CEPOB
College of Europe POlicy Brief

1.21

FEBRUARY 2021

Cyber sanctions: towards a European Union cyber intelligence service?

Yuliya Miadzvetskaya

Executive Summary

> In the global cyber policy context, sanctions are important as they represent a central component of deterrence that actors like the European Union can employ in response to malicious cyber activities that threaten critical infrastructures, democratic institutions and processes. In the EU, the success of such cyber sanctions depends on the Council of the EU's solid situational awareness and the access to comprehensive cyber intelligence information.

> While the Council enjoys a considerable degree of discretion over sanctions designations, cyber sanctions are not immune to judicial review and must satisfy a set of procedural requirements. Most notably, they must include clear-cut and specific reasons for listing and be substantiated with comprehensive evidence.

> Most of the EU sanctions listings are supported by evidence presented by the Member States. In the past, the Council lost several sanctions-related cases due to the Member States' unwillingness to disclose confidential information in court for considerations of national security.

> To allow the Council to access comprehensive intelligence information and to decrease its dependency on the voluntary decision of Member States to disclose intelligence, the EU needs its own fully-fledged intelligence service. This can be achieved, inter alia, via the enhancement of the Intelligence Centre's (INTCEN) central role in supporting EU foreign policy decision-making in the area of (cyber)security, but also in foreign policy more widely (e.g. fight against terrorism, human rights abuses worldwide).

The European Union (EU) cyber sanctions framework offers a new foreign policy tool that came into effect in May 2019. It consists of two legal acts: Council Decision (CFSP) 2019/797 and Council Regulation 2019/796 providing for targeted restrictive measures against cyber-attacks threatening the Union or its Member States. These measures include travel bans, asset freezes and prohibition to make funds and economic resources available to those responsible for cyber-attacks. The EU cyber sanctions framework is not country-specific but global in scope. Its main feature is indeed the shift to individual listings – the inclusion of natural or legal persons on sanctions lists – decoupled from a specific geographic area. This contrasts with most of the EU sanctions packages that are taken in response to major political crises in third countries (e.g. Belarus, Syria, Ukraine, Venezuela).

In trying to take a more assertive position on cyberspace matters, the EU has to date aligned itself to a large extent with the US cyber-related sanctions programme. For instance, in July 2020 the EU introduced targeted sanctions against Russian, Chinese and North Korean entities and individuals that were already on the US cyber sanctions listings. While the US cyber sanctions programme is more advanced and benefits from less fragmented decision-making, EU decision-making on sanctions still requires unanimity, even though a shift towards a qualified majority voting is contemplated.

Both in the US and in the EU, blacklisted cyber criminals are subject to a travel ban and their financial assets are frozen. Yet, in contrast to courts in the US, the Court of Justice of the EU (CJEU) applies a more stringent standard of judicial review for sanctions listings. In the past, this caused the Council of the EU to lose a considerable amount of sanctions-related cases. The Kadi saga is one of the most significant examples of thorough control by the EU judiciary over the respect for fundamental rights of

listed individuals (C-584/10 P, C-593/10 P & C-595/10 P – *European Commission and Others v Yassin Abdullah Kadi*, ECLI:EU:C:2013:518). The Kadi judgements imply that the EU's competent authorities must ascertain that any sanctioned individual is informed of the reasons for their listing and that the alleged reasons were well-founded and supported by evidence. If either the statement of reasons is insufficient or the evidence is lacking, the restrictive measures will be struck down by the Court.

Against this backdrop, the EU's current cyber sanctions framework comes across as too weak to hold up to extensive judicial review. The potential repeated annulments of restrictive measures on 'due process' grounds bear substantial reputational risks for the EU and may undermine the credibility, legitimacy and effectiveness of the EU's external policy choices. Thus, it is crucial for the EU to strike the right balance between foreign and (cyber)security policy objectives and the need to protect individuals from arbitrary sanctions designations.

This policy brief argues that the Council must come up with a workable legal standard in order to reconcile cyber diplomacy objectives with 'due process' rights. In particular, the Council will need to address two main weaknesses of cyber designations: it has to (i) provide clear-cut and specific reasons for listing and (ii) substantiate those with comprehensive intelligence information. To enable this, the EU needs to overcome its dependency on Member States for intelligence information and establish its own fully-fledged intelligence service to support its decision-making in the area of (cyber)security, but also foreign policy more widely. After addressing these points, the policy brief concludes by discussing EU competences that could solidly serve as a legal foundation for establishing such a fully-fledged EU cyber intelligence service.

The thematic nature of the EU cyber sanctions regime

Out of thirty-seven sanctions regimes in place in the EU, only four are horizontal and thematic in nature. Apart from cyber sanctions, these are sanctions addressing the use of chemical weapons, the EU's terrorist list, and the newly adopted Magnitsky-type Act against human rights abusers. The EU also contemplates thematic sanctions for spreading disinformation and undermining trust in democratic institutions. There are also some quasi-thematic sanctions regimes that pursue a specific objective while being tied to a particular country, for instance measures against Iran's nuclear programme.

The targeted nature of cyber sanctions allows the EU to avoid the sensitive question of attribution of responsibility for cyber-attacks to a third country within the currently still underspecified international legal framework. EU targeted sanctions constitute personalised deterrence measures against perpetrators of malicious cyber activities. Examples include the 2015 hack of the German Federal Parliament and the disrupting ransomware cyber-attacks known as 'WannaCry' and 'NotPetya', which paralyzed the work of corporations and government agencies in 2017. As individual designations circumvent the establishment of state responsibility, the EU has de facto never attributed a cyber-attack to a third country but has limited its actions to the expression of concerns and condemnations.

The EU's Member States, in turn, are free to take their sovereign political decisions and make their own determinations with respect to the attribution of cyber-attacks to a third country (Council 2019). However, the delimitation between targeted measures and attribution of responsibility to a state remains rather superficial since a vast majority of cyber-attacks with high impact, such as the abovementioned 'WannaCry' and 'NotPetya', were widely understood to have been orchestrated at the request and with the support of the governments of, allegedly, North Korea and Russia.

The thematic nature of cyber sanctions offers a higher degree of flexibility in contrast to country-specific measures. First of all, it allows to act faster by updating the existing sanctions listings instead of enacting a completely new legal framework each time a new sanction has to be imposed. Complex and lengthy procedures that are prone to Member State vetoes and which are typical for new country-specific designations are thus not required. Second, its personalised character better suits the present dynamics in the cyberspace in which states often rely on non-state actors, so-called 'proxies', to project their strategic interests.

While sanctions in response to cyber-attacks constitute a novel personalised cyber deterrence tool, they are not immune to judicial review and must satisfy a set of procedural requirements. However, the EU's recent cyber sanctions framework comes across as too weak to hold up to extensive judicial review. Its first procedural weakness is due to the vague formulation of reasons for listing, which increases the likelihood of arbitrary decision-making. Its second procedural weakness results from the confidential nature of evidence supporting the listing. In the next sections, we will explore the main weaknesses of cyber sanctions in more detail and propose a way forward in order to overcome the identified deficiencies.

Weakness 1: Vagueness of listing criteria

There is a downside to the increased flexibility offered by the cyber sanctions framework, namely the vague

character of the reasons for listing individual perpetrators. Sanctions are foreseen in response to cyber-attacks with a significant effect which constitute an external threat to the EU or its Member States (Council 2019). The concepts of 'significant effect' and 'external threat' are not well-defined and pave the way for inconsistent assessments. Listing criteria still remain blurry despite the fact that the Council provided a few elements to evaluate an attack's significance such as on 'the scope, scale, impact or severity of disruption caused' and 'the number of natural or legal persons, entities or bodies' affected by a cyber-attack (ibid.). This obscurity increases the likelihood of arbitrary decision-making.

At the same time, the vagueness of the listing criteria might be a result of earlier judicial intervention in the Council's decision-making on sanctions. In the past, the Council's legal service could not substantiate the narrow reasons for sanctions designations with sufficient evidence. An example was the difficulty the Council experienced when attempting to prove a direct link between the Iranian company 'Fulmen', active in the electrical equipment sector, and the Iranian nuclear program (C-280/12 P, *Council v Fulmen and Mahmoudia*, ECLI:EU:C:2013:775). Precise and narrow listing criteria thus set a standard which was too demanding. As a consequence, the CJEU struck down several sanctions listings for the lack of supporting evidence (ibid.). The Council, in turn, expanded the listing criteria in order to make its designations more immune to judicial review and decrease the likelihood of sanctions annulment. The broader the listing criteria, the easier it is for the Council to comply with 'due process' requirements concerning reasons and evidence (Chachko 2018).

At the same time, the EU risks opening a Pandora's box if it does not determine with sufficient detail when and against whom a cyber-sanctions mechanism can be triggered. The decision to subject a person or entity to targeted restrictive measures requires clear-cut designation criteria, tailored to each specific case (Art. 296 TFEU; C-176/13 P, *Council v Bank Mellat*, ECLI:EU:C:2016:96, § 76). Accurate, up-to-date and defendable statements of reasons are necessary for avoiding inconsistent policies that could be manipulated by different lobby groups. Thus, the EU has to strike the right balance between two incompatible objectives: on the one hand, the need for flexibility and elasticity of the legal framework; on the other hand the principle of legal certainty. According to the latter, listing criteria must be crafted with sufficient detail and clarity to avoid any arbitrary designations.

Weakness 2: Evidentiary standard

Clear reasons for listings are not the only requirement that the Council has to respect. There is also the need to provide sufficient evidence to back up those reasons in order to withstand scrutiny by the CJEU. The well-known judgment in Kadi II established the bases on which the Council would have to defend its listings (C-584/10 P, C-593/10 P & C-595/10 P – *European Commission and Others v Yassin Abdullah Kadi*, ECLI:EU:C:2013:518, § 130). In particular, the Council must comply with the requirement to provide a sufficiently solid factual basis. Correspondingly, at least one of the reasons for listing will have to be backed up substantially by evidence. Otherwise, sanctions can be struck down for non-compliance with the 'standard of proof' requirement and the Court not being in a position to take a fully informed decision.

In this context, two observations can be made with regard to cyber sanctions. First, the evidence-gathering process is cumbersome due to the intrinsic features of the cyberspace such as its decentralised nature and anonymity. Malicious actors apply different deception techniques to avoid leaving a discernible footprint. Moreover, the Council might have difficulties to present a solid technical proof confirming the presumed perpetrator's link with the incident. In the absence of such evidence, the Union faces a dilemma as to whether to go with a listing of this individual or comply with heavy 'due process' requirements.

Second, cybersecurity policies require some level of confidentiality since they rely on intelligence data. The Council Decision to impose sanctions depends on individual decisions by each Member State's competent authorities and all-source intelligence that they possess. In order to preserve the confidentiality of these documents each Member State is entitled to apply the rule of originator control (ORCON). According to the ORCON rule, classified information cannot be disclosed to other parties, unless the originator agrees to declassify it (Eckes 2013). While confidential information is often shared within the Council, Member States showed reluctance in the past to disclose it in court due to considerations of confidentiality and international security (ibid.). This implies that the Council might not be able to share the collected evidence in court since the disclosure of classified data can compromise various intelligence sources and bears considerable security risks for Member States and the entire EU. As an illustration, France and the UK refused for reasons of national security to adduce evidence supporting sanctions listings (T-284/08, *People's*

Mojahedin Organization of Iran v Council of the European Union, ECLI:EU:T:2008:550, § 71-72; C-280/12 P, *Council v Fulmen and Mahmoudia*, ECLI:EU:C:2013:775, § 77). In such cases, the Council's inability or unwillingness to provide evidence caused the annulment of sanctions since the Court was unable to review the cases on their merits.

The lack of willingness of national authorities to share intelligence data with other Member States and the CJEU unveils the problems of trust in the confidential treatment of information that is crucial for national security interests. The problem of confidential information-sharing is exacerbated by the fact that the EU judiciary does not have a well-established procedural framework on how to deal with sensitive evidence.

Against this backdrop, the relatively recent semi-closed and closed evidence procedures open up an alternative avenue for the Council to defend its sanctions listings when sensitive information cannot be disclosed to the General Court. Those procedural adaptations are a direct result of the 2015 revisions of the Rules of Procedure of the General Court, in which the Council's Security Committee actively participated (Abazi and Eckes 2018). Under the new rules, it is up to the General Court to assess the confidentiality of presented information and decide on the procedure to follow (open evidence, semi-closed evidence or closed evidence procedures). While the semi-closed evidence procedure requires a non-confidential summary to be shared with the applicant, the closed evidence procedure allows to proceed without any disclosure of information.

Accordingly, the Council now possesses the legal means of defending sanctions without evidence disclosure. This is meant to help avoid situations in which it loses sanctions-related cases in court due to national classification rules or a Member State's failure to declassify relevant documents in time. However, the downside to the closed evidence procedure is its negative impact on the right of defence and effective judicial protection in the EU alongside the broader risks it might entail for the fundamental rights of listed individuals (ibid.).

The way forward: enhancing the EU's (cyber)intelligence capabilities

A higher level of shared situational awareness across the EU would enhance the effectiveness of the EU cyber sanctions mechanism. Enhancing the EU's cyber intelligence capabilities would contribute both to providing more precise listing criteria (e.g. the assessment of an attack's significance, scope, and threat level etc.) as well as to the collection and management of supporting evidence. This, in turn, would strengthen the EU's capacity to prevent, deter and respond to cyber threats.

At this stage, the exchange of finished intelligence reports by states takes place within the Intelligence Centre (INTCEN), which is run by the European External Action Service (EEAS). Even though INTCEN is often referred to as an EU intelligence body, it remains a purely analytical structure with a substantial part of its analysts seconded by Member States (Arcos and Palacios 2020). Furthermore, it does not have collection capabilities and mostly relies on open-source, diplomatic data and intelligence shared by national authorities. As a result, the EU remains dependent on Member States' willingness to submit and declassify sensitive information necessary for foreign policy decision-making. The creation of a fully-fledged EU intelligence structure would be an important step towards breaking down these silos in the area of security and foreign policy.

This would be in line with the 'need-to-share' mind-set of the EU 2020 Cybersecurity Strategy, which calls for the establishment of an EU cyber intelligence working group within INTCEN in order to advance strategic intelligence cooperation on cyber threats and activities (European Commission 2020). The EU 2020 Cybersecurity Strategy also foresees the establishment of a Joint Cyber Unit as a platform for technical and operational cooperation between different EU structures, such as the Computer Security Incident Response Team (CSIRTs) network, the European Cybercrime Centre, and the European Union Agency for Cybersecurity (ENISA).

The idea of creating a fully-fledged European intelligence service has already been floated by leaders including French President Macron. However, the German government is afraid that such a duplication of national intelligence services at the EU level will cause efficiency losses. The debate on the institutional framework of intelligence collection reflects the contentious issue of the division of competences enshrined in Article 4(2) TEU, known as the 'national identity clause'. It requires the EU to respect some core areas of Member States' national identities and essential state functions, including national security. In a similar vein, Article 72 TFEU establishes that EU action in the Area of Freedom, Security and Justice cannot interfere with the exercise of Member States' actions with regard to the safeguarding of internal security. National security and intelligence services lie at the heart of national sovereignty and, thus, belong to the area of Member States' sole responsibility. Governments are reluctant to give the EU powers that could interfere with their existing laws and practices.

The present competences constellation therefore does not facilitate the development of the Union's own intelligence capabilities. In practice, it is hard to draw a line between national, internal, external and European (cyber)security policies due to their intrinsically interconnected nature. This challenge is exacerbated in the case of cyber-attacks that usually have a cross-border impact on security, economy and societal well-being in general. In this context, the internal market legal basis (Article 114 TFEU) can be relied upon for building a more coherent EU approach towards cyber intelligence collection and management. In particular, it can serve for incentivizing Member States to share more information and for expanding the EU institutions' powers in terms of cyber intelligence management. This would help to bridge the existing gap between external and internal dimensions of (cyber)security.

Moreover, there is a recent tendency towards the (cyber)securitisation of the internal market legal basis. Cybersecurity is seen as one of the essential elements of the smooth functioning of the digital single market. As an illustration, the Directive on security of network and information systems, a central piece of the EU's cybersecurity-related legal framework, finds its legal basis in internal market harmonisation provisions. Article 114 TFEU was relied upon for establishing ENISA, which is responsible for the development and implementation of EU policy and law on network and information security. The functional nature of the internal market legal basis may therefore also serve as a solid legal foundation for enhancing the central role of INTCEN in supporting the EU's foreign and (cyber)security policy decision-making.

Conclusion

Given their overall impact on the fundamental rights of listed individuals, targeted cyber sanctions are prone to undergo the scrutiny of the CJEU. The likelihood that they are – successfully – challenged on 'due process' grounds (reasons for listing and evidentiary standard) is high. The Council's difficulties in providing and substantiating reasons for sanctions listings is exacerbated by the EU's dependency on Member States' intelligence capabilities. The latter have so far been reluctant to share their intelligence due to the lack of trust in the EU's institutional framework and confidential treatment of information provided by their national security authorities.

The lack of a fully-fledged EU intelligence service is often viewed as the main obstacle to a well-functioning and autonomous EU foreign and security policy. For the purposes of better decision-making and evidence collection, the EU should thus gradually enhance its own cyber intelligence capabilities and decrease its dependency on the voluntary decision of Member States to disclose intelligence. This can be achieved inter alia via the enhancement of INTCEN's central role in supporting the EU's foreign policy decision-making in the area of (cyber)security, but also foreign policy more widely (e.g. fight against terrorism, human rights abuses worldwide). To realize this objective, the functional nature of the internal market legal basis (Article 114 TFEU) may serve as the bridge that closes the gap between internal and external dimensions of (cyber)security and enhances the coherence in the EU's approach towards intelligence collection and management.

Further reading

Abazi, V., Eckes, C. 2018. "Closed Evidence in EU Courts: Security, Secrets and Access to Justice", *Common Market Law Review* 55(3): 753-782.

Arcos, R., Palacios, J. 2020. "EU INTCEN: a Transnational European Culture of Intelligence Analysis?", *Intelligence and National Security* 35(1): 72-94.

Chachko, E. 2018. "Foreign Affairs in Court: Lessons from CJEU Targeted Sanctions Jurisprudence", *Yale Journal of International Law* 44(1): 1-51.

Council of the European Union. 2019. "Decision Concerning Restrictive Measures against Cyber-attacks Threatening the Union or its Member States", 7299/19. Brussels, 14 May.

Eckes, C. 2013. "Decision-making in the Dark? Autonomous EU Sanctions and National Classification". In *EU Sanctions: Law and Policy Issues Concerning Restrictive Measures*, edited by I. Cameron, pp. 177-198. Cambridge: Intersentia.

European Commission. 2020. "The EU's Cybersecurity Strategy for the Digital Decade", JOIN(2020) 18 final. Brussels, 16 December.

About the Author

Yuliya Miadzvetskaya is a researcher at the Centre for IT & IP Law at the University of Leuven (KU Leuven). Prior to this, she worked as an academic assistant at the Department of European Legal Studies at the College of Europe, Bruges, and interned with the Legal Service of the European Parliament in Brussels. She holds an LLM in European Law from the College of Europe. Her research interests include (cyber)security, EU external relations, and EU Neighbourhood Policy.
