- Understand the full set of CI and do not only consider the most obvious ones like gas, power, water, food, health, transport and phones. CI such as law and order and financial services (e.g., ATMs, electronic payments, availability of cash) may be critical to EM operations too.
- Know the CI nodes located within their own area of responsibility and understand their dependencies on CI outside this area. This includes knowledge of the geographical location, their function within the whole infrastructures, and the CI operating companies and points of contact involved.
- Prepare for the worst and expect that one's command, coordination and response centres all will be affected by a common mode failure event. Relocation to a location at a much larger distance than currently is planned for needs to be prepared and practiced.
- Multiple CI may fail at the same time either due to common mode failure or cascading effects. Measures taken by CI operators and by one's own EM operations take into account a single CI failure.
- CI and EM operations in non-normal mode depend upon quite another set of CI as is outlined by [3] and Figure 1. EM planning should asses and plan for its CI dependencies in non-normal mode of operation.
- Increasingly, Internet and ICT are becoming a CI for EM operations. One should plan for maintaining fall-back mode operation when such means become unavailable to EM operations due to common mode failure. Sets of communication links for EM command and coordination shall be redundant and regularly checked for independence and lack of single-point-of-failure. CI operators shall not believed upfront as operational reasons may cause independent links to become rerouted through the same ducts and switches.

The reward in understanding CI and dependencies by EM can be high. Especially, when one understand the potentials of still operating and protected CI for the population in the emergency area, EM operations can become very effective. Some people entrapped underneath a collapsed house in Sri Lanka after the 2004 tsunami survived the disaster because of such an understanding of how CI operate [5].

## REFERENCES

[1] European Commission, “Council Directive 2008/114/EC, on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”, Brussels, December 8, 2008.

[2] E.M. Brunner and M. Suter, “International CIIP Handbook 2008/2009”, Center for Security Studies, ETZ Zurich, 2008.

[3] Nieuwenhuijs, A.H., Luiijf, H.A.M., Klaver M.H.A., “Modeling Critical Infrastructure Dependencies”, in: IFIP International Federation for Information Processing, Volume 290, Critical Infrastructure Protection II, eds. P. Mauricio and S. Shenoi, (Boston: Springer), October 2008, pp. 205-214, ISBN 978-0-387-88522-3.

[4] TNO, CI disruption database, version 207, April 2009 (containing over 4350 reported CI disruption events including over 1260 dependencies).

[5] Luiijf, H.A.M., Nieuwenhuijs, A.H., Klaver, M.H.A., Eeten, M. van, Cruz, E., *Empirical findings on Critical Infrastructure Dependencies in Europe*. CRITIS’2008 – 3rd International Workshop on Critical Information Infrastructures Security, October 13-15, 2008, Rome, Italy, ENEA Italian National Agency for New Technologies.

[6] Luiijf, H.A.M. and Klaver, M.H.A. (2005), ‘Critical Infrastructure Awareness required by Civil Emergency Planning’, in *Proceedings 1st IEEE Workshop on Critical Infrastructure Protection*, November 2005 Darmstadt, Germany, publ. IEEE P2426 pp 110-117. Library of Congress 2005928245, ISBN 0-7695-2426-5.

[7] Brewer, G.A., *Technology lessons learned from New Yorks City’s Response to 9/11*, The Council of New York, August 2002.

[8] NN, *Lessons learned from the World Trade Center Attack*, LI NYC Emergency Management Conference, June 2000.

[9] Von Kirchbach, H-P. et al, *Bericht der Unabhängigen Kommission der Sächsischen Staatsregierung Flutkatastrophe 2002*, 2003.

[10] http://www.environment-agency.gov.uk/static/documents/Research/infrastructurestudy_1917458.pdf and http://uk.reuters.com/article/Internal_ReutersCoUkService_3/idUKNOA62536520070726

[11] Delsasso, R. and Zomerhuis, A. (2007), *De rampenbestrijding en crisisbeheersing vitaal*, report TNO-DV 2007 S052, TNO Defensie en Veiligheid, The Hague, The Netherlands.

[12] IOOV, *Stroomstoring Haaksbergen 25-28 november 2005*, Netherlands Ministry of the Interior and Kingdom Relations. last accessed 2009-04-26: http://www.ioov.nl/contents/pages/71011/2006040306ioov_stroomstoring.pdf

## BIOGRAPHIES

*Marieke Klaver PhD* studied Mathematics at the University of Leiden. After her PhD in 1990, she joined TNO. Since 1997, Marieke takes part in TNO’s R&D efforts in information operations and information assurance, and Critical (Information) Infrastructure Protection (C(I)IP). She is involved in Dutch CIP studies like the one in support of the Dutch Strategic Council for Critical Infrastructures (SOVI), and in EU CIP projects. As programme manager, she is responsible for a TNO R&D programme on Security and Infrastructures commissioned by the Ministry of Interior and Kingdom Relations.

*Eric Luiijf M.Sc(Eng)Delft* works as Principal Consultant at the Netherlands Organisation for Applied Scientific Research TNO in the area of Defence, Security and Safety. He obtained his Masters degree in Mathematics at the Technical University Delft in 1975. His research comprises information operations and information assurance, and the protection of Critical (Information) Infrastructures, both nationally and at the European level in projects like ACIP, VITA, CI$^2$RCO, IRRIIS, EURAM, EURACOM, and DIESIS.