Sharing the scale, seriousness and perception of ICT incidents to help build confidence, transparency and interstate cooperation

OSCE CBM 15 implementation: OSCE steps to enhance the protection of critical infrastructures

Vienna, 11th March 2019

Why and how a severity scale to classify ICT incidents can help meet objectives of the CBM 15?

What kind of severity scale? Feedback and lessons learned from the French national one.

What virtuous and smart uses are possible for regional and subregional collaboration?

What could be the next steps?

Why and how a severity scale to classify ICT incidents can help meet objectives of the CBM15?

- Management of incidents and their impacts at national level: core of **sovereignty** and exclusive competence of **States**.
- Cooperation in this area is **not natural or easy**.
- But more and more potential **collateral damages**: interstate cooperation at regional or subregional level is **welcome.**
- **Building confidence** in day-to-day and adopting voluntary cooperation processes: one of the CBM 15's objectives.

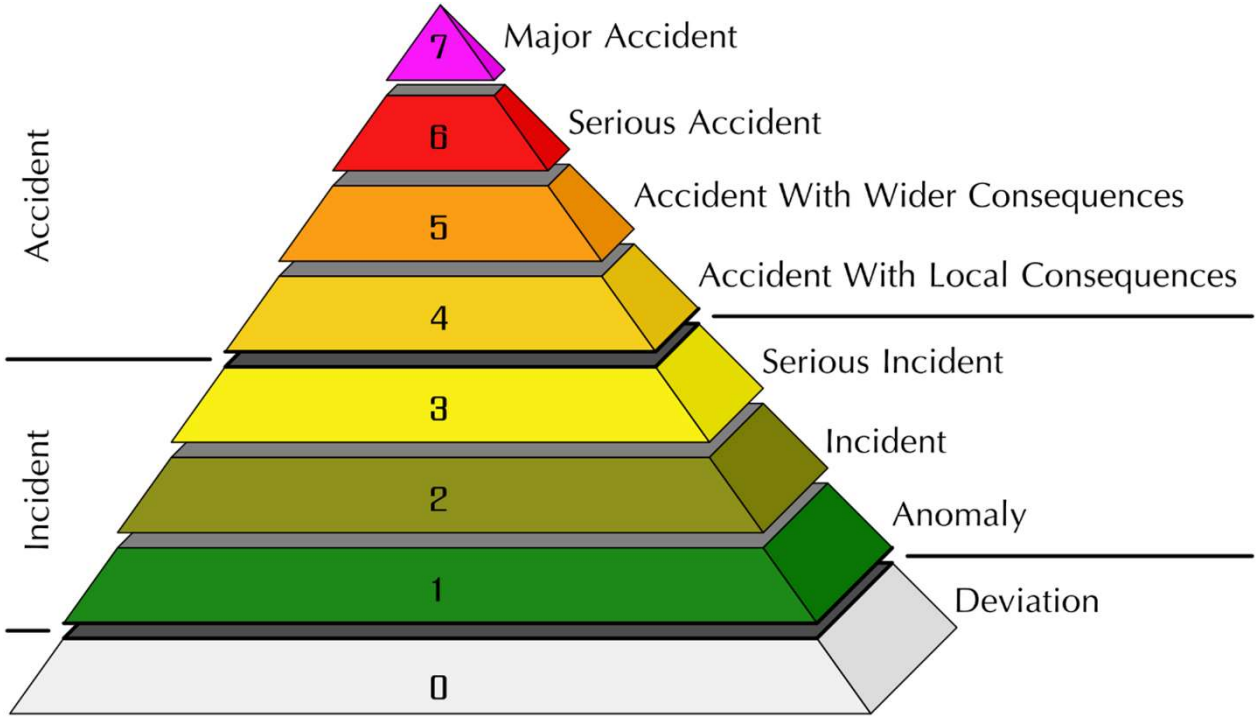
Why and how a severity scale to classify ICT incidents can help meet objectives of the CBM15?

- **A starting point:** developing a common severity scale or framework to classify ICT incidents in terms of impacts (on national economies, health, safety of citizens, etc.)
- **Help shared understanding and perception** of incidents
- **Encourage international collaboration** in the event of a serious ICT incident, especially in case of impact asymmetry among entities

Why and how a severity scale to classify ICT incidents can help meet objectives of the CBM15?

- Currently **no internationally recognized** or widely used incident scale for such purpose.
- Why not building an “INES” scale for cyber incidents?

The International Nuclear and Radiological Event Scale



What kind of severity scale? Feedback from the French national arrangements to classify the scale and seriousness of ICT incidents

SOVEREIGNTY AND DEMOCRACY, CONTINUITY OF STATE AND GOVERNMENTAL ACTION, INTEGRITY OF TERRITORY, CIVIL SECURITY AND SAFETY, HEALTH AND BASIC NEEDS OF THE POPULATION, ECONOMY, SECURITY AND ARMED FORCES,

Gravity scale	Impacts	***Characterization as armed aggression within the meaning of Article 51 of the United Nations***	***Possible defensive actions at national level***
Level 5 – Extreme Emergency	Extreme impact	*Probably possible: to be considered on a case by case basis.*	*Use of force in case of armed aggression only (notwithstanding measures below)*
Level 4 – Major Crisis	Major impact		
Level 3 – Crisis	Strong and extensive impact	*Probably not possible: actions corresponding to these levels could nonetheless constitute other internationally wrongful acts (intervention, violation of sovereignty, use of force, etc.).*	*Retaliation and/or peaceful countermeasures*
Level 2 – Serious incident	Strong and circumscribed impact		
Level 1B – Incident	Medium and circumscribed impact		
Level 1A – Significant event	Low impact		*N/A*
Level 0 – Event	Negligible impact		

What virtuous and smart uses are possible for regional and subregional collaboration?

Mains use cases:

- During an ICT incident: reduce the risks of misperception, escalation, and conflict.
- In a post-mortem phase: assess past ICT incidents for other CBM 15 arrangements.
- Every day to build cooperation and confidence in day-to-day.

What could be the next steps?

1. Defining together a common severity scale or framework for classifying ICT incidents in terms of impacts at national or transnational level

2. Defining possible cooperation within CBM 15 arrangements (e.g. sharing information on ICT threats, shared responses)

3. Assessing some past ICT incidents in order to share our respective perception and to adjust the framework and arrangements

What could be the next steps?

Success keys:

- NOT a mechanism for automatic response to an ICT incident!
- Sharing the perception and understanding of a regional or subregional incident in terms of severity of the impacts.
- Proposing, where appropriate, shared responses to common challenges in case of widespread or transnational disruption of ICT-enabled critical infrastructure.