Handling Cyber Incidents & Cyber Crisis: terminology, perspective & attribution

ETH zürich

«Cyber incidents are a bit like a bar brawl – you might have a pretty good idea who started it, but you will never be absolutely sure!»

Content

Terminology & key issues in dealing with cyber-incident and cyber-crisis!

1. Introduction
   - Main issues & goals

2. Emergency & Crisis Management
   - What defines a crisis situation and what are the challenges?
   - How does an emergency evolve into a crisis?

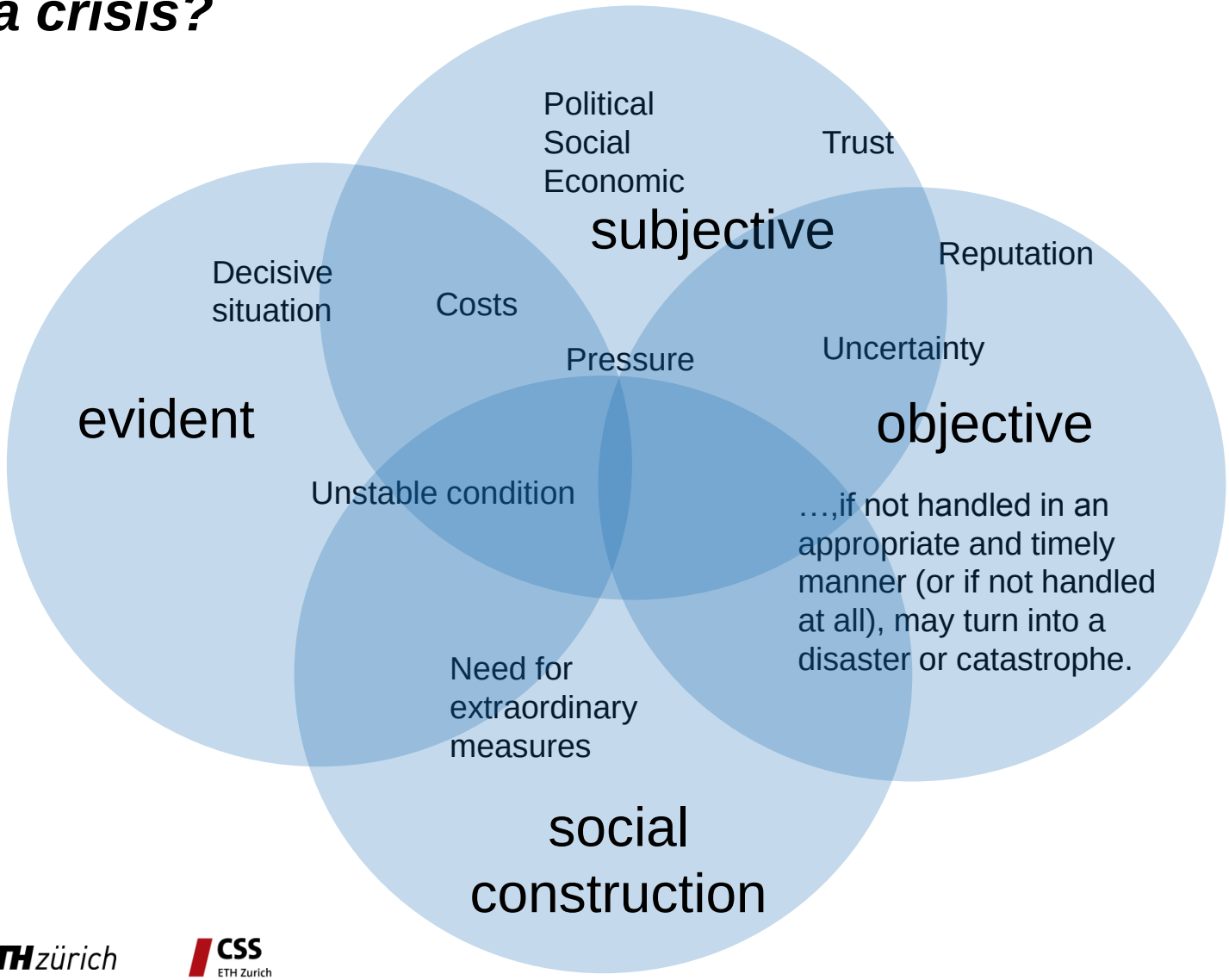
3. Terminology
   - «Cyber Crisis» - terminology in public and private domain

4. (Cyber) Incident and (Cyber) Crisis Management
   - How does an incident become a crisis?
   - What defines a cyber incident and crisis?
   - Similarities & Differences to general crisis management

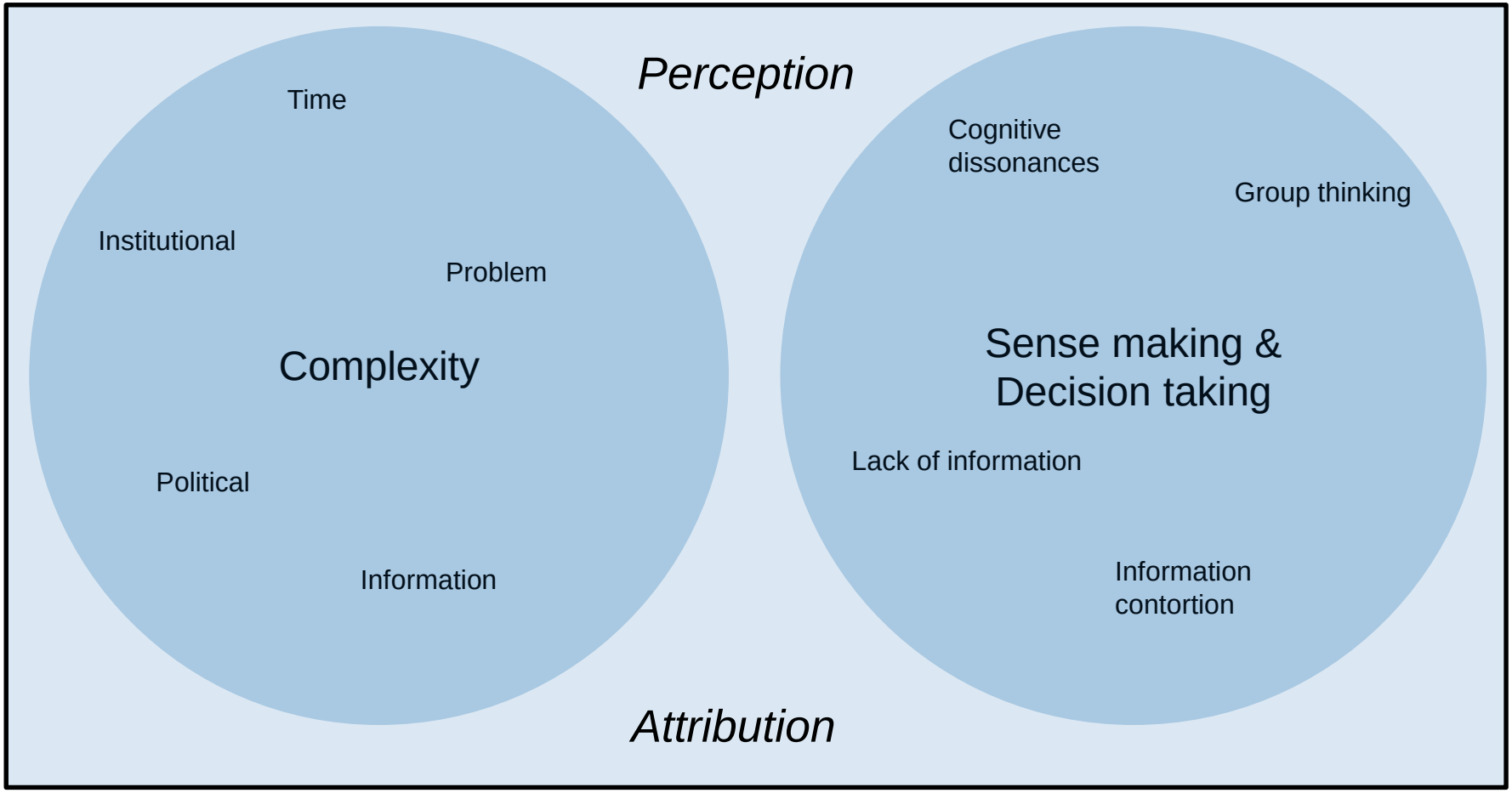
5. Attribution and Perception in the Threat Typology

6. Next steps & Questions

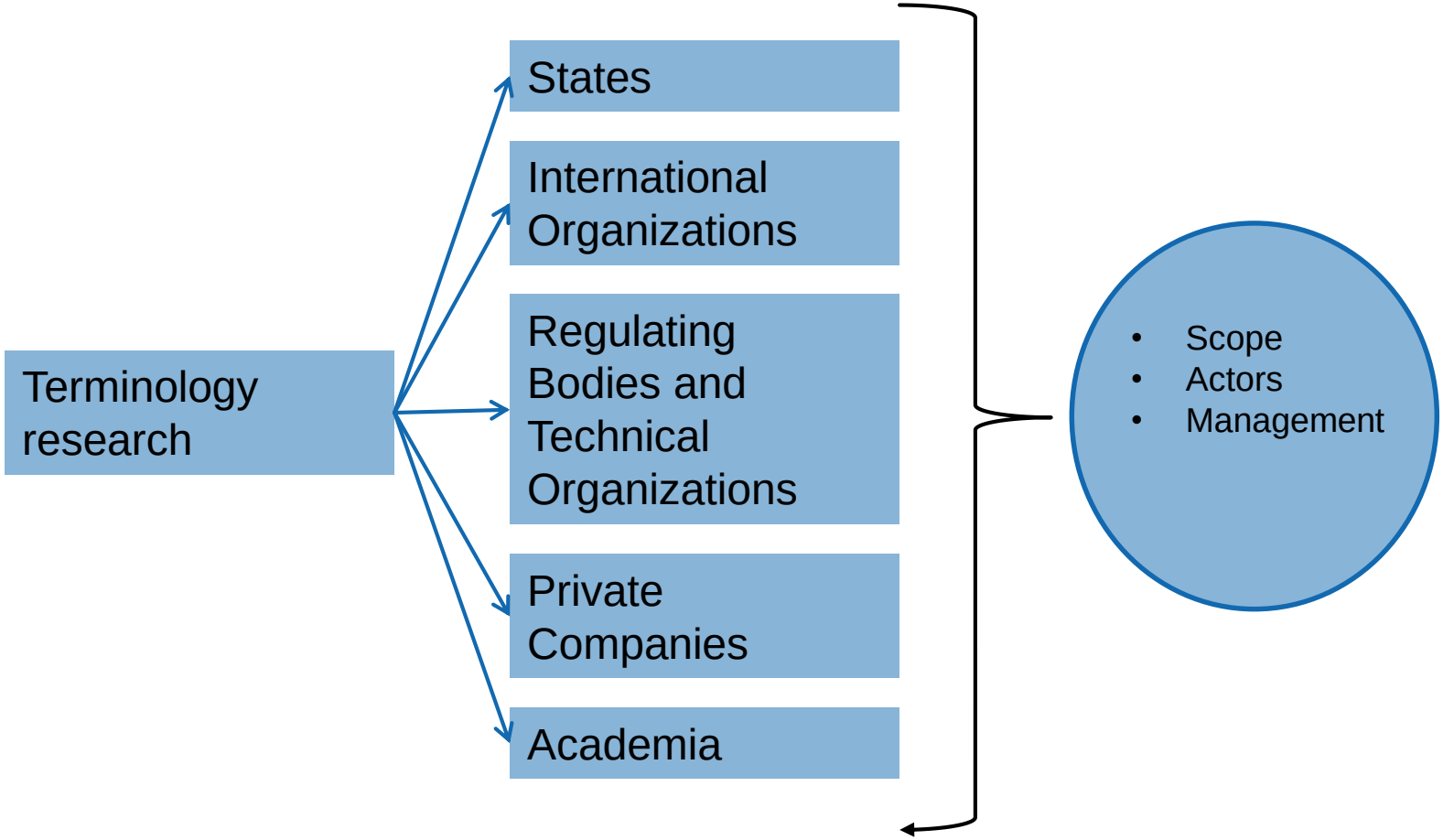
2. Crisis & Emergency: How does an emergency become a crisis?



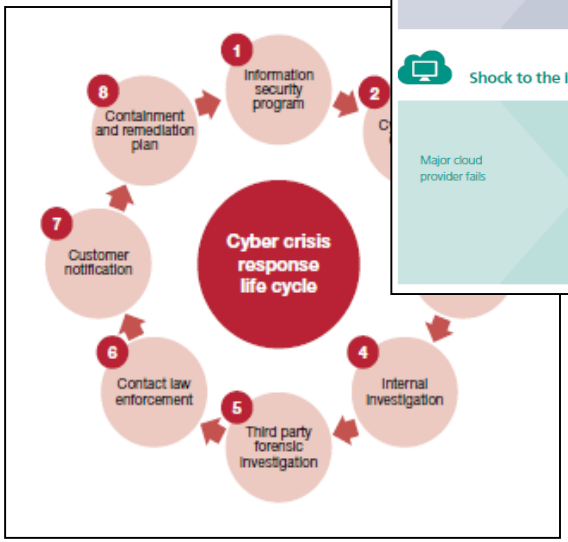
2. Crisis Management: Main Challenges

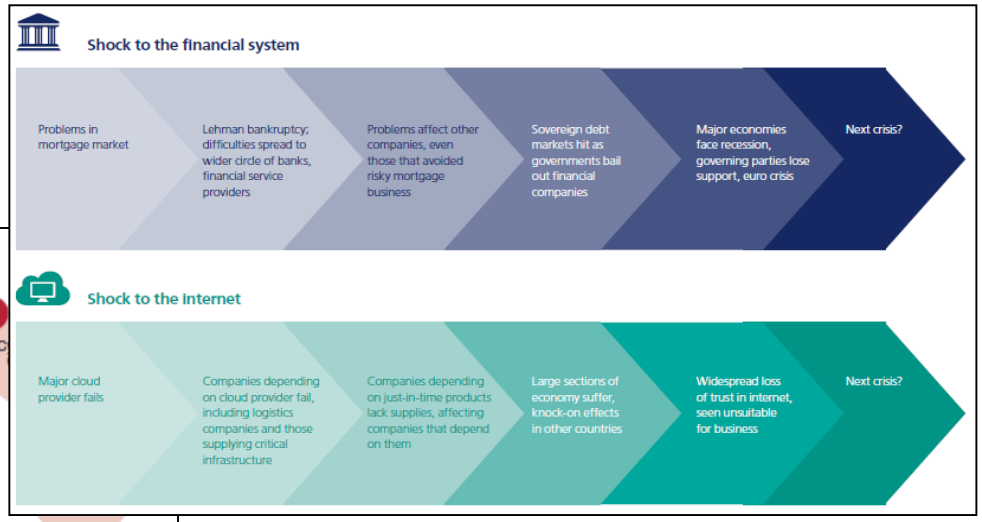


3. Terminology & increased use



3. Terminology: from data theft incident to global shock





«One or many events which lead to a complete or large-scale outage of the world wide web or one of its services. These events can be triggered intentionally (e.g. by paralyzing a internet backbone) or without malicious intent (natural causes, e.g. leading to a power outage and cascading effects for the world wide web infrastructure). To be a crisis, a big part of the population must be affected directly throughout days.»

precision

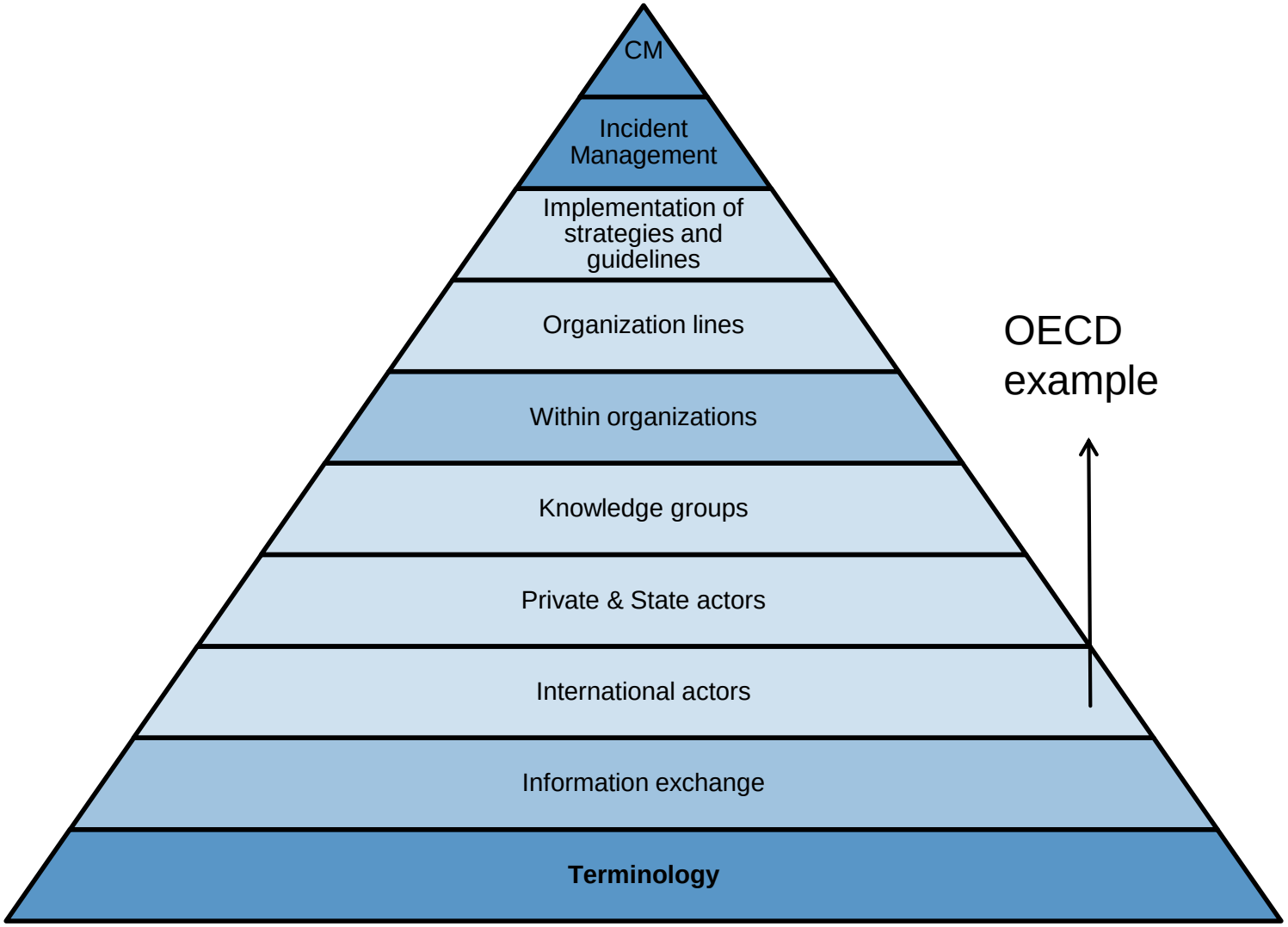
impact

«A cyber crisis is, when the consequences of a cyber security incident can't be controlled anymore.»

«Crisis, which has been triggered by a cyber incident, and influences components in regard to the confidentiality, integrity and availability of information.»

«Coordinated, large-scale cyber events that result in or have the potential to result in a widespread outage or disrupt multiple infrastructures are a national security concern. These events can be referred to as cyber crisis. »

3. Terminology: Relevance



3. Terminology: Conclusion

- Crisis combined with cyber is rarely defined, increasing the vagueness of both terms even more
- Overlap between different spheres (business, governments, I.O.) pretty vague
- «Cyber crisis» is used on three different organizational levels: strategic, operational and technical
- Initiatives to consolidate are there, but very difficult due to different perspective, priorities and interdisciplinary character

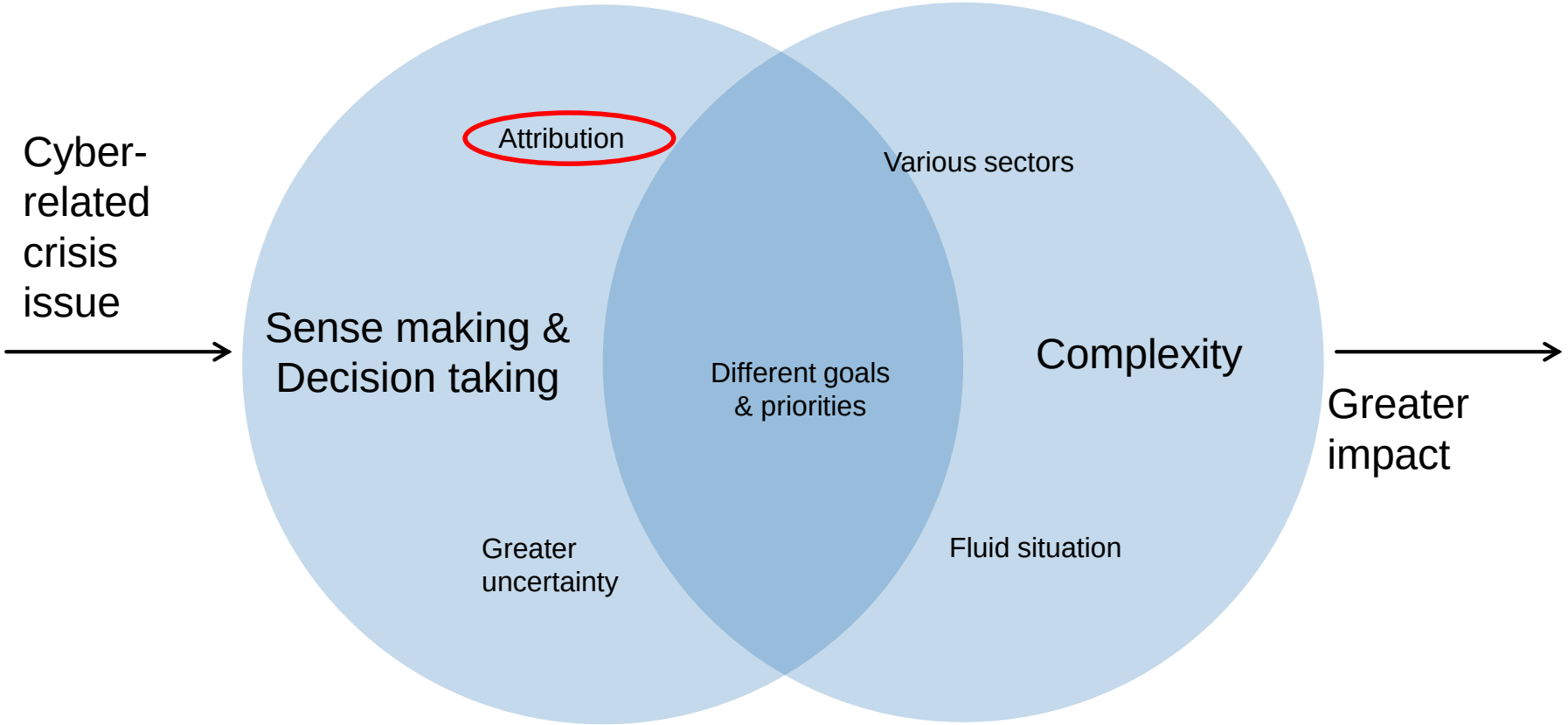
4. Cyber Crisis Management: Introduction

- Cyber-related crisis are basically the same as general crisis, just with a cyber component. Consequently, managing a cyber-crisis doesn't substantially diverge from general crisis management!

- «National Crisis Management for Crisis with Cyber characteristic»

- *Crisis understanding is taken from the general crisis management framework: it becomes a crisis when it exceeds the emergency-frame and needs decisions on a strategic level!*

4. Crisis Management Main Challenges – bringing in the Cyber component



«Intention may be the only line separating the attack from the accident.»

5. Threat landscape: attribution aspect

States:
- Numerous states have substantial capabilities
- Wide range of activities
- ➢ *Attribution varies depending on goals of activity and operation itself!*

Corporations:
- Potentially significant cyber capabilities
- Activities: Wide range of activities
- ➢ *Attribution difficult, as success of operations will depend on remaining clandestine and therefore remaining unidentified!*

Hacktivists/Cyber Fighters:
- Very heterogeneous group and therefore motivation and goals
- Activities: Ideological support
- ➢ *Attribution mostly less of a problem due to goals of activity!*

Cyber Terrorists:
- Potentially harming national security and society
- Activities: High-key attacks
- ➢ *Attribution mostly less of a problem due to goals of activity!*

Cybercriminals:
- Engaging in illegal/criminal activities in cyberspace with the goal of gaining profit
- Activities: Various kind of services
- ➢ *Attribution will be very difficult in most cases, as remaining unknown is key to establish business!*

Internal actors/Employees:
- Very heterogeneous activities, but big issue
- Activities: Malicious and non-malicious
- ➢ *Attribution will vary on a case-to-case basis, but mostly possible!*

5. Threat landscape & attribution in Cyber-Crisis Management: Trends & Conclusion

- Increased sophistication of attacks
- Especially nation-states have developed substantial capabilities

- Additional challenges increase problem of managing a cyber incident & cyber-crisis:
  - Terminology & attribution: When does an incident become a crisis?
  - Information & attribution
    - What happened and who is responsible?
    - Time sensitivity
    - Diverging interests
  - Increased interconnectedness = more coordination
  - Less tested and experienced cooperation networks
  - Dynamic due to new technological developments (big data, internet of things)

- Law-enforcement becoming increasingly successful
- More data on cyber-threats also means better quality of available information
- Increased cooperation for assessing and defending against cyber-threats

6. Next steps

- Increase bodies for cooperation and collaboration
  - Private companies, public sector
  - International cooperation

- Common understanding and terminology
  - Private companies, public sector, international

- Preparedness & Trust
  - Lack of experience with high-profile cyber-crisis situations
  - Increase trust between all stakeholders

- Intelligence & investigation capacities
  - Reducing the challenges of attribution
  - Code of conduct / legal questions: e.g. “hack back”

«Cyber incidents are a bit like a bar fight – you might have a pretty good idea who started it, but you will never be absolutely sure!»

Questions?