European Commission - Press release

EU Cybersecurity: Commission proposes a Joint Cyber Unit to step up response to large-scale security incidents

Brussels, 23 June 2021

The Commission is today laying out a vision to build a new **Joint Cyber Unit** to tackle the rising number of serious cyber incidents impacting public services, as well as the life of businesses and citizens across the European Union. Advanced and coordinated responses in the field of cybersecurity have become increasingly necessary, as cyberattacks grow in number, scale and consequences, impacting heavily our security. All relevant actors in the EU need to be prepared to respond collectively and exchange relevant information on a ‘need to share', rather than only ‘need to know', basis.

First announced by President Ursula **von der Leyen** in her political guidelines, the Joint Cyber Unit proposed today aims at bringing together resources and expertise available to the EU and its Member States to effectively prevent, deter and respond to mass cyber incidents and crises. Cybersecurity communities, including civilian, law enforcement, diplomatic and cyber defence communities, as well as private sector partners, too often operate separately. With the Joint Cyber Unit, they will have a virtual and physical platform of cooperation: relevant EU institutions, bodies and agencies together with the Member States will build progressively a European platform for solidarity and assistance to counter large-scale cyberattacks.

The Recommendation on the creation of the Joint Cyber Unit is an important step towards completing the European cybersecurity crisis management framework. It is a concrete deliverable of the EU Cybersecurity Strategy and the EU Security Union Strategy, contributing to a safe digital economy and society.

As part of this package, the Commission is reporting today on progress made under the Security Union Strategy over the past months. Furthermore, the Commission and the High Representative of the Union for Foreign Affairs and Security Policy have presented the first implementation report under the Cybersecurity Strategy, as requested by the European Council, while at the same time they have published the Fifth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats. Finally, the Commission has issued the decision on establishing the office of the European Union Agency for Cybersecurity (ENISA) in Brussels, in accordance with the Cybersecurity Act.

A new Joint Cyber Unit to prevent and respond to large-scale cyber incidents

The Joint Cyber Unit will act as a platform to ensure an **EU coordinated response** to large-scale cyber incidents and crises, as well as to offer **assistance** in recovering from these attacks. Today, the EU and its Member States have many entities involved in different fields and sectors. While the sectors may be specific, the threats are often common – hence, the need for **coordination, sharing of knowledge** and even **advance warning**.

The participants will be asked to provide operational resources for mutual assistance within the Joint Cyber Unit (see proposed participants here). The Joint Cyber Unit will allow them to share best practice, as well as information in real time on threats that could emerge in their respective areas. It will also **work at an operational and at a technical level** to deliver the EU Cybersecurity Incident and Crisis Response Plan, based on national plans; establish and mobilise EU Cybersecurity Rapid Reaction Teams; facilitate the adoption of protocols for mutual assistance among participants; establish national and cross-border monitoring and detection capabilities, including Security Operation Centres (SOCs); and more.

The EU cybersecurity ecosystem is wide and varied and through the Joint Cyber Unit, there will be a **common space** to work together across different communities and fields, which will enable the existing networks to tap their full potential. It builds on the work started in 2017, with the Recommendation on a coordinated response to incidents and crises - the so-called Blueprint.

The Commission is proposing to build the Joint Cyber Unit through a **gradual and transparent**

process in four steps, in co-ownership with the Member States and the different entities active in the field. The aim is to ensure that the Joint Cyber Unit will move to the operational phase by 30 June 2022 and that it will be fully established one year later, by 30 June 2023. The European Union Agency for Cybersecurity, ENISA, will serve as secretariat for the preparatory phase and the Unit will operate close to their Brussels offices and the office of CERT-EU, the Computer Emergency Response Team for the EU institutions, bodies and agencies.

The investments necessary for setting up the Joint Cyber Unit, will be provided by the Commission, primarily through the Digital Europe Programme. Funds will serve to build the physical and virtual platform, establish and maintain secure communication channels, as well as improve detection capabilities. Additional contributions, especially to develop Member States' cyber-defence capabilities, may come from the European Defence Fund.

Keeping Europeans safe, online and offline

The Commission is reporting today on the **progress** made under the EU Security Union Strategy, towards keeping Europeans safe. Together with the High Representative of the Union for Foreign Affairs and Security Policy, it is also presenting the first implementation report under the new EU Cybersecurity Strategy.

The Commission and the High Representative presented the **EU Cybersecurity strategy** in December 2020. Today's report is taking stock of the progress made under each of the **26 initiatives** set out in this strategy and refers to the recent approval by the European Parliament and the Council of the European Union of the regulation setting up the **Cybersecurity Competence Centre and Network**. Good progress has been made to strengthen the legal framework for ensuring resilience of essential services, through the proposed Directive on measures for high common level of cybersecurity across the Union (revised NIS Directive or 'NIS 2'). Regarding the **security of 5G communication networks**, most Member States are advancing in the implementation of the EU 5G Toolbox, having already in place, or close to readiness, frameworks for imposing appropriate restrictions on 5G suppliers. Requirements on mobile network operators are being reinforced through the transposition of the European Electronic Communications Code, while the European Union Agency for Cybersecurity, ENISA, is preparing a candidate EU cybersecurity certification scheme for 5G networks.

The report also highlights the progress made by the High Representative on the promotion of **responsible state behaviour in cyberspace**, notably by advancing on the establishment of a Programme of Action at United Nations level. In addition, the High Representative has started the **review process of the Cyber Defence Policy Framework** to improve cyber defence cooperation, and is conducting a 'lessons learned exercise' with Member States to improve the **EU's cyber diplomacy toolbox** and identify opportunities for further strengthening EU and international cooperation to this end. Moreover, the report on the progress made in countering hybrid threats, that the Commission and the High Representative have also published today, highlights that since the 2016 Joint Framework on countering hybrid threats – a European Union response was established, EU actions have supported increased **situational awareness**, **resilience in critical sectors**, **adequate response** and **recovery** from the ever increasing hybrid threats, including disinformation and cyberattacks, since the onset of the coronavirus pandemic.

Important steps were also taken over the last 6 months under the **EU Security Union Strategy** to ensure **security in our physical and digital environment**. Landmark EU rules are now in place that will oblige online platforms to remove terrorist content referred by Member States' authorities within one hour. The Commission also proposed the **Digital Services Act**, which puts forward harmonised rules for the removal of illegal goods, services or content online, as well as a new oversight structure for very large online platforms. The proposal also addresses platforms' vulnerabilities to amplifying harmful content or the spread of disinformation. The European Parliament and the Council of the European Union agreed on temporary legislation on the **voluntary detection of child sexual abuse online by communications services**. Work is also ongoing to better **protect public spaces**. This includes supporting Member States in managing the threat represented by drones and enhancing the protection of places of worship and large sports venues against terrorist threats, with a €20 million support programme underway. To better support Member States in countering serious crime and terrorism, the Commission also proposed in December 2020 to upgrade the mandate of Europol, the EU Agency for law enforcement cooperation.

Members of the College said:

Margrethe **Vestager**, Executive Vice-President for a Europe Fit for the Digital Age, said: *"Cybersecurity is a cornerstone of a digital and connected Europe. And in today's society, responding to threats in a coordinated manner is paramount. The Joint Cyber Unit will contribute to that goal. Together we can really make a difference."*

Josep **Borrell,** High Representative of the Union for Foreign Affairs and Security Policy, said: *"The Joint Cyber Unit is a very important step for Europe to protect its governments, citizens and businesses from global cyber threats. When it comes to cyberattacks, we are all vulnerable and that is why cooperation at all levels is crucial. There is no big or small. We need to defend ourselves but we also need to serve as a beacon for others in promoting a global, open, stable and secure cyberspace."*

Margaritis **Schinas**, Vice-President for Promoting our European Way of Life, said: *"The recent ransomware attacks should serve as a warning that we must protect ourselves against threats that could undermine our security and our European Way of Life. Today, we can no longer distinguish between online and offline threats. We need to pool all our resources to defeat cyber risks and enhance our operational capacity. Building a trusted and secure digital world, based on our values, requires commitment from all, including law enforcement."*

Thierry **Breton**, Commissioner for the Internal Market, said: *"The Joint Cyber Unit is a building block to protect ourselves from growing and increasingly complex cyber threats. We have set clear milestones and timelines that will allow us - together with Member states- to concretely improve crisis management cooperation in the EU, detect threats and react faster. It is the operational arm of the European Cyber Shield."*

Ylva **Johansson**, Commissioner for Home Affairs, said: *"Countering cyberattacks is a growing challenge. The Law Enforcement community across the EU can best face this new threat by coordinating together. The Joint Cyber Unit will help police officers in Member States to share expertise. It will help build law enforcement capacity to counter these attacks."*

Background

Cybersecurity is a top priority of the Commission and a cornerstone of the digital and connected Europe. The increase of cyberattacks during the coronavirus crisis has shown how important it is to protect health and care systems, research centres and other critical infrastructure. Strong action in the area is needed to future-proof the EU's economy and society.

The EU is committed to delivering on the EU Cybersecurity Strategy with an unprecedented level of investment in Europe's green and digital transition, through the long-term EU budget 2021-2027, notably through the Digital Europe Programme and Horizon Europe, as well as the Recovery Plan for Europe.

Moreover, when it comes to cybersecurity, we are as protected as our weakest link. Cyberattacks do not stop at the physical borders. Enhancing cooperation, including cross-border cooperation, in the cybersecurity field is therefore also an EU priority: in recent years, the Commission has been leading and facilitating several initiatives to improve collective preparedness, as EU joint structures have already supported Member States, both at technical and at operational level. Today's recommendation on building a Joint Cyber Unit is another step towards greater cooperation and coordinated response to cyber threats.

At the same time, the Joint EU Diplomatic Response to Malicious Cyber Activities, known as the cyber diplomacy toolbox, encourages cooperation and promotes responsible state behaviour in cyberspace, allowing the EU and its Member States to use all Common Foreign and Security Policy measures, including, restrictive measures, to prevent, discourage, deter and respond to malicious cyber activities.

To ensure security both in our physical and digital environments, the Commission presented in July 2020 the EU Security Union Strategy for the period 2020 to 2025. It focuses on priority areas where the EU can bring value to support Member States in fostering security for all those living in Europe: combatting terrorism and organised crime; preventing and detecting hybrid threats and increasing the resilience of our critical infrastructure; and promoting cybersecurity and fostering research and innovation.

For More Information

Factsheet: Joint Cyber Unit

Infographic: EU Cybersecurity Ecosystem

Recommendation on building a Joint Cyber Unit

First implementation report on the EU Cybersecurity Strategy

Decision on establishing the office of the European Union Agency for Cybersecurity (ENISA) in Brussels

Second Progress Report under the EU Security Union Strategy (see also Annex 1 and Annex 2)

Fifth Progress Report on the implementation of the 2016 Joint Framework on countering hybrid threats

Press release: New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient

EU Security Union Strategy

IP/21/3088

Press contacts:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email

Related media

Cybersecurity