European Union
EXTERNAL ACTION

Framework for a joint EU diplomatic response to malicious cyber activities "cyber diplomacy toolbox“

European External Action Service

European Union
EXTERNAL ACTION

- The European Union and its Member States are firm promoters of an open, stable and secure cyberspace, respectful of human rights, fundamental freedoms and the rule of law.
- The European Union and its Member States underline their commitment to continue to promote responsible behaviour in cyberspace through the:
  - Application of international law;
  - Norms of responsible state behaviour;
  - Regional confidence building measures;
  - Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("cyber diplomacy toolbox").

European Union
EXTERNAL ACTION

- The **Framework** is part of EU's approach to cyber diplomacy, contributing to conflict prevention, mitigation of cybersecurity threats and greater stability in international relations.
- Contributes to strengthening the rules-based order in cyberspace, including the application of international law and the adherence to norms of responsible state behaviour.
- Encourages cooperation, facilitates mitigation of threats and influences behaviour at longer term.
- Enables the EU and its Member States to leverage the full continuum of EU policies and instruments, including if necessary restrictive measures, to keep cyberspace open, stable and secure.

European Union
EXTERNAL ACTION

Institutional Framework

- Council Conclusions (2017)
- Implementing Guidelines (2017)
- Adoption of a horizontal cyber sanctions regime (2019)
- Guidelines on 'Coordinated Attribution at EU level' (2019)
- Regular exercises (2017, 2018, 2019).

European Union
EXTERNAL ACTION

EU autonomous horizontal cyber sanctions regime

- Establishes a legal framework for sanctions against cyber-attacks.
- The cyber sanctions regime addresses persons and entities involved in cyber-attacks or attempted cyber-attacks with a significant effect, which constitute an external threat to the Union or its Member States.
- A listing is also possible for a cyber-attack against a third state or international organisation.
- A listing does not amount to attribution.

European Union
EXTERNAL ACTION

Coordinated Attribution at EU Level

- Not all measures require attribution.
- Attribution is a sovereign political decision by a State.
- EU Member States can coordinate attribution at EU level.
- Attribution may be communicated and/or accompanied by a diplomatic response.
- Attribution is part of wider cyber diplomacy efforts and no measure or strategy in itself.

European Union
EXTERNAL ACTION

"Measures may be public or private, and may or may not be accompanied with coordinated attribution at EU level."

- Declaration by the High Representative on behalf of the EU condemning the cyber-attack against Georgia (February 2020)
- Declaration by the High Representative on behalf of the EU stressing the need to respect the rules-based order in cyberspace (April 2019)
- Statement by Commission President Juncker, High Representative Mogherini and Council President Tusk on the targeted cyber-attack against OPCW (October 2018)
- Council Conclusions responding to malicious cyber activities, including Wannacry and NotPetya (April 2018)