Memorandum of Understanding

between

The European Union Agency for Network and Information Security (ENISA) of the first part,

The European Defence Agency (EDA) of the second part,

Europol's European Cybercrime Centre (EC3) of the third part,

and

The Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (CERT-EU) of the fourth part;

The European Union Agency for Network and Information Security (hereinafter referred to as ENISA), represented for the purpose of the signature of this Memorandum of Understanding by its Executive Director, Udo Helmbrecht, of the first part,

The European Defence Agency (hereinafter referred to as EDA), represented for the purposes of the signature of this Memorandum of Understanding by its Chief Executive, Jorge Domecq, of the second part,

Europol's European Cybercrime Centre (hereinafter referred to as EC3), represented for the purposes of the signature of this Memorandum of Understanding by its Head, Steven Wilson, of the third part,

and

The Computer Emergency Response Team for the EU Institutions, Agencies and Bodies (hereinafter referred to as CERT-EU), represented for the purposes of the signature of this Memorandum of Understanding by its Acting Head, Ken Ducatel, of the fourth part,

hereinafter collectively referred to as the "Parties", or individually as the "Party",

Having regard to Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security, in particular Article 11 read together with Recital 18 thereof,

Having regard to Council Decision (CFSP) 2015/1835 of 12 October 2015 defining the statute, seat and operational rules of the European Defence Agency, in particular Article 10 read together with Recital 8 thereof,

Having regard to 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), in particular Article 23 thereof,

Having regard to Arrangement 2018/C12/01 between the European Parliament, the European Council, the Council of the European Union, the European Commission, the Court of Justice of the European Union, the European Central Bank, the European Court of Auditors, the European External Action Service, the European Economic and Social Committee, the European Committee of the Regions and the European Investment Bank on the organisation and operation of a computer emergency response team for the Union's institutions, bodies and agencies (CERT-EU) of 20 December 2017, in particular Articles 3 and 5 thereof,

Whereas:

(1) In line with their respective mandates, the cooperation between the Parties can contribute to developing further the provision of expertise, operational and technical support to the EU, its Member States, and its institutions, bodies and agencies, in the area of cyber security.

(2) In line with the EU Cyber Security Strategy communicated in 2013, the EU Cyber Defence Policy Framework adopted by the Council in 2014, and the 2017 Joint Communication JOIN(2017)450 to the European Parliament and the Council: Resilience, Deterrence And Defence: Building Strong Cybersecurity for the EU, there is a need for EU bodies and agencies to cooperate and contribute to EU-level situation awareness, and enhanced cooperation between the civil cyber security and military cyber defence communities can contribute to identifying and capitalising on synergies in the respective policy areas.

(3) Having regard to the General Affairs Council Conclusions of 25 June 2013, calling for strengthening cooperation and emphasising that synergies and complementarities between EU institutions, agencies and bodies involved in cybersecurity can contribute to the aim of achieving an open, safe and secure cyberspace.

(4) Building on their existing competencies and avoiding establishing duplicative processes or creating duplicative structures, the development of cooperation frameworks between the Parties engaged in the interrelated and complementary fields of cyber security, cyber defence, and investigating cybercrime can foster collaboration in meeting the increasingly complex challenges in the cyber domain.

(5) Having regard to the Council Conclusions on the Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (14435/17 of 20 November 2017)

(6) Having regard to Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises,

(7) It is in the common interest of the Parties to establish a Memorandum of Understanding in the areas of mutual interest.

Have agreed as follows:

Article 1

Purpose

The purpose of this Memorandum of Understanding is to establish a cooperation framework between the Parties by identifying the areas of cooperation based on common interest and setting the objectives and principles of such cooperation.

Article 2

Scope

This Memorandum of Understanding does not create legally binding obligations, nor does it supersede any legal obligation of any of the Parties. It only covers cooperation between the Parties in as far as supported by their respective mandates. For any aspects of cooperation that are not covered by the mandate of any of the Parties, cooperation may take place between the other Parties.

Article 3

Areas of cooperation

The Parties cooperate by exchanging expertise and best practices in the areas of cyber security, cyber defence, and investigating cybercrime developed in carrying out their respective mandates, in particular, in the following areas:

a. Exchange of information;
b. Education & Training;
c. Cyber Exercises;
d. Technical cooperation;
e. Strategic and administrative matters;
f. Other areas identified as mutually important.

The scope of the cooperation is further refined by the following Articles 4 to 8. These areas

will be supported by a cooperation working programme, which will be negotiated and agreed on an annual basis. The activities included in this working programme will be reflected in the respective programming documents, such as Single Programming Documents, of the Parties.

Article 4

Exchange of information

1. The Parties agree, where appropriate, to exchange information collected and processed, statistics, analyses, and reports acquired in the delivery of their respective mandates, in accordance with their founding legal acts (where applicable), and any internal rules that may be in place. Exchange of EU classified information is not foreseen and is out of scope of this Memorandum of Understanding.

2. When setting up the exchange of information, statistics, analyses and reports, the respective internal procedures of the Parties will be followed.

3. The Parties agree, where appropriate, to cooperate in exchanging information on the findings resulting from the monitoring of relevant research initiatives to improve the understanding of cyber security, cyber defence, and cybercrime.

4. The exchange of information can include, but it is not limited to:
   a. General observations and general findings resulting from the Parties' activities that could be of help for the work of the other Parties;
   b. Exchange of best practices, tools and recommendations that could help the Parties to strengthen their cooperation in the fields covered by the present Memorandum of Understanding.

Article 5

Education Training & Cyber Exercises

1. The Parties agree to cooperate, where appropriate, in the identification and development of new training and exercise formats in areas of common or overlapping interest.

2. Where appropriate, the Parties undertake to share coordination platforms in the area of cyber security and cyber defence training and exercises.

3. The Parties may, where appropriate, exchange strategies, methodologies and plans related to training and exercises on a regular basis, as well as share relevant materials of common interest.

4. The Parties agree to explore, where appropriate:

    a. The possibilities to enable cross-access to cyber ranges training and exercise infrastructures for other Parties to the Memorandum of Understanding.

    b. The possibilities of mutual participation in training and exercise programmes, and launching of joint training and exercise activities, aiming to promote synergies and avoid duplicative efforts.

5. The Parties may, within the confines of their respective mandates, engage in further cooperation related to training and exercises, including the exchange of information on trainers and experts, and exploring potential use of one another's facilities or logistics.

6. The contribution of one Party to the training materials or activities of the other one will be duly acknowledged by the latter.

Article 6

Technical cooperation

1. The Parties agree, where appropriate, to engage in cooperation on the relevant aspects of their respective activities within the remit of their respective mandates.

2. In as far as the respective mandates, sharing rules and agreements permit, the Parties intend to engage in threat intelligence sharing in order to improve information and intelligence sharing.

3. The Parties will seek to improve their cooperation in the context of cybersecurity incident response and in particular as regards the activities and procedures foreseen in the Blueprint for coordinated response to large scale cybersecurity incidents and crises at EU level (C/2017/6100) and in the context of the EU Law Enforcement Emergency Response Protocol for Major Cross-Border Cyber-Attacks.

4. The Parties intend, in particular, to cooperate by identifying and acting in areas of common interest and joint research.

5. The Parties may, within the confines of their respective mandates, engage in further cooperation that has added value and is in the mutual interest of the Parties.

Article 7

Strategic matters

1. The Parties agree to consult one another, where relevant, when preparing their strategic documents, such as strategies and action plans on the areas of cooperation identified in this Memorandum of Understanding.

2. Each Party may, where appropriate, invite the other Party to participate in any of its planning activities to ensure consultation and the coordination of the relevant activities.

3. The Parties agree, where appropriate, to facilitate communication with respective networks or entities or experts and when necessary to play an interface role so as to maximise benefits from this cooperation by ensuring synergies.

4. The Parties agree to pursue cooperation and interaction as regards consultation of EU policy documents related to cyber security, cyber defence, and cybercrime.

Article 8

Administrative matters

The Parties agree, where appropriate, to cooperate in administrative matters by sharing experience, expertise and best practices, including in the fields of human resource management, management of premises, internal and external audits, quality and risk management, internal control standards, finance and procurement.

Article 9

Confidentiality and Security

1. Each Party undertakes to keep in confidence any information, document or other material provided by the other Party, not to disclose it to third parties without a prior written consent of that Party and not to use any such information for any purpose other than the implementation of this Memorandum of Understanding.

2. Each Party will ensure that information provided or exchanged under this Memorandum of Understanding is protected according to their respective security rules and principles as referred to in their respective establishing acts without prejudice to the role of their respective governing bodies to put these security rules and principles in practice.

3. The Party supplying the information may indicate, at the moment of providing the information, any restriction on access thereto or the use to be made thereof, in general or specific terms, including as regards its transfer, erasure or destruction.

4. The Parties agree to cooperate, as appropriate, in the field of security in particular as regards measures necessary for the protection of sensitive information by means of consultation, mutual support or exchange of best practices.

Article 10

Expenses

The Parties will bear their own expenses which may arise when implementing the present Memorandum of Understanding unless otherwise mutually agreed on a case-by-case basis.

Article 11

Contact points

The Parties will appoint, in line with their internal rules and procedures, appropriate points of contact for the implementation of this Memorandum of Understanding. The relevant contact points will be communicated to the other Parties within a reasonable time following the signature of this Memorandum of Understanding.

Article 12

Rotating Chair of the cooperation framework

1. The cooperation framework established in this Memorandum of Understanding will be led by one of the Parties on a rotating basis. The designated Party will lead for a period of one year.

2. Annually, at least one meeting at the level of the Signatories of the Parties will be hosted by the designated leading Party of the given year.

3. At these meetings, the Parties will, among other things, assess progress made in the implementation of this Memorandum of Understanding, and discuss and agree further cooperation activities.

Article 13

Working Group of the cooperation framework

1. The Parties will establish a Working Group composed of the contact points set out in Article 11 from their respective organisations within the framework of this

Memorandum of Understanding. Each contact point may invite additional experts from its own organisation as appropriate to any meeting.

2. The leading party of the cooperation framework will also serve as Chair of the Working Group.

3. The Working Group will annually prepare a cooperative working programme or roadmap with a horizon of two to three years.

4. The Chair's representative(s) on the Working Group will report to the Signatories of the Parties at their annual meeting.

5. The Working Group will meet at least two times per year with rotational hosting.

6. Additional meetings may be scheduled by the Chair on the Chair's initiative, or upon request of one or more of the other Parties.

Article 14

Settlement of disputes

Any disputes which may emerge in connection with the interpretation or application of the present Memorandum of Understanding will be settled by means of consultations and negotiations between representatives of the Parties.

Article 15

Amendments and supplements to the Memorandum of Understanding

1. This Memorandum of Understanding may be amended or supplemented at any time by mutual consent between the Parties.

2. All amendments and supplements will be done in writing. They will enter into force on the day following the signature by the last Party.

Article 16

Termination

1. Any of the Parties may terminate their commitment under this Memorandum of Understanding by giving three months' notice in writing to all other Parties to the Memorandum.

2. This Memorandum of Understanding will stay in force between the remaining Parties until such a time as they submit their own written notice of termination in accordance with this article.

Article 17

Entry into force

This Memorandum of Understanding will enter into force on the day following its signature by the last Party.

Done in Brussels on 23 May 2018 in quadruplicate copy in the English language.

For ENISA,

Executive Director,

Udo HELMBRECHT

For EDA,

Chief Executive,

Jorge DOMECQ

For EC3,

Head of EC3,

Steven WILSON

For CERT-EU,

Acting Head of CERT-EU,

Ken DUCATEL