Official Journal of the European Union

L 237

English edition

Legislation

Volume 64

5 July 2021

Contents

EN

Acts whose titles are printed in light type are those relating to day-to-day management of agricultural matters, and are generally valid for a limited period.

The titles of all other acts are printed in bold type and preceded by an asterisk.

II

(Non-legislative acts)

RECOMMENDATIONS

COMMISSION RECOMMENDATION (EU) 2021/1086

of 23 June 2021

on building a Joint Cyber Unit

THE EUROPEAN COMMISSION,

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

Whereas:

(1) Cybersecurity is essential to the success of the digital transformation of the economy and society. The EU is committed to unprecedented levels of investment in ensuring people, businesses and public authorities have confidence in digital tools.

(2) The COVID-19 pandemic has increased the importance of connectivity and Europe's reliance on stable network and information systems and showed the need to protect the whole supply chain. Reliable and secure network and information systems are particularly important for entities in the frontline of the fight against the pandemic, such as hospitals, medical agencies and vaccine manufacturers. Coordinating EU efforts to prevent, detect, discourage, deter, mitigate and respond to the most impactful cyber attacks against such entities could prevent the loss of life and attempts to undermine the EU's ability to defeat the pandemic in the swiftest possible manner. Moreover, strengthening the EU's ability to counter cyber-attacks effectively contributes to advancing a global, open, stable and secure cyberspace.

(3) Faced with the cross-border nature of cybersecurity threats and the continuous surge of more complex, pervasive and targeted attacks ([1]), relevant cybersecurity institutions and actors should increase their ability to respond to such threats and attacks by harnessing existing resources and better coordinating efforts. All relevant actors in the EU need to be prepared to respond collectively and exchange information on a 'need to share', rather than 'need to know', basis.

(4) Despite the major progress achieved through cooperation between Member States on cybersecurity, most notably through the Cooperation Group ('NIS Cooperation Group') and the Computer Security Incident Response Teams (CSIRTs) network set up under Directive (EU) 2016/1148 of the European Parliament and of the Council ([2]), there is still no common EU platform where information gathered in different cybersecurity communities can be exchanged efficiently and safely and where operational capabilities can be coordinated and mobilised by relevant actors. As a result, cyber threats and incidents risk being addressed in silos with limited efficiency and increased vulnerability. Furthermore, an EU-level channel for technical and operational cooperation with the private sector, both in terms of information sharing and incident response support, is missing.

([1]) ENISA, 2020 Threat Landscape; Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020

([2]) 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).

(5) Existing frameworks, structures and the resources and expertise available in Member States and relevant EU institutions, bodies and agencies provide a strong basis for a collective response to cybersecurity threats, incidents and crises ([3]). This existing architecture includes, on the operational side, the Blueprint for a Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('the Blueprint') ([4]), the CSIRTs network and the European Cyber Crises Liaison Organisation ('EU CyCLONe') network ([5]), as well as the European Cybercrime Centre ('EC3') and the Joint Cybercrime Taskforce ('J-CAT') at the European Union Agency for Law Enforcement Cooperation ('Europol'), and the EU Law Enforcement Emergency Response Protocol ('EU LE ERP'). The NIS Cooperation Group, the EU Intelligence and Situation Centre ('EU INTCEN'), and the Cyber Diplomacy Toolbox ([6]) and cyber defence-related projects launched under the Permanent Structured Cooperation (PESCO) ([7]) also contribute to policy and operational cooperation in different cybersecurity communities. The European Agency for Cybersecurity ('ENISA'), by virtue of its reinforced mandate, is tasked with supporting operational cooperation ([8]) with regard to the cybersecurity of network and information systems, the users of such systems, and other persons affected by cyber threats and incidents. Through the Integrated Political Crisis Response ('IPCR') arrangements, the EU is able to coordinate its political response to major crises, including in the event of large-scale cyber attacks.

(6) However, a mechanism for harnessing existing resources and providing mutual assistance across the cyber communities responsible for network and information systems security, for combating cybercrime, for conducting cyber-diplomacy, and, where appropriate, for cyber-defence in the event of a crisis does not yet exist. Nor is there a comprehensive mechanism at EU level for technical and operational cooperation in situational awareness, preparedness as well as response, between all communities. Moreover, synergies with the law enforcement and intelligence communities should be achieved respectively through Europol and INTCEN.

(7) The Commission, the High Representative of the Union for Foreign Affairs and Security Policy (High Representative), Member States and relevant EU institutions, bodies and agencies recognise the importance of analysing the strengths, weaknesses, gaps and overlaps of the current EU cybersecurity architecture which has been created over recent years. In consultation with Member States, the Commission, with the involvement of the High Representative, has developed a concept for a Joint Cyber Unit as a response to this analysis and as an important component of the Security Union Strategy ([9]), the Digital Strategy ([10]) and the Cybersecurity Strategy ([11]).

([3]) The EU Cyber Crisis Liaison Organisation Network (EU CyCLONe) was established by Member States in response to the Blueprint Recommendation. It is a network of national operational and crisis management experts the Commission proposed to be codified through the Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final, 2020/0359 (COD) proposed in December 2020.

([4]) Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

([5]) This recommendation takes into account the Blueprint Operational Level Exercise (Blue OLEx) 2020 After Action Report and in particular the Chair's summary of the Strategic Policy Discussion on the Joint Cyber Unit.

([6]) Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") of 19 June 2017 (9916/17).

([7]) In particular, the PESCO projects on 'cyber rapid response teams and mutual assistance in cyber security' coordinated by Lithuania and on 'cyber and information domain coordination centre' coordinated by Germany

([8]) Article 7 of Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15) requires the Agency to support operational cooperation among Member States, Union institutions, bodies, offices and agencies, and between stakeholders. This includes supporting Member States with respect to operational cooperation within the CSIRTs network, preparing a regular in-depth EU Cybersecurity Technical Situation Report on incidents and cyber threats and contribute to developing a cooperative response at Union and Member States level to large-scale cross-border incidents or crises. In addition, ENISA contributes to training activities with the European Security and Defence College (ESDC).

([9]) Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: on the EU Security Union Strategy, COM/2020/605 final.

([10]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Shaping Europe's digital future, COM/2020/67 final.

([11]) Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade, JOIN/2020/18 final.

(8) In cases of crisis, Member States should be able to rely on EU solidarity in the form of coordinated assistance, including from all four cyber communities, i.e. civilian, law enforcement ([12]), diplomacy and, where appropriate, defence. The degree of intervention of participants from one or more communities may depend on the nature of a large-scale incident or crisis and, consequently, on the type of countermeasures that will be required to respond to it. When confronted with cyber threats, incidents and crises, well-trained experts and technical equipment represent essential assets that can contribute to avoid serious damage and bring effective recovery. Therefore, clearly identified technical and operational capabilities, primarily experts and equipment, ready to be deployed to Member States in case of need, will be at the centre of the Joint Cyber Unit. Within that platform, participants will be in a unique position to nurture and coordinate such capabilities through EU Cybersecurity Rapid Reaction teams, while ensuring appropriate synergies with the already existing Cyber projects conducted in the framework of PESCO.

(9) The Joint Cyber Unit provides for a virtual and physical platform and does not require the creation of an additional, standalone body. Its set-up should not affect the competencies and powers of national cybersecurity authorities and relevant Union entities. The Joint Cyber Unit should be anchored in memoranda of understanding between its participants. It should build on, and add value to, existing structures, resources and capabilities as a platform for secure and rapid operational and technical cooperation between EU entities and Member State authorities. It should also bring together all cybersecurity communities, i.e. civilian, law enforcement, diplomacy and defence. Participants in the platform should have either an operational or supporting role. Operational participants should include ENISA, Europol, the Computer Emergency Response Team for the EU Institutions, bodies and agencies ('CERT-EU'), the Commission, the European External Action Service (including INTCEN), the CSIRTs Network and EU-CyCLONe. Supporting participants should include the European Defence Agency ('EDA'), the NIS Cooperation Group Chair, the Council Horizontal Working Party on Cyber Issues Chair, and one representative of the relevant PESCO projects ([13]). Since the Member States have operational capabilities and competences to respond to large-scale cyber threats, incidents and crises, the platform's participants should primarily rely on their capacities, with the help of relevant Union entities, to achieve their objectives.

(10) The Joint Cyber Unit should provide a new impetus to the process started in 2017 with the Blueprint. It should further operationalise the Blueprint architecture and mark a decisive step towards a European cybersecurity crisis management framework where threats and risks are identified, mitigated and responded to in a coordinated and timely manner. By taking such a step, the Joint Cyber Unit should help the EU respond to current and impending threats.

(11) By participating in the Joint Cyber Unit, operational and supporting participants should be able to engage with a wider range of stakeholders as part of the EU Cybersecurity Crisis Response Framework. While exercising their functions within the limits of their mandates, participants should benefit from enhanced preparedness and wider situational awareness covering all aspects related to cybersecurity threats and incidents, and leverage additional cybersecurity expertise. For instance, participants should be regularly involved in cross-community exercises, acquire a well-defined role in the EU Crisis Response Plan, enhance the visibility of their actions through shared public communication, and conclude operational cooperation agreements with the private sector. In parallel, contributing to the Joint Cyber Unit should enable participants to strengthen existing networks, such as the CSIRTs Network and EU CyCLONe, providing them with secure information exchange tools and better detection capabilities (i.e. Security Operation Centres, 'SOCs') and allowing them to tap into available EU operational capabilities.

(12) Participants in the Joint Cyber Unit should focus on technical and operational cooperation, including joint operations. Participants should contribute to such cooperation to the extent permitted by their mandates. Cooperation should build on and complement ongoing efforts. Depending on the type of cooperation concerned, additional participants may take part.

([12]) Also relevant for judicial cooperation.

([13]) See footnote 5. EEAS and EDA, through their role as PESCO secretariat, will liaise with coordinators of relevant PESCO projects.

(13) The platform should gather technical and operational crisis management experts from Member States and EU entities with a view to coordinating responses to cyber threats, incidents and crises by making use of existing capabilities and expertise. Experts participating in the Joint Cyber Unit will be able to monitor and protect a much wider attack surface by making use of both the physical and virtual platform. To this end, participants should coordinate efforts in the case of cross-border incidents and crises, as well as the delivery of assistance to incident stricken countries through the platform.

(14) Building the Joint Cyber Unit requires an incremental process harnessing and consolidating existing frameworks and structures mentioned in this Recommendation, including the collaboration mechanisms established under Member States' led fora (e.g. the CSIRTs network, EU CyCLONe, the Council Horizontal Working Party on Cyber Issues, J-CAT and relevant PESCO projects) and on the side of the EU Institutions, Bodies and Agencies, the structured cooperation between ENISA and CERT-EU as well as of the inter-Institutional Cybersecurity Information Exchange Group. Frameworks for hybrid threats, civil-protection ([14]) and sector-specific ([15]) should be adequately involved. Similarly, a structured link with the IPCR ([16]) should be created. This will allow, in case of crisis, to swiftly and effectively transmit information to decision-makers at political level gathered in Council.

(15) The creation of the Joint Cyber Unit should therefore follow a gradual and transparent process to be completed over the next two years. For this reason, the objectives set out in this Recommendation should be achieved through a four steps process, as described in the Annex to this Recommendation. A preparatory process, organised and supported by ENISA, involving operational and supporting participants at EU and Member State level, should be launched in the first two steps and take place under a working group to be set up by the Commission. The preparatory work should be guided by the principles of mutual engagement, inclusiveness and consensus building. The engagement of all participants should be fostered, allowing for diverse views and positions to be expressed and endeavouring to find solutions which command the widest possible support. Depending on the needs and based on well-justified conditions, the timeline for the different steps indicated in this Recommendation may be adjusted.

(16) Under step one, the preparatory process should start with the identification of relevant available EU operational capabilities and the launch of an assessment of the roles and responsibilities of participants within the platform. Step two should include the development of the EU Incident and Crisis Response Plan, consistent with the Blueprint ([17]) and the EU Law Enforcement Emergency Response Protocol, the roll-out of preparedness and situational awareness related activities, consistent with the Cybersecurity Act and the Europol Regulation ([18]), and the conclusion of the assessment on the roles and responsibilities of participants within the platform. The working group should present the results of that assessment to the Commission and the High Representative, which subsequently will share those results with the Council. The Commission and the High Representative should work together, in line with their respective competences, to draw up a joint report based on that assessment and invite the Council to endorse that report via Council conclusions.

(17) Following that endorsement, the Joint Cyber Unit will be made operational, with a view to completing the two remaining steps of the process. Under step three, participants should be able to deploy EU Rapid Reaction teams within the Joint Cyber Unit , along the lines of procedures defined in the EU Incident and Crisis Response Plan, leveraging both the physical and virtual platform and contributing to various aspects of incident response (from public communication to ex-post recovery). Finally, under step four, private sector stakeholders, including both users and providers of cybersecurity solutions and services, will be invited to contribute to the platform, allowing participants to improve information sharing and enhance the EU's coordinated response to cyber threats and incidents.

([14]) In this context, the Joint Cyber Unit should establish synergies with the EU Civil Protection Mechanism (UCPM) to enhance European preparedness and response in case of multi-disasters and emergencies that include a cyber-element.

([15]) Such as the financial sector one envisaged under the Regulation (EU) 2021/xx of the European Parliament and of the Council* [DORA].

([16]) See Recital (5).

([17]) See footnote 3

([18]) Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ L 135, 24.5.2016, p. 53).

(18) By the end of the four step process, participants should draw up an activity report on progress made in the implementation of the four steps set out in the Recommendation, describing achievements and challenges faced, which should be presented to the Commission and the High Representative. Based on that report, the Commission and the High Representative should carry out an assessment of those outcomes and draw conclusions for the future of the Joint Cyber Unit.

(19) The Commission, ENISA, Europol and CERT-EU should provide administrative, financial and technical support to the Joint Cyber Unit as set out in Section IV of this Recommendation, subject to budget and human resource availability. The reinforcement of relevant EU institutions', bodies' and agencies' operational cybersecurity capacities will be key to ensure effective preparation and sustainability of the Joint Cyber Unit. The Commission intends to ensure that the forthcoming regulation on common binding rules on cybersecurity for EU Institutions, Bodies and Agencies (October 2021) will provide the legal base for this contribution in the case of CERT-EU.

(20) In view of its reinforced mandate under Regulation (EU) 2019/881 ('Cybersecurity Act'), ENISA is in a unique position to organise and support the preparation of the Joint Cyber Unit, as well as to contribute to its operationalisation. In line with the provisions of the Cybersecurity Act, ENISA is currently establishing a Brussels office to support its structured cooperation with CERT-EU. That structured cooperation, including adjacent offices, provides a useful framework to facilitate the creation of the Joint Cyber Unit, including the establishment of its physical space which should be made available to participants in case of need, as well as to staff from other relevant EU institutions, bodies and agencies. The physical platform should be combined with a virtual platform composed of collaboration and secure information sharing tools. Those tools will leverage the wealth of information gathered through the European Cyber-Shield ([19]), including Security Operation Centres ('SOCs') and Information Sharing and Analysis Centres ('ISACs').

(21) The EU Law Enforcement Emergency Response Protocol for major cross-border cyber-attacks, adopted by the Council in 2018, gives a central role to Europol's European Cybercrime Centre ('EC3') ([20]) as part of the 'Blueprint' framework. That Protocol allows EU law enforcement authorities to provide a response to large-scale cross-border attacks of a suspected malicious nature on a 24/7 basis through rapid reaction and assessment, as well as the secure and timely sharing of critical information for the effective coordination of responses to cross-border incidents. The Protocol further elaborates on the collaboration with other EU institutions and EU-wide crisis protocols, as well as crisis cooperation with the private sector. The law enforcement community, with the support of Europol when appropriate, should contribute to the Joint Cyber Unit by taking the necessary steps within the full investigation cycle, in line with the requirements of the criminal justice framework and the applicable electronic evidence handling procedures. Europol has been providing operational support and facilitating operational cooperation against cyber threats since the inception of EC3 in 2013. Europol should support the platform according to its mandate and the intelligence-led policing approach, while leveraging all types of in-house expertise, products, tools and service of pertinence for the incident or crisis response.

(22) The 2013/40/EU Directive on Attacks against information systems also requires Member States to ensure that they have an operational national point of contact available 24 hours a day and seven days a week for the purpose of exchanging information relating to the offences defined in that Directive. The network of operational national points of contact should also contribute to the Joint Cyber Unit by ensuring involvement of Member State law enforcement authorities where appropriate.

(23) The EU cyber diplomacy community contributes to promoting and protect a global, open, stable and secure cyberspace and to prevent, deter and respond to malicious cyber activities in this regard. In 2017, the EU established a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ('Cyber Diplomacy Toolbox'). This framework is part of EU's wider cyber diplomacy policy. It contributes to conflict prevention and greater stability in international relations. It allows the EU and Member States, in cooperation with international partners where relevant, to use all Common Foreign and Security Policy ('CFSP') measures, in line with the respective procedures for their attainment, to encourage cooperation, mitigate threats and influence current and potential future malicious behaviour in cyberspace. The cyber diplomacy community should cooperate under the Joint Cyber Unit by using and providing support in using the full range of diplomatic measures, notably as regards public communication, supporting shared situational awareness and engagement with third countries in the event of a crisis.

([19]) JOIN/2020/18 final, section 1.2.
([20]) Established through the Regulation (EU) 2016/794.

(24) In line with the Blueprint framework, the High Representative, including through INTCEN, should contribute to the Joint Cyber Unit by providing continuous intelligence-based shared situational awareness on existing and emerging threats, including the necessary strategic situational awareness to any given event.

(25) Within the cyber defence community, the EU and Member States aim to strengthen cyber defence capabilities and enhance further synergies, coordination and cooperation between relevant EU institutions, bodies and agencies, as well as with and between Member States, including as regards the Common Security and Defence Policy ('CSDP') missions and operations. The community functions based on an intergovernmental governance at EU level, national military command structures and military, or dual-use capabilities and assets. In light of its different nature, specific interfaces with the Joint Cyber Unit should be built to enable information sharing with the cyber defence community ([21])

(26) The Permanent Structured Cooperation is a legal framework introduced by the Treaty of Lisbon ([22]) and established in 2017 within the Union framework. Structured cooperation led to the establishment of a number of PESCO projects in the cyber domain, contributing to the fulfilment of the commitment 11 ([23]) to "ensure increasing efforts in the cooperation on cyber defense, such as information sharing, training and operational support". EEAS, including the EU Military Staff and EDA, form the PESCO secretariat, which provides a single point of contact within the Union's framework for all PESCO matters, including supporting and coordinating functions related to the PESCO projects (e.g. the assessment of new project proposals, preparation of the projects' progress reports, etc.). Representatives of relevant PESCO projects should support the Joint Cyber Unit notably in relation to situational awareness and preparedness.

(27) Through the Joint Cyber Unit, participants should adequately integrate private sector stakeholders, including both providers and users of cybersecurity solutions and services, to support the European cybersecurity crisis management framework, with due regard to the legal framework for data sharing and security of information. Cybersecurity providers should contribute to the initiative by sharing threat intelligence and providing incident responders to quickly expand the Unit's capacity to respond to large scale attacks and crises. Users of cybersecurity goods and services, primarily those under the scope of the NIS Directive, should be able to seek help and advice through currently missing structured channels linked to EU-level Information Sharing and Analysis Centres (ISACs) ([24]). The platform could also contribute to strengthen cooperation with international partners.

(28) Developing and maintaining situational awareness requires cutting-edge intrusion detection and prevention capabilities. The Joint Cyber Unit should rely on a state-of-the-art network that is able to analyse malicious threats and incidents that may impact key communication and information systems across the Union. This means that, among other sources, threat knowledge extracted from communication networks monitored by national, sectoral and cross-border SOCs should feed into the Joint Cyber Unit to improve participants' assessment of the EU threat landscape.

(29) In order to support the exchange of operational information, possibly including confidential material, the platform should rely on appropriately secure communication channels. Such channels could also build on existing infrastructure, such as the secure information exchange network application ('SIENA') used by Europol and the law enforcement community. As announced in the Cybersecurity Strategy, tools used by EU institutions, bodies and agencies should respect rules on information security that the Commission will soon propose.

([21]) Notably through EEAS representation, in order to enable the appropriate involvement of the cyber defence community, which is based on the voluntary national contributions.

([22]) Article 42.6, 46 and Protocol 10 of the TEU.

([23]) Each of the Member States participating in PESCO undertakes 20 individual commitments, split into the five key areas set out by art.2 of Protocol N°10 on PESCO annexed to the Treaty on the European Union.

([24]) Notable examples of existing ISACs which could be involved in such sharing include the European Energy ISAC (EE-ISAC) or the European Financial Institutes ISAC (FI-ISAC).

(30) The Commission, primarily through the Digital Europe Programme, will support the necessary investments to set up the physical and virtual platform and build and maintain secure communication channels and training capabilities as well as developing and deploying detection capabilities. In addition, the European Defence Fund could help fund key cyber defence technologies and cyber defence capabilities which would reinforce national cyber defence preparedness,

HAS ADOPTED THIS RECOMMENDATION:

I. **PURPOSE OF THIS RECOMMENDATION**

(1) The purpose of this Recommendation is to identify the actions necessary to coordinate EU efforts to prevent, detect, discourage, deter, mitigate and respond to large-scale cyber incidents and crises through a Joint Cyber Unit. In order to do so, this Recommendation also defines the process, milestones and timeline that Member States and relevant EU institutions, bodies and agencies should pursue in relation to the creation and development of that platform.

(2) Member States and relevant EU institutions, bodies and agencies should ensure that, in cases of large-scale cybersecurity incidents and crises, they coordinate their efforts through a Joint Cyber Unit which enables mutual assistance ([25]) through expertise from Member State authorities and relevant EU institutions, bodies and agencies. The Joint Cyber Unit should also allow participants to engage in cooperation with the private sector.

II. **DEFINITIONS**

(3) For the purposes of this Recommendation:

(a) 'EU Cybersecurity Incident and Crisis Response Plan' means a compilation of roles, modalities and procedures leading to the completion of the EU Cybersecurity Crisis Response Framework described in point (1) of the Commission Recommendation of 13 September 2017 on Coordinated Response to Large Scale Cybersecurity Incidents and Crises ('Blueprint').

(b) 'Cybersecurity communities' means collaborative civilian, law enforcement, diplomacy and defence groups representing both Member States and relevant EU institutions, bodies and agencies which exchange information in pursuit of shared goals, interests and missions in relation to cybersecurity.

(c) 'Private sector participants' means representatives of private sector entities providing or using cybersecurity solutions ([26]) and services ([27]).

(d) 'Large-scale incident' means an incident as defined under Article 4(7) of Directive (EU) 2016/1148 with a significant impact in at least two Member States.

(e) 'Integrated EU Cybersecurity Situation report' means a report gathering input from participants in the Joint Cyber Unit, building on the EU Cybersecurity Technical Situation Report defined under Article 7(6) of Regulation (EU) 2019/881.

(f) 'EU Cybersecurity Rapid Reaction team' means a team composed of recognised cybersecurity experts, drawn notably from the CSIRTs of the Member States, with support from ENISA, CERT-EU and Europol, which is ready to remotely assist participants impacted by large-scale incidents and crises.

(g) 'Memoranda of understanding' means an agreement between participants setting out the necessary modalities of cooperation, including a definition of assets and procedures necessary to establish and mobilise EU Cybersecurity Rapid Reaction teams, as well as to allow for mutual assistance.

([25]) Coherently with the approach and principles stated in Directive (EU) 2016/1148 and Article 222 (TFEU). Without prejudice to Article 42(7) of the Treaty on European Union.
([26]) Including software vendors.
([27]) Including threats intelligence.

III. OBJECTIVE OF THE JOINT CYBER UNIT

(4) Member States and relevant EU institutions, bodies and agencies should ensure a **coordinated EU response** to and recovery from large-scale cyber incidents and crises. In particular, such a response should be ensured between operational participants, notably ENISA, Europol, CERT-EU, the Commission, the European External Action Service (including INTCEN), the CSIRTs Network, EU-CyCLONe, and supporting participants, notably the NIS Cooperation Group Chair, the Council Horizontal Working Party on Cyber Issues Chair, the European Defence Agency and one representative of the relevant PESCO projects ([28]). Operational participants should be in a position to swiftly and effectively mobilise operational resources for mutual assistance within the Joint Cyber Unit. To that end, within the Joint Cyber Unit, mutual assistance mechanisms should be coordinated subject to the request from one or more Member States.

(5) In order to provide an effective coordinated response, operational and supporting participants listed in point (4) should be able to share best practices, harness continuous **shared situational awareness**, and ensure necessary **preparedness** to the extent allowed by their mandates. Those participants should take into account existing processes and the expertise of the different cybersecurity communities.

IV. DEFINING THE OPERATION OF THE JOINT CYBER UNIT

(6) Member States and relevant EU institutions, bodies and agencies, building on ENISA's contribution in accordance with Article 7(7) of Regulation (EU) 2019/881, should ensure a **coordinated response** to and recovery from large-scale incidents and crises through:

(a) The establishment, training, testing and coordinated deployment of **EU Cybersecurity Rapid Reaction Teams** leveraging on Article 7(4) of Regulation (EU) 2019/881 and Articles 3 and 4 of Regulation (EU) 2016/794;

(b) The coordinated deployment of a **virtual and physical platform**, leveraging the ENISA and CERT-EU structured cooperation enshrined in Article 7(4) of Regulation (EU) 2019/881, which should serve as a supporting infrastructure for technical and operational cooperation between participants and to gather relevant staff and other resources from participants;

(c) The creation and maintenance of an inventory **of operational and technical capabilities available in the EU** across cybersecurity communities ([29]) in the Union that are ready to be deployed in the case of large-scale cybersecurity incidents or crises.

(d) The reporting to the Commission and the High Representative on experience gained in **cybersecurity operational cooperation activities** within and across cybersecurity communities.

(7) Member States and relevant EU institutions, bodies and agencies should ensure that the Joint Cyber Unit provides continuous shared **situational awareness** and **preparedness** against cyber-enabled crises across cybersecurity communities, as well as within those communities, pursuing the objectives set out in Article 7 of Regulation (EU) 2019/881 and Article 3 of Regulation (EU) 2016/794. To that end, Member States and relevant EU institutions, bodies and agencies, in accordance with Regulation (EU) 2019/881 and Regulation (EU) 2016/794, should enable the implementation of the following **supporting** operations:

(a) The development of the **Integrated EU Cybersecurity Situation report** by gathering and analysing all relevant information and threat intelligence;

(b) The use of adequate and secure **tools**, in line with Article 7(1) of Regulation (EU) 2019/881, for rapid information-sharing among participants and with other entities;

(c) The **exchange of information and expertise** necessary to prepare the Union to manage cyber-enabled large-scale incidents and crises, with the support of ENISA as set out under Article 7(2) of Regulation (EU) 2019/881;

(d) The adoption and testing of national **Cybersecurity Incident and Crisis Response Plans** ([30]) in accordance with Article 7(2), (5) and (7) of Regulation (EU) 2019/881;

([28]) Cyber and Information Domain Coordination Centre" (CIDCC) and "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security" (CRRT).

([29]) Including , where appropriate, the cyber defence community.

([30]) Proposed under Article 7(3) of the Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020) 823 final, 2020/0359 (COD).

(e) The development, management and testing, including through cross-community exercises and trainings, of the **EU Cybersecurity Incident and Crisis Response Plan**, in accordance with the 'Blueprint' recommendation and building upon Article (7)(3) of the Commission's proposal for a revised Directive (EU) 2016/1148 on measures for a high common level of cybersecurity across the Union ([31]);

(f) The assistance of participants in concluding information-sharing agreements, as well as operational cooperation agreements with **private sector entities** providing, among others, threats intelligence and incident response services, with the support of ENISA as set out in Article 7(1) of Regulation (EU) 2019/881;

(g) The establishment of structured synergies with national, sectoral and cross-border **monitoring and detection capabilities**, in particular with Security Operation Centres;

(h) The assistance of participants in the **management** of large-scale incidents and crises, in line with the supporting role of ENISA as set out in Article (7) of Regulation (EU) 2019/881. This includes, contributing to shared situational awareness, supporting diplomatic action, political attribution as well as attribution in the context of criminal investigations, including through Europol ([32]), aligning public communication and facilitating incident recovery.

(8) In order to implement points (6) and (7), Member States and relevant EU institutions, bodies and agencies should ensure:

(a) The definition of the organisational aspects of the Joint Cyber Unit and the **roles and responsibilities** of operational and supporting participants within the platform, allowing for the effective functioning of the platform in line with the aspects and principles specified in the Annex to this Recommendation;

(b) The conclusion of **memoranda of understanding** setting out necessary modalities of cooperation among participants referred to in point (4).

(9) In accordance with Article 7 of Regulation (EU) 2019/881, ENISA should ensure the coordination and support of Member States and relevant EU institution, agencies and bodies within the Joint Cyber Unit, including by acting as secretariat, organising meetings and contributing to the implementation of actions both at Member State and EU level. ENISA should set up both a secure virtual platform and physical space to host meetings and facilitate the necessary implementing actions.

V. **BUILDING THE JOINT CYBER UNIT**

(10) Member States and relevant EU institutions, bodies and agencies should ensure that the Joint Cyber Unit moves into the operational phase as of **30 June 2022**. By that point in time, operational participants should make available operational capabilities and experts that can form the basis of EU Cybersecurity Rapid Reaction teams. Plans for a physical and virtual platform should be well advanced.

(11) Member States and relevant EU institutions, bodies and agencies should contribute to the functioning of the Joint Cyber Unit and ensure that its operationalisation is fully completed by **30 June 2023**. This should be done by taking four subsequent steps, which will be aimed at completing the following activities:

(a) Step one - Assessment of the Joint Cyber Unit's organisational aspects and identification of available EU operational capabilities by **31 December 2021**;

(b) Step two - Preparing Incident and Crisis Response Plans and rolling-out joint preparedness activities by **30 June 2022**;

(c) Step three - Operationalising the Joint Cyber Unit by **31 December 2022**;

(d) Step four - Expanding the cooperation within the Joint Cyber Unit to private entities and reporting on progress made by **30 June 2023**.

More detailed actions to be undertaken under the four sequential steps are set out in the Annex to this Recommendation.

([31]) COM(2020) 823 final.
([32]) In line with Regulation (EU) 2016/794.

(12) Under the first two steps, ENISA should organise and support the preparation of the Joint Cyber Unit. The Commission services should convene a Working Group gathering operational and supporting participants to complete such preparatory work. The Commission services should appoint a representative as co-chair of the Working Group and should invite to act as co-chairs a representative nominated by the High Representative, each contributing on agenda points in accordance with their respective competences, and a representative chosen by the Member States.

(13) By the end of step two, the working group should conclude its assessment of the organisational aspects of the Joint Cyber Unit and the roles and responsibilities of operational participants within that platform. The working group should present the results of that assessment to the Commission and the High Representative. The Commission and the High Representative should then share such assessment with Council. The Commission and the High Representative should draw up a joint report on the basis of that assessment and invite the Council to endorse that report via Council conclusions.

(14) The Joint Cyber Unit should be operational as of step three.

(15) ENISA and the Commission should ensure the use of existing resources under the EU financing programmes, primarily the Digital Europe Programme, in line with the applicable rules for establishing the respective work programmes, for equipping participants in the Joint Cyber Unit with additional training capabilities, communication capabilities and secure information sharing infrastructure allowing for the exchange of classified information including across communities.

VI. **REVIEW**

(16) Member States should cooperate with the Commission and the High Representative, in line with their respective competences, to assess the effectiveness and efficiency of the Joint Cyber Unit by **30 June 2025**, with a view to draw conclusions for the future of the Joint Cyber Unit. This assessment should take into account the implementation of the aforementioned four steps.

Done at Brussels, 23 June 2021.

For the Commission
Thierry BRETON
Member of the Commission

ANNEX

Steps for building the Joint Cyber Unit

This Annex further describes the core and supporting actions needed to establish and operationalise the Joint Cyber Unit.

1. *Step 1 – Assessment of the Joint Cyber Unit's organisational aspects and identification of available EU operational capabilities*

CORE ACTIONS

Operational participants of the Joint Cyber Unit, gathered in a Working Group set up by the Commission and with the support of ENISA, should gather information about existing operational capabilities, including a list of available recognised professionals with an indication of their relevant expertise, available incident handling tools, functions and assets, available training and exercise portfolios, and existing information and intelligence analysis products. Based on that input, operational participants should prepare **a list of available EU operational capabilities** ready to be deployed in case of cyber incidents or crises, notably through EU Cybersecurity Rapid Reaction teams.

The working group should launch an assessment of **organisational aspects of** the Joint Cyber Unit **and the roles and responsibilities of operational participants within that platform**.

In order to acquire an overview of capabilities and agree on procedures, core and, to the extent possible, supporting actions under step one should be completed by **31 December 2021 [6 months after adoption]**.

2. *Step 2 – Preparing Incident and Crisis Response Plans and roll-out joint preparedness activities*

CORE ACTIONS

Operational participants in the working group, in consultation with supporting participants, should prepare the **EU Cybersecurity Incident and Crisis Response Plan** on the basis of the national Cybersecurity Incident and Crisis Response Plans. The EU Cybersecurity Incident and Crisis Response Plan should include objectives of EU preparedness, identified procedures and secure information exchange channels, including ways of handling information, as well as criteria for activating the mutual assistance mechanism based on an agreed incident classification taxonomy and on the list of available EU capabilities.

By the end of step two, the working group should conclude its assessment of the organisational aspects of the Joint Cyber Unit and the roles and responsibilities of operational participants within that platform. The working group should present the results of that assessment to the Commission and the High Representative. The Commission and the High Representative should share such assessment with Council. The Commission and the High Representative should work together, in line with their respective competencies, to draw up a joint report based on that assessment and invite the Council to endorse that report via Council conclusions.

SUPPORTING ACTIONS

The EU Cybersecurity Incident and Crisis Response Plan should build on the main elements of national Cybersecurity Incident and Crisis Response Plans. In line with the Commission's proposal for a Directive on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 ([1]), Member States should adopt national Cybersecurity Incident and Crisis Response Plans. The national plans, which may possibly be subject to peer review, should define objectives and modalities in the management of large scale cybersecurity incidents and crises. The national plans should address, in particular, the following issues:

(a) objectives of national preparedness measures and activities;

(b) roles and responsibilities of the national competent authorities at national level;

(c) national crisis management procedures and information exchange channels;

(d) the identification of preparedness measures, including exercises and training activities;

(e) the identification of relevant public and private stakeholders and infrastructure involved;

(f) the national procedures and arrangements between relevant national authorities and bodies, including those responsible for all cyber communities, to ensure Member State effective participation in and support to the coordinated management of large-scale cybersecurity incidents and crises at EU level.

Based on the input provided by Member States and EU institutions, bodies and agencies, the operational participants should perform the following supporting actions within the framework of the Joint Cyber Unit:

(a) set the first EU Integrated Situational report building on national Cybersecurity Incident and Crisis Response Plans;

([1]) COM(2020) 823 final 2020/0359 (COD), Brussels, 16.12.2020.

(b) establish communication capabilities and secure information sharing tools;

(c) facilitate the adoption of protocols for mutual assistance among participants;

(d) organise cross-community exercises and trainings for experts included in the list of EU available operational capabilities;

(e) develop a multi-annual plan to coordinate exercises.

When needed, operational participants should consult supporting participants. ENISA, with the support of the Commission, Europol and CERT-EU, should enable information sharing by establishing communication capabilities and secure information sharing tools.

To ensure that the necessary plans are set-out and joint activities start to be rolled-out, core and, to the extent possible, supporting actions under step two should be completed by **30 June 2022 [6 months after the end of step 1]**.

3. *Step 3 – Operationalising the Joint Cyber Unit*

CORE ACTIONS

Following the Council's endorsement of the Commission's conclusions on the report under step two, operational participants should coordinate the deployment of **EU Cybersecurity Rapid Reaction teams** within the Joint Cyber Unit and establish a **physical platform** for allowing teams to carry out technical and operational activities. Based on the preparatory work carried out under step two, participants should finalise the EU Cybersecurity Incident and Crisis Response Plan. Operational participants should make sure that the experts and capabilities included in the list of EU available operational capabilities are available and ready to contribute to the activity of EU Cybersecurity Rapid Reaction teams.

In order to implement the EU Cybersecurity Incident and Crisis Response Plan, participants should define an annual work programme.

SUPPORTING ACTIONS

The Joint Cyber Unit may be used by the cyber diplomacy community to align public communication. The platform may allow participants to contribute to political attribution as well as attribution within the criminal justice framework employed at police and judicial level. In addition, it may facilitate recovery and allow for structured synergies with national and cross-border monitoring and detection capabilities.

To ensure the operationalisation of the Joint Cyber Unit, core and, to the extent possible, supporting actions under step three should be completed by **31 December 2022 [6 months after the end of step 2]**.

4. *Step 4 – Expanding the cooperation within the Joint Cyber Unit to private entities and reporting on progress made*

CORE ACTION

Participants in the Joint Cyber Unit should draw up an activity **report on progress made in the implementation of the four steps set out in the Recommendation, describing achievements and challenges faced**. That report should include statistical information regarding operational cooperation activities carried out throughout the four steps. The report should be submitted to the Commission and the High Representative.

SUPPORTING ACTIONS

In order to extend the capabilities and information available to EU Cybersecurity Rapid Reaction teams, participants should ensure that the Joint Cyber Unit assists in the conclusion **of information-sharing and operational cooperation agreements between participants and private sector** entities providing, among others, threat intelligence and incident response services. They should also ensure, among other activities, that the Joint Cyber Unit supports in regular dialogue and information sharing activities on threats and vulnerabilities with users of cybersecurity solutions, primarily those under the scope of the NIS Directive or gathered in **EU-level Information Sharing and Analysis Centres (ISACs).**

Member States should support entities operating within their territory, in particular those under the scope of the NIS Directive, in having access and contributing to public-private dialogues with EU-level ISACs.

To guarantee a proper involvement of the private sector, core and, to the extent possible, supporting actions under step four should be completed by **30 June 2023 [6 months after the end of step 3]**.

HOW TO SWIFTLY MOBILISE EU OPERATIONAL CAPABILITIES

WHO PROVIDES CAPABILITIES: Operational participants

WHO MANAGES THE CAPABILITIES: Participants, within the Joint Cyber Unit, in line with agreed roles and responsibilities

Step	Objective	Task	Core action	Supporting action
Step 1 - Define by **31 December 2021 [6 months after adoption]**	PREPAREDNESS	**Identify capabilities**	**Operational participants to establish a list of EU available operational capabilities.**	
Step 2 - Prepare by **30 June 2022 [6 months under the end of step 1]**	PREPAREDNESS	**Define relevant procedures and arrangements to activate capabilities in case of need**	**Operational participants to prepare the EU Cybersecurity Incident and Crisis Response Plan (EU Cybersecurity Crisis Response Framework under the Blueprint), based on adopted national Plans**	**Operational participants to develop EU Integrated Situational reports based on the EU Cybersecurity Technical Situation report**
	PREPAREDNESS	**Exercise capabilities**		**Participants to organise joint exercise and training (cross-community)** **Participants to work on a multi-annual plan to coordinate exercises.**
	SITUATIONAL AWARENESS	**Establish tools to share information and requests of support**		**Participants to develop secure and rapid information-sharing**
JCU IS OPERATIONAL Based on the preparatory work carried out by participants under a Working Group to be set up by the Commission				
Step 3 – Deploy by **31 December 2022 [6 months after the end of step 2]**	PREPAREDNESS	**Adopt relevant procedures, arrangements and memoranda of understanding to activate capabilities in case of need**	**Operational participants to finalise the EU Cybersecurity Incident and Crisis Response Plan and define its implementation through annual work programmes.**	**Participants to support to the establishment national and cross-border monitoring and detection capabilities, including the establishment of SOCs**
	COORDINATED RESPONSE	**Deploy capabilities in case of need**	**Operational participants to coordinate operational EU Cybersecurity Rapid Reaction teams through the JCU virtual and physical platform in Brussels.**	**Participants to coordinate public communication and contribute to political attribution, as well as attribution in the context of the criminal justice**

Step 4 – Expand and Report by **30 June 2023 [6 months after the end of step 3]**	SITUATIONAL AWARENESS COORDINATED RESPONSE	**Ensure scalability by involving the private sector to provide for emerging needs**	**Participants to submit an activity report about progress made, describing achievements and challenges with the support of statistical information.**	**Participants to conclude information-sharing agreements, as well as operational cooperation agreements with cybersecurity providers** **Participants to conclude information sharing agreements with cybersecurity users, primarily entities under the NIS Directive scope and EU-ISACs**

ISSN 1977-0677 (electronic edition)
ISSN 1725-2555 (paper edition)

Publications Office
of the European Union
L-2985 Luxembourg
LUXEMBOURG

EN