RÉPUBLIQUE FRANÇAISE

SÉNAT

EUROPEAN AFFAIRS COMMITTEE

Paris, 9 July 2020

POLITICAL OPINION

on the fight against cybercrime

The Senate European Affairs Committee,

Having regard to Articles 67 and 82 to 89 of the Treaty on the Functioning of the European Union,

Having regard to the Council of Europe Convention on Cybercrime of 23 November 2001, also known as the Budapest Convention,

Having regard to the Renewed Internal Security Strategy for the European Union 2015-2020,

Having regard to the Joint Communication of the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament and the Council of 13 September 2017 entitled "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU", JOIN (2017) 450 final,

Having regard to the Declaration by the High Representative on behalf of the EU on respect for the rules-based order in cyberspace of 12 April 2019,

Having regard to Senate European Resolution no. 117 (2018-2019) of 21 June 2019 on judicial cooperation in

criminal matters and the establishment of a European Public Prosecutor's Office,

Having regard to the strategic report entitled Internet Organized Crime Threat Assessment, 2019 of Europol's European Cybercrime Centre,

Having regard to the relevant conclusions of the JHA Council of 9 June 2016, of the General Affairs Council of 15 and 16 November 2016, of the JHA Council of 18 May 2017, of the General Affairs Council of 20 November 2017, of the Foreign Affairs Council of 16 April 2018, of the General Affairs Council of 26 June 2018, of the European Council of 18 October 2018, of the General Affairs Council of 19 February 2019, of the General Affairs Council of 19 March 2019, of the Transport, Telecommunications and Energy Council of 3 December 2019 and of the General Affairs Council of 10 December 2019,

Notes that the sharp increase in cybercrime constitutes a threat affecting the European Union and its Member States, which takes a variety of forms with potentially very severe consequences;

Observes that cyberspace has no borders, which presents a challenge to law enforcement and judicial authorities in terms of criminal investigation and prosecution, with a high risk of impunity; considers therefore that cybercrimes must be dealt with in a context of judicial cooperation in criminal matters, with the backing of the European Judicial Cybercrime Network;

Notes that the effectiveness of cybercrime investigations and prosecutions is particularly dependent on obtaining and retaining data as digital evidence; regrets the absence of a data retention system at European Union level; therefore calls for the adoption of a European data retention system which can meet the operational needs of the law enforcement and judicial authorities, which takes into account the requirements of the case law of the Court of Justice of the European Union and of national courts, and which is respectful of fundamental rights, such as the right to privacy, the protection of personal data, non-discrimination and the presumption of innocence;

Deems it necessary, to be able to fight cybercrime better and guarantee cybersecurity, to provide the law enforcement and judicial authorities of the Member States, Europol and Eurojust with enough financial and human resources to cope with the new challenges posed by technological progress and the changes in the threats, including by reinforcing partnerships with the private sector; emphasises the importance of training in digital security and considers that the relevant European agencies have a role to play in these matters;

Emphasises the central role of Europol and its European Cybercrime Centre; invites all the Member States to cooperate at best with this agency and to populate its databases with complete, high-quality information; calls for the reinforcement of Europol's role in the fight against cybercrime by extending the scope of the EU Internet Referral Unit (*EU IRU*) to the reporting of all illegal online content and to the corresponding adaptation of the European illegal content database (*IRMa*), and for the development of a platform for reporting fraudulent bank transactions, as well as supports the creation of national victim support schemes and their networking; requests that the innovation laboratory be quickly set up within Europol, which will enable law enforcement authorities to be involved in and aware of technological changes and developments at an earlier stage;

Supports the action of ENISA with a view to the creation of a European cybersecurity certification framework; wishes that this agency will join the network of agencies operating in the area of freedom, security and justice; invites ENISA to strengthen its operational cooperation with the law enforcement and judicial authorities;

Considers that the fight against cybercrime requires effective international cooperation capable of promoting security and stability in cyberspace; believes that the improvement of that cooperation requires the ratification of the Budapest Convention by all the Member States of the European Union and the conclusion at the earliest opportunity of the negotiations on the Second Additional Protocol to this Convention; wishes to see a reinforcement of cooperation between the European Union and the Council of Europe in the fight against cybercrime, in line with their respective mandates;

Considers that the United Kingdom must remain an indispensable partner in the fight against cybercrime; requests therefore that the new partnership between the United Kingdom and the European Union allow for the closest cooperation possible, whilst respecting the autonomy of the European Union and the sovereignty of the United Kingdom, in the fields of cybersecurity and the fight against cybercrime, including in matters relating to judicial cooperation; considers that this new partnership must guarantee the United Kingdom's relations with Europol, Eurojust and ENISA, as well as the conditions of extradition and mutual judicial assistance, which will replace the European arrest warrant;

Considers that the European Union must get organised to prosecute cybercriminals more effectively; observes that all too often the territoriality of criminal law still constitutes an obstacle to prosecution, in particular when cybercrimes involve several Member States; therefore asks that a thorough reflection be conducted on the ways and means to extend the competences of the European Public Prosecutor's Office to the fight against cybercrime; is aware that such a change can only occur, where applicable, if several conditions are met, in particular unanimity in the European Council, respect for the principle of subsidiarity and the convincing operation of the European Public Prosecutor's Office in its initial areas of competence; indeed considers that centralising cross-border cybercrime cases at the European Public Prosecutor's Office would allow for greater integration of the functioning of the European Union in the face of growing threats.