Lecture 2: Sociotechnical perspectives on dangers in cyberspace

Sarah Backman
PhD Candidate in International Relations,
Stockholm University/Swedish Defence University

Lecture 1: the securitization and militarization of cyberspace

1. The development of cyberspace: governance and culture
2. The securitization of cyberspace
3. The militarization of cyberspace
4. Q&A

Aim: after these lectures, you should be able to

1) reflect around socio-technical vulnerabilities as a basis for dangers in cyberspace/incidents and
2) Reflect critically around developments in the international cyber(security) landscape.

Lecture 2: sociotechnical perspectives on dangers in cyberspace

1. Sociotechnical (non antagonist based) perspectives on dangers in cyberspace
2. Large-scale cyber incidents affecting critical infrastructure – response challenges & success factors
3. Normal Accidents & High Reliability Organizations /sociotechnical systems perspectives
4. Q&A

Why do we need a socio-technical perspective on large-scale cyber incidents & dangers in cyberspace

- Rather than focusing on antagonist action, it focuses on the system(s) attacked and socio-technical vulnerabilities.
- Needed considering the **proneness of accidents** and **proliferation of malware (sometimes beyond intent of threat actor)** is in the international cyber landscape.
- Large-scale cyber incidents as crisis events, its **connection to generic crisis management structures.**

Large-scale cyber incidents affecting critical infrastructure - Response challenges and success factors

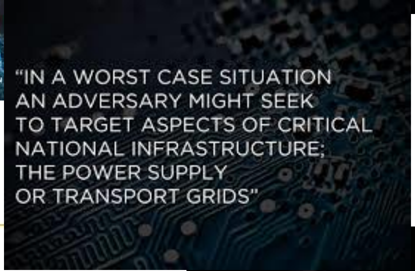
Large-scale cyber incidents

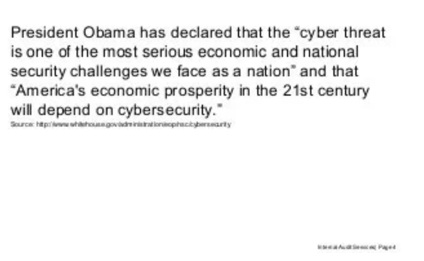
- (in the definition of) cyber induced disruptions affecting critical infrastructure.
- Events surrounded by hype and fear
  - Often used in securitizing narratives & speech acts

- Despite the hype: surprisingly few empirical examinations or theoretical contributions within security studies

- When these events have been discussed in the literature, they have often been approached from strategic-military perspectives (as the potential consequence of cyber war, for example).

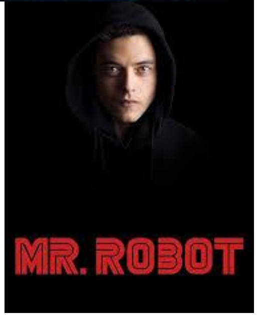
- My PhD project has aimed to investigate these phenomena empirically and to examine the foundation for some of the common assumptions surrounding them
  - What are their characteristics?
  - How are they managed and perceived in nat + int context, has this changed over time?
  - How can we understand and explain these events beyond antagonist focused theoretical approaches?


"IN A WORST CASE SITUATION AN ADVERSARY MIGHT SEEK TO TARGET ASPECTS OF CRITICAL NATIONAL INFRASTRUCTURE; THE POWER SUPPLY OR TRANSPORT GRIDS"


President Obama has declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."

Source: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity

Internal Audit Services| Page4

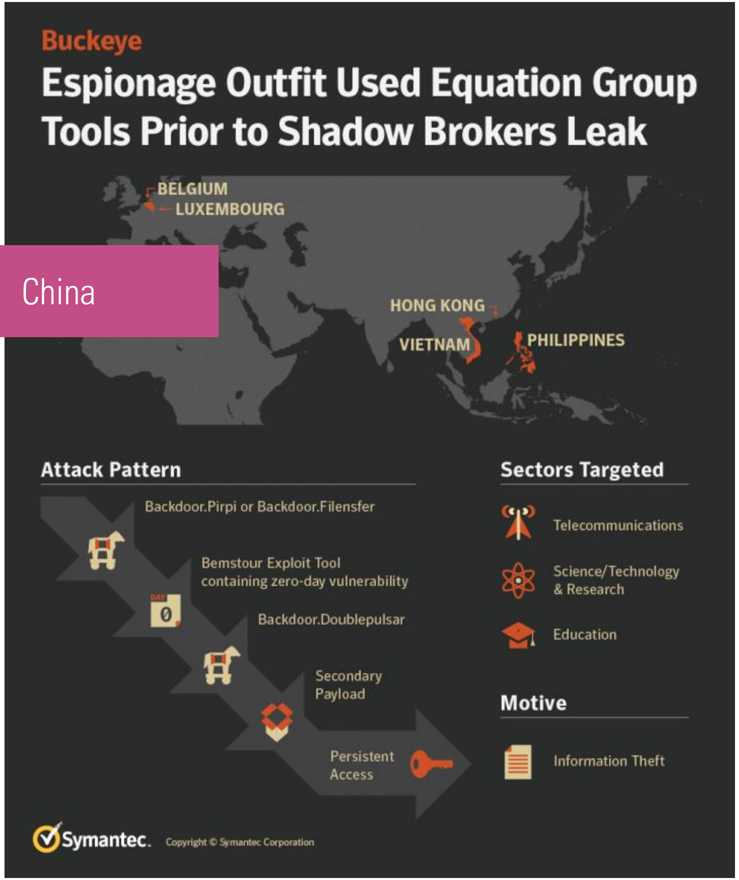


Large scale cyber incidents - transboundary crises

- Question the uniqueness of large-scale cyber incidents as crisis phenomena.
- What characterizes crises in a traditional sense is an event threatening core values or life-sustaining systems, which requires an urgent response under conditions of deep uncertainty (Boin & Rhinard, 2008; Rosenthal et al., 1989, 2001).
- What sets the transboundary crisis apart from the "traditional" crisis is, simply put, its tendency to not be limited geographical, political, sectoral, economic, social or legal boundaries.
- More specifically, a transboundary crisis can be defined as a crisis which transcends:
  - Political boundaries (such as geographical borders, jurisdictions or levels of governance),
  - Functional boundaries (such as sectoral, policy and industry domains) and
  - Time boundaries (temporal definitions; Ansell et al., 2010; Rose & Kustra, 2013).

The transboundary nature of threats

China



Buckeye

Espionage Outfit Used Equation Group Tools Prior to Shadow Brokers Leak

BELGIUM
LUXEMBOURG
HONG KONG
VIETNAM
PHILIPPINES

Attack Pattern

- Backdoor.Pirpi or Backdoor.Filensfer
- Bemstour Exploit Tool containing zero-day vulnerability
- Backdoor.Doublepulsar
- Secondary Payload
- Persistent Access

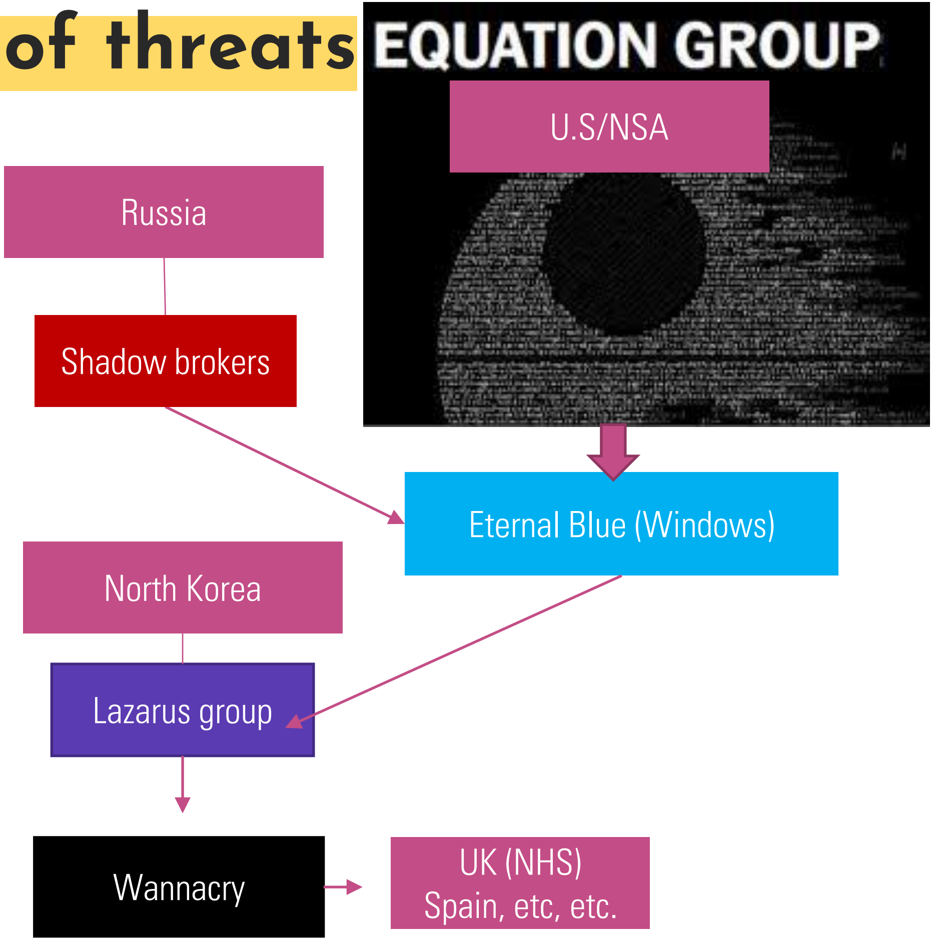
Sectors Targeted

- Telecommunications
- Science/Technology & Research
- Education

Motive

- Information Theft

Symantec. Copyright © Symantec Corporation



EQUATION GROUP

U.S/NSA

Russia

Shadow brokers

Eternal Blue (Windows)

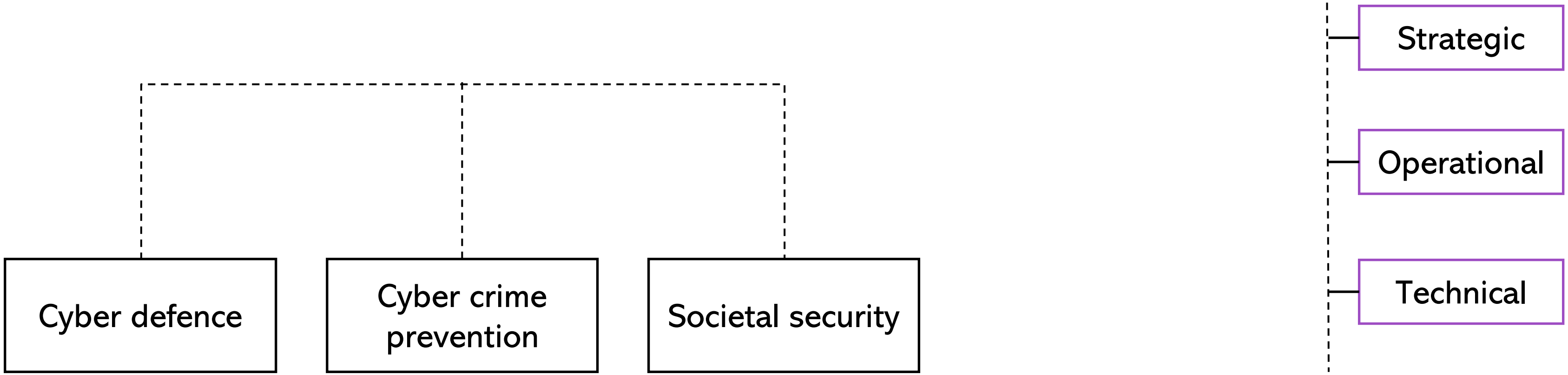
North Korea

Lazarus group

Wannacry

UK (NHS)
Spain, etc, etc.

Cybersecurity: horizontally and vertically



Cyber defence

Cyber crime prevention

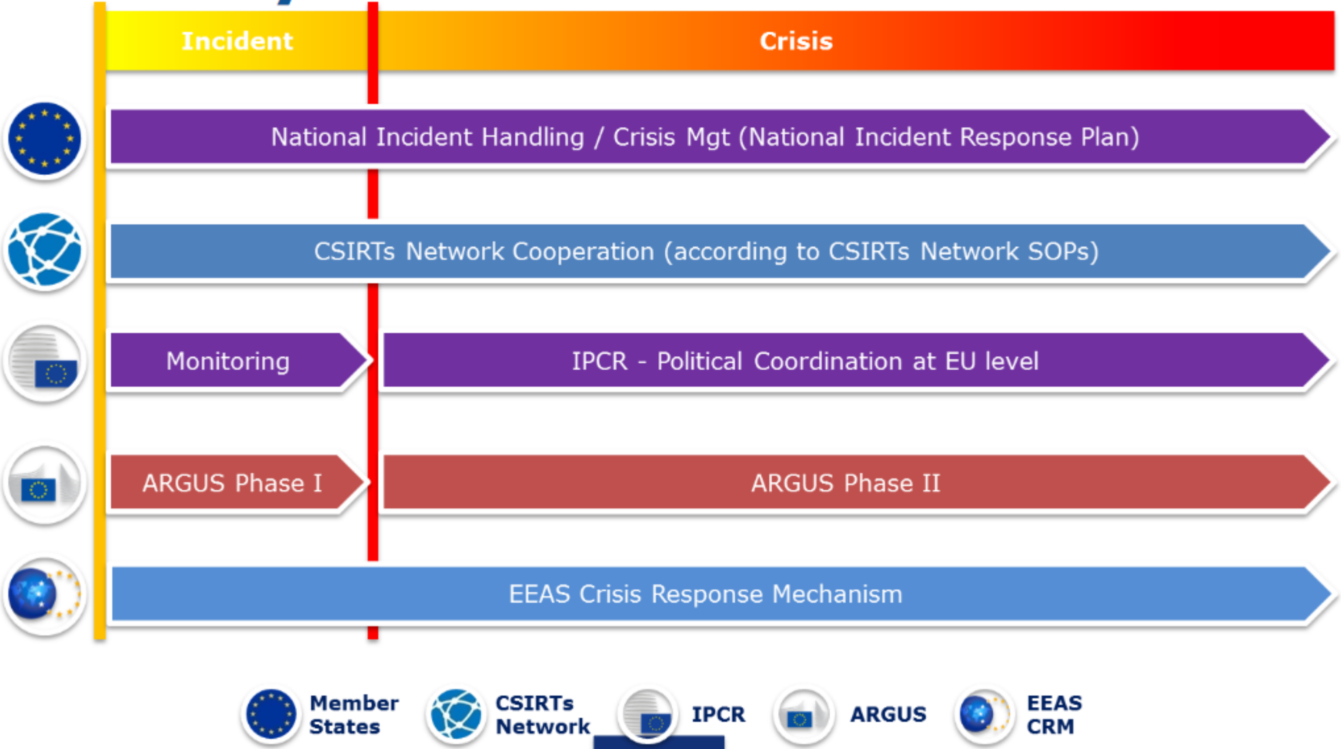
Societal security

Strategic

Operational

Technical

Blueprint – key mechanisms



Incident

Crisis

National Incident Handling / Crisis Mgt (National Incident Response Plan)

CSIRTs Network Cooperation (according to CSIRTs Network SOPs)

Monitoring

IPCR - Political Coordination at EU level

ARGUS Phase I

ARGUS Phase II

EEAS Crisis Response Mechanism

Member States

CSIRTs Network

IPCR

ARGUS

EEAS CRM

Central crisis management tasks

Detection

Sense-making

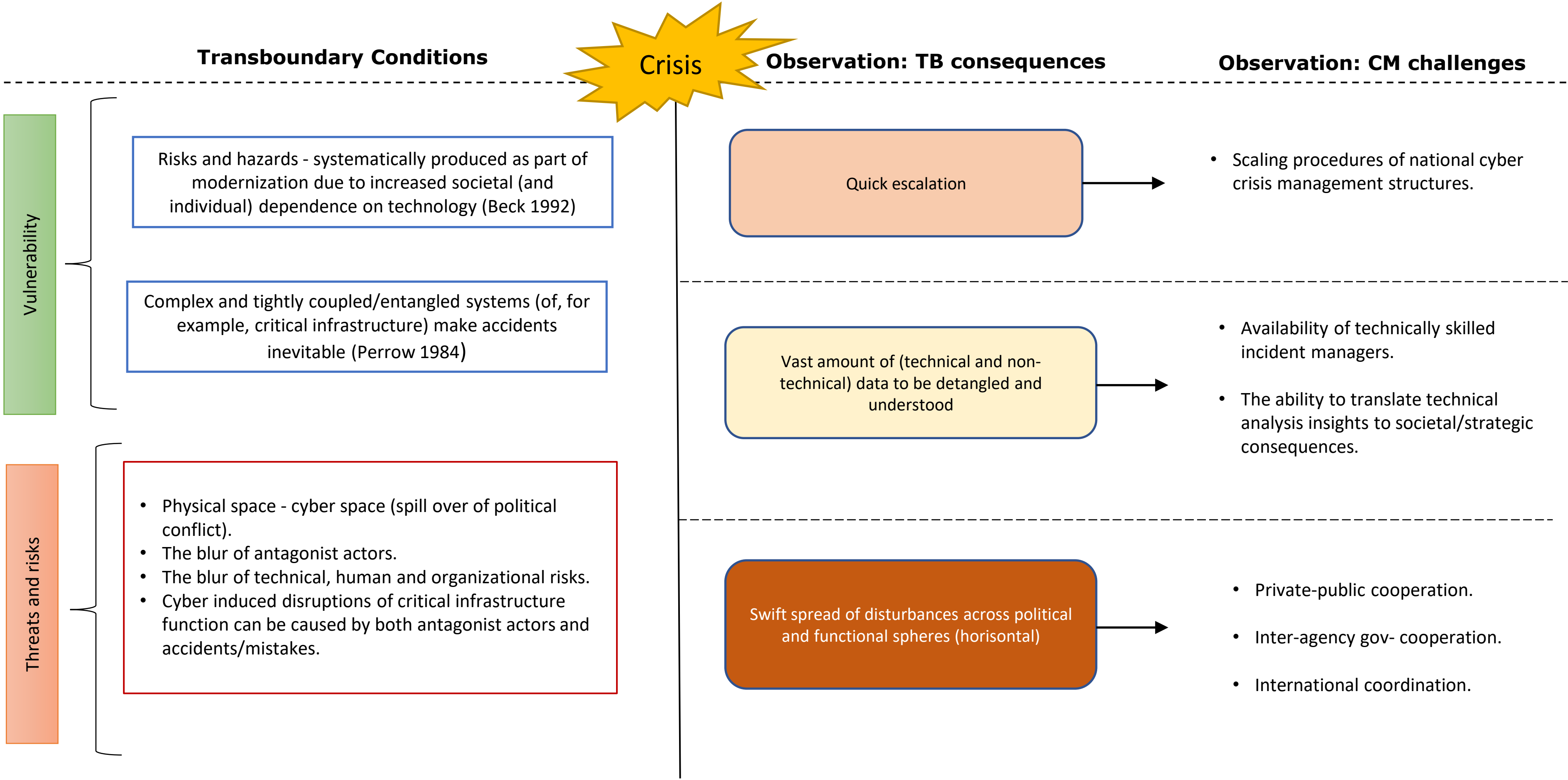
Decision-making

Coordination

Meaning-making & Communication

Crisis ending

Crisis Management task domain 1: Detection



Crisis

Transboundary Conditions

Vulnerability

Risks and hazards - systematically produced as part of modernization due to increased societal (and individual) dependence on technology (Beck 1992)

Complex and tightly coupled/entangled systems (of, for example, critical infrastructure) make accidents inevitable (Perrow 1984)

Threats and risks

- Physical space - cyber space (spill over of political conflict).
- The blur of antagonist actors.
- The blur of technical, human and organizational risks.
- Cyber induced disruptions of critical infrastructure function can be caused by both antagonist actors and accidents/mistakes.

Observation: TB consequences

Quick escalation

Vast amount of (technical and non-technical) data to be detangled and understood

Swift spread of disturbances across political and functional spheres (horisontal)

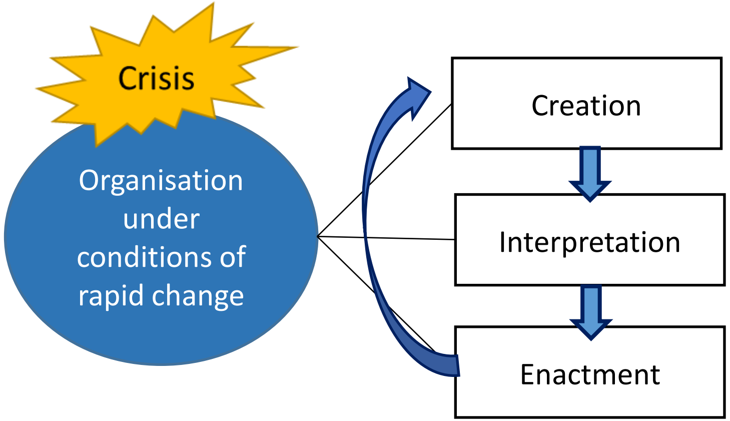
Observation: CM challenges

- Scaling procedures of national cyber crisis management structures.

- Availability of technically skilled incident managers.
- The ability to translate technical analysis insights to societal/strategic consequences.

- Private-public cooperation.
- Inter-agency gov- cooperation.
- International coordination.

Crisis Management task domain 2: Sense-making (in Cyber Crises)



Cyber crisis sense-making challenges

- Many involved actors = many parallel sense-making processes = difficulty to reach a common inter-organizational understanding and situational picture.
- Technical nature of information adds to the challenge of sense-making, not everyone can detangle it and understand it.
- A challenge to put together a clear situational picture which can be understood by decision makers and the public.
- As a complex type of crisis, the situational understanding of a cyber crisis might be diffused by faulty or competing accounts, from other organizations and/or media.
- Lots of stress on a few individuals in the national cybersecurity structures who are key for several important tasks in connection to information management (collecting, managing, analyzing and sharing).

Crisis Management task domain 3: Decision-making (in cyber crises)

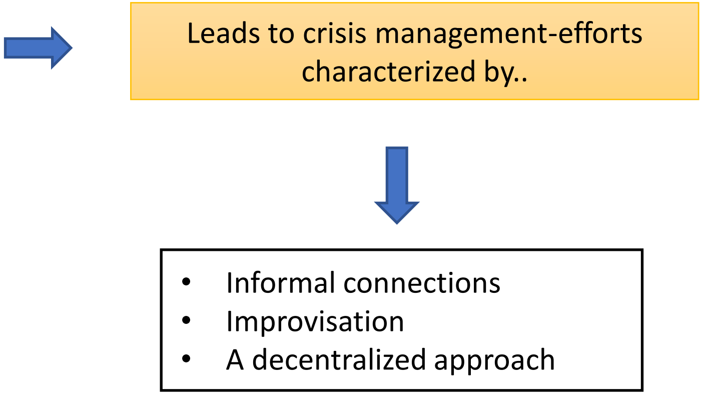
Decision-making challenges in cyber crises

Vague and/or complex situational picture to base decisions on

- As a result of a challenging sense-making process/complex problem.
- Technical aspects can make it difficult for decision-makers to understand the crisis enough to make informed decisions.

Dispersion of authority across functional and political spheres (privat/public – inter-agency)

- Leads to overlaps in some places, and gaps in others.
- Parallel crisis management processes, lack of overarching authority.
- Not clear who “owns” the crisis, and who should be in charge.
- This challenge is enhanced by the lack of formal structures and pre-established authority relations.



Leads to crisis management-efforts characterized by..

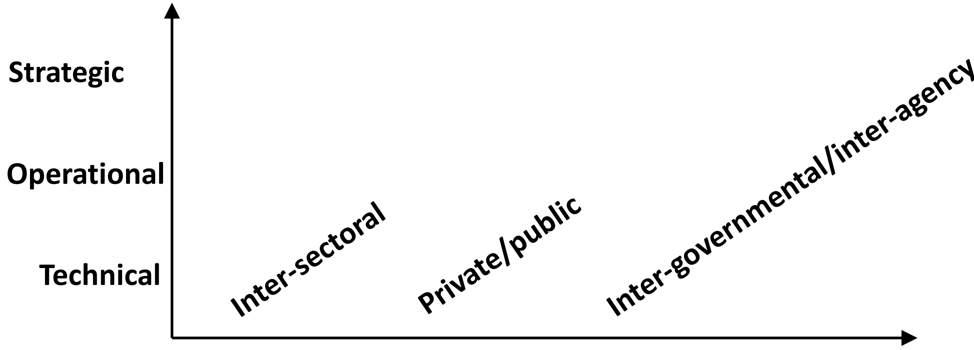
- Informal connections
- Improvisation
- A decentralized approach

Crisis Management task domain 4: Coordination (in cyber crises)

Cyber crisis coordination challenges

- The challenge of private-public and inter-agency coordination and collaboration when the cyber crisis' consequences proliferate across political and functional borders.
- The transboundary nature of cyber crises creates a complex ecology of involved (and interdependent) actors and institutions across political and functional spheres.
- Interdependent linkages between actors who are not always used to working together
- Several tracks of cyber crisis management working simultaneously but with different timelines, goals, expertise and challenges.
- Lack of formal structures for supporting the needed coordination (creating a need for improvisation of incident/crisis managers).

Spheres of coordination and collaboration in cyber crises (examples..)



Strategic

Operational

Technical

Inter-sectoral

Private/public

Inter-governmental/inter-agency

Technical incident management

- ○ Mitigation of technical causes
- ○ Technical analysis/malware analysis

Generic crisis management

- ○ Focus on saving lives
- ○ Mitigation of societal consequences
- ○ Manage media and communication

Crisis Management task domains 5-6: Communication and meaning-making

Communication & meaning-making challenges in transboundary crises

- In a crisis, political leaders are expected to reduce uncertainty and provide an authoritative account of what is going on, why it is happening and what needs to be done (’t Hart, 1993).

- When a crisis involves an increasing number of political, administrative and sectoral authorities, it becomes harder to produce one clear and coherent message that relieves collective stress and provides people with actionable advice (Ansell et al 2010)

- The many involved actors and the complex features of transboundary crises create conditions for multiple accounts on a given situation (Boin et al., 2017).

- The transboundary crisis may be subjected to “framing contests”.

Crisis Management task domains 5-6: Communication and Meaning-making (in cyber crises)

S.Backman 2022 - do not distribute without permission

Communication and Meaning-making challenges in cyber crises

“One of the biggest challenges was communication. Getting the right communication out at the right time, providing guidance in order to keep people from jumping to conclusions.” (Interviewee 3).

“Cyber crises are good examples of media-driven crises. Our experience is that it is easy for media and the general public to draw faulty conclusions in connection to cyber incidents (and make them worse) because the knowledge on how cyber-attacks and incidents work is rather low.” (Interviewee 1).

“It's a huge challenge to get control of the information surrounding a cyber crisis, to be able to put together a message of what has happened and then to communicate it to decision-makers and the public” (Interviewee 7).

“It is easy to build a doomsday scenario around the event of 2007 and cyber incidents in general. A lot of the later coverage on it was a bit exaggerated. The sense of panic that is often depicted by foreign coverage does not match the experience of those who were actually there.” (Interviewee 5).

Stockholm University

Crisis Management task domain 7: crisis ending (in cyber crises)

Crisis ending challenges in transboundary crises

- Transboundary crises tends to be hard to chart as causes will often be unclear, and they might not have an easily identified beginning or end.

> “The traditional nature of major incidents has been that they are either very intense but are over within a number of hours (such as a major traffic incident or physical terror attack) or they are long lasting but slow moving (such as strike action).
>
> Cyber-attacks create the potential for a long running, highly intense incident.”(Smart, 2018:34).

Crisis ending challenges in cyber crises

- Difficult to know to what extent the vulnerability is still present as well as the extent of the breach (due to lack of reporting etc) and therefore whether and to what extent services could be disrupted again.
- Long term consequences of a cyber crisis can be difficult to estimate.
- Accountability (and the possibility for legal action) against attackers delayed and/or hindered by the difficulty of attribution.
- Technical analysis, mitigation & accountability processes long-term activities involving many stakeholders.

Large-scale cyber incidents: some research findings

- From a governance perspective, these events are seen and responded to largely as civilian transboundary crises (affecting critical infrastructure) – similarities with other transboundary crises

- Key cyber crisis management capacities of national administrations:
  - surge capacity of civilian technical expert teams (CERTs, for instance)
  - formal scaling procedures of generic crisis management structures
  - established private-public partnerships
  - clear ownership and decision-making roles
  - coordination of parallel cm processes vertically and horizontally
  - Improvisation and creativity of responders

- **Many of the instances of large-scale cyber incidents affecting ci have seen so far have been the result of collateral damage rather than directed attacks:**

  - **Colonial pipeline incident**
  - **WannaCry**
  - **NotPetya, etc..**

Q & A

+10 min break

Normal Accidents & High Reliability Organizations

Normal Accidents theory

Charles Perrow (1984)

The combination of **complex interactivity** and **tight coupling between components** in high-risk systems will inevitably lead to “accidents”, making them “normal”.

Normal Accidents theory: modern adaptation

1) with modern technological invention, innovation and expansion, we constantly multiply and expand high-risk technologies, such as ICS (industrial control systems) for critical infrastructure operations, nuclear technologies, and space technology (such as satellites).

   These technologies are high-risk because we rely upon their operation for our safety or daily life, and their failure would have extensive disruptive effects or even threaten lives

Normal Accidents theory: modern adaptation

2) In an effort to control these technologies and make them manageable, we create complex systems, or inject them in complex systems. These systems could be technical or systems in an organizational sense (ie organization of organisations).

We build in complexity in the systems through creating interactive-ness between the components of the system or between systems. The components could be made up of (for example) code, parts, procedures or operators.

Normal Accidents theory: modern adaptation

3) What makes accidents in these systems inevitable or “normal” has to do with the way failures in the components can interact and the way the system is tied together.

When two or more failures of components happens in an interactive way, the result can be both unexpected and unpredictable, even for the designers of the system.

Normal Accidents theory: modern adaptation

4) This interactive complexity would not be as dangerous were it not for an additional system characteristic: tight coupling.

Perrow defines tight coupling as a condition where “..processes happen very fast and can’t be turned off, the failed parts cannot be isolated from other parts, or there is no other way to keep the production going safely” (Perrow 1990).
The result is that there is “no slack” in the system. Recovery becomes very difficult, and the initial disturbance may proliferate quickly and irreversibly.

As the combination of interacting components increases, an error in any of those components, or combination of components, could have a catastrophic net effect on the functioning of the overall system, if adequate separation and segregation is not in place.

Adapted framework to understand large-scale cyber incidents (affecting ci)

- 4 layers where the NA-dynamic (the combination of interactive complexity and tight coupling between components) is prevalent, and which contributes to the proliferating tendency of malware+cyber incidents:

  1. Technology – interdependent layers of legacy code, hardware, systems
  2. Cognitive – lack of a comprehensive cognitive understanding of system ecology
  3. Organization – hidden/unknown tight coupled interactions between organizational components (technical and admin, for example)
  4. Macro – complex global interdependencies (supply chain actors/vendors, inter-sectoral dependencies/bottle-necks etc.)

Implications of Normal Accidents- dynamics for cyber defence and offense

Implications: defence

- Threat actors are constantly looking for systems with NA-dynamics to utilize for attack (especially centralized ones for maximum proliferation).
- Systems that have NA-dynamics (especially on multiple layers) are more likely to be affected by collateral damage/non-directed attacks.
- Perrow: It’s not feasible to reduce complexity, but it is feasible to reduce tight coupling:
  - Less centralization
  - More redundancy
- High Reliability Organizations:
  - HROs tend to:
    - allow flexible and decentralized decision making,
    - have strong external preferences for failure-free operations and
    - invest heavily in reliability improvement, including redundancy and training.

Implications: offense

- Democratic states are increasingly developing offensive cyber capabilities+tools and are showing an increased willingness to use them to achieve strategic advantages.
- This raises ethical concerns with regards to our empirical observations of the proness of malware to proliferate, and with the common existance of NA-dynamics in high-risk systems.
    - How will we be able to ensure compliance with just war principles and international law (especially our ability to prevent collateral damage and ensure proportionality) if we attack systems with NA-dynamics (with purpose or by mistake)?
    - How will triggered security dilemmas in cyber space be prevented?
    - And will the increasing use of offensive cyber contribute to increased malware proliferation across the globe? Short term vs. long term ethical implications of normative turn.

Discussion of assignment for distinction

Explain a cyber security incident of your choice (caused by a cyberattack) in a written report (1500 words +/- 10 %).

The report should contain three parts. The first should introduce the incidents briefly (about 200-400 words). The second should focus on explaining the incident from a threat and threat actor perspective, using the listed threat models (from Alan’s lecture). The third should reflect around socio-technical causes of the incident, such as socio-technical vulnerabilities and developments in the international cyber(security) landscape.

Thank you!
Q&A