
From information security to cyber warfare: some paradigm shifts and research challenges
Jan van den Berg
Delft University of Technology
Faculty of Technology, Policy and Management, section of ICT

Abstract

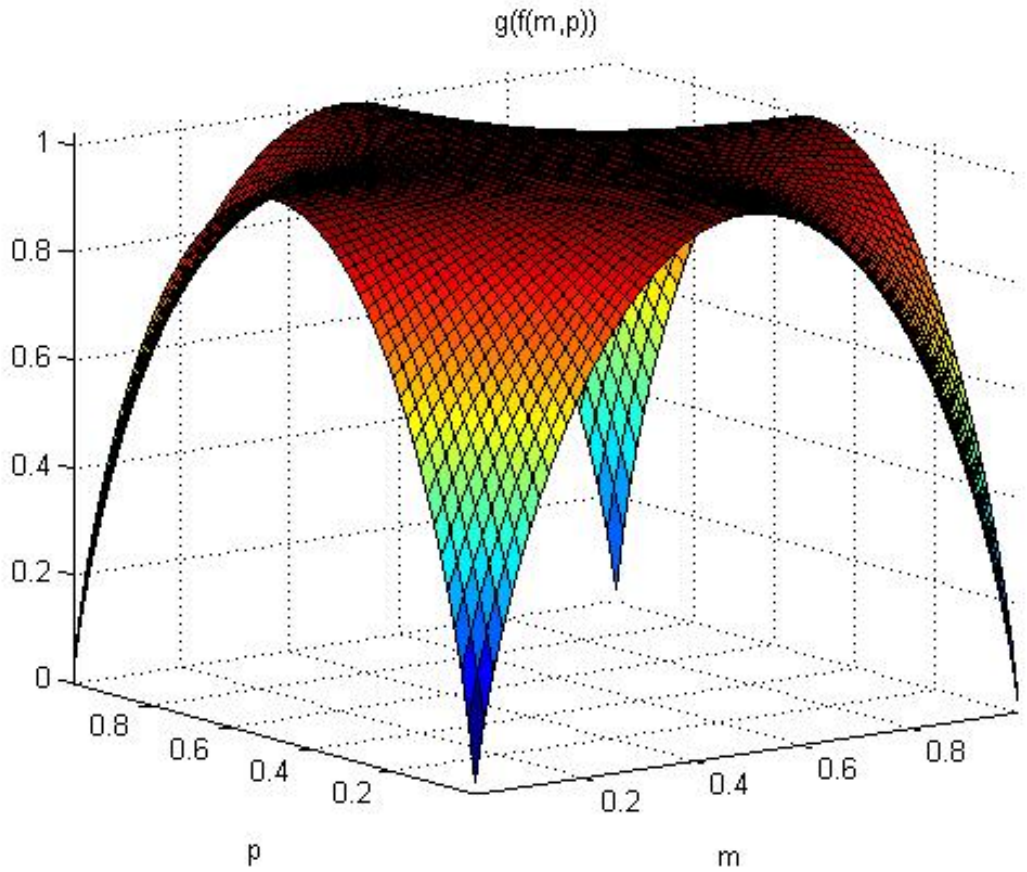
In the last two decades, classical information security has transformed into cyber security and cyber warfare. Analyzing this transformation makes us aware of the emergence of cyberspace as the 5th domain (next to land, water, air and space). Cyberspace concerns a hyper-connected dynamic world with many stakeholders in which we can act and have made our critical infrastructures highly dependent on. This can be illuminated by *several paradigm shifts having taken place* in the field.

In short, *keeping cyberspace a safe and secure domain is much more than securing information (the original goal of information security). This relates to new research challenges, which will be introduced based on an appropriate risk management framework.*

Agenda

- Appetizer
- The emergence of cyberspace as 5th domain
- Paradigm shifts
- Some research challenges
- What's in it for the WIC?
- Dessert

Entropy of a binary source generating two complemenary fuzzy events (m,1-m) and (1-m,m) with probability distribution (p, 1-p)



Nota bene:
Surface is almost everywhere strictly concave (!)

Agenda

- Appetizer
- The emergence of cyberspace as 5th domain
- Paradigm shifts
- Some research challenges
- What's in it for the WIC?
- Dessert

Information Security

BS7799 [1999: **sic!**], some citations:

- "Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected"
- "Information security is characterized here as the preservation of confidentiality, integrity, availability"
- "Information security is achieved by implementing a suitable set of controls (which could be policies, practices, procedures, organizational structures and software functions).
- These controls need to be established to ensure that the specific security objectives of the organization are met".

- So??

Cyber Security

- "is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, the term *security* implies cybersecurity" [ref]
- "concerns the measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" [ref]
- "is the collection of tools, policies, security concepts, (...) that can be used to protect the cyber environment and organization and user's assets" [ref]

- So?

Cyberspace (as socio-technical system)

- "is a time-dependent set of interconnected information systems and the human users that interact with these systems" [definition by NATO]
- is an **eco-system** according the paper "Enabling Distributed Security in Cyberspace - Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action" [definition US DHS, 2011]:
- "the cyber ecosystem comprises a variety of diverse participants – private firms, non-profits, governments, individuals, processes, and cyber devices (computers, software, and communicationstechnologies) – that interact for multiple purposes" [NATO Security Framework Manual]

- So?

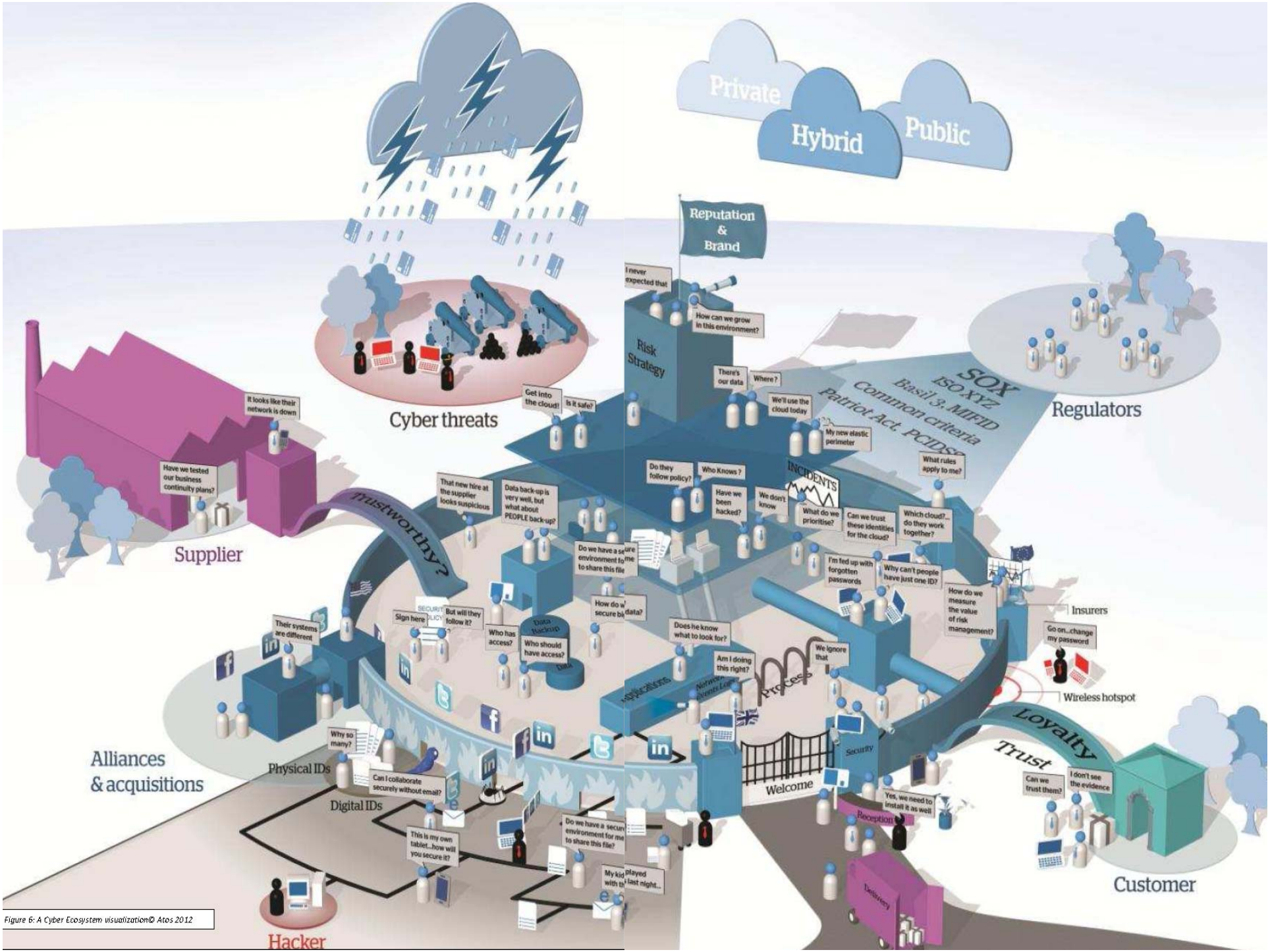


Figure 6: A Cyber Ecosystem visualization© Atos 2012

In cyberspace (like other domains)

- you can 'cyber act': do cyber transactions, cyber date, ... travel, visit, join social networks, steal, deface, perform cyber search or intelligence (including e-**spionage!**), spy, spam, create & 'use' malware (digital weapons), defend, hack, crack & attack, monitor, supervise bots, extort money, tease, seduce, social engineer, disrupt vital infrastructures (including (nuclear) power plants ...), open lock-gates, ...
- are many actors with different roles
- it is natural to define certain rules & regulations about behavior and responsibilities for all stakeholders (even cyber warriors have their legal obligations [Paul Ducheine], what about individuals?): see also discussions on bits for freedom, responsible disclosure, ethical hacking, ...

- ... and more ?

Cyber Warfare

- Cyberwar is war in 5th domain: need for cyber warriors
- Basic operations defined are Computer Network Operations (CNO) being intelligence, defense and attack: for each of them frameworks are available
- More details in MSc thesis (#130) on CyberTest Range development: describes in detail functionalities as desired by various militarists

Cyber Warfare cont.

- Obama doctrine on cyberwar: “Special Ops, drones, spy games, civilian soldiers, proxy fighters, and cyber warfare are the new stuff of global warfare”
  (see also book by D. Sanger: Confront & Conceal: link to YouTube)

- Problems related to *collateral damage:* Yemen story

More signals showing the importance of cyberspace as 5th domain?

- You may fill this in yourself...

Agenda

- Appetizer
- The emergence of cyberspace as 5th domain
- Paradigm shifts
- Some research challenges
- What's in it for the WIC?
- Dessert

From information security to cyberwarfare: some paradigm shifts

- *Asset change:* from data protection to socio-technical eco-system protection (including vital infrastructures) (sic!)
- *Stakeholder change:* from individual organizations to the globally networked world with many different stakeholders (from individuals up to states)
- *Dynamics' change:* from a purely defensive approach (CIA) towards dynamic CNO type of interactions in game- to warfare-type of ways: CIA changed into CNO?
- *Research approach change:* from local technical-management problems towards a complex multidisciplinary societal issues that hit us all

How to deal with these shifts?

- Need to change the
  - individual organization-wide risk management approach of information security (like ISO-27001)

  into a
  - national and international *integrated* risk management approach of cyberspace security

  to be implemented based on the (ministerial) 'manthra'
  - public-private-partnership (PPP) and cooperation in the golden triangle (government, business, academia) !!??

- Question: *will this be effective??*

Changed Risk Management

- **Bowtie** model helps to identify the key issues:
- *Assets:* from information via networks and controllers to (inter)dependent (critical) infrastructures (like energy, ICT, transport, ...)
- *Hazards:* from script skiddies via e-criminals and terrorists to states
- *Consequences = Risks = Expected Impact = Prob * Impact:* from small information breaches to disrupted vital infrastructures and killed people: welcome in the 21st century !

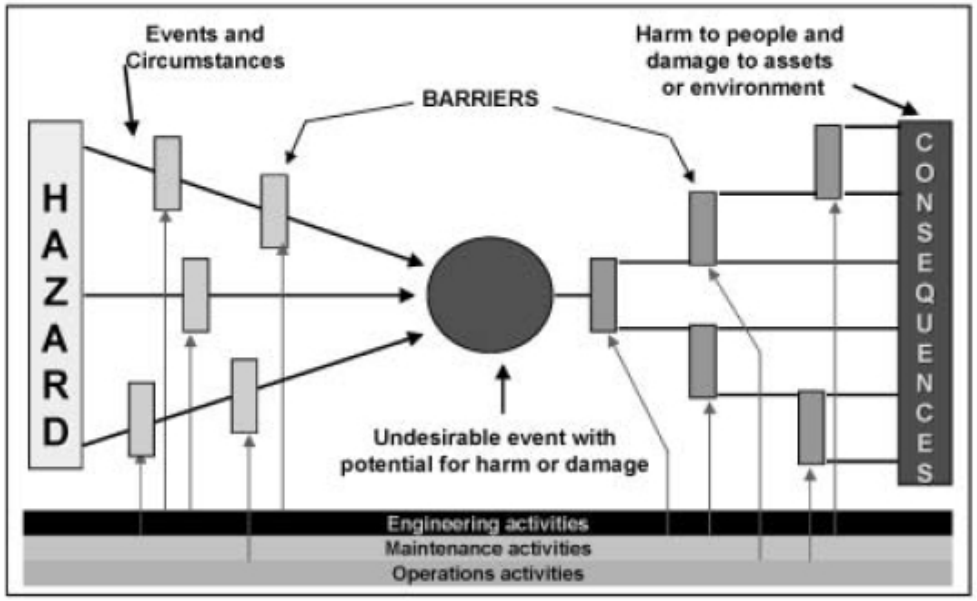
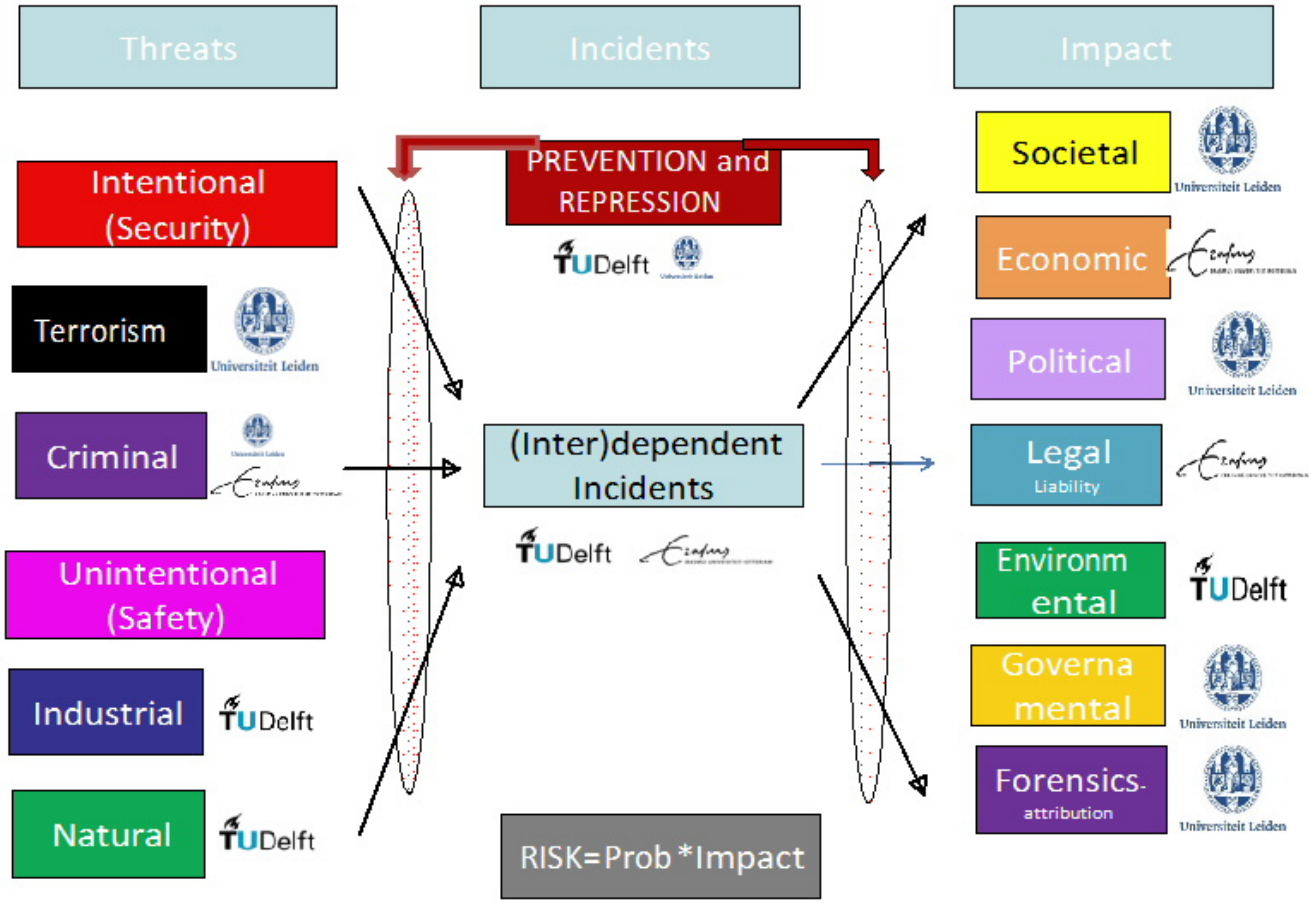
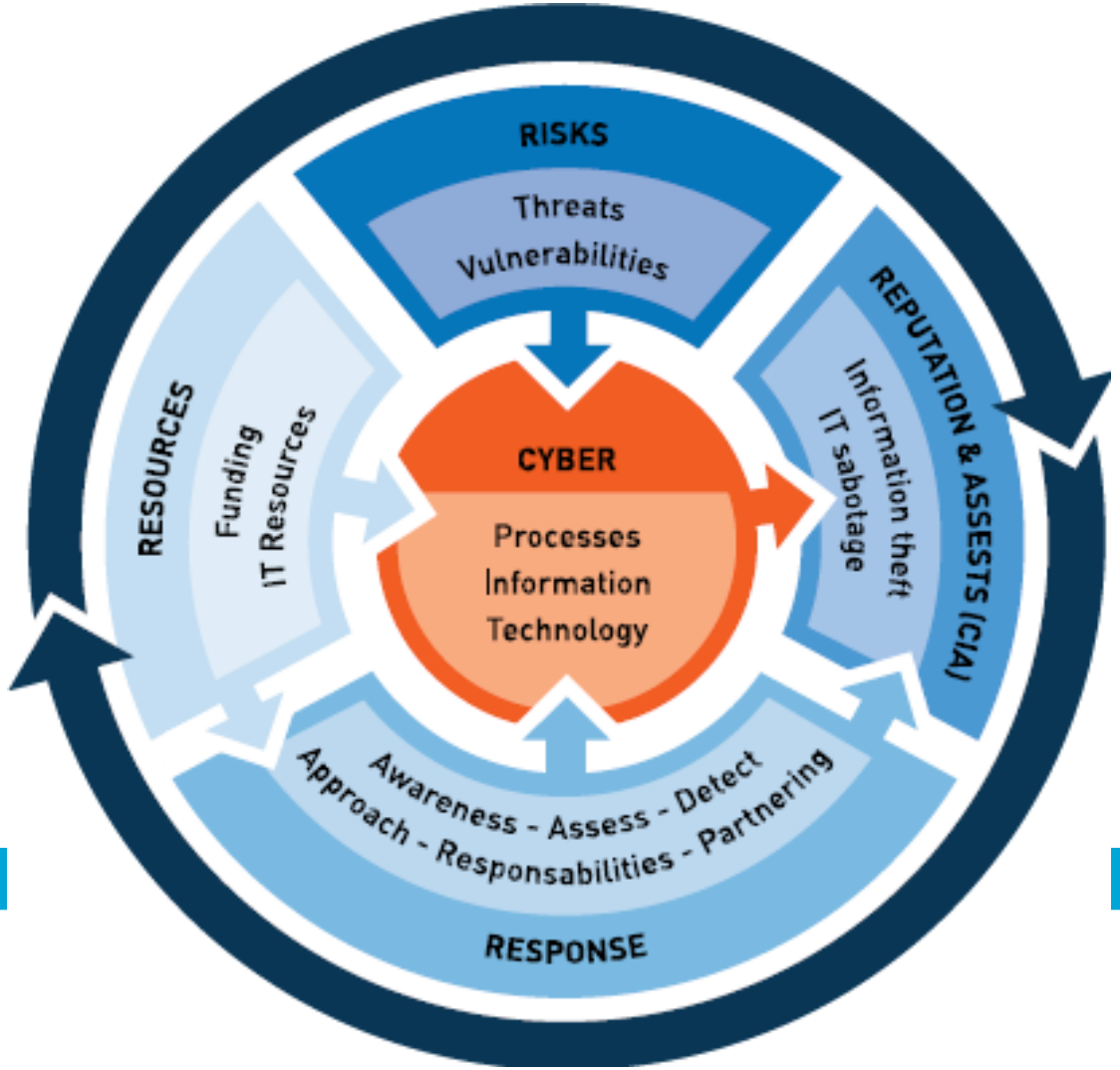


Figure 2 *The Bow Tie (courtesy Shell International Exploration & Production).*

Ex. 1: LDE initiative



Ex. 2: ATOS Cyber Risk Governance framework (CRG)



Agenda

- Appetizer
- The emergence of cyberspace as 5th domain
- Paradigm shifts
- ***Some*** research challenges
- What's in it for the WIC?
- Dessert

Research Challenges 1

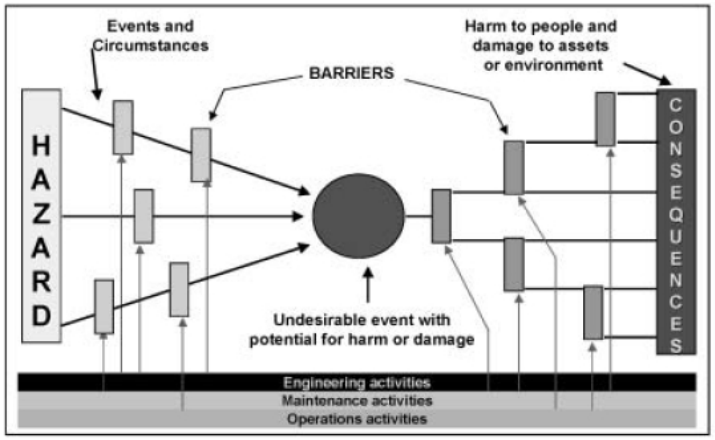


Figure 2 The Bow Tie (courtesy Shell International Exploration & Production).

First: *Understanding* (!)

Having defined assets of interest: e.g., vital infrastructures (smart grid & other energy supply systems, transport of goods & people, financial system, healthcare, governmental services (including law enforcement), crisis management services, ...)

- Analyze their
  - growing **dependencies of ICT**
  - interdependencies showing possible **cascading effects**
  - intentional and non-intentional threats,
- Determine their risks
- Help to fix acceptable risk levels and prioritize solution areas (~ political/strategic decision on new *generic* deltaplan??)

TU Delft

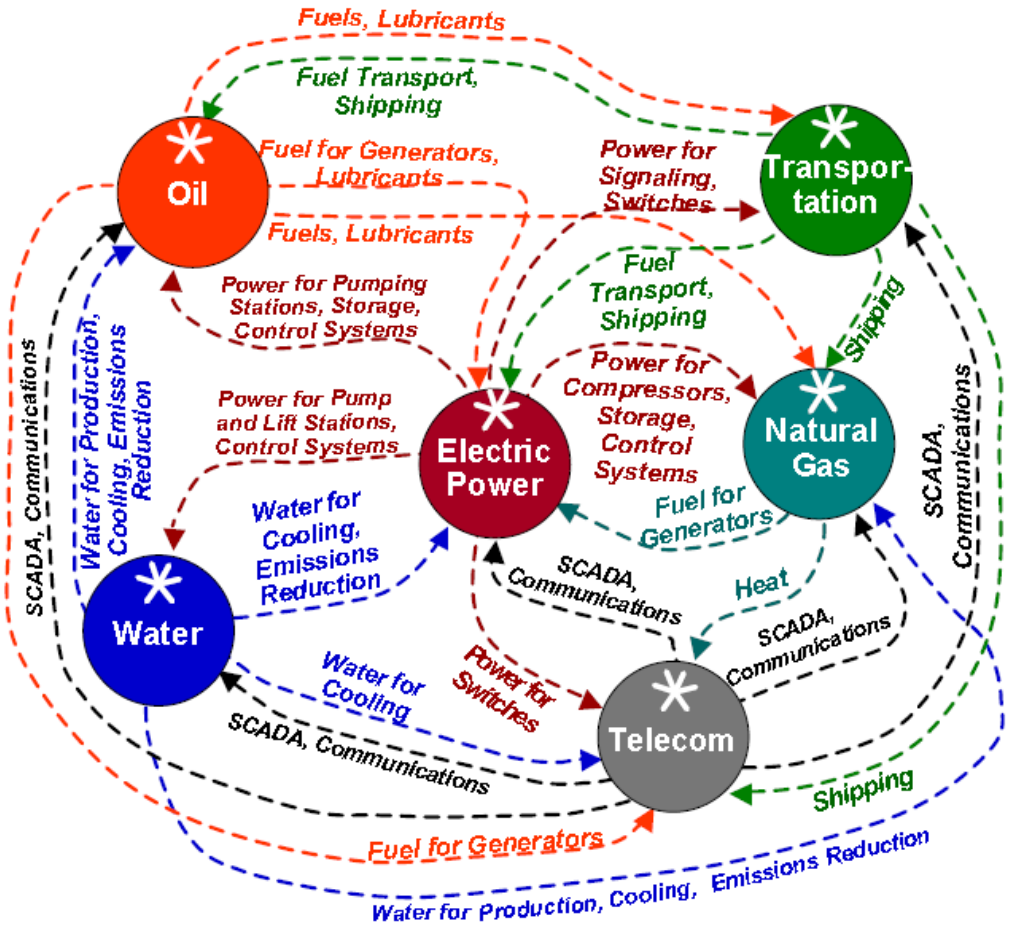
Research Challenges 1, more details

- Models for depencies of ICT: TNO is doing much work here
- Interdependency models: → (USA and Sweden as frontrunners have some models)
- Threats: determine
  - hacking threats
  - warfare threats

  to improve situational awareness

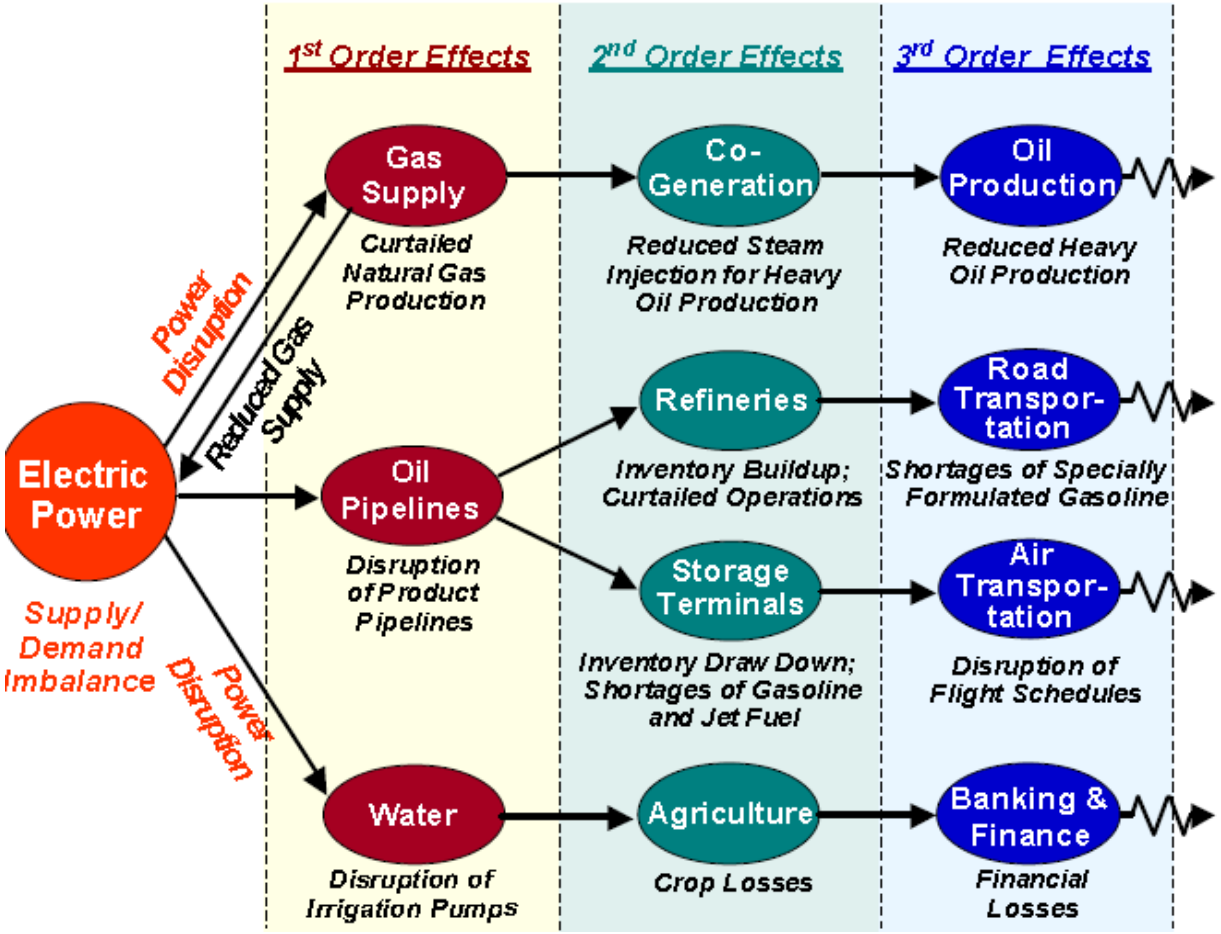
  by improved intelligence based on
  - multimedia monitoring
  - multimedia mining

  (cyber.sys research proposal with Fox-IT and NCSC)



Research Challenges 1, cont.

- Cascading effects: →
- Risk calculation: what is the impact (of all kinds!) of occurring incidents and their probability?



Research Challenges 2

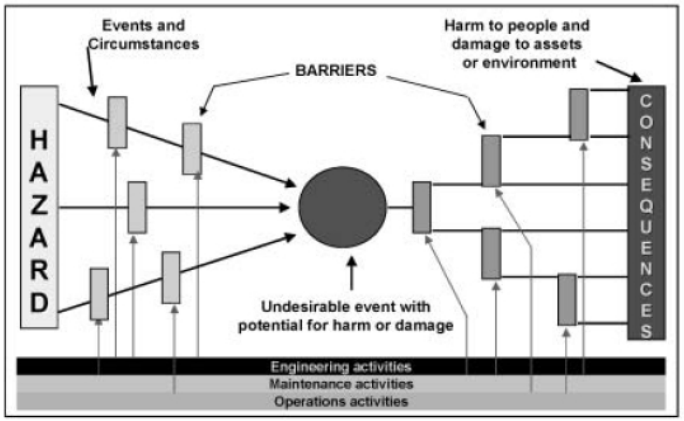


Figure 2 The Bow Tie (courtesy Shell International Exploration & Production).

Second: *Finding effective barriers*

Understanding threat – incident – impact of chosen assets, what can we do to reduce risks to acceptable levels?:

- *Preventative:*
  - dismantling of terroristic organisations
  - securing the ICT supply chain: hardware & software (how?)
  - security by design at global level: e.g., design of a global chain of trust for secure ICT-services in international supply chain of goods
  - analysis of malware (soft and hard)
  - be prepared for the enemy: development of cyber weapons

while being aware of *high dynamics/changing attack-defense scenarios!*

TU Delft

Research Challenges 2, cont.

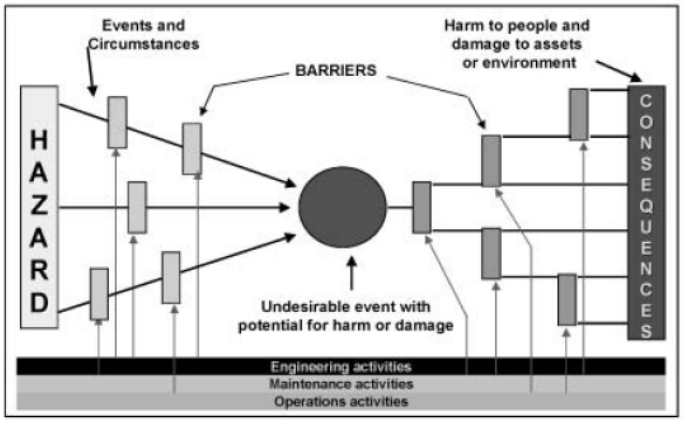


Figure 2 *The Bow Tie (courtesy Shell International Exploration & Production).*

- *Preventative, cont.:*
  - disconnecting critical IT systems from the Internet
  - take away market failures (offering insecure software can be lucrative)
  - define balanced set of rules & regulations: responsible disclosure, ethical hacking, ... (e.g., let's try them out and learn as society!)
  - ...
- *Repressive:*
  - develop advanced intrusion detection (of APTs)
  - organize adequate cyber crisis management
  - enable intelligent forensics...
  - ...

TU Delft

Agenda

- Appetizer
- The emergence of cyberspace as 5th domain
- Some paradigm shifts
- Some research challenges
- What's in it for the WIC?
- Dessert

What's in it for the WIC?, some crazy ideas

DelftTopTech

Probably a lot... it is about research challenges in the context of the dynamic cyber domain

- Theoretical research including
  - principles of large scale information sharing (EPD, ov-chip, credit card, DigID, C2000, etc. solutions) in the networked world, both in times of peace and in times of crisis & (cyber)war
  - principles of creating & detecting malware
  - architectural principles of creating an intrinsically secure Internet
- Applied research around issues like
  - confidentiality-preserved information sharing (e.g. in ISACs): *balancing* data sharing and data confidentiality
  - intelligent forensics in cyberspace
  - an updated version of the ISO-27001 (best practices, per domain?)
  - secure (remote) control of SCADA-systems

TU Delft

Agenda

- Appetizer
- The emergence of cyberspace as 5th domain
- Paradigm shifts
- Some research challenges
- What's in it for the WIC?
- Dessert

My own hobbies

- are often in data & text mining/data analytics for, e.g.,
  - improved (national) cyber situational awareness
  - understanding cyberwarfare capabilities of enemies
  - better intrusion detection (combination of signature- and anomaly-based methods)
  - e-fraud detection (like financial transactions, fraudulent gambling syndicates in soccer, ...)
- *probabilistic fuzzy systems* including probabilistics fuzzy decision trees combine linguistic interpretability (of fuzzy systems) and statistical aspects of data: are applicable here as well...

Jan van den Berg, Uzay Kaymak, and Rui Jorge Almeida. Conditional Density Estimation Using ProbabilisticFuzzy Systems. *IEEE Transactions on Fuzzy Systems*. Accepted for publication on November 6 2012.

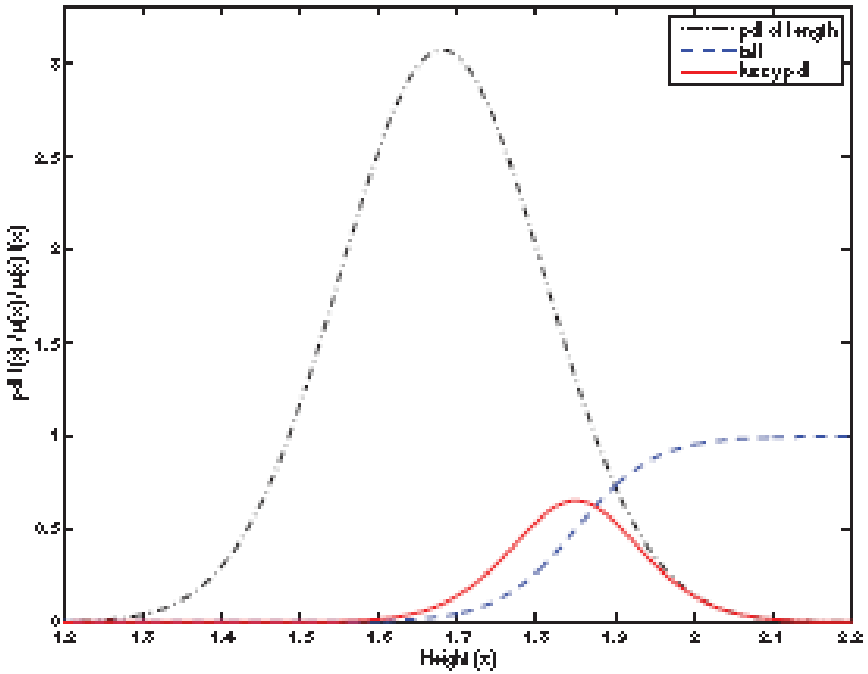


Fig. 1. pdf $f(x)$ of the height of Dutch women, the membership function $u(x)$ defining tallness, and the "fuzzy pdf" $u(x)f(x)$.

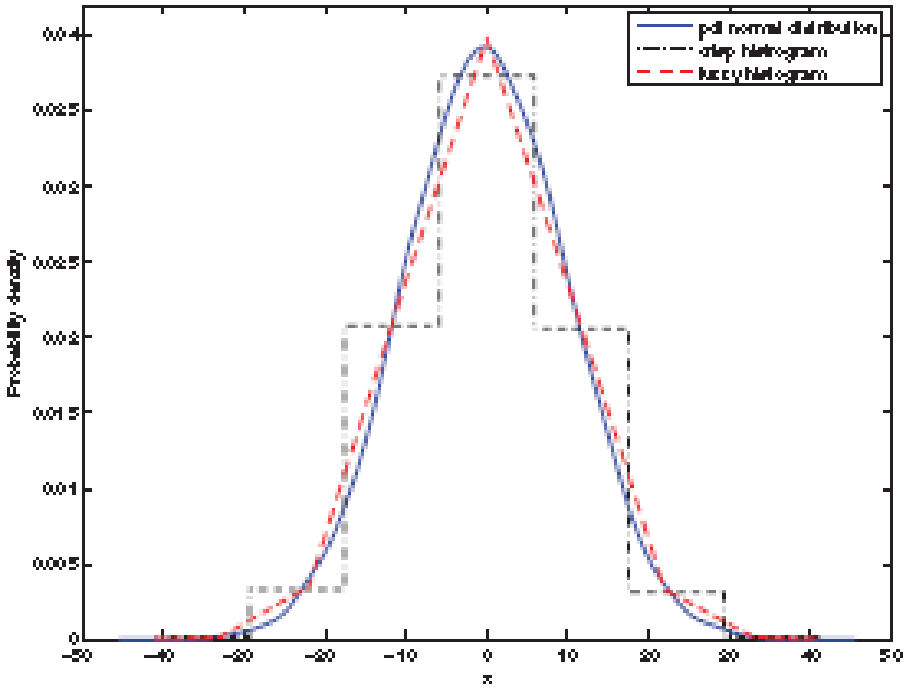


Fig. 3. Fuzzy histogram better approximates a pdf than a crisp histogram.

THANK YOU!

Other signals showing growing awareness of problems in cyberspace

- Daily news in newspapers mentioning cyberincidents
- Countries
  - define and update national cyber strategies (NCSC)
  - improve monitoring to improve situational awareness
  - start to define laws, rules and regulations
  - advocate Public Private Partnership (PPP)
  - start studies on (inter)depencies between vital infrastructures
- Growing number of cyber specialists in e.g. police and europol (European Cyber Crime Centre = EC3 in The Hague)
- Conferences on cyber issues every week...

- *Interesting question:* is this all *effective?*