European Union
EXTERNAL ACTION

The EU Cyber Diplomacy Toolbox

3 June 2019

European Union
EXTERNAL ACTION

Toolbox/Framework

- Adopted 19 June 2017;
- Helps improve cooperation, prevent conflict, mitigate potential cyber threats as well as deter and influence the behaviour of potential aggressors;
- Response to growing concern at the increased ability and willingness of state and non-state actors to undertake malicious cyber activities.

European Union
EXTERNAL ACTION

Main principles of the Framework:

- serve to protect the integrity and security of the EU, its Member States and their citizens,
- take into account the broader context of the EU external relations with the State concerned,
- provide for the attainment of the CFSP objectives as set out in the Treaty on the European Union (TEU) and the respective procedures provided for their attainment,
- be based on a shared situational awareness agreed among the Member States and correspond to the needs of the concrete situation in hand,
- be proportionate to the scope, scale, duration, intensity, complexity, sophistication and impact of the cyber activity,
- respect applicable international law and must not violate fundamental rights and freedoms.

European Union
EXTERNAL ACTION

NEXT STEPS

- **16 April 2018**, the Council adopted conclusions on malicious cyber activities which underlined the importance of a global, open, free, stable and secure cyberspace, and expressed concern about the activity of malicious actors;
- **28 June 2018 and 18 October 2018** the European Council called for work on the capacity to respond to and deter cyber-attacks to be taken forward;
- **12 April 2019**, the High Representative issued a declaration on behalf of the EU stressing the need to respect the rules-based order in cyberspace, urging actors to stop undertaking malicious cyber activities including the theft of intellectual property, and calling on all partners to strengthen international cooperation to promote security and stability in cyberspace.

European Union
EXTERNAL ACTION

RESTRICTIVE MEASURES

17 May 2019, the Council established a framework which allows the EU to impose targeted restrictive measures to deter and respond to cyber-attacks which constitute an external threat to the EU or its member states, including cyber-attacks against third States or international organisations where restricted measures are considered necessary to achieve the objectives of the Common Foreign and Security Policy (CFSP).

European Union
EXTERNAL ACTION

SANCTION REGIME

Cyber-attacks falling within the scope of this new sanctions regime are those which have significant impact and which:

- **originate or are carried out from outside the EU or**
- **use infrastructure outside the EU or**
- **are carried out by persons or entities established or operating outside the EU or**
- **are carried out with the support of person or entities operating outside the EU.**

Attempted cyber-attacks with a potentially significant effect are also covered by this sanctions regime.

European Union
EXTERNAL ACTION

This framework allows the EU for the first time to impose sanctions on persons or entities that are responsible for cyber-attacks or attempted cyber-attacks, who provide financial, technical or material support for such attacks or who are involved in other ways.

Sanctions may also be imposed on persons or entities associated with them.

Restrictive measures include a ban on persons travelling to the EU, and an asset freeze on persons and entities. In addition, EU persons and entities are forbidden from making funds available to those listed.

European Union
EXTERNAL ACTION

MISSION

The EU remains committed to keeping cyberspace open, stable and secure and reiterates its attachment to the settlement of international disputes in cyberspace by peaceful means.

In this context, all of the EU's diplomatic efforts should aim as a matter of priority to promote security and stability in cyberspace through increased international cooperation, and reduce the risk of misperception, escalation and conflict that may stem from Information and Communications Technologies (ICT) incidents.

European Union
EXTERNAL ACTION

Questions?

agnieszka.wierzbicka@eeas.europa.eu