EUROPEAN
COMMISSION

Brussels, 13.9.2017
C(2017) 6100 final

COMMISSION RECOMMENDATION

of 13.9.2017

on Coordinated Response to Large Scale Cybersecurity Incidents and Crises

COMMISSION RECOMMENDATION

of 13.9.2017

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 on 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

[1] Council conclusions on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber security", document 10299/11 , Brussels, 27 May 2011

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] 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[4] 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[5]; the Commission will use the ARGUS[6] 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)[7] will be activated.

[2] COM(2016) 410 final, 5 July 2016

[3] Directive (EU) 2016/1148 on Security of Network and Information Systems ('NIS Directive') aiming at achieving a high common level of security of network and information systems within the Union

[4] Document 14540/16, 15 November 2016

[5] Further information can be found in Section 3.1. of the Appendix on Crisis management, cooperation mechanisms and actors at EU level

[6] Ibid

[7] Ibid

(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 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 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 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)[8].

(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.

[8] Under development; expected to be adopted by the end of 2017.

(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[9].

(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[10] or the EU operational protocol for countering hybrid threats[11], 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 complimentary 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 co-operation 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.

(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').

[9] The guidelines are intended to be finalised by the end of 2017.

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

[11] Joint Staff Working Document EU operational protocol for countering hybrid threats, 'EU Playbook', SWD(2016) 227 final, 5.7.2016

(26) The Council Conclusions[12] 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 Organization 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 end 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 there-in.

(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 crises 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 co-operation 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 on-going work within the

[12] ST 15283/16, 6 December 2016

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 cyber diplomacy and NATO cybersecurity exercises. In particular, they should be tested in the context of the CyberEurope exercises organised by ENISA. CyberEurope 2018 presents a first such opportunity.

(9) Member States and the EU Institutions should regularly practice 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, 13.9.2017

For the Commission
Mariya GABRIEL
Member of the Commission

CERTIFIED COPY
For the Secretary-General,

Jordi AYET PUIGARNAU
Director of the Registry
EUROPEAN COMMISSION