

Future C(I)IP challenges

A view from the financial sector

Leon Strous
De Nederlandsche Bank (DNB)
International Federation for Information
Processing (IFIP)
CRITIS 2013, Amsterdam

Agenda

- Perspective
- Setting the scene
- Challenges
- Issues

Perspective

- De Nederlandsche Bank (DNB) : Central Bank, Reserve Bank, National Bank

Compare:

- US Federal Reserve Bank (Fed), Banca d'Italia (BdI), Bundesbank (BuBa), Bank of England (BoE), Swiss National Bank (SNB)

But not:

- Deutsche Bank, First National Bank

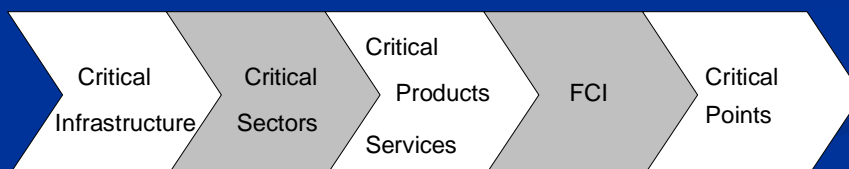
3

Perspective

- Presenter
 - IT auditor, information security
 - Current work area: business continuity, operational crisismanagement
 - Financial sector, not only DNB
- Disclaimer: the views expressed in this presentation are personal views of the presenter and do not represent the position of DNB

4

Setting the scene



5

Setting the scene

Retail payments

- Payments “over the counter” (*Toonbankbetalingsverkeer*)
 - Cash (banknotes, coins)
 - Electronic: debit card, creditcard, e-purse
- “Giral payments” (*Massaal giraal betalingsverkeer*)
 - Credit transfer, accept giro, direct debit
 - Internetbanking, mobile banking

6

Setting the scene

Wholesale payments

- *Interbank payments, large value payments*

Securities

- *Securities transactions, clearing and settlement*

7

Setting the scene

- NL population: 17 million
- NL GDP: 603,5 EUR billion in 2011

Financial services:

- 257.000 people employed (2011)
- Gross added value ~ 38 EUR billion
- Banks: balance sheet total ~ 2.500 EUR billion (Oct 2011)

8

Setting the scene

Banks:

- < 100 in total
- 3 – 5 major
- Half a dozen midsize
- Rest very small

9

Setting the scene

Netherlands	2011 # trx	Value million €	Average value
Retail - Remote	3.011.369.609	5.632.554	1.870
Retail - POS	2.495.679.600	87.381	35
Retail - Cash	466.936.000	95.314	204
Wholesale – TARGET2	8.329.575	75.003.345	9.004.462

10

Challenges

- Technology
- International context
- Interdependencies between sectors
- Expectations of stakeholders
- Scarce resources, what is critical
- Forensics
- Information sharing and analysis
- Social / behavioural aspects

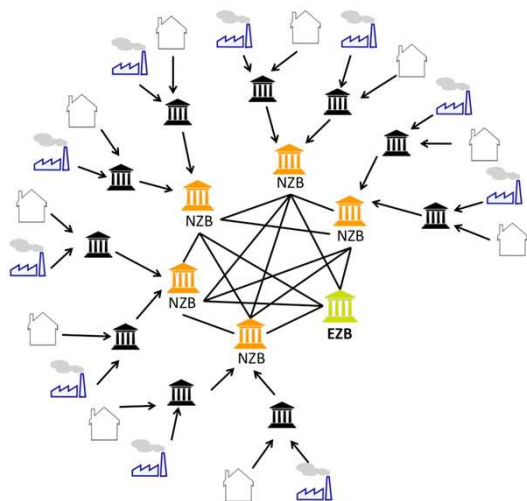
11

Technology

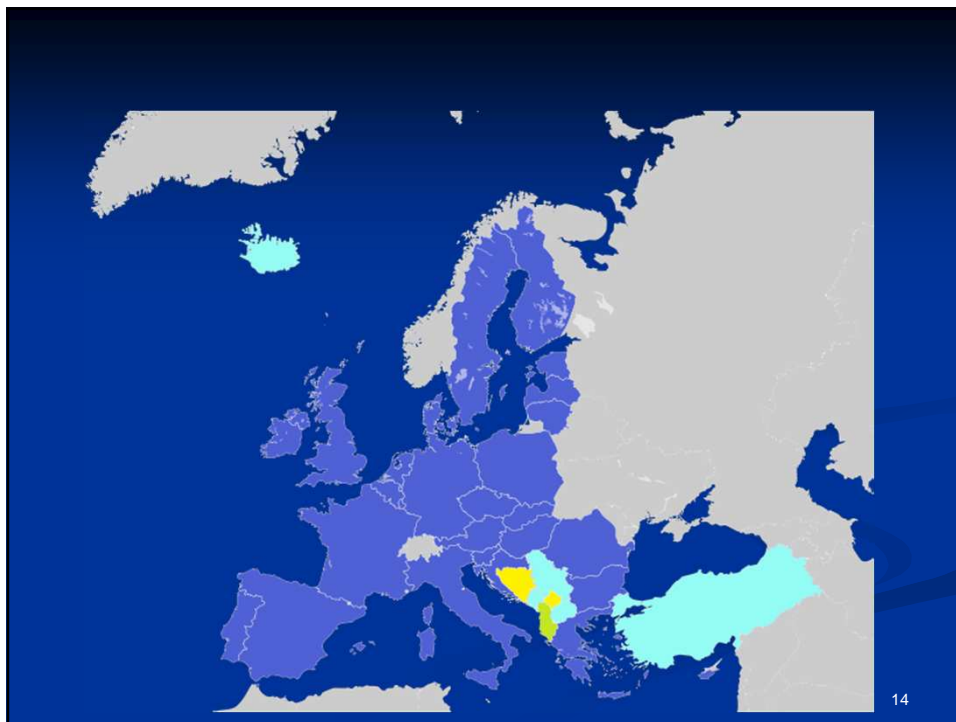
- Software and hardware errors
 - How to continue processes (eg in second site) in case of hardware or software errors
- Means and skills of attackers
 - How to keep up with attackers

12

International context



13



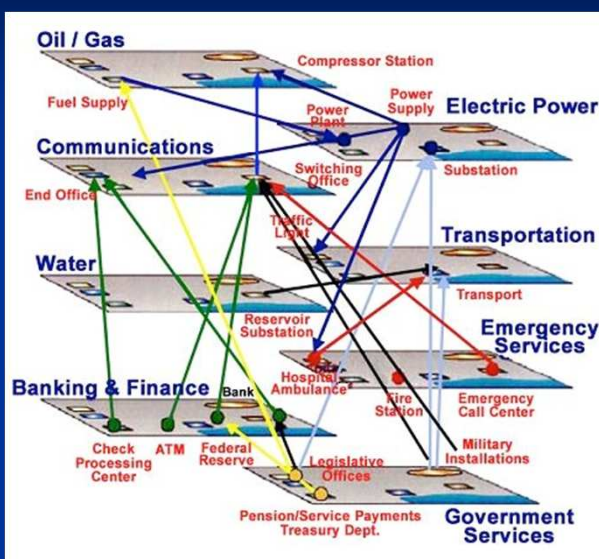
14

International context

- Risk assessment
- Measures
- Regulators and legislation
- Crisis management

15

Interdependencies sectors



16

Interdependencies sectors

- How to assess the “real” dependency and the impact in case of failure
- When is the picture of the chain complete
- How to get assurance about the measures of “the other”
- Who gets priority in worst case scenario’s

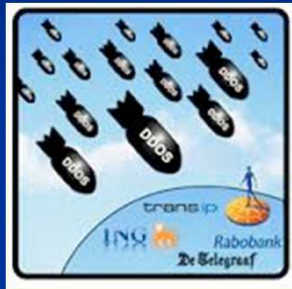
17

Expectations of stakeholders

- April and May top 4 Dutch retail banks have been hit by severe DDoS attacks
- Once a bank was hit, DDoS attacks continued with varying intensity and duration
- (note: in the same period also other sectors and companies were hit, e.g. KLM)
- DDoS coincided with other problems that caused unavailability of some services

18

Expectations of stakeholders



alle stringen .nl



19

Expectations of stakeholders

- Very strong reactions from customers, retailers, politicians
- Communication (ao role social media)
- Call for 24/7 availability, zero problems, separate internet
- Criticism on DNB and ministers

20

Expectations of stakeholders



21

Expectations of stakeholders

- *Unavailability* internet banking of individual banks
 - First attacks: unavailability of approx. 30 min/attack
 - After mitigation: unavailability of approx. 2 min
- No financial losses or integrity breaches have been reported

22

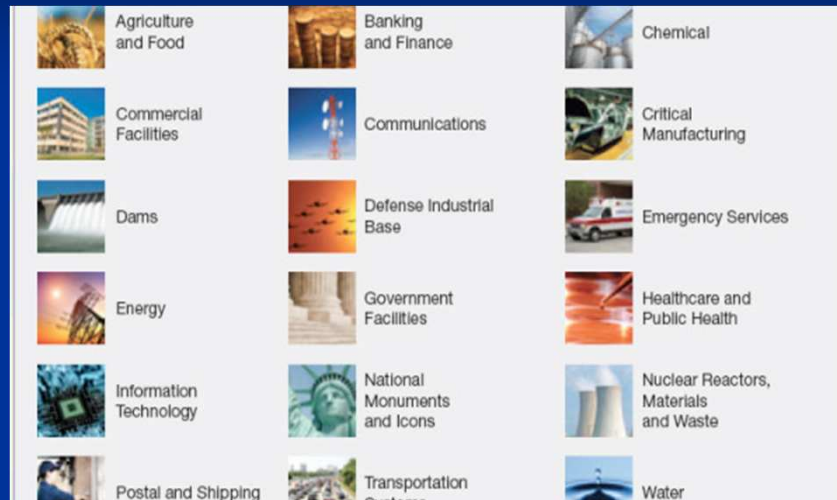


Expectations of stakeholders

Expectation management

- Are expectations realistic ?
- Communication
- Find balance between possibilities and cost
- Alternatives

Scarce resources, what is critical



25

Scarce resources, what is critical

- Expectation management
 - not everything can be protected in the same way and to the same extent
 - 10+ sectors, 30+ subsectors, X processes and services, Y assets
- Scarce resources, worst case scenario's

26

Scarce resources, what is critical

- Rethinking the approach
- Criteria
 - Which processes / services / assets
 - Critical, disaster, problem, not nice
 - Disruption of society, local / regional disruption, economic impact, social impact, lives

27

Forensics

- Cases earlier this year
- Technical means
- Training
- Trust (to share information)



28

Information sharing and analysis

- Trust mechanisms for sharing information with
 - Competitors
 - Regulators
 - Governments
 - Experts
- Regulated / self-regulated
- Development of analysis tools and mechanisms

29

Social and behavioural aspects

- <http://www.youtube.com/watch?v=F7pYHN9iC9I>

30

Issues

- Different disciplines / expertise
 - Information security
 - Business continuity
 - Physical security
 - Risk management
 - in fact all disciplines involved in developing, building and maintaining systems and processes



31

Issues

- Different forms and ways of cooperation
 - Public – public / Public – private / Private – private
 - Formal / Informal
 - Cross disciplines
 - Cross borders
 - ??

32

Thank you for your attention

Questions and discussion please

33