# EU cyber sanctions: Moving beyond words

The EU recognises that cybersecurity and cyber-defence are critical for its prosperity, security and global ambitions. Offensive cyber-attacks by malicious actors show no sign of slowing down (not even during the coronavirus pandemic) and thus require concrete dissuasive measures. In July 2020, the EU Member States decided for the first time to use the 'teeth' rooted in the EU cyber-diplomacy framework and to 'bite cyber perpetrators back' by placing sanctions on them. This precedent has helped reinforce the EU's cyber policy action.

## Cyber facts: A deluge

Today, cyber threats are more sophisticated than ever and will likely continue with a constant stepping-up in capability. The World Economic Forum ranks cyber-attacks among the top 10 global risks in 2020. Some argue that the damages they currently inflict stand at around €530 billion worldwide, while others estimate that these damages would amount to US$5.2 trillion over the next five years. Yet others estimate that cyber-espionage operations put at risk up to €60 billion in economic growth and up to 289 000 jobs in the EU. The costs involved are therefore enormous, especially if compared to how less costly it is for perpetrators to set up malicious cyber operations.

Recently, while the attention of citizens, businesses and governments has been focused on battling the coronavirus pandemic, there has been an explosion of cyber-attacks. A '6 000 per cent increase in Covid-related spam' was reported at the height of the pandemic in the spring of 2020. In Europe, targets include the Lithuanian Defence Ministry, the Prague Airport and several Czech hospitals, and medical institutes working on developing a vaccine against the coronavirus, to name a few. These have even prompted Interpol to launch a '#WashYourCyberHands' public awareness campaign. Europol expect that such attacks will further increase in scope and scale.

The damage caused by cyber-attacks goes beyond economy and finance, affecting the very democratic foundations of the EU. Deployed together with other offensive actions, such as disinformation, economic pressure and conventional armed attacks, cyber becomes part of hybrid operations – highly impactful malicious strategies seeking to sow societal division and unrest, and to foster a deep distrust of the state.

## The EU approach to cyber threats: Growing teeth

Over eight in 10 (87 %) EU citizens see cybercrime as an important challenge, and over seven in 10 fear the risk of becoming a cybercrime victim. Starting with its first cybersecurity strategy in 2013 and continuing with the EU Global Strategy, the EU has gradually developed the ambition to be a 'forward-looking cyber player'. To date, all EU Member States have developed national cyber strategies. In 2017, the European Commission bolstered EU-level cybersecurity through the adoption of a number of cybersecurity-related initiatives. The resulting Cybersecurity Act strengthened the EU cybersecurity agency (ENISA) and created a blueprint for rapid crisis response, among others. Also established in 2017, the permanent structured cooperation in defence (PESCO) framework addresses a number of cyber-capability shortfalls through its dedicated projects.

Diplomacy has always been the EU's preferred response to security matters and disputes. This approach also applies to cyberspace and has materialised in the EU **cyber-diplomacy toolbox**. Rooted in the conclusions of the Council of the EU in June 2017, the toolbox creates a framework for 'a joint EU diplomatic response to malicious cyber activities'. The toolbox is also meant to embody the principles underpinning the EU foreign, security and defence policies, namely: primacy of international law; rules-based order in cyberspace; international cooperation; and resilience.

## A cyber sanctions regime: Baring the teeth

In May 2019, the cyber-diplomacy toolbox was outfitted with teeth. Seeking to give a credible response to cyber-attacks constituting 'an external threat to the Union', the Council adopted a decision establishing the framework through which the EU can impose targeted restrictive measures – **sanctions in the form of**


Author: Tania Lațici, Members' Research Service
PE 652.092 – September 2020

**travel bans, arms embargos, and freezing of assets** – 'with a significant effect against third states or international organisations'. Capacity-building, awareness-raising, and cooperative and stability measures are among the additional instruments in the toolbox.

Imposing sanctions or targeted restrictive measures is not the same as attributing responsibility to a third state for an attack, which remains a prerogative of national governments, subject to a sovereign political decision. To impose sanctions on individuals or organisations that have been found to be behind a cyber-attack, the Council must act by unanimity, following a proposal from a Member State or from the High Representative. In May 2020, the Council decided to extend the cyber-sanctions regime until 18 May 2021.

## Unanimous sanctions: Biting

In April 2020, the High Representative, Josep Borrell, condemned malicious cyber activities exploiting the pandemic and reaffirmed the resolute commitment of the EU and its Member States to 'prevent, discourage, deter and respond to them', including by making use of the cyber-diplomacy toolbox. The declaration once more signalled the EU's intention to act and therefore set the stage for the unanimous adoption of (the EU's first ever) restrictive measures by the Council on 30 July 2020.

Thus far, sanctions have been imposed on two Chinese and four Russian citizens, and on three entities: one in China, another in North Korea, and a third in Russia. These have been found to have been involved in various offensive cyber operations, such as the 'WannaCry' attack, which spread to 300 000 computers in 150 countries, the 'NotPetya', which inflicted financial losses worth hundreds of millions, 'Operation Cloud Hopper', one of the largest corporate espionage campaigns in history, and the attempted attack against the Organisation for the Prohibition of Chemical Weapons. The measures included a travel ban, an asset freeze, and a ban on any funding originating from the EU. Two documents form the legal basis of the restrictions: a Council decision and a Council implementing regulation, both adopted on 30 July 2020. These apply until 18 May 2021, when the listings as such, together with the cyber-diplomacy regime, must be renewed. If the listing of sanctions requires amending, it will be added to the founding Decision (CFSP) 2019/797, which will be amended overall.

## Paving the way to increased cyber-resilience

It is clear that cyber threats are a growing presence in the EU threat landscape and will persist as such. The EU has already taken strong measures, especially since 2017, and is continuing to do so. For instance, the communication on the EU security union strategy of 24 July 2020 emphasises the need to ensure the resilience and protection of critical infrastructure, to limit dependencies and to design a whole-of-society approach in ensuring that 'cybersecurity capabilities keep pace with reality'. The communication reinforces the need for open strategic autonomy, namely working with partners but decreasing the EU's dependence on non-EU players. The communication also paves the way for a revision of the EU cybersecurity strategy and for better preparedness against hybrid threats. It also aims to create a 'joint cyber unit' in order to structure and coordinate operational cooperation, including a mutual assistance mechanism at the EU level.

The EU continues to support multilateral cyber capacity- and confidence-building measures, such as the 'Paris Call for Trust and Security in Cyberspace' and the High-level Panel on Digital Cooperation created by the UN Secretary General, António Guterres. Some experts have suggested appointing an EU Special Representative for international cyberspace policy to 'defend the EU's positions on the international stage', while others have argued that closer engagement between EU Member States can hone a more systematic approach to fixing weak links and gaps as well as generate more robust and effective EU action on cyber-defence and diplomacy.

The European Parliament has repeatedly advocated robust EU measures in the cyber realm, insisting on effective deterrence, defence and resilience. In June 2018, it welcomed the Commission's cyber package and urged Member States to prioritise cyber-defence capabilities. Consequently, in March 2019, Parliament adopted the Cybersecurity Act. In January 2020, Parliament called for increased EU efforts to confront cyber threats, deeming active EU-NATO cooperation as being of vital importance. Last but not least, Parliament also recalled that cyber-attacks 'could constitute sufficient grounds for a Member State to invoke the EU Solidarity Clause' (Article 222 of the Treaty on the Functioning of the European Union).