MUNI
LAW

Crisis Management
EU Cyber Diplomacy Toolbox

Jakub HARAŠTA

MUNI
LAW

Crisis Management

Crisis

- *‘abnormal or extraordinary event or situation which threatens an organisation or community and requires a strategic, adaptive and timely response in order to preserve its viability and integrity‘* (ISO 22361:2022)
- *‘an event that affects many people and large parts of society and threatens fundamental values and functions. Crisis is a condition that cannot be handled with ordinary resources and organisation. A crisis is unexpected, far removed from the ordinary and mundane. Resolving the crisis requires coordinated action from several players/actors‘*

  (Report on Cyber Crisis Cooperation and Management, ENISA, 2014)

‚Measuring‘ Crisis

- Uncertainty, risk, potential for severe consequences
- Time sensitivity
  - Creeping Crisis: hidden/latent, under-the-radar, erupts suddenly/unexpectedly
  - Acute Crisis: sudden, unforeseen, massive impact in short amount of time
  - Recurring Crisis: regular occurrence, cyclic nature
- Transboundary/cross-sectoral impact

Cyber Incident vs. Cyber Crisis

- Cybersecurity incident is *‘an event compromising the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, network and information systems’* (NIS2 Directive)
- Large-scale cybersecurity incident *‘causes a level of disruption that exceeds a MS capacity to respond to it or which has a significant impact on at least two MS’* (NIS2 Directive)
- Cyber Crisis is defined by its scope / impact / frequency. Transition is largely a political decision (‚do we treat this large-scale cyber incident as a crisis?‘)

Causes of Cyber Crisis

- Physical: fire, flood, power failure
- Non-physical: action by malicious actors (cyberattack), human error, malfunction

- Hybrid nature of cyber domain as a challenge: Origin of incident / crisis as a mixture of conventional / unconventional, military / non-military, overt / covert, by state / non-state actor etc.

Nature of Crisis

- Generally (regardless of the definition):
  - Low-probability event
  - High-damage impact
  - Causes / effect might be (initially) unknown
  - Crisis management / mitigation requires multi-option decision-making
  - Time-sensitive response

(Cyber) Crisis Management: Tasks

- Sense-making
  - What is happening? Why is it happening?
- Meaning-making
  - Communication to others
  - Why is this a ‚crisis‘? Why must we act?
- Decision-making
  - What to do?
  - Logistical / time / legal constraints
  - Penetration through all levels (strategic / operational / technical)
- Termination
  - When is the crisis over?
  - Switching to non-crisis measures
- Learning / reform
  - Changes in policies / practices

(Cyber) Crisis Management: Phases

- Phase 1: Prevention (before, during, after)
  - Goal: Crisis does not occur; should it arise, it is quickly contained (effects are minimised / anticipated)
- Phase 2: Preparedness (before)
  - Goal: plans to support crisis response / management; building resilience (‚antifragility‘ by Taleb); building confidence
- Phase 3: Response (during)
  - Goal: prevent further damage; prevent spreading of crisis
- Phase 4: Recovery (after)
  - Goal: restoration; lessons learned

Best Practice?

- Difficult to formulate as specific mechanisms closely relate to national political / legal / economic ecosystem
- E.g. *Best Practices for Cyber Crisis Management,* ENISA, 2024

Phase 1: Prevention

- Adopt national definition of ‚cyber crisis‘ and take into account transboundary dimension
- Develop information security standards specific to the national public sector. Review and update regularly.
- Foster national initiative promoting the creation of prevention programs (e.g. centralised DDoS mitigation programmes)

Phase 2: Preparedness

- Define a governance structure, provide specific capabilities and appoint crisis coordinator. Ensure the department has the necessary operational and technical cyber skills to directly coordinate stakeholders during crisis.
- Map and gather information on critical entities and their most critical assets to enable rapid actions.
- Establish instantaneous and secure communication channels during a crisis.

Phase 2: Preparedness (II)

- Formalise a clear allocation of roles between stakeholders involved in responding to cyber crisis in an overall plan.
- Develop escalation criteria for activating the cyber crises plan / deploying relevant units. Take into account time, priority, severity etc.
- Develop methodology and risk assessment tools to optimise coordination and interoperability.

Phase 2: Preparedness (III)

- Test the overall plan through multiannual programme of cyber crisis management exercises and training sessions.
- Set up training sessions for current and future staff responsible for cyber crisis management at the operational level.
- Develop communication strategy including clear format for messaging, stakeholders to involve, priority levels and time factor and communication channels to be used.

Phase 3: Response

- Encourage the mobilisation of private-sector certified ‚trusted providers‘ to provide technical assistance to victims.
- Support victims‘ crisis communication via unified and transparent message.

- YOU PLANNED – NOW YOU ACT ACCORDINGLY!

Phase 4: Recovery

- Develop and implement business resumption plans with regular reviewing and updates. Consult with relevant stakeholders.
- Establish unit tasked with gathering feedback, drawing lessons learn and producing recommendation. Review, update, modify procedures. Refine action plans.

Policy / Law

- Policy:
  - Outline of goals (what we hope/want to achieve?)
  - Outline of methods and principles (how we want to achieve it?)
- Law:
  - Standards, procedures, principles that must be followed

Legal Framework for Crisis Management

- Roles, Responsibilities, Limitations
- Extra Powers (investigative, executive), ‚extraordinary legislation‘
  - Anti-terrorist Laws (e.g. Searches / arrests without judicial authorization)
  - Disaster Relief Legislation (e.g. Use of special funds)
  - State of War Legislation (e.g. Requisition of movables / immovables)
  - Cyber Emergency Legislation

EU-CyCLONe

- European cyber crisis liaison organisation network (EU-CyCLONe)
- Representatives of Member States‘ cyber crisis management authorities + Commission

MUNI
LAW

EU Cyber Diplomacy Toolbox

EU Cyber Diplomacy Toolbox (2017)

- Joint EU diplomatic response to malicious cyber activities
- Part of EU‘s approach within Common Foreign and Security Policy
- Contribution to conflict prevention, mitigation of cybersecurity threats, greater stability in international relations
- Aims to influence the behavior of potential aggressors

EU Cyber Diplomacy Toolbox (2017) (II)

- Shared situational awareness between Member States
- Proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity
- Respect towards applicable international law / fundamental rights / freedoms

EU Cyber Posture (2022)

- 5 core components:
  - Cyber resilience and capacity-building to prevent / protect against malicious cyber activities
  - Solidarity and comprehensive crisis management capabilities
  - Vision of global, open, free, stable and secure cyberspace, with international law, rules-based order and with UN framework for responsible state behaviour at its centre
  - Strong global partnerships, including through capacity-building efforts in third countries
  - Ability to prevent, discourage, deter and respond to threat actors seeking to deny / disrupt [our] secure and open access to cyberspace as well as critical functions, and affect the EU‘s strategic interests, including the security of its partners

Council Decision 2019/797 + Council Regulation 2019/796

- Restrictive measures against cyber-attacks threatening the EU/MS
- Sanctions against subjects directly responsible for cyber attacks + all subjects providing financial / technical / material support + subjects otherwise involved + subjects associated with those involved
- Sanctions against natural / legal persons, and other entities of bodies different from a State (non-state actors)
- State actors out of scope (attribution of cyber attacks to state is a sovereign political decision of every MS)
- Freezing assets, travel ban sanctions

MUNI
LAW

Questions?

Group tasks (discussion)

Please form groups of *[Jakub looks around, counting kind of quickly]* students.

Task #1

- What are useful powers/tools/capabilities to have when dealing with cyber crises?

- List 5 powers/tools/capabilities.

Task #2

- How to implement the tools from #1 into law?

Task #3

- Which body should handle cyber crisis management?

- Think of pros/cons.

Task #4

- Attack from computers in state A causes power outage in EU. As a result, people die (N<5). What is appropriate / proportionate response?

MUNI
LAW

Questions?