EU Cyber Diplomacy 101

Written by Clara Cotroneo, Frank Lavadoux, Olivia Brown and Mathias Delmeire

Blog 6, of the series 'Possible impacts of the current pandemic on international negotiation processes'.

By Clara Cotroneo, Frank Lavadoux, Olivia Brown, and Mathias Delmeire

In our previous blog posts, we dived headfirst into the world of **online diplomacy** (or e-diplomacy), which we broadly understand as diplomacy conducted online in **cyberspace**. We have discussed how **digitalisation and the surge of online platforms has changed diplomacy** profoundly (here and here if you'd like a refresher). Under the constraints posed by the latest pandemic, digital tools and online platforms are now the place where diplomatic negotiations and strategies develop and unfold.

Never has the question of how 'cyberspace' and 'diplomacy' relate to each other been so important. The European Commission (EC) has identified 'digital transformation' as a priority for years to come, as is evident from the quick expansion of the EU's realm of cyber and digital policies such as: the EU digital strategy, the data strategy, the White Paper on Artificial Intelligence: a European approach to excellence and trust, the cybersecurity strategy and legal framework, the EU cyber diplomacy toolbox and the autonomous cyber sanctions regime.

To help us all get to grips with this advancing field, we have asked EIPA cybersecurity and digitalisation expert Clara Cotroneo to guide us in the world of cyber diplomacy.

In this blog post, we look at cyberspace not as an environment in which diplomatic negotiations take place, but rather as the **object of online negotiations** themselves. Cyber diplomacy is a very recent strand of diplomacy. Its objective is to ensure that the use of information and communication technologies (ICTs) does not harm countries' democracies, political systems, critical infrastructures and, ultimately, citizens. Let us think, for example, about the most recent cyberattacks in the healthcare sector in Europe, from Belgium to Ireland, or the attack on the German Parliament. Against these risks, cyber diplomacy aims at ensuring that there is a set of rules which define responsible state behaviour in cyberspace. Before we start, it is important to clarify some relevant terminology.

Terminology first: what do we talk about when we discuss 'cyber diplomacy'?

In media, political and policy discourses, we often hear about 'cyber diplomacy', an expression which combines 'diplomacy' and 'cybersecurity'. In order to understand this expression, let us take a step back and clarify these terms separately first. *Diplomacy* is the work that diplomats do to advance the interests of the state institutions or organisations they represent, through representation, communication and negotiation, among other processes. Cyber security is the set of measures that individuals, organisations and institutions put in place in order to protect their tangible assets (for example people, buildings or infrastructures) from cyberattacks and/or intangible assets (for example data, knowledge, the ability to deliver a service, power or ideas). Due to the increasingly digital nature of our lives, cyber security is becoming an ever-pressing issue in all aspects of society.

Cyber diplomacy, in turn, in the international and EU contexts refers to the work of governmental actors to come up with a series of *norms* that **regulate the behaviour of state and non-state actors in cyber space**. More specifically, the objective of cyber diplomacy is to define a set of norms which meets the following criteria:

- achieve an **open, free, stable and secure cyberspace**;
- apply to **state** and **non-state actors**;
- adopted under the auspices of **international law**;
- promoted, incorporated, implemented and enforced through **multilateral agreements**.

In summary, cyber diplomacy refers to efforts made by state representatives to shape, at the global level, the governance of cyberspace in order to prevent or penalise cyberattacks. However, as we shall see shortly in the next section, in the EU context, the term 'cyber diplomacy' is not used only in reference to the EU's efforts towards setting legally binding, multilateral agreements for responsible behaviour in cyberspace. Rather, the term is used in reference to a range of strategies and measures that the EU puts in place to promote cybersecurity. In this introduction, we explore here two axes across which the EU's approach to cyber diplomacy develops: *international* and *internal cybersecurity*. The former is outward looking and focuses on the development of multilateral and global strategies; the latter focuses on the impact of cyber attacks on the Union's internal security.

International cybersecurity: the EU's approaches to multilateral cybersecurity negotiations 101

The quest for a regulatory framework for the security of cyberspace has been undertaken by different actors. At the global level, the United Nations has set up a Group of Governmental Experts (GGE) to discuss the 'norms, rules and principles' of responsible state behaviour in cyberspace, in order to advance international security. At the regional level, the Organization for Security and Cooperation in Europe (OSCE) has also recently taken steps to identify irresponsible behaviour in cyberspace which causes insecurity and instability. The European Union has also actively participated in these international forums, developing its tools and influence in the field of cyber diplomacy.

The EU's approach to international cyber diplomacy is driven by principles, necessity and ambition. These are some of its main features. It is based on the **EU's commitment to multilateral agreements and rule-based orders**. It builds on a **joint diplomatic response** against cyberattacks which may pose a threat to the EU and/or its Member States. It addresses both prevention and incident management. The culmination of an EU cyber diplomacy strategy is the cyber diplomacy toolbox which allows EU Member States to formulate concerted and coordinated responses to cyberthreats and cyberattacks. The Council used one such measure for the first time in 2020, when it sanctioned six natural persons and three legal entities responsible for having facilitated cyberattacks 'which targeted information systems of multinational companies in six continents, including companies located in the Union'. The EU cyber diplomacy toolbox, as shown in 2020, deploys one of the most powerful diplomatic instruments – sanctions.

With regards to the drives of EU cyber diplomacy strategies, these have arisen from the need to **defend the stability of the Union's own internal democratic systems,** and to **affirm its global geopolitical influence**. The EU and its Member States have increasingly been victims of cyberattack and disinformation campaigns, such has been the case of the Macron campaign (2017) and the German Parliament (2021). In addition, from the standpoint of power politics, advantages in the digital domain are of strategic importance in the context of the rising power battle between China and the US. From a multipolar context follows the EU's ambition of advancing EU's independence, influence, and interest in managing cyber risks and cyberthreats.

Internal and external cybersecurity

As clear from the EU cyber diplomacy toolbox, the expression 'cyber diplomacy' is used by EU state representatives in reference to the development of diplomatic strategies that foster international cooperation towards a common set of norms. However, the same term, cyber diplomacy, also has another application in the EU context. It also refers to a series of programmatic and operational actions to combat cybercrime and minimise the risk and impact of cyberattacks on people and essential infrastructures.

The EU's approach has so far achieved the realisation of instruments for coordinated action against cyberattacks.

1. It has developed a first legislative package to build stronger cybersecurity in the EU. The European Commission and the High Representative for Security Policy have proposed the Cybersecurity Act, the Directive on the Security of Network and Information Systems (NIS, which is currently being amended).

2. As part of its cybersecurity strategy, the EU is now developing a coordinated crisis response mechanism.

3. It has provided for Member States to coordinate their action against cyberattacks.

4. It falls under the umbrella of the EU's cyber diplomacy toolbox, meaning that the EU utilises foreign diplomacy as an instrument for internal security.

5. It includes measures under the Common Foreign and Security Policy, in order to prevent a domino effect on the EU's internal security and to contribute to international stability in the cyberspace.

6. It has promoted research in the field of cybersecurity, for the development of technological capability and expertise in this field, both necessary to limit the EU's dependence on foreign technologies and skills.

Challenges and opportunities ahead

As stated in the EU cyber diplomacy toolbox, the EU has an invested interest in setting up standards and norms for the stability and safety of cyberspace. At stake here are the EU's safety and stability, as well as its foreign influence in the international security arena. Therefore, EU diplomatic missions should strategically deploy a coherent, ambitious and coordinated action in the field of cybersecurity. This action should focus on the following three main areas:

- Further develop and deploy its cyber diplomacy toolbox, which is currently in its infancy. Particularly, the further development of measures that increase the accountability of individuals and entities responsible for carrying out cyberattacks against the Union's security should be a priority.

- Invest in carving itself a leading role in shaping international norms for responsible state behaviour in cyberspace. An integral part of EU's diplomatic missions in partner countries should be the active promotion of international norms for an open, free and secure cyberspace.

- Strengthen cooperation between Member States in the field of prevention and management of cyberattacks.

As you can see, there is a lot to unpack in the field of cyber diplomacy. In the next blog post, we've asked Clara to go further and talk us through the main cyberthreats that menace foreign diplomacy and put the work of diplomatic negotiators at risk.

Read blog one, two, three (part 1), and (part 2), four and five of the series 'Possible impacts of the current pandemic on

international negotiation processes' by the Negotiation Team.

Do you have questions? Contact the Negotiation Team negotiationteam@eipa.eu.

The views expressed in this blog are those of the authors and not necessarily those of EIPA.