The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?

by Erica Moret and Patryk Pawlak

Despite numerous declarations about the need for stability in cyberspace, the evidence shows that governments are both able and willing to undertake malicious cyber activities for political, economic or security gains, including through attacks on infrastructure, cyber-espionage or intellectual property theft. Russia's alleged involvement in the attacks on the networks of the Democratic Party in 2016 – described as 'the crime of the century' by the *Washington Post* – or the mounting evidence that the North Korean cyber-gang Lazarus Group might be behind the WannaCry ransomware are just two recent examples.

State-sponsored operations against EU members and institutions are increasing, too. Originating from Russia, China or Turkey, the malicious activities go beyond cyber-espionage and include critical infrastructure vulnerability scanning and disruptive attacks. Attacks on critical infrastructure are particularly common as a tactic in ongoing conflicts where the EU has taken sides. For instance, cyber operations against the Ukrainian energy grid conducted by pro-Russian groups like *Sprut*, *Beregini* or *Sandworm* are quite frequent. In recognition of the growing political importance of cyberspace, both state and non-state actors also exercise influence through limiting access to the internet, launching disinformation campaigns, or the use of online platforms for propaganda.

Faced with a rapidly evolving threat environment and a stalemate in the global discussion about norms of responsible state behaviour and international law in cyberspace, in June 2017, the EU ministers of foreign affairs decided to endorse the development of a framework for a joint EU diplomatic response to malicious cyber activities – the so-called Cyber Diplomacy Toolbox (CDT). The primary intention behind the CDT – which includes, among a panoply of instruments, the imposition of sanctions – is to develop signalling and reactive capacities at an EU and member state level with the aim to influence the behaviour of potential aggressors, taking into account the necessity and proportionality of the response. The remaining challenge, however, is to translate these provisions into an effective foreign policy instrument.

Norms and sanctions: where we stand

Legal scholars argue that cyber-attacks could fall under the banner of Article 2.4 of the UN Charter according to which states 'shall refrain in their international relations from the threat

or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations'. Consequently, a cyber-attack that cripples a country's banking system, energy network or causes significant damage otherwise could be comparable to a situation in which this infrastructure is attacked through conventional military methods.

In general, states agree that international law and certain norms of behaviour apply to cyberspace. That includes, for instance, not interfering with each other's critical infrastructure or abstaining from targeting each other's computer emergency response teams – the equivalent of fire brigades in cyberspace. The problems start, however, when the discussion hones in on potential punishment for states deemed responsible for a perceived misdemeanour. Disagreement over the potential use of countermeasures was one of the main reasons why the UN Governmental Group of Experts failed to produce a report by the end of June 2017.

Given that consensus in the UN is unlikely to emerge any time soon, the proliferation of bilateral agreements and unilateral or regional sanction regimes appears now as a more plausible scenario, especially among like-minded countries. That would not be unusual given that over 70% of UN targeted sanctions imposed since the end of the Cold War have been preceded by similar or identical sanctions put in place by individual nations or regional groups – often working in unison – including in the cases of Libya and Haiti.

To date, the US remains the only country that has implemented unilateral cyber sanctions. Used for the first time in 2015 by President Obama against North Korea in response to the country's alleged cyber-attack on Sony Pictures, cyber sanctions emerged as a response against perpetrators operating beyond the reach of law enforcement agencies. The established US cyber sanctions regime authorises the imposition of sanctions on individuals and entities deemed responsible for (or complicit in) malicious cyber-enabled activities that 'harm or significantly compromise' the provision of critical services, 'significantly disrupt' the availability of a computer or network of computers, or 'cause a significant misappropriation' of funds, resources or intellectual property.

This list was amended in the last days of the Obama presidency in reaction to the Russian government's cyber operations aimed at the US presidential campaign to include tampering with, altering, or causing misappropriation of information 'with the purpose or effect of interfering with or undermining election processes or institutions'. Currently, the US cyber sanctions targets include senior North Korean officials, two Russian intelligence services – the Main Intelligence Directorate (GRU) and the Federal Security Service (FSB) – as well as a number of high ranking intelligence officials, and three companies that provided material to support GRU's cyber operations.

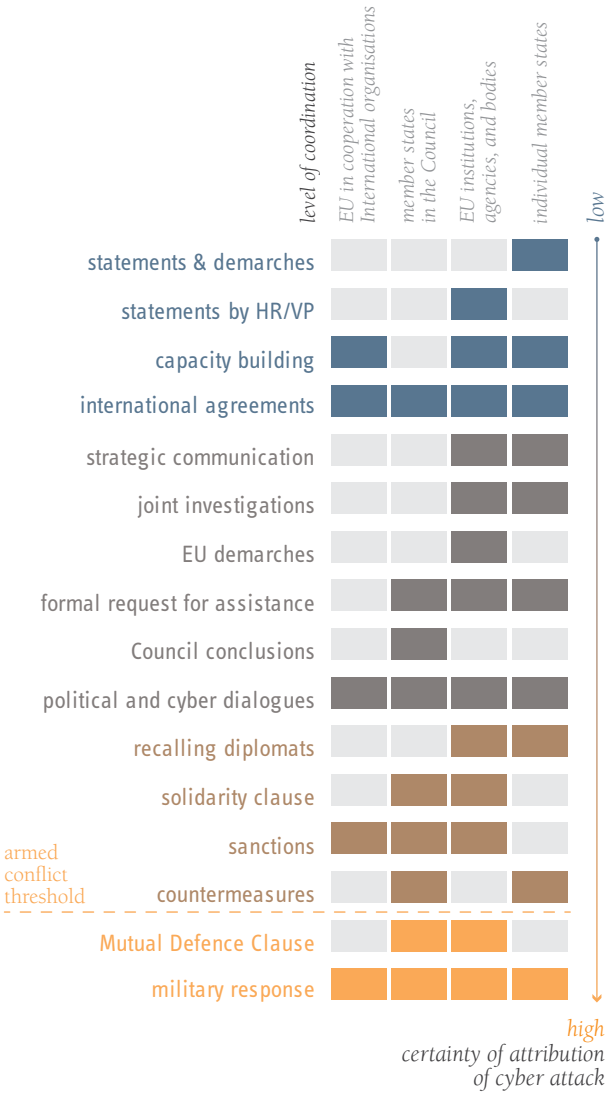
EU sanctions and cyber

The EU has played a key role in a number of high-profile sanctions regimes in recent years, including in relation to the nuclear talks with Iran and North Korea. With 37 sanctions regimes currently in place, the EU has resorted to this tool for conflict management (Libya and Syria in 2011), countering international terrorism (Libya in 1999 and sanctions against al-Qaeda) and in the support of democracy, human rights, the rule of law (Belarus in 2006). Its use of sanctions has trebled over the past three decades and while being, admittedly, an imperfect instrument, it remains an appealing option to policymakers at a time when diplomacy has reached its limits and war remains an option of last resort.

The establishment of a new EU sanctions regime is based upon a sophisticated, complex, and time-consuming mechanism that governs how the member states arrive at legally-binding decisions within the EU's legal framework. The Treaty on European Union (TEU) cites 'restrictive measures' as one of a number of possible instruments that can be used in pursuit of Common Foreign and Security Policy (CFSP) goals, as outlined in Article 21 and governed by Article 30 TEU. In addition, the EU's sanctions policy is guided by a number of key documents – such as the Council guidelines on the implementation and evaluation of restrictive measures or the EU best practices for the effective implementation of restrictive measures - which provide direction on how and when they should be employed, designed and implemented, along with indicators of effectiveness. They also provide recommendations on logistical matters such as the identification of targets and the granting of exceptions.

It is worth noting that when the EU puts sanctions in place, other countries tend to follow suit, either in part or in full, including the European Free Trade Association (EFTA) members, the EU candidate countries and other partners and neighbours (such as Ukraine and Moldova). As such, the EU's new cyber sanctions regime could inspire other nations to rapidly follow suit, particularly if

Cyber diplomacy tools and the certainty of attribution



Actions that do require a low certainty about attribution or no attribution at all.

Actions that require a moderate certainty about attribution.

Actions that require high certainty about attribution.

Actions that require an almost absolute certainty about attribution.

Disclaimer: The categories proposed in this figure are a simplification. In reality, each action needs to be taken on a case-by-case basis and be preceded by a detailed legal analysis.

Data: EUISS

the attack is global or regional in its reach, and would contribute to strengthening global compliance with the existing norms. The EU's cyber sanctions might also push forward the conversation about similar measures within the UN context, as was the case with some past sanctions regimes, such as arms embargoes imposed on the Federal Republic of Yugoslavia, Sudan and the Democratic Republic of Congo.

Five lessons to consider

While the paucity of examples of cyber sanctions presents a challenge to predicting their likely effectiveness, similar measures used against states or to deal with drug traffickers, criminal rings and terrorist cells can offer valuable lessons. Best practices can also be derived from former and existent sanctions regimes used for other purposes.

Lesson one: sanctions should be situated in the wider context of the Union's foreign policy strategy. Restrictive measures must always be combined with other policy instruments if they are to stand a chance of succeeding. These could include diplomacy, trade talks, covert methods, law enforcement, collaboration with other countries and multilateral institutions, cooperation with the private sector and, in some instances, even military deterrence. How sanctions should be combined with other instruments in the Cyber Diplomacy Toolbox therefore requires careful thought.

Lesson two: the logic of sanctions should be defined prior to their creation. This should include a vision on whether the sanctions are intended to *coerce* targets to change their behaviour, *constrain* their activities or access to resources, or *signal* to the target and other would-be detractors that the sender will not tolerate such actions. Research by the Geneva-based Targeted Sanctions Consortium suggests that sanctions are most likely to be effective in the area of signalling, with constraining and coercing achieving lower respective success rates.

Lesson three: shared situational awareness plays a crucial role. This is particularly relevant in the cyber context where certainty about attribution, necessity and proportionality are the conditions for the legality of any countermeasures under international law. Currently, international efforts to tackle the threat of cyber-attacks are hindered by a number of constraints (including reluctance at national level to share sensitive information pertaining to cyber capabilities or vulnerabilities) and exacerbated by the scale and fast-evolving nature of the threat.

Lesson four: sanctions are not only about politics, and thus cooperation with industry and the private sector is crucial. Developments in the EU's financial sanctions in recent years have established sophisticated banking expertise and close working relations between the government and the financial sector, helping those

implementing such measures. A similar body of expertise and network of relations with the tech world would be beneficial for those establishing cyber-sanctions, in particular with regard to monitoring compliance and exchanging information on latest threats.

Lesson five: the economic and political costs of a new sanctions regime cannot be ignored. Such a new regime is likely to generate a response from the target country, including the risk of retaliation, or to produce unintended consequences that need to be evaluated carefully. These could include a 'rally-around-the-flag' effect, whereby citizens of a targeted country increase their support to the government, or strengthened ties between the target and third countries or groups that may be seen as undesirable in the eyes of the sanctioning party.

Possible ways forward

Difficulties with reliable attribution represent a key challenge in planning cyber sanctions – but problems with providing evidence that a target has committed an international offence are not unique to the cyber case: while Russia's annexation of Crimea was indisputable, the violations linked to the Iranian nuclear programme and the arming and funding of rebel groups have been harder to prove. Therefore, greater investment in improving attribution in the case of malicious cyber activities will be vital to strengthen, in turn, the credibility of retaliatory options that include sanctions, legal measures, or covert counter-attacks. The implementation of sanctions based on inaccurate evidence or a wrong assessment of attribution could in itself contravene international law.

Since there is no 'international law of evidence', the international legal system is still based on decentralised interpretation and application of law, which stipulates a decentralised judgement. This process takes place through international practice where evidence is important but does not follow precise legal regulations. Furthermore, providing evidence of attribution typically draws on intelligence material, which can be difficult to use to justify sanctions as it could compromise sensitive information about sources or tools used to gather that evidence.

The effectiveness of a new EU cyber sanctions regime will also depend on its complementarity with other instruments in the Cyber Diplomacy Toolbox. The EU acknowledges that attribution to a state or non-state actor remains a sovereign political decision of individual member states. That leaves the member states in the driver's seat for measures such as the cyber-specific Council Conclusions or the imposition of sanctions against third countries, entities and individuals. At the same time, because not all measures of the EU's joint diplomatic response require attribution, the EEAS and the European Commission can take several actions, including statements by the HR/VP, signalling through bilateral and multilateral dialogues, diplomatic demarches, or the formal joint requests for technical assistance from third countries.

More generally, the success of EU cyber diplomacy will depend on the answers given to a number of questions. First, how will the EU balance off different policy objectives and ensure that its values and interests are mutually reinforcing when dealing with third countries? With growing demand for EU expertise in the digital domain, it needs to be clear that the general provisions applicable to the whole external action of the EU (e.g. promotion of the rule of law and respect for human rights) are also a backbone of the Union's cyber engagements.

Second, how can the EU ensure shared situational awareness? The quality and timeliness of information-sharing and forensic cooperation between EU agencies and bodies (e.g. ENISA, Europol's EC3, the EU CSRIT network, the Hybrid Fusion Cell) and member states will be essential in the successful identification of perpetrators and sound decisions on the necessary and proportionate responses.

Finally, does the application of the CDT stop at the Union's borders or will the EU extend its diplomatic arm in support of its allies and partners? The US, for instance, already declared the need for strengthening 'like-minded coalitions'. Therefore, the choice between a primarily inward-looking and a more globally-oriented Cyber Diplomacy Toolbox – or a credible combination of both – may be looming.

Erica Moret is a Senior Researcher at the Graduate Institute of International and Development Studies, Geneva, and a Senior Associate Analyst at the EUISS.

Patryk Pawlak is the Brussels Executive Officer and is responsible for cyber-related issues at the EUISS.

 | QN-AK-17-024-2A-N | ISBN 978-92-9198-591-3 | ISSN 2315-1110 | doi:10.2815/399444