RECOMMENDATIONS

COMMISSION RECOMMENDATION (EU) 2017/1584

of 13 September 2017

on coordinated response to large-scale cybersecurity incidents and crises

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 292 thereof,

Whereas:

(1) The use of and dependence on information and communication technologies have become fundamental aspects in all sectors of economic activity as our companies and citizens are more interconnected and interdependent across sectors and borders than ever before. A cybersecurity incident affecting organisations in more than one Member State or even the entire Union with potential serious disruptions to the internal market and more broadly to the network and information systems on which the Union economy, democracy and society rely is a scenario that Member States and EU institutions have to be well-prepared for.

(2) A cybersecurity incident may be considered a crisis at Union level when the disruption caused by the incident is too extensive for a concerned Member State to handle on its own or when it affects two or more Member States with such a wide-ranging impact of technical or political significance that it requires timely coordination and response at Union political level.

(3) Cybersecurity incidents can trigger a broader crisis, impacting sectors of activity beyond network and information systems and communication networks; any appropriate response must rely upon both cyber and non-cyber mitigation activities.

(4) Cybersecurity incidents are unpredictable, often occur and evolve within very short periods of time and therefore affected entities and those with responsibilities as regards responding to and mitigating the effects of the incident must coordinate their response quickly. Furthermore, cybersecurity incidents are often not contained with any specific geographical area and may occur simultaneously or spread instantly across many countries.

(5) An effective response to large-scale cybersecurity incidents and crises at the EU level requires swift and effective cooperation amongst all relevant stakeholders and relies on the preparedness and capabilities of individual Member States as well as coordinated joint action supported by Union capabilities. Timely and effective response to incidents relies therefore on the existence of previously established and, to the extent possible, well-rehearsed cooperation procedures and mechanisms having clearly defined the roles and responsibilities of the key actors at national and Union level.

(6) In its conclusions ([1]) on Critical Information Infrastructure Protection of 27 May 2011, the Council invited the EU Member States to 'strengthen collaboration among Member States and contribute, on the basis of national crisis management experiences and results and in cooperation with ENISA to the development of European cyber incident cooperation mechanisms to be tested in the framework of the next Cyber Europe exercise in 2012'.

(7) The 2016 Communication 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry' ([2]) encouraged Member States to make the most out of the NIS Directive ([3])

([1]) Council conclusions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber security', document 10299/11, Brussels, 27 May 2011.
([2]) COM(2016) 410 final, 5 July 2016
([3]) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, p. 1).

cooperation mechanisms and to enhance cross-border cooperation related to preparedness for a large-scale cyber incident. It added that a coordinated approach to crisis cooperation across the various elements of the cyber ecosystem to be set out in a 'blueprint' would increase preparedness and that such a blueprint should also ensure synergies and coherence with existing crisis management mechanisms.

(8) In the Council Conclusions ([1]) on the aforementioned Communication, Member States called on the Commission to submit such a blueprint for consideration by the bodies and other relevant stakeholders. However the NIS Directive does not provide for a Union cooperation framework in case of large-scale cybersecurity incidents and crises.

(9) The Commission, consulted with Member States in two separate consultation workshops held in Brussels on 5 April and 4 July 2017 with Member States representatives from Computer Security Incident Response Teams (CSIRTs), the Cooperation Group established by the NIS Directive and the Council Horizontal Working Party on Cyber Issues as well as representatives from the European External Action Service (EEAS), ENISA, Europol/EC3 and the General Secretariat of the Council (GSC).

(10) The present Blueprint for coordinated response to large-scale cybersecurity incidents and crises at the Union level, annexed to this Recommendation, is the outcome of the aforementioned consultations and complements the Communication on 'Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry'.

(11) The Blueprint describes and sets out the objectives and modes of cooperation between the Member States and EU institutions, bodies, offices and agencies (hereafter referred to as 'EU institutions') in responding to large-scale cybersecurity incidents and crises and how existing Crisis Management mechanisms can make full use of existing cybersecurity entities at EU level.

(12) In responding to a cybersecurity crisis in the sense of recital 2, coordination of the response at political Union level in the Council will use the Integrated Political Crisis Response (IPCR) arrangements ([2]); the Commission will use the ARGUS ([3]) high-level cross-sectoral crisis coordination process. If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the European External Action Service (EEAS) Crisis Response Mechanism (CRM) ([3]) will be activated.

(13) In certain areas, sectoral crisis management mechanisms at EU level provide for cooperation in case of cybersecurity incidents or crisis. For example, in the framework of the European Global Navigation Satellite System (GNSS), Council Decision 2014/496/CFSP ([4]) already defines the respective roles of the Council, the High Representative, the Commission, the European GNSS Agency and the Member States within the chain of operational responsibilities set up in order to react to a threat to the Union, to the Member States or to the GNSS, including in case of cyber-attacks. Therefore, this recommendation should be without prejudice to such mechanisms.

(14) Member States have the primary responsibility for the response in case of large-scale cybersecurity incidents or crises affecting them. The Commission, the High Representative and other EU institutions or services have however an important role, stemming from Union law or from the fact that cybersecurity incidents and crises may impact all sections of economic activity within the single market, the security and international relations of the Union, as well as the institutions themselves.

(15) At Union level, the key actors involved in response to cybersecurity crises include the newly established NIS Directive structures and mechanisms, namely the Computer Security Incident Response Teams (CSIRTs) network, as well as the relevant agencies and bodies namely the European Union Agency for Network and Information Security (ENISA), the European Cybercrime Centre at Europol (Europol/EC3), the EU Intelligence Analysis Centre (INTCEN), EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (Sitroom) working together as SIAC (the Single Intelligence Analysis Capacity), the EU Hybrid Fusion Cell (based in INTCEN), the Computer Emergency Response Team for the EU institutions (CERT-EU) and the Emergency Response Coordination Centre in the European Commission.

(16) Cooperation amongst Member States in responding to cybersecurity incidents at technical level is provided by the CSIRTs Network established by the NIS Directive. ENISA provides the secretariat for the Network and actively

([1]) Document 14540/16, 15 November 2016.
([2]) Further information can be found in Section 3.1 of the Appendix on Crisis management, cooperation mechanisms and actors at EU level.
([3]) Ibid.
([4]) Council Decision 2014/496/CFSP of 22 July 2014 on aspects of the deployment, operation and use of the European Global Navigation Satellite System affecting the security of the European Union and repealing Joint Action 2004/552/CFSP (OJ L 219, 25.7.2014, p. 53).

supports the cooperation among the CSIRTs. The national CSIRTs and the CERT-EU cooperate and exchange information on a voluntary basis including, when necessary, in response to cybersecurity incidents that affect one or more Member States. At the request of a representative of a Member State's CSIRT, they may discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State. Relevant procedures will be set out in CSIRTs Network's Standard Operating Procedures (SOPs) ([1]).

(17) The CSIRTs network is also tasked with discussing, exploring and identifying further forms of operational cooperation, including in relation to categories of risks and incidents, early warnings, mutual assistance, principles and modalities for coordination, when Member States respond to cross-border risks and incidents.

(18) The Cooperation Group established by Article 11 of the NIS Directive is tasked with providing strategic guidance for the activities of the CSIRTs network and discussing capabilities and preparedness of the Member States, and, on a voluntary basis, evaluating national strategies on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice.

(19) A dedicated work stream within the Cooperation Group is preparing incident notification guidelines, pursuant to Article 14(7) of the NIS Directive, concerning the circumstances in which operators of essential services are required to notify incidents pursuant to Article 14(3) and the format and procedure for such notifications ([2]).

(20) Awareness and understanding of the real-time situation, risk posture, and threats gained through reporting, assessments, research, investigation, and analysis, is vital to enable well-informed decisions This 'situational awareness' — by all relevant stakeholders — is essential for an effective coordinated response. Situational awareness includes elements about the causes as well as the impact and origin of the incident. It is recognised that this depends on exchange and sharing of information between relevant parties in a suitable format, using a common taxonomy to describe the incident and in an appropriately secure manner.

(21) Responding to cybersecurity incidents may take many forms, ranging from identifying technical measures which may entail two or more entities jointly investigating the technical causes of the incident (e.g. malware analysis) or identifying ways through which organisations may assess whether they have been affected (e.g. indicators of compromise), to operational decisions on applying such measures and, at the political level, deciding on the use of other instruments such as the Framework for a Joint response to malicious cyber activities ([3]) or the EU operational protocol for countering hybrid threats ([4]), depending on the incident.

(22) European citizens' and businesses' trust in digital services is essential for a flourishing digital single market. Therefore, crisis communication plays a particularly important role in mitigating the negative effects of cybersecurity incidents and crises. Communication may also be used in the context of the Framework for a Joint Diplomatic Response as a means to influence the behaviour of (potential) aggressors acting from third countries. Aligning the public communication to mitigate the negative effects of cybersecurity incidents and crises and the public communication to influence an aggressor is essential for a political response to be effective.

(23) Providing the public with information on how they can mitigate at user and organisational level the effects of an incident (for example by applying a patch or taking complementary actions to avoid the threat, etc.) could be an effective measure to mitigate a large-scale cybersecurity incident or crisis.

(24) The Commission, through the Connecting Europe Facility (CEF) cybersecurity Digital Service Infrastructure, is developing a Core Service Platform cooperation mechanism, known as MeliCERTes, between participating Member States CSIRTs to improve their levels of preparedness, cooperation and response to emerging cyber threats and incidents. The Commission, through competitive calls for proposals for grant awards under CEF is co-funding CSIRTs in the Member States with a view to improving their operational capacities at national level.

([1]) Under development; expected to be adopted by the end of 2017.
([2]) The guidelines are intended to be finalised by the end of 2017.
([3]) Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'), Doc. 9916/17
([4]) Joint Staff Working Document EU operational protocol for countering hybrid threats, 'EU Playbook', SWD(2016) 227 final, 5 July 2016.

(25) Cybersecurity exercises at EU level are essential to stimulate and improve cooperation among the Member States and the private sector. To this end, since 2010, ENISA organises regular pan-European cyber incident exercises ('Cyber Europe').

(26) The Council Conclusions ([1]) on the Implementation of the Joint Declaration by the President of the European Council, the President of the European Commission and the Secretary-General of the North Atlantic Treaty Organisation calls for the strengthening cooperation in cyber exercises through reciprocal staff participation in respective exercises, including in particular Cyber Coalition and Cyber Europe.

(27) The constantly evolving threat landscape and recent cybersecurity incidents are an indication of the increasing risk faced by the Union, Member States should act on the present recommendation without further delay and in any case by the end of 2018,

HAS ADOPTED THIS RECOMMENDATION:

(1) Member States and EU institutions should establish an EU Cybersecurity Crisis Response Framework integrating the objectives and modalities of cooperation presented in the Blueprint following the guiding principles described therein.

(2) The EU Cybersecurity Crisis Response Framework should in particular identify the relevant actors, EU institutions and Member State authorities, at all necessary levels — technical, operational, strategic/political — and develop, where necessary, standard operating procedures that define the way in which these cooperate within the context of EU crisis management mechanisms. Emphasis should be placed on enabling the exchange of information without undue delay and coordinating the response during large-scale cybersecurity incidents and crises.

(3) To this end, Member States' competent authorities should work together towards further specifying information-sharing and cooperation protocols. The Cooperation Group should exchange experiences on these matters with relevant EU institutions.

(4) Member States should ensure that their national crisis management mechanisms adequately address cybersecurity incident response as well as provide necessary procedures for cooperation at EU level within the context of the EU Framework.

(5) As regards existing EU crisis management mechanisms, in line with the Blueprint, Member States should, together with Commission services and the EEAS, establish practical implementation guidelines as regards the integration of their national crisis management and cybersecurity entities and procedures into existing EU crisis management mechanisms, namely the IPCR and EEAS CRM. In particular, Member States should ensure that appropriate structures are in place to enable the efficient flow of information between their national crisis management authorities and their representatives at EU level in the context of EU crisis mechanisms.

(6) Member States should make full use of the opportunities offered by the Cybersecurity Digital Service Infrastructures (DSI) programme of the Connecting Europe Facility (CEF), and cooperate with the Commission to ensure that the Core Service Platform cooperation mechanism, currently under development, provides the necessary functionalities and fulfils their requirements for cooperation also during cybersecurity crises.

(7) Member States, with the assistance of ENISA and building on previous work in this area, should cooperate in developing and adopting a common taxonomy and template for situational reports to describe the technical causes and impacts of cybersecurity incidents to further enhance their technical and operational cooperation during crises. In this regard, Member States should take into account the ongoing work within the Cooperation Group on incident notification guidelines and in particular aspects related to the format of national notifications.

(8) The procedures laid out in the Framework should be tested and when necessary revised following lessons learnt from Member State participation in national, regional, and Union as well as cyber diplomacy and NATO cybersecurity exercises. In particular, they should be tested in the context of the Cyber Europe exercises organised by ENISA. Cyber Europe 2018 presents a first such opportunity.

([1]) ST 15283/16, 6 December 2016.

(9) Member States and the EU institutions should regularly practise their response to large-scale cybersecurity incidents crisis at national and European level, including their political response, where necessary and with the involvement of private sector entities as appropriate.

Done at Brussels, 13 September 2017.

For the Commission
Mariya GABRIEL
Member of the Commission

ANNEX

Blueprint for coordinated response to large-scale cross-border cybersecurity incidents and crises

INTRODUCTION

This Blueprint applies to cybersecurity 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.

Such large-scale cybersecurity incidents are considered a cybersecurity 'crisis'.

In case of an EU-wide crisis with cyber elements, coordination at Union political level of the response shall be carried out by the Council, using the Integrated Political Crisis Response (IPCR) arrangements.

Within the Commission, coordination will take place in accordance with the ARGUS rapid alert system.

If the crisis entails an important external or Common Security and Defence Policy (CSDP) dimension, the EEAS Crisis Response Mechanism is activated.

The Blueprint describes how these well-established Crisis Management mechanisms should make full use of existing cybersecurity entities at EU level as well as of cooperation mechanisms between the Member States.

In doing so, the Blueprint takes into account a set of guiding principles (proportionality, subsidiarity, complementarity and confidentiality of information), presents the core objectives of cooperation (effective response, shared situational awareness, public communication messages) at three levels (strategic/political, operational and technical), the mechanisms and the actors involved as well as the activities to meet said core objectives.

The Blueprint does not cover the full crisis management lifecycle (prevention/mitigation, preparedness, response, recovery) but focuses on response. Nevertheless, certain activities, in particular those related to achieving a shared situational awareness, are addressed.

It is also important to note that cybersecurity incidents can be at the origin or part of a broader crisis, impacting other sectors. Given that most cybersecurity crises are expected to have effects on the physical world, any appropriate response must rely upon both cyber and non-cyber mitigation activities. Cyber crisis response activities should be coordinated with other crisis management mechanisms at EU, national or sectoral levels.

Finally, the Blueprint does not replace and should be without prejudice to existing sector-specific or policy-specific mechanisms, arrangements or instruments such as the one set up for the European Global Navigation Satellite System (GNSS) programme ([1]).

Guiding principles

In working towards the objectives, in identifying the necessary activities and assigning roles and responsibilities to respective actors or mechanisms, the following guiding principles have been applied and also need to be respected when preparing future implementing guidelines.

Proportionality: The great majority of cybersecurity incidents affecting Member States fall well below anything that may be considered a national 'crisis', much less a European one. The foundation of cooperation amongst Member States in responding to such incidents is provided by the Computer Security Incident Response Teams (CSIRTs) Network established by the NIS Directive ([2]). The national CSIRTs cooperate and exchange information voluntarily on a daily basis including, when necessary, in response to cybersecurity incidents that affect one or more Member States in line with the CSIRTs Network's Standard Operating Procedures (SOPs). The Blueprint should therefore make full use of these SOPs and any additional cybersecurity crisis specific tasks should be reflected therein.

([1]) Decision 2014/496/CFSP.
([2]) Directive (EU) 2016/1148.

Subsidiarity: The principle of subsidiarity is key. Member States have the primary responsibility for the response in case of large-scale cybersecurity incidents or crises affecting them. The Commission, the European External Action Service and other EU institutions, offices, agencies and bodies have however an important role. This role is clearly set out in the IPCR arrangements but also stems from Union law or simply from the fact that cybersecurity incidents and crises may impact all sections of economic activity within the single market, the security and international relations of the Union, as well as the institutions themselves.

Complementarity: The Blueprint takes fully into account existing crisis management mechanisms at EU level, namely the Integrated Political Crisis Response (IPCR) arrangements, ARGUS, and the EEAS Crisis Response Mechanism, integrates therein the new NIS Directive structures and mechanisms, namely the CSIRTs Network, as well as the relevant agencies and bodies namely the European Union Agency for Network and Information Security (ENISA), the European Cybercrime Centre at Europol (Europol/EC3), the EU Intelligence Analysis Centre (INTCEN), EU Military Staff Intelligence Directorate (EUMS INT) and Situation Room (Sitroom) in INTCEN, working together as SIAC (the Single Intelligence Analysis Capacity); the EU Hybrid Fusion Cell (based in INTCEN); and the Computer Emergency Response Team for the EU Institutions, Bodies and Agencies (CERT-EU). In doing so, the Blueprint should also ensure that their interaction and cooperation achieves maximum complementarity and minimum overlap.

Confidentiality of information: All information exchanges in the context of the Blueprint must comply with applicable rules on security ([1]), on the protection of personal data and the Traffic Light Protocol ([2]). For the exchange of classified information, regardless of the classification scheme applied, available accredited tools shall be used ([3]). As regards the processing of personal data, it will respect the applicable EU rules, in particular the General Data Protection Regulation ([4]), the ePrivacy Directive ([5]) as well as the Regulation ([6]) 'on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data'.

Core objectives

Cooperation under the Blueprint follows the three-level approach mentioned above — political, operational and technical. At each level, cooperation may include exchanging information as well as joint actions, and aims to achieve the following core objectives.

— Enable an effective response. Response may take many forms, ranging from identifying technical measures which may entail two or more entities jointly investigating the technical causes of the incident (e.g. malware analysis) or identifying ways that organisations may assess whether they have been affected (e.g. indicators of compromise), to operational decisions on applying such technical measures and, at the political level, deciding to trigger other instruments such as the EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox') or the EU operational protocol for countering hybrid threats depending on the incident.

— Share situational awareness. A sufficiently good understanding of events as they unfold by all relevant stakeholders on all three levels (technical, operational, political) is essential for a coordinated response. Situational awareness may include technological elements about the causes as well as the impact and origin of the incident. As cybersecurity incidents may affect a wide variety of sectors (finance, energy, transport, healthcare, etc.), it is imperative that the appropriate information, in the suitable format, reaches all relevant stakeholders in a timely manner.

([1]) Commission Decision (EU, Euratom) 2015/443 of 13 March 2015 on Security in the Commission (OJ L 72, 17.3.2015, p. 41) and Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information (OJ L 72, 17.3.2015, p. 53); Decision of the High Representative of the Union for Foreign Affairs and Security Policy of 19 April 2013 on the security rules for the European External Action Service (OJ C 190, 29.6.2013, p. 1). Council Decision 2013/488/EU of 23 September 2013 on the security rules for protecting EU classified information (OJ L 274, 15.10.2013, p. 1).

([2]) https://www.first.org/tlp/

([3]) In June 2016, these transmission channels included CIMS (Classified Information Management System), ACID (encryption algorithm), RUE (secure system to create, exchange and store RESTREINT UE/EU RESTRICTED documents) and SOLAN. Other means of, e.g. transmitting classified information include PGP or S/MIME.

([4]) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

([5]) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

([6]) Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ L 8, 12.1.2001, p. 1) — under review.

— Agree on key public communication messages ([1]). Crisis communications play an important role in mitigating the negative effects of cybersecurity incidents and crises but may also be used as a means for influencing the behaviour of (potential) aggressors. An appropriate message can also serve to clearly signal the likely consequences of a diplomatic response to influence the behaviour of aggressors. Aligning the public communication to mitigate the negative effects of cybersecurity incidents and crises and the public communication to influence an aggressor is essential for a political response to be effective. Particularly important in cybersecurity is the dissemination of accurate actionable information on how the public can mitigate the effects of an incident (e.g. applying a patch, taking complementary actions to avoid the threat, etc.).

COOPERATION BETWEEN MEMBER STATES AND MEMBER STATES AND EU ACTORS AT TECHNICAL, OPERATIONAL AND STRATEGIC/POLITICAL LEVELS

Effective response to large-scale cybersecurity incidents or crisis at EU level depends on effective technical, operational and strategic/political cooperation.

At each level, the actors involved should perform specific activities as regards achieving three core objectives:

— coordinated response,

— shared situational awareness,

— public communications.

Throughout the incident or crisis, lower levels of cooperation will alert, inform and support the higher levels; the higher levels will provide guidance ([2]) and decisions to the lower levels, as appropriate.

Cooperation at the technical level

Scope of activities:

— Incident handling ([3]) during a cybersecurity crisis

— Monitoring and surveillance of incident including continuous analysis of threats and risk.

Potential actors

At the technical level, the central mechanism for cooperation in the Blueprint is the CSIRTs Network, chaired by the Presidency and with secretariat provided by ENISA.

— Member States:

  — Competent authorities and single points of contact established by the NIS Directive

  — CSIRTs

— EU bodies/offices/agencies

  — ENISA

  — Europol/EC3

  — CERT-EU

([1]) It is important here to note that public communication can refer to both communication about the incident to the public as a whole, and communication of more technical or operational information with critical sectors and/or those who have been affected. This may require the use of confidential dissemination channels and the use of specific technical tools/platforms. In either case, communication with operators and to the wider public within any Member States is the prerogative and responsibility of each Member State. Therefore, in line with the principle of subsidiarity presented above, Member States and national CSIRTs have the ultimate responsibility for the information that is disseminated within their territory and to their constituency respectively.

([2]) 'Permissions to act' — in light of a cybersecurity crisis, short reaction times are of vital importance in order to set appropriate mitigation actions. In order to provide these short reaction times, voluntary 'permissions to act' can be issued from one Member State to another, giving a Member State permission to act immediately, without having to consult with higher levels or EU institutions and going through all of the normally required, official channels, if it is not required in a particular incident (e.g. a CSIRT should not have to consult with higher levels to forward valuable information to a CSIRT in another Member State).

([3]) 'Incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto.

— European Commission

  — The ERCC (24/7 operational service located in DG ECHO), and the designated lead service (to be chosen between DG CNECT and DG HOME depending on the particular nature of the incident), the Secretariat-General (ARGUS secretariat), DG HR (Security Directorate), DG DIGIT (IT Security Operations).

  — For other EU agencies ([1]) the respective parent DG in the Commission or the EEAS (first point of contact).

— EEAS

  — SIAC (Single Intelligence Analysis Capacity: EU INTCEN and EUMS INT)

  — EU Situation Room and the nominated geographic or thematic service.

  — EU Hybrid Fusion Cell (part of EU INTCEN — cybersecurity in a hybrid context).

Shared situational awareness:

— As part of the regular cooperation at technical level to support Union situational awareness, ENISA should on a regular basis prepare the EU Cybersecurity Technical Situation Report on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NIS Directive single points of contact, European Cybercrime Centre (EC3) at Europol and CERT-EU and where appropriate the European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission, the HRVP and the CSIRTs Network.

— In case of major incident, the CSIRTs Network Chair, with the assistance of ENISA, prepares an EU Cybersecurity Incident Situation Report ([2]) which is presented to the Presidency, the Commission and the HRVP via the CSIRT of the rotating Presidency.

— *All other EU agencies* report to their respective parent DGs who in turn report to the Commission lead service.

— *CERT-EU* provides technical reports to the CSIRTs Network, EU institutions and agencies (as appropriate) and ARGUS (if activated).

— *Europol/EC3* ([3]) *and CERT-EU* provides expert forensic analysis of technical artefacts and other technical information to the CSIRTs Network.

— EEAS SIAC: On behalf of INTCEN, the EU Hybrid Fusion Cell reports to relevant the EEAS departments.

Response:

— *The CSIRTs Network* exchanges technical details and analysis on the incident, such as IP addresses, indicators of compromise ([4]), etc. Such information should be provided without undue delay to ENISA and not later than 24 hours from when the incident is detected.

— In accordance with the CSIRTs Network Standard Operating Procedures, its members cooperate in their efforts to analyse the available technical artefacts and other technical information related to the incident with a view of determining the cause and possible technical mitigation measures.

— ENISA assists CSIRTs' in their technical activities relying on its expertise and in accordance with its mandate ([5]).

([1]) Depending on the nature and the impact of the incident on different sectors of activity (finance, transport, energy, healthcare, etc.) the relevant EU agencies or bodies will be involved.

([2]) The EU Cybersecurity Incident Situation Report is an aggregation of national reports provided by national CSIRTs. The format of the report should be described in the CSIRTs Network SOPs.

([3]) In accordance and under the conditions and procedures set in EC3's legal framework.

([4]) 'Indicator of compromise' (IOC) in computer forensics is an artefact observed on a network or in an operating system that with high confidence indicates a computer intrusion. Typical IOCs are virus signatures and IP addresses, MD5 hashes of malware files or URLs or domain names of botnet command and control servers.

([5]) Proposal for a Regulation on the ENISA, the European Cybersecurity Agency and repealing Regulation (EU) No 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act'), 13 September 2017.

— Member States' CSIRTs coordinate their technical response activities with the assistance of ENISA and the Commission.

— EEAS SIAC: On behalf of INTCEN, the EU Hybrid Fusion Cell sets the collection process to gather initial evidence in motion.

Public communications:

— CSIRTs produce technical advisories [1] and vulnerability alerts [2] and disseminate them to their respective communities and the public following the authorisation procedures applicable in each case.

— ENISA facilitates the production and dissemination of common CSIRTs Network communications.

— ENISA coordinates its public communication activities with the CSIRTs Network and the Commission's Spokesperson service.

— ENISA and EC3 coordinate their public communication activities based on the shared situational awareness agreed among Member States. They both coordinated their public communication activities with the Commission's Spokesperson service.

— If the crisis entails an external or Common Security and Defence Policy (CSDP) dimension, the public communication should be coordinated with the EEAS and the HRVP Spokesperson service.

Cooperation at the operational level

Scope of activities:

— 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.

Potential actors

— Member States:

  — Competent authorities and single points of contact established by the NIS Directive

  — CSIRTs, cybersecurity agencies

  — Other national sectoral authorities (in case of multi-sectoral incident or crisis)

— EU bodies/offices/agencies

  — ENISA

  — Europol/EC3

  — CERT-EU

— European Commission

  — the (Deputy) Secretary-General SG (ARGUS process)

  — DG CNECT/HOME

  — Commission Security Authority

  — Other DGs (in case of multi-sectoral incident or crisis)

[1] Advice of technical nature as to the causes of the incident and possible mitigations.
[2] Information about the technical vulnerability which is being exploited to negatively impact IT systems.

— EEAS

  — the (Deputy) Secretary-General for Crisis Response and SIAC (EU INTCEN and EUMS INT)

  — EU Hybrid Fusion Cell

— Council

  — the Presidency (Chair Horizontal Working Party on Cyber Issues or Coreper ([1])) supported by the GSC, or PSC ([2]) and — if activated — with the support of the IPCR arrangements.

Situational awareness:

— Support the production of politico/strategic situation reports (e.g. the ISAA in case of IPCR activation)

— The *Council Horizontal Working Party on Cyber Issues* prepares the Coreper or PSC meeting as appropriate

— In case of IPCR activation:

  — The Presidency may call round table meetings to support its preparation for Coreper or PSC, bringing in relevant stakeholders in the Member States, the institutions, the agencies, and third parties such as non-EU countries and international organisations. These are crisis meetings to identify bottlenecks and produce proposals for action for cross-cutting issues.

  — The *Commission lead service or the EEAS* as ISAA lead prepares the ISAA report with contributions from ENISA, CSIRTs Network, Europol/EC3, EUMS INT, INTCEN and all other relevant actors. The ISAA report represents an EU-wide assessment based on correlation of technical incidents and crisis assessment (threat analysis, risk assessment, non-technical consequences and effects, non-cyber aspects of the incident or crisis, etc.) which is tailored to the needs of operational and political levels.

— In case of ARGUS activation

  — CERT-EU and EC3 ([3]) contribute directly to the exchange of information within the Commission.

— In case of the EEAS Crisis Response Mechanism activation:

  — The SIAC will intensify its information collection and aggregate the all-source information and prepare an analysis and assessment on the incident.

Response (upon request from the political level):

— Cross-border cooperation with single points of contact and national competent authorities (NIS Directive) to mitigate the consequences and effects.

— Activate all technical mitigation measures and coordinate technical capacities needed to stop or reduce the impact of the attacks on the targeted information systems.

— Cooperation and, if decided, coordination of technical capacities towards a joint or collaborative response in accordance with the ***CSIRTs Network SOPs***.

— Assess the need to cooperate with relevant third parties.

— (where activated) Decision-making within the ARGUS process.

— (where activated) Preparing decisions and coordinating under the IPCR arrangements.

— (where activated) support EEAS decision-making through the EEAS Crisis Response Mechanism including as regards contacts with third countries and international organisations as well as any measure aimed at protecting CSDP missions and operations and EU delegations.

([1]) The Permanent Representatives Committee or Coreper (Article 240 of the Treaty on the Functioning of the European Union — TFEU) is responsible for preparing the work of the Council of the European Union.

([2]) The Political and Security Committee is a Committee of the Council of the European Union dealing with the common foreign and security policy (CFSP) mentioned in Article 38 of the Treaty on European Union.

([3]) In accordance and under the conditions and procedures set in EC3's legal framework.

Public communications:

— Agree upon public messages regarding the incident.

— If the crisis entails an external or Common Security and Defence Policy (CSDP) dimension, the public communication should be coordinated with the EEAS and the HRVP Spokesperson service.

Cooperation at the strategic/political level

Potential actors

— For Member States, Ministers responsible for cybersecurity

— For the European Council, the President

— For the Council, the rotating Presidency

— When measures within the 'Cyber Diplomatic Toolbox', PSC and Horizontal Working Party

— For the European Commission, the President or the delegated Vice-President/Commissioner

— The High Representative of the Union for Foreign Affairs Security Policy/Vice-President of the Commission.

Scope of activities: 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.

Shared situational awareness:

— Identify the impacts of the disruptions caused by the crisis on the functioning of the Union.

Response:

— Activate additional crisis management mechanisms/instruments depending on the nature and impact of the incident. These may include, for example, the Civil Protection Mechanism.

— Take measures within the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

— Make available emergency support to affected Member States for example activating the Cybersecurity Emergency Response Fund ([1]) once applicable.

— Cooperation and Coordination with international organisations where appropriate such as the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE) and particularly NATO.

— Assess national security and defence implications.

Public communications:

Decide upon a common communication strategy towards the public.

COORDINATED RESPONSE WITH MEMBER STATES AT THE EU LEVEL IN THE FRAMEWORK OF THE IPCR ARRANGEMENTS

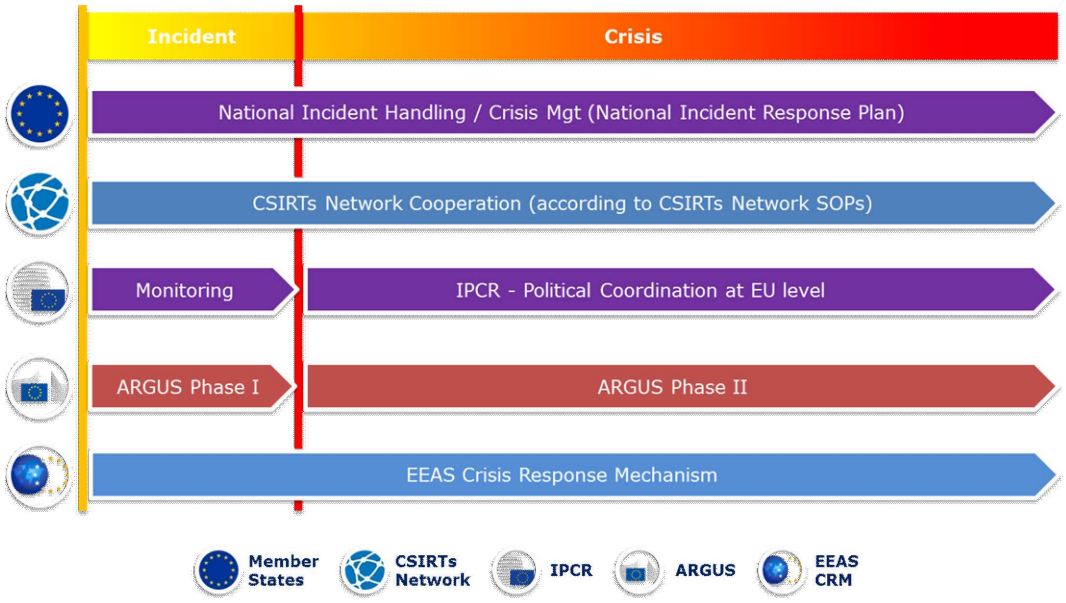
Following the principle of complementarity at EU level, this section introduces and focuses in particular on the core objective and the responsibilities and activities of the Member States Authorities, the CSIRTs Network, ENISA, CERT-EU, Europol/EC3, INTCEN, the EU Hybrid Fusion Cell and the Council Horizontal Working Party on Cyber issues within the IPCR process. Actors are assumed to act in line with established procedures at EU or national level.

It is essential to note that, as illustrated by Figure 1, irrespective of the activation of the EU crisis management mechanisms, activities at national level as well as cooperation within the CSIRTs Network (where necessary) take place throughout any incident/crisis following the principles of subsidiarity and proportionality.

([1]) The Cybersecurity Emergency Fund is a proposed action under the Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU', JOIN(2017) 450/1.

Figure 1

Cybersecurity incident/crisis response at EU level



All of the activities described below are to be carried out in accordance with and following the standard operating procedures/rules of the cooperation mechanisms involved and in line with the established mandates and competencies of individual actors and institutions. These procedures/rules may need some additions or modifications in order to achieve best possible cooperation and effective response to large-scale cybersecurity incidents and crises.

Not all actors presented below may be required to take action during any one particular incident. Nevertheless, the Blueprint and the relevant standard operating procedures of the cooperation mechanisms should foresee their potential involvement.

Given the different degree of impact on society that a cybersecurity incident or crisis may have, a high degree of flexibility as regards the involvement of sectoral actors on all levels and any appropriate response will rely upon both cyber and non-cyber mitigation activities.

Cybersecurity crisis management — Integrating cybersecurity in the IPCR process

The IPCR arrangements, described in the IPCR SOPs ([1]), follow sequentially the steps described hereunder (the use of some of these steps will depend on the situation).

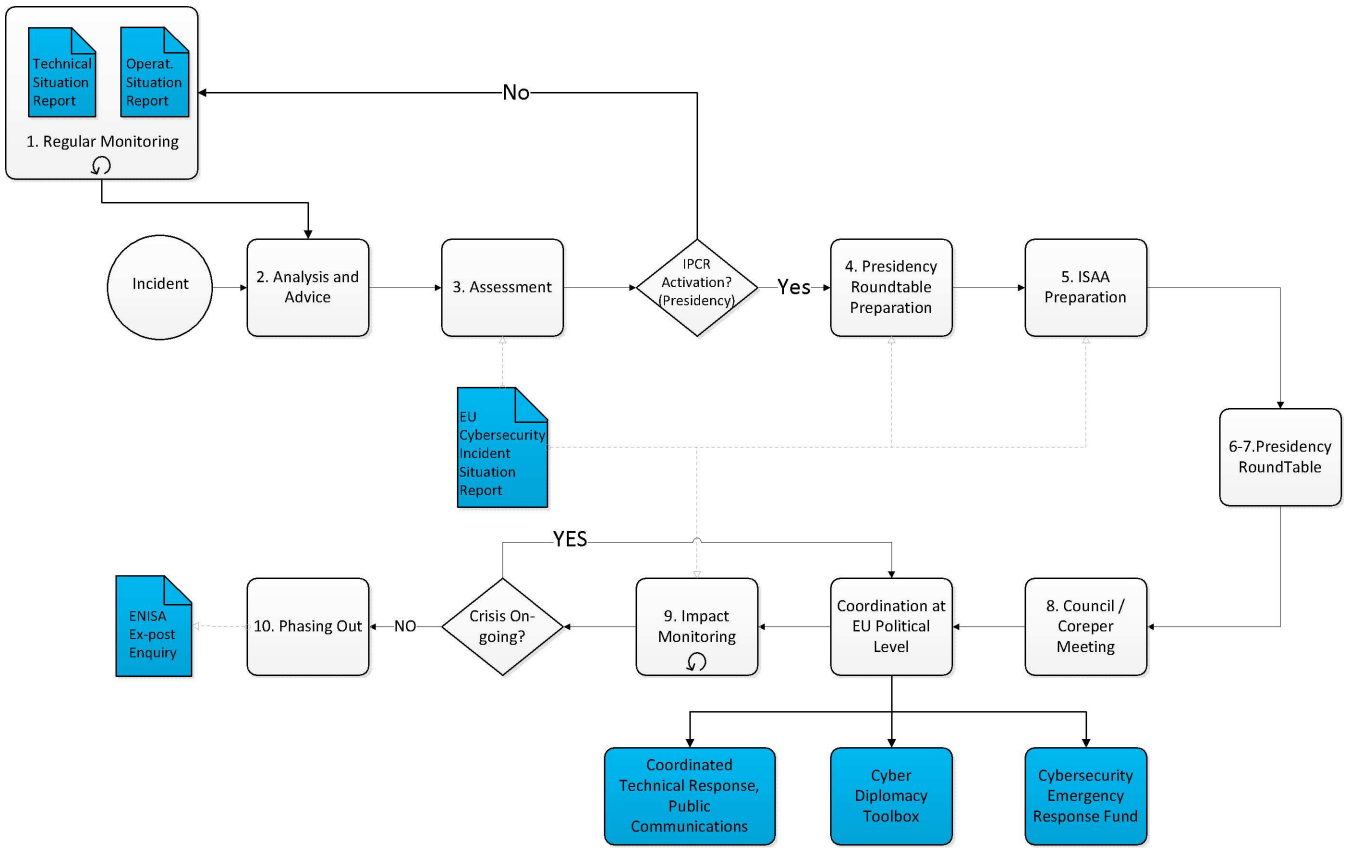
At each step we specify cybersecurity-specific activities and actors. For the reader's convenience, at each step the text from the IPCR SOPs is provided followed by the Blueprint-specific activities. This step-by-step approach also allows for clear identification of existing **gaps** in necessary capabilities and procedures that hamper an effective response to cybersecurity crises.

Figure 2 (below ([2])) is a graphical representation of the IPCR process where the new elements being introduced are highlighted in blue.

([1]) From Document 12607/15 'IPCR Standard Operating Procedures', agreed by Friends of the Presidency group and noted by Coreper in October 2015.
([2]) A larger version of the figure may be found in the appendix.

Figure 2

Cybersecurity-specific elements in IPCR



Note: Given the nature of hybrid threats in the cyber domain that are designed to stay below the threshold of a recognisable crisis, the EU needs to undertake preventive and preparedness measures. The EU Hybrid Fusion Cell is tasked to rapidly analyse relevant incidents and inform the appropriate coordination structures. The regular reporting from the Fusion Cell can contribute to inform sectoral policymaking to enhance preparedness.

— **Step 1 — Regular sectoral monitoring and alerting**: the existing, regular sectoral situation reports and alerts provide indications to the Council Presidency on a developing crisis and its possible evolution.

— **Identified gap**: There are currently no regular and coordinated cybersecurity situation reports and alerts as regards cybersecurity incidents (and threats) at EU level.

— **Blueprint: EU Cybersecurity situation monitoring/reporting**

— **A regular EU Cybersecurity Technical Situation Report** on cybersecurity incidents and threats will be prepared by ENISA on incidents and threats, based on publicly available information, its own analysis and reports shared with it by Member States' CSIRTs (on a voluntary basis) or NIS Directive single points of contact, European Cybercrime Centre (EC3) at Europol, CERT-EU and European Union Intelligence Centre (INTCEN) at the European External Action Service (EEAS). The report should be made available to the relevant instances of the Council, the Commission and the CSIRTs Network.

— On behalf of SIAC, the EU Hybrid Fusion Cell should compile an **EU Cybersecurity Operational Situation Report**. The report also supports the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities.

— Both reports are disseminated to EU and national stakeholders to contribute to their own situational awareness and inform decision-making and facilitate cross-border regional cooperation.

After an incident has been detected

— **Step 2 — Analysis and advice**: based on available monitoring and alerting, the Commission services, the EEAS, and the GSC keep each other informed on possible developments, in order to be ready to advise the Presidency for a possible activation (in full or in information-sharing mode) of the IPCR.

  — **Blueprint:**

    — For the Commission, DG CNECT, DG HOME, DG HR.DS and DG DIGIT, supported by ENISA, EC3 and CERT-EU.

    — EEAS. Drawing on the work of the Sitroom, and intelligence sources, the EU Hybrid Fusion Cell provides situational awareness on actual and potential hybrid threats affecting the EU and its partners including cyber threats. Therefore, when the analysis and assessment of the EU Hybrid Fusion Cell indicates the existence of possible threats directed against a Member State, partner countries or organisation, INTCEN will inform (in the first instance) on the operational level, according to established procedures. The operational level will then prepare recommendations for the political strategic level, including the possible activation of crisis management arrangements in monitoring mode (e.g. EEAS Crisis Response Mechanism or the IPCR monitoring page).

    — The CSIRTs Network Chair assisted by ENISA prepares an EU Cybersecurity Incident Situation Report ([1]) which is presented to the Presidency, the Commission and the HRVP via the CSIRT of the rotating Presidency.

— **Step 3 — Assessment/decision on IPCR activation**: the Presidency evaluates the need for political coordination, information exchange or decision-making at EU level. To this end, the Presidency may convene an informal round table meeting. The Presidency carries out an initial identification of the areas requiring Coreper or Council involvement. This will form the basis of the guidance for the production of Integrated Situational Awareness and Analysis (ISAA) reports. The Presidency will decide, in light of the characteristics of the crisis, its possible consequences, and the related political needs, on the appropriateness of convening meetings of the relevant Council Working Parties and/or Coreper and or PSC.

  — **Blueprint:**

    — Round table participants:

      — The Commission services and the EEAS will advise the Presidency on their respective areas of competence.

      — Member States' representatives in the Horizontal Working Party on Cyber Issues supported by experts from the capitals (CSIRTs, Cybersecurity Competent Authorities, others).

      — Political/Strategic Guidance for ISAA reports based on the latest EU Cybersecurity Incident Situation Report and additional information provided by the round table participants.

      — Relevant Working Parties and Committees:

        — Horizontal Working Party on Cyber Issues.

  The Commission, EEAS and GSC, in full agreement and associating the Presidency, can also decide to activate the IPCR in information-sharing mode by generating a crisis page, in order to prepare the ground for a possible full activation.

— **Step 4 — IPCR Activation/Information gathering and exchange**: upon activation (whether in information-sharing mode or in full), a crisis page is generated on the IPCR web platform, allowing specific exchanges of information focusing on aspects that will contribute to feed ISAA and to prepare the discussion at political level. The ISAA lead service (one of the Commission services or EEAS) will depend on the circumstances of the case.

— **Step 5 — ISAA production**: the production of ISAA reports will be initiated. The Commission/EEAS will issue ISAA reports as outlined in the ISAA SOPs and may further foster information-exchange on the IPCR web platform,

([1]) The EU Cybersecurity Incident Situation Report is an aggregation of national reports provided by national CSIRTs. The format of the report should be described in the CSIRTs Network SOPs.

or issue specific requests for information. The ISAA reports will be tailored to the needs of the political level (i.e. Coreper or the Council) as defined by the Presidency and laid out in its guidance, thus allowing a strategic overview of the situation and an informed debate on the agenda items defined by the Presidency. In accordance with the ISAA SOPs, the nature of the cybersecurity crisis will determine whether the ISAA report is prepared by one of the Commission Services (DG CNECT, DG HOME) or the EEAS.

Following the activation of the IPCR, the Presidency will outline the specific areas of focus for ISAA in order for it to support the political coordination and/or decision-making process in the Council. The Presidency will also specify the timing of the report, following consultations with the Commission services/EEAS.

— **Blueprint:**

— The ISAA report includes contributions from relevant services including:

— The CSIRTs Network in the form of the EU Cybersecurity Incident Situation Report.

— EC3, Sitroom, the EU Hybrid Fusion Cell, CERT-EU. The EU Hybrid Fusion Cell will support and provide contributions to the ISAA lead service and the IPCR round table, as appropriate.

— EU sectoral agencies and bodies depending on the impacted sectors

— Member States authorities (other than the CSIRTs).

— Gathering ISAA inputs ([1]):

— Commission and EU Agencies. The ARGUS IT system will provide the internal backbone network for ISAA. EU Agencies shall send their contributions to their respective responsible DGs, which in turn will feed the relevant information into ARGUS. Commission services and Agencies will gather information from existing sectorial networks with Member States and international organisations and from other relevant sources.

— For the EEAS. The EU Situation Room supported by the other relevant EEAS departments, will provide the internal backbone network and single point of contact for ISAA. The EEAS will gather information from third countries and relevant international organisations.

— **Step 6 — Preparation of the informal Presidency round table**: the Presidency, assisted by the General Secretariat of the Council, will define the timing, agenda, participants, and expected outcome (possible deliverables) of the informal Presidency round table meeting. The GSC will relay relevant information on the IPCR web platform on behalf of the Presidency, and will issue in particular the meeting's notice.

— **Step 7 — Presidency round table/preparatory measures for EU political coordination/decision-making**: the Presidency will gather an informal round table to review the situation, and to prepare and review the items to be brought to the Coreper or Council's attention. The informal Presidency round table will also be the forum to develop, review and discuss all proposals for action to be submitted to Coreper/Council.

— **Blueprint:**

— The Council Horizontal Working Party on Cyber Issues should prepare PSC or Coreper.

— **Step 8 — Political coordination and decision-making at Coreper/Council**: The results of the Coreper/Council meetings concern the coordination of response activities at all levels, decisions on exceptional measures, political declarations, etc. These decisions also constitute an updated political/strategic guidance for the further production of ISAA reports.

— **Blueprint:**

— The political decision to coordinate the response to the cybersecurity crisis is implemented through the activities (performed by the corresponding actors) described above in Section 1 'Cooperation at Strategic/political, operational and technical levels' as regards **Response** and **Public Communication**.

— ISAA production continues based on cooperation at technical, operational and political/strategic levels as regards **Situational awareness** also described above in Section 1.

([1]) ISAA SOPs.

— **Step 9 — Impact monitoring**: the ISAA lead service will provide, with the support of ISAA contributors, information on the evolution of the crisis and on the impact of the political decisions taken. This feedback loop will support an evolving process and support the Presidency's decision in continuing the involvement of the EU political level or in phasing down the IPCR.

— **Step 10 — Phasing out**: following the same process as for the activation, the Presidency may convene an informal round table meeting to assess the opportunity to maintain the IPCR active or not. The Presidency can decide to close or downgrade the activation.

— **Blueprint:**

— ENISA may be invited to contribute to or carry out an *ex post* technical inquiry of the incident in accordance with the provisions in its mandate.

APPENDIX

1. CRISIS MANAGEMENT, COOPERATION MECHANISMS AND ACTORS AT EU LEVEL

Crisis management mechanisms

Integrated Political Crisis Response arrangements (IPCR): the Integrated Political Crisis Response arrangements (IPCR), approved by the Council on 25 June 2013 ([1]), are designed to facilitate a timely coordination and response at EU political level in the event of a major crisis. The IPCR also support the coordination at political level of the response to the invocation of the solidarity clause (Article 222 TFEU), as defined in Council Decision 2014/415/EU on the implementation by the Union of the solidarity clause adopted on 24 June 2014. The ICPR Standard Operating Procedures ([2]) (SOPs) set out the activation process and subsequent actions to be taken.

ARGUS: Crisis coordination system established by the European Commission in 2005 to provide a specific coordination process in case of a major multisectoral crisis. It is supported by a general rapid alert system (IT tool) with the same name. ARGUS foresees two phases, with Phase II (in case of major multi-sectoral crisis) triggering meetings of the Crisis Coordination Committee (CCC) under the authority of the Commission President or a Commissioner to whom responsibility was assigned. The CCC brings together representatives of relevant Commission DGs, Cabinets, and other EU services in order to lead and coordinate the Commission's response to the crisis. Chaired by the Deputy Secretary-General, the CCC assesses the situation, considers options and takes actionable decisions as regards the EU tools and instruments under the Commission's responsibility, and ensures that the decisions are implemented ([3]) ([4]).

EEAS Crisis Response Mechanism: The EEAS Crisis Response Mechanism is a structured system for the EEAS to respond to crisis and emergencies having an external nature or an important external dimension — including hybrid threats — potentially or actually impacting the EU interests or those of any Member States. By ensuring participation of relevant Commission as well as Council Secretariat officials to its meetings, the CRM facilitates synergy between diplomatic, security and defence efforts with financial, trade and cooperation instruments managed by the Commission. The Crisis Cell can be activated for the duration of the crisis.

Cooperation mechanisms

CSIRTs Network: The Computer Security Incident Response Team Network brings together all the national and governmental CSIRTs and CERT-EU. The purpose of the network is to enable and enhance information-sharing amongst the CSIRTs on threats and cybersecurity incidents and also to cooperate in responding to cybersecurity incidents and crises.

Council Horizontal Working Party on Cyber Issues: the Working Party was established to ensure the strategic and horizontal coordination of cyber policy issues in the Council and can be involved in both legislative and non-legislative activities.

Actors

ENISA: The European Union Agency for Network and Information Security was set up in 2004. The Agency works closely with Members States and the private sector to deliver advice and solutions on issues such as the pan-European Cyber Security Exercises, the development of national cyber security strategies, CSIRTs cooperation and capacity building. ENISA collaborates directly with CSIRTs throughout the EU and is the Secretariat of the CSIRTs network.

ERCC: The Emergency Response Coordination Centre in the Commission (under the Directorate-General for European Civil Protection and Humanitarian Aid Operations — DG ECHO) supports and coordinates a wide range of prevention, preparedness and response activities on 24/7 basis. Inaugurated in 2013, it acts as the hub of the Commission's crisis response (liaising with other EU crisis rooms) including as the central IPCR 24/7 contact point.

([1]) 10708/13 on the 'Finalisation of the CCA Review process: the EU Integrated Political Crisis Response Arrangements', approved by the Council on 24 June 2013.
([2]) 12607/15 'IPCR Standard Operating Procedures', agreed by Friends of the Presidency group and noted by Coreper in October 2015.
([3]) Commission provisions on 'ARGUS' general rapid alert system, COM(2005) 662 final, 23 December 2005.
([4]) Commission Decision 2006/25/EC, Euratom of 23 December 2005 amending its internal Rules of Procedure (OJ L 19, 24.1.2006, p. 20), on setting up the 'ARGUS' general rapid alert system.

Europol/EC3: The European Cybercrime Centre (EC3) set up in 2013 within Europol supports the law enforcement response to cybercrime in the EU. EC3 offers operational and analytical support to Member States' investigations and serves as the central hub for criminal information and intelligence supporting operations and investigations by Member States with operational analysis, coordination and expertise as well as highly specialised technical and digital forensic support capabilities.

CERT-EU: the Computer Emergency Response Team of the EU Institutions, Bodies and Agencies has a mandate to improve the protection of the EU institutions, bodies and agencies against cyber threats. It is a member of the CSIRTs network. CERT-EU has technical agreements on sharing information about cyber threats with NATO CIRC, some third countries and major commercial actors in the field of cybersecurity.

The EU Intelligence Community comprises the EU Intelligence Analysis Centre (**INTCEN**) and EU Military Staff (EUMS) Intelligence Directorate (EUMS INT) under the SIAC arrangement of the **Single Intelligence Analysis Capacity** (SIAC). SIAC mission is to provide intelligence analyses, early warning and situational awareness to the High Representative of the European Union for Foreign Affairs and Security Policy and to the European External Action Service (EEAS). SIAC offers its services to the various EU decision making bodies in the fields of the Common Foreign and Security Policy (CFSP), the Common Security and Defence Policy (CSDP) and counterterrorism (CT), as well as to the Member States. EU INTCEN and EUMS INT are not operational agencies and do not have any collection capability. The operational level of intelligence is the Member States' responsibility. SIAC only deals with strategic analysis.

EU Hybrid Fusion Cell: The Joint Communication on Countering Hybrid Threats of April 2016 designates the EU Hybrid Fusion Cell (EU HFC) as the focal point for all source analysis on hybrid threats in the EU: its mandate was approved in December 2016 by the Commission through an inter-services consultation. Based in the INTCEN, the EU Hybrid Fusion Cell is part of the SIAC and hence works jointly with the EUMS INT and has a permanent military member assigned. Hybrid refers to the deliberate use by a State or non-State actor of a combination of multiple covert/overt, military/civilian tools and levers, such as cyber-attacks, disinformation campaigns, espionage, economic pressure, use of proxy forces or other subversive activity. The EU HFC works with an extensive network of points of contact (PoCs), both within the Commission and Member States to provide the integrated response/whole of government approach required to counter diverse challenges.

EU Sitroom: The EU Situation Room is part of the EU Intelligence and Situation Centre (EU INTCEN) and provides the EEAS with operational capacity to ensure an immediate and effective response to crises. It is a permanent civilian-military stand-by body that provides worldwide monitoring and situational awareness with a 24/7 capacity.

Relevant instruments

Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities: The Framework, agreed in June 2017, is part of the EU's approach to cyber diplomacy, which contributes to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. The framework makes full use of measures within the Common Foreign and Security Policy, including, if necessary, restrictive measures. The use of the measures within the Framework should encourage cooperation, facilitate mitigation of immediate and long-term threats and influence the behaviour of the responsible perpetrator and potential aggressors in the long term.

2. CYBERSECURITY CRISIS COORDINATION IN THE IPCR ARRANGEMENTS — HORIZONTAL COORDINATION LAYER AND POLITICAL ESCALATION

The IPCR arrangements can be (and have been) used to address technical and operational issues, but always from a political/strategic angle.

In terms of escalation, the IPCR can be used according to the level of the crisis by moving from 'monitoring mode', to 'information-sharing mode' which is the first level of IPCR activation, and 'IPCR full activation'.

Activation in full mode is a decision of a rotating Presidency of the Council of the EU. The Commission, EEAS and GSC can activate the IPCR in information-sharing mode. Monitoring and information-sharing trigger different levels of

information exchange, with information-sharing activating a demand for the production of ISAA reports. Full activation adds IPCR round table meetings to the toolbox, bringing to the table the Presidency (typically the Coreper II chair, or a subject expert at PermRep Counsellor level but exceptionally round tables were held at Ministerial level).

Actors

The rotating Presidency (typically Coreper Chair) is in the lead

For the European Council, the Cabinet of the President

For the European Commission, DSG/DG level and/or subject experts

For the EEAS, DSG/MD level and/or subject experts

For the GSC, the Cabinet of the SG, the IPCR team and the responsible DGs.

Scope of activities: Generating a common integrated picture of the situation and escalating awareness of bottlenecks or shortcomings at each of the three levels in order to the address them at the political level, generating decisions at the table if they fall within the remit of the participants, or to generating proposals for action that go to Coreper II and up to Council.

Shared situational awareness:

(not active): IPCR monitoring pages can be generated to track developing situations that might escalate into a crisis with EU ramifications

(IPCR information-sharing): ISAA reports will be drafted by the ISAA lead on the basis of input from the Commission services, EEAS, and Member States (through the IPCR questionnaires)

(IPCR full activation): in addition to ISAA reports, informal IPCR round tables bring together different actors concerned in the MS, the Commission, EEAS, relevant agencies, etc. to discuss shortcomings and bottlenecks.

Cooperation and response:

Activate/synchronise additional crisis management mechanisms/instruments depending on nature and impact of the incident. These may include, for example the Civil Protection Mechanism, the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities or the 'Joint Framework on countering hybrid threats'.

Crisis communications:

The IPCR Crisis Communicator's Network may be activated by the Presidency, after consultation with the relevant services in the Commission, GSC and EEAS, in order to support the creation of common messages, or elaborate on the most effective communication tools.

3. CYBERSECURITY CRISIS MANAGEMENT IN ARGUS — INFORMATION-SHARING WITHIN THE EUROPEAN COMMISSION

Facing unexpected crises that required action at European level, i.e. the Madrid terrorist attacks (March 2004), the South-East Asia Tsunami (December 2004) and the London terrorist attacks (July 2005), the Commission in 2005 established the ARGUS coordination system, supported by an eponymous general rapid alert system ([1]) ([2]). It aims to provide a specific **crisis coordination process** in case of a major multisectoral crisis, to enable sharing crisis-related information in real time and ensure rapid decision-making.

ARGUS defines two phases depending on the severity of the event:

Phase I: is used for 'information-sharing' on a crisis of limited scale

([1]) Commission of the European Communities, 23 December 2005, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission Provisions on 'ARGUS' General Rapid Alert System, COM(2005) 662 final.

([2]) Decision 2006/25/EC, Euratom.

Examples of recent Phase I reported events include the forest fires in Portugal and Israel, the 2016 Berlin attack, floods in Albania, Hurricane Matthew in Haiti and the drought in Bolivia. Any DG can open a Phase I event when it judges that a situation in its domain of competence is serious enough to warrant or benefit from information-sharing. For instance, DG CNECT or DG HOME can open a Phase I event when they judge that a cyber situation in their respective domain of competence is serious enough to warrant or benefit from information-sharing.

Phase II: is triggered in case of major multisectoral crisis or foreseeable or imminent threat for the Union.

Phase II triggers a specific coordination process enabling the Commission to take decisions and manage a rapid, coordinated and coherent response, at the highest level in its domain of competence and in cooperation with the other institutions. Phase II is meant for a major multisectoral crisis or foreseeable or imminent threat thereof. Examples of real-life Phase II events include the migration/refugee crisis (2015-ongoing), Fukushima triple disaster (2011) and the eruption of *Eyjafjallajökull* volcano in Iceland (2010).

Phase II is activated by the President on his own initiative or at the request of a Member of the Commission. The President may allocate the political responsibility for the Commission response to a Commissioner responsible for the service most concerned by the crisis at hand or decide to keep the responsibility to himself.

It foresees emergency meetings of the Crisis Coordination Committee (CCC). These are called under the authority of the President or a Commissioner to whom responsibility was assigned. The meetings are convened by SG through the ARGUS IT tool. The CCC is a specific operational crisis management structure established to lead and coordinate the Commission's response to the crisis, bringing together representatives of relevant Commission DGs, Cabinets, and other EU services. Chaired by the Deputy Secretary-General, the **CCC assesses the situation, considers options and takes decisions, as well as ensures that decisions and actions are implemented** while ensuring the coherence and consistency of the response. Support to the CCC is provided by the SG.

4. EEAS CRISIS RESPONSE MECHANISM

The EEAS Crisis Response Mechanism (CRM) is activated upon occurrence of a serious situation or emergency concerning or anyway involving the external dimension of the EU. CRM is activated by DSG for Crisis Response, after consultation with the HRVP or the Secretary-General. DSG for Crisis Response can also be requested to initiate the Crisis Response Mechanism by the HRVP, or the SG, or another DSG or MD.

The CRM contributes to EU's coherence in crisis response within the Security Strategy. In particular, the CRM facilitates sinergy between diplomatic, security and defence efforts with financial, trade and cooperation instruments managed by the Commission.

The CRM is linked to the Commission's general emergency response system (ARGUS) and the EU Integrated Political Crisis Response arrangements (IPCR) in order to exploit synergies in case of simultaneous activation. The Situation Room in the EEAS acts as communication hub between the EEAS and the emergency response systems in the Council and Commission.

Normally, the first action related with the CRM implementation is the calling of a **Crisis Meeting** among EEAS, Commission and Council senior managers directly affected by the crisis in question. The Crisis Meeting assesses the short-term effects of the crisis and may agree on taking immediate action, or activating the Crisis Cell, or convening a Crisis Platform. Those courses can be implemented in any time sequence.

The **Crisis Cell** is a small-scale operations room where representatives of EEAS, Commission and Council services involved in the response to the crisis gathers to monitor the situation continuously in order to provide support to the EEAS Headquarters decision-makers. When activated, the Crisis Cell is operational 24 hours a day, 7 days a week.

The **Crisis Platform** gathers relevant EEAS, Commission and Council services to provide assessment on medium and long-term effects of crises and agree on action to be taken. It is chaired by the HRVP, or the Secretary-General, or the DSG for Crisis Response. The Crisis Platform evaluates the effectiveness of EU action on crisis country or region, decides on amendments of additional measures and discusses proposals for Council action. The Crisis Platform is an ad hoc meeting; therefore, it is not permanently activated.

The **Task Force** is composed of representatives of the services involved in the response and can be activated to follow and facilitate the implementation of the EU response. It evaluates the impact of EU action, prepares policy documents and options papers, contributes to the preparation of the Political Framework for Crisis Approach (PFCAs), contributes to the Communication Strategy, and adopts any other arrangements that can facilitate the implementation of the EU response.

5. REFERENCE DOCUMENTS

Below is a list of reference documents that have been taken into account in preparation of the Blueprint:

— The European Cyber Crises Cooperation Framework, Version 1, 17 October 2012.

— Report on Cyber Crisis Cooperation and Management, ENISA, 2014

— Actionable Information for Security Incident Response, ENISA, 2014

— Common practices of EU-level crisis management and applicability to cyber crises, ENISA, 2015

— Strategies for Incident Response and Cyber Crisis Cooperation, ENISA, 2016

— EU Cyber Standard Operating Procedures, ENISA, 2016

— A good practice guide of using taxonomies in incident prevention and detection, ENISA, 2017

— Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410 final, 5 July 2016

— Council Conclusions on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry — Council conclusions (15 November 2016), 14540/16

— Council Decision 2014/415/EU of 24 June 2014 on the arrangements for the implementation by the Union of the solidarity clause (OJ L 192, 1.7.2014, p. 53)

— Finalisation of the CCA review process: the EU Integrated Political Crisis Response (IPCR) arrangements, 10708/13, 7 June 2013

— Integrated Situational Awareness and Analysis (ISAA) — Standard Operating Procedures, DS 1570/15, 22 October 2015

— Commission provisions on 'ARGUS' general rapid alert system, COM(2005) 662 final, 23 December 2005

— Commission Decision 2006/25/EC, Euratom of 23 December 2005 amending its internal Rules of Procedure (OJ L 19, 24.1.2006, p. 20)

— ARGUS Modus Operandi, European Commission, 23 October 2013

— Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'), Doc. 9916/17

— EU operational protocol for countering hybrid threats 'EU Playbook', Doc. SWD(2016) 227

— EEAS Crisis Response Mechanism, 8 November 2016 (Ares(2017)880661) Joint Staff Working Document EU operational protocol for countering hybrid threats, 'EU Playbook', SWD(2016) 227 final, 5 July 2016

— Joint Communication to the European Parliament and the Council: Joint Framework on countering hybrid threats — a European Union response JOIN/2016/018 final, 6 April 2016

— EEAS(2016) 1674 — Working Document of the European External Action Service — EU Hybrid Fusion Cell — Terms of Reference

6. CYBERSECURITY-SPECIFIC ELEMENTS IN IPCR PROCESS