Annika Sachs, Imke Schmalfeldt, Alisa Jazxhi, Kerstin Zettl-Schabath (Heidelberg University)

EU Cyber Diplomacy Toolbox Dataset – Codebook Version 1.0

Purpose

The EU Cyber Diplomacy Toolbox was implemented in 2017 and is meant to serve as a framework for joint EU diplomatic responses to malicious cyber activities. The objective of this dataset is to provide the first empirical record of the application of measures and guidelines within the Toolbox by EU institutions/actors until 31 May 2023. The dataset provides descriptive data from specific EU institutions that have applied the Cyber Diplomacy Toolbox so far. By tracking the actual application of the different Toolbox measure types, we can therefore analyse their intended effects and effectiveness.

Sources and data

The Cyber Diplomacy Toolbox is a diplomatic instrument of the European Union; thus, it is part of the European Union's Common Foreign and Security Policy (CFSP). The selection of the examined sources is therefore based on the most relevant EU institutions/actors regarding the policy field of foreign policy (Figure 1). The institutions explicitly mentioned in the Cyber Diplomacy Toolbox are included. As a first step, the data is pre-filtered by the keyword "cyber" to narrow down the relevant study sample.

Institution	Link	Document types
European Council	https://www.consilium.europa.eu/de/press/press-releases/?keyword=cyber&dateFrom=&dateTo=	Press releases, declarations
EEAS/High Representative (HR)	https://www.eeas.europa.eu/eeas/press-material_en?f%5B0%5D=pm_category%3AStatement/Declaration&f%5B1%5D=pm_category%3AStatement/Declaration	Statements, declarations
European Commission	https://ec.europa.eu/commission/presscorner/advancedsearch/en	Speeches, statements, press releases
European Parliament	https://www.europarl.europa.eu/news/en/press-room?searchQuery=Cyber&minDate=01-01-2016&maxDate=30-04-2023&contentType=placeholder	Not further specified

Coding

Categorisation of "Cyber Diplomacy Measures"

A measure is categorised for the purpose of this Codebook as a "cyber diplomatic measure" if it, as a diplomatic measure, explicitly addresses the issue of cybersecurity and addresses either the general public or a third actor besides EU institutions. A measure is a cyber diplomatic measure if it aims to change the behaviour of actors in cyberspace, or if it aims to support a third actor in cyberspace. These "cyber diplomatic measures" are categorised as measures of the Cyber Diplomacy Toolbox and are divided into five distinct categories.

Cyber Diplomacy Measures

Cate-gory	Title	Further description
1	**preventive**	
	Confidence-building	Confidence-Building Measures (CBMs) are broadly defined as measures that address, prevent, or **resolve uncertainties among states** (CSIS).
	Awareness-raising*	These may take the form of EU **démarches** or EU-led political and thematic **dialogues** → awareness-raising regarding the **EU's strategic orientation**, informing about the framework, improving the understanding of national policies, identifying other preventive/cooperative measures, etc. Example: mentioning the rising number of cyber threats or announcing new cybersecurity measures
	Capacity-building	Cyber capacity-building measures may, for instance, aim at further advancing capabilities to investigate and prosecute cyber criminals or increasing incident response capacities in third-countries; data sources: https://www.eucybernet.eu/ccb-table/; https://cybilportal.org/projects-advanced/?_sft_region=europe Example: The video message of the commissioner Olivér Várhelyi, in which he announced a new cyber capacity-building program for the Western Balkans, starting in 2023 (#194)
2	**cooperative**	
	political & thematic dialogues	These **signal the seriousness of a situation** for the EU and its member states, facilitate a peaceful resolution to an ongoing incident, **ask for assistance or cooperation to mitigate malicious activity,** or to ask a third country to join in the response to malicious cyber activity (commission, EEAS, Council),
	démarches	These **signal seriousness of the situation** for the EU and its member states, facilitate a peaceful resolution to an ongoing incident, **ask for assistance or cooperation to mitigate malicious activity,** or to ask a third country to join in the response to malicious cyber activity (commission, EEAS, Council).
3	**stabilising**	
	statements	These **express concern or condemn general cyber trends or certain cyber activities** (i.e., through signalling likely consequences/awareness of activities/strategic communications). They may come from High Representative (HR) activity on behalf of the EU; HR statements; Spokesperson statements; local EU statements (may be requested by Member States, the HR/Vice President of the European Commission, the HR/VP Cabinet, or

	the Spokesperson's Team; may also be proposed by an EU delegation).
EU Council conclusions	These are **general or specific** Council conclusions on malicious cyber activities: they may express a **political position**, invite another EU institution to act, or **prepare a proposal** for coordinated action among Member States (**signalling function;** may set out **action** or highlight **awareness** and **determination** to **prevent** and **respond** to potential attempted cyber operations).
diplomatic démarches by EU delegations	EU Delegations or Member states may act when one or more Member States are **impacted** by a malicious cyber activity (e.g., EU delegations/Member States may jointly contact States exercising jurisdiction over territories that have been used for conducting malicious activities). They may raise **concerns** about certain malicious activities, **signal the seriousness** of a situation for the EU and its member states, **facilitate the peaceful resolution** of an ongoing incident, **ask for assistance or cooperation** to mitigate malicious activity or ask a third country to join in the response to malicious cyber activity, **signal the likely consequences** of malicious cyber activity, or they may **signal** that the **origins of activities are known** and that these are considered to be contrary to international voluntary non-binding norms of responsible State behaviour or to international law (possible without attribution).
signalling trough dialogues	This is used to **raise concerns** about certain malicious cyber activities; **signal the seriousness** of a situation for the EU and its member states; **facilitate the peaceful resolution** of an ongoing incident; **signal** the **likely consequences** of malicious cyber activity or to signal the **origin of the activity (when known);** and to signal that these are considered to be contrary to international voluntary non-binding norms of State behaviour or to international law. EEAS; Commission may be invited by Member States or the EU Council to Dialogues with third countries and international organisations.

Example: "Russia also must stop its disinformation campaign and cyber-attacks" (#168, #179, #182) or "The European Council condemns recent malicious cyber activities against Member States, including in Ireland and Poland. It invites the Council to explore appropriate measures within the framework of the Cyber Diplomacy Toolbox" (#109).

4	**Restrictive**	
	Sanctions	These may be conducted against third countries, entities, or individuals on the basis of a Council decision adopted under Article 29 TEU; such measures can include, i.e., travel bans, arms embargoes, freezing funds or economic resources. For further information about the EU Cyber Sanctions regime, see Council Conclusion 2019/797.
5	**EU support for Member States' lawful responses**	(has not been applied so far)
	Upon request of the concerned Member State(s), the EU can provide support to Member States that individually or collectively resort to responses in accordance with international law that are not available within the CFSP (lawful measures, ranging from diplomatic steps to the use of stronger individual or cooperative responses); in grave instances, Member States may choose to exercise their inherent right to individual or collective self-defence, as recognized in Article 51 of the Charter of the United Nations and in accordance with international law, including international humanitarian law. A Member State may also choose to invoke Article 42 (7) TEU to call on other Member States to provide aid and assistance. → Solidarity Clause (Art. 222 TFEU); Mutual-Assistance Clause (Art. 42 (7) TEU); Article 51 UN Charter.	

#id
To facilitate working with our data, we assigned an ID to each case for clear assignment.

Date
Depends on the exact measures;

- For speeches, démarches, dialogues etc., the date of publication/press release applies.
- For sanctions, the date of publication of the regulation applies.
- For capacity-building measures, the first day of the month in which the measure is implemented applies.
- The measures referred to in number 5 have not been applied so far, therefore no further date format is specified.

Title
This refers to the title of the respective speech/statement/measure.

Category ("Cat")
This refers directly to the measures of the Cyber Diplomacy Toolbox; each regarded application of the Cyber Diplomacy Toolbox must be categorised with at least one of the categories mentioned within the section "Cyber Diplomacy measures;" if a measure falls within several categories, this is considered in the "Cat+" section; the Cat section always considers the highest category (the categories are conceptualised as gradually escalatory).

Category+ ("Cat+")
If a measure combines several categories, the additional lower categories are listed within this section; the classification of the measures is also conducted according to the section "Cyber Diplomacy measures."

Linked cyber incident

- If any cyber incident is mentioned within in a respective measure, it is named here; there is no further specification as to whether it is used only as an example or if the measure is explicitly tied to the specific cyber incident.
- Mentioning more than one cyber incident is also possible.
- If a specific initiator or initiator state is named, it is mentioned here.

Short description/inclusion criteria

This describes the content of a statement, démarche, dialogue, etc. and elaborates on the exact criteria as to why this measure counts as measure and justifies the categorisation. If the measure is a capacity-building measure, only the region of implementation is indicated in the description.

Link

This references the respective measure [last access 10.07.2023].

Ukraine

From 2021 onward, we also differentiate as to whether Ukraine is explicitly mentioned regarding cyber incidents/threats; we consider this as a dichotomy variable: 1 = yes, Ukraine mentioned; 0 = not mentioned/not mentioned in the context of cyber threats.

Institution

This section differentiates between the specific acting/executing EU institutions; the relevant institution which published a respective statement/speech, etc. is named here; in case of duplicates, we mention both institutions and consider the measures to be one single measure.

Literature

Council of the European Union (2019). *Council Decision (CFSP) 2019/797*. Council of the European Union. Available at https://web.archive.org/web/20240119111936/https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797 [Archived on: 19.01.2024].

General Secretariat of the Council (2017). *Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities*. Council of the European Union. Available at https://web.archive.org/web/20240119112130/https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf [Archived on: 19.01.2024].