Blueprint
European coordinated response to large-scale cybersecurity incidents and crises

Artificial Intelligence – An opportunity for the EU cyber-crisis management

Athens, 3 June 2019

Ioannis Askoxylakis
Cybersecurity Policy Officer
Unit H1: Cybersecurity Technology & Capacity Building
Directorate H: Digital Society, Trust and Cybersecurity
Directorate General for Communication Networks, Content & Technology
DG CONNECT
European Commission
'Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.'

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017
Building EU Resilience to cyber attacks
- Reformed ENISA
- EU cybersecurity Certification Framework

Creating effective EU cyber deterrence
- Identifying malicious actors
- Stepping up the law enforcement response

Strengthening international cooperation on cybersecurity
- Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace

Cybersecurity Act
- NIS Directive Implementation

Communication
- Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund

Recommendation
- Cybersecurity competence network with a European Cybersecurity Research and Competence Centre
- Building strong EU cyber skills base, improving cyber hygiene and awareness

Building cybersecurity deterrence through the Member States' defence capability
- Stepping up public-private cooperation against cybercrime
- Stepping up political response

Strengthening cyber dialogues
- Modernising export controls, including for critical cyber-surveillance technologies
- Continue rights-based capacity building model

Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence

RECOMMENDATIONS

COMMISSION RECOMMENDATION (EU) 2017/1584
of 13 September 2017
on coordinated response to large-scale cybersecurity incidents and crises
Blueprint - Response
Definition: large-scale cybersecurity incidents and crises

• incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level
Blueprint – key mechanisms

- Incident
  - National Incident Handling / Crisis Mgt (National Incident Response Plan)
  - CSIRTs Network Cooperation (according to CSIRTs Network SOPs)
  - Monitoring
  - ARGUS Phase I

- Crisis
  - IPCR - Political Coordination at EU level
  - ARGUS Phase II
  - EEAS Crisis Response Mechanism

Member States
CSIRTs Network
IPCR
ARGUS
EEAS CRM
Blueprint – key mechanisms

- Integrated Political Crisis Response (IPCR)
- ARGUS rapid alert system
- EEAS Crisis Response Mechanism for CSDP
What is IPCR?

• The Integrated Political Crisis Response
• the EU crisis mechanism
• ... for cross sectorial / complex crises requiring coordination ...
• ... @ strategic / political level in the Council / European Council
IPCR Tools

- An informal roundtable
- The Integrated Situational Awareness and Analysis (ISAA) report
- The IPCR web platform
- The central IPCR 24/7 contact point
The IPCR architecture

- **IPCR Web Platform**
  - Situation monitoring
  - Stepped-up information exchange
  - Structured information collection
  - Internal communication

- **Integrated Situational Awareness and Analysis (ISAA)**

- **Presidency roundtable:**
  - Situation and possible evolution
  - Breaking points (thresholds of irreversibility)
  - Policy options/Proposals for action
  - Communication

- **Coreper**
  - Council preparatory bodies when and if relevant
  - Council/European Council

- **Political decision-making/coordination**
ARGUS rapid alert system

Covers a full range of policies/tools

- transport, energy
- disaster management
- nuclear/radiological
- migration, health, food
- financial, customs
- etc...

Can involve 42 DGs, EEAS EU Agencies, Cabinets...

40+ sectoral rapid alert and communication systems

- CECIS, CIWIN, ECURIE, RAS-BICHAT, EWRS, CRMS-RIF, EFAS, EFFIS, EMS, NOAH, etc...
- (incl. with EC-external stakeholders: MS, los...)

(ARGUS rapid alert system)
ARGUS Phase II

- Activated by Commission President
  - in a major multisectoral crisis or imminent threat
- Crisis Coordination Committee:
  - Convened on a short notice
  - Chaired by (Deputy) Secretary General
  - Brings all relevant CABs, DGs, Agencies + EEAS (Core: SG, COMM, DIGIT, ECHO, ENV, HOME, HR, JUST, SANTE, TAXUD, TRADE, JRC, SJ)
  - Purpose: Information exchange & Decision-making
ARGUS Phase II so far

- A/H1N1 influenza pandemic threat (2009)
- Volcanic ash cloud (Eyjafjallajökull, 2010)
- Japan triple disaster (Fukushima, 2011)
- Migration and refugee crisis (2015- (ongoing))
Blueprint – core objectives

- Cooperation
- Shared Situational Awareness
- Effective Response
- Common Message
Recap: Blueprint – Cooperation at all levels

Technical
- Incident handling during a cybersecurity crisis.
- Monitoring and surveillance of incident including continuous analysis of threats and risk.

Operational
- Preparing decision-making at the political level.
- Coordinate the management of the cybersecurity crisis (as appropriate).
- Assess the consequences and impact at EU level and propose possible mitigating actions.

Political / Strategic
- Strategic and political management of both cyber and non-cyber aspects of the crisis including measures under the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities
Recap: Blueprint – integration in IPCR arrangements

1. Regular Monitoring
2. Analysis and Advice
3. Assessment
4. Presidency Roundtable Preparation
5. ISAA Preparation
6-7. Presidency Roundtable
9. Impact Monitoring

Incident

Yes

4. Presidency Roundtable Preparation

EU Cybersecurity Incident Situation Report

8. Council / Coreper Meeting

Coordinate Technical Response, Public Communications

Crisis Ongoing?

ENISA Event Enquiry

10. Phasing Out

NO

Yes

IPCR Activation? (Presidency)

Coordinated Technical Response, Public Communications

Cyber Diplomacy Toolbox
Blueprint Taxonomy – as a Political Decision support mechanism

- **Nature of the Incident**
  - Root cause category: (1 of 5)
    - System failures, natural phenomena, human errors, malicious actions, 3rd party failures
  - Severity of threat: (1 of 3)
    - High, medium, low

- **Impact**
  - Sectors impacted: (1 or more of 11)
    - Energy, transport, banking, finance, health, drinking water, digital infrastructure (7 NISD sectors with OES)
    - Communications (EU ecomms framework directive)
    - Trust and identification (EIDAS)
    - Digital services (NISD DSP)
    - Government services
  - Scale of impact: (1 of 4)
    - Red – very large, Yellow – large, Green - minor, White – no
  - Outlook: (1 of 3)
    - Improving, stable, worsening
Parallel and Coordinated Exercise 2018 (EU HEX-ML PACE 2018)

- Double exercise containing a CSDP planning (ML) and an event driven (HEX) crisis management exercise, coordinated with and conducted in parallel with NATO.
- It took place between 5-23 November, with the conduct phase held between 19-23 November
The objective was twofold:

- to improve and enhance the EU’s ability to respond to a complex crisis of a hybrid nature with an internal and an external dimension
- to improve cooperation with NATO in response to a hybrid crisis
PACE 2018 – Policy areas

- The **policy areas** where the crisis responses mechanisms were triggered during the exercise were:
  - **Cybersecurity, terrorism, CBRN, maritime, energy, health/food security, poly-criminal exchange of information and communication**
PACE 2018 – Cybersecurity objectives

• Test cyber threat assessment capacity and threat information exchange with other EU stakeholders.
• Test the capacity of the EU institutions and relevant EU Agencies (including ENISA, EU-LISA, Europol and CERT-EU) to coordinate and to respond to large-scale cybersecurity incidents and crises at the operational and political/strategic level.
PACE 2018: Main observations 1/2

- Positive involvement of various actors allowing for testing Blueprint to a broad extent – **overall successful use of Blueprint** during the exercise
- **Good cooperation** among the actors within the cyber community as well as with NATO
- **Reinforced knowledge about Blueprint** among the communities less accustomed with cyber issues but still using the cyber tools; **still lacking of proper awareness** about the Blueprint among some (“less usual”) services
PACE 2018: Main observations 2/2

• There is a certain lack of operational clarity in the design of Blueprint favouring different interpretation of the Blueprint by the various the actors;

• There are challenges due to the use of different taxonomies by the different communities (in particular cyber vs law enforcement) for the same phenomena

• The information exchange among different communities (e.g. cyber vs law enforcement) is very difficult or sometimes impossible due to: technical, legal and practical obstacles;
Next steps

• [Blue Olex 2019]
• SOPs
• Cyber Europe 2020
Thank you for your attention!