CHAPTER 1

NAVIGATING THE STARS

Ten questions to make cyber sanctions more effective

INTRODUCTION

In times of political instability and faced with serious security or foreign policy challenges, governments are under pressure to act. Sometimes, the decisions they take prove to be the right ones and politicians save their face in the court of public opinion. Sometimes, however, despite their good intentions, in the heat of the moment or under political pressure policymakers make mistakes or suboptimal decisions. Uncertainty about the policy outcome is an inherent part of policymaking. There are simply too many factors that determine the success of any given policy measures. The dilemma, however, is always the same: does it make more sense to do nothing and wait or is it better to take risks and take a concrete stand? Consequently, success and failure are inherent elements of foreign and security policymaking. One way to minimise the risk of failure is to learn from past experiences. This chapter looks at the existing scholarship on sanctions with a view to answering one simple question: which lessons might be useful to make the cyber sanctions regime more effective? These 'lessons learned' and the issues they identify will guide the analysis of the different aspects and dimensions of the cyber sanctions regime adopted by the EU.

DO SANCTIONS WORK?

Whether sanctions 'work' or not is the classic question raised about this commonly used tool of foreign and security policy. Although the question has been addressed in several studies over the past couple of decades, assessing the effectiveness of any given sanctions regime remains a challenge, given the difficulties in conclusively ascertaining a causal link between the imposition of sanctions and compliance or constraint. One thing is certain, however: sanctions are not a silver bullet solution for violations of international law or the enforcement of norms in cyberspace. Sanctions do not operate in a vacuum and the way in which they are combined with other tools of foreign, security and trade policy has a considerable impact on their ultimate effectiveness.[1] Identifying the effects of sanctions in isolation from other factors is a complicated, and sometimes impossible, task.[2] Many of those who maintain that

[1] Margaret P. Doxey, *Economic Sanctions and International Enforcement* (Oxford: Oxford University Press, 1971); Robert A. Pape, "Why Economic Sanctions Do Not Work", *International Security*, vol. 22, no. 2 (1997): pp. 90–136; David A. Baldwin, "The Sanctions Debate and the Logic of Choice", *International Security*, vol. 24, no. 3 (1999/2000): pp. 80–107; Gary C. Hufbauer *et al.*, *Economic Sanctions Reconsidered* (Washington, DC: Peterson Institute for International Economics, 2007).

[2] Erica Moret, "Humanitarian Impacts of Economic Sanctions on Iran and Syria", *European Security*, vol. 24, no. 1 (2015).

sanctions are not effective instruments are relying on a behavioural change approach, assuming that the target will adjust its policy or activities after the imposition of sanctions. However, this approach is now considered inadequate to account for the complexity of sanctions. A more nuanced analytical framework is therefore necessary in order to go beyond the limitations of the behavioural change paradigm.

Changing the behaviour of targets (*coercion*) certainly remains one of the principal objectives that sanctions are designed to achieve; however, this remains conditional on the political objectives of both the senders and targets being compatible. If senders and targets share economic or political interests and their mindsets align, then sanctions can be imposed to induce a change in behaviour. Otherwise, behavioural change becomes less likely. Sanctions can, nonetheless, fulfil other functions. When there is a lower likelihood of cooperation between targeted and sanctioning entities, then sanctions can be imposed to limit the possibility of the target embarking on an undesired course of action (*constraint*). This, for example, justifies the utilisation of sanctions against terrorist organisations/individuals, conflict spoilers and warlords. In such scenarios, sanctions are imposed as preventive mechanisms to make sure that certain events do not occur. Beyond coercing and constraining, sanctions also send strong messages of disapproval to different audiences (*signalling*) in order to shape their expectations about future events. Sanctions can warn targets about possible escalation, but they can also stigmatise certain types of behaviour as unacceptable in the eyes of an international audience. This means that sanctions play a powerful role in determining what norms and interests actors will have to take into account when making foreign policy decisions.

Sanctions are not a silver bullet solution for violations of international law or the enforcement of norms in cyberspace.

Studies evaluating the efficacy and impact of targeted sanctions imposed over the past 30 years conclude that sanctions are largely ineffective in achieving their stated aims, but have beneficial consequences in some circumstances.[3] The Targeted Sanctions Consortium (TSC) found that UN sanctions were effective in reaching their stated aims on average only 22% of the time, with a 28% success rate in constraining, a 27% success rate at sending effective signals, and a 10% success rate in coercing change in the target.[4] The emergence of targeted sanctions has contributed to altering the understanding of how sanctions function in at least three fundamental ways. First, the multitude of targets that can be listed at any given time creates the opportunity to pursue different objectives with a variety of people/entities at the same time. Second, a targeted sanctions regime is more easily malleable than a comprehensive sanctions regime. The mere adding or removal of several individuals can provide valuable leverage in a negotiation and alter the scope of the sanctions altogether. Finally, sanctioning powers can narrowly tailor the desired impact of targeted regimes to the salience of the problem at hand. This factor has contributed to making targeted sanctions a ‘cheaper’ option compared to other foreign policy alternatives. However, targeted sanctions have also been criticised for their lack of ‘teeth’, the evasion opportunities that they inherently offer, and, in the EU context, the rather complex decision-making process that precedes their introduction. This has been an especially strong criticism in comparison with sanctions regimes imposed by different actors (e.g. the US and UN). Ultimately, however, this has neither

[3] Thomas Biersteker, Sue E. Eckert, Marcos Tourinho and Zuzana Hudáková, *The Effectiveness of United Nations Targeted Sanctions: Findings from the Targeted Sanctions Consortium (TSC)* (Geneva: Graduate Institute of International and Development Studies, 2013).

[4] Targeted Sanctions Consortium (TSC), 2018, https://graduateinstitute.ch/research-centres/global-governance-centre/targeted-sanctions-initiative.

affected the expansion of sanctions nor the frequency with which they are utilised.

WHEN DO SANCTIONS WORK?

The absence of a sufficiently broad sample of previous examples of cyber sanctions makes it difficult to predict their future effectiveness. This does not mean however that we are navigating in uncharted waters without any guidance. Quite the opposite. Similar measures employed to tackle drug traffickers, criminal networks and terrorist cells can provide many useful lessons for heightening the efficiency of sanctions.[5] This section provides a 'checklist' with a constellation of questions that guide the analysis in the subsequent chapters of this *Chaillot Paper.*

Is the logic of the sanctions regime clearly defined?

The underlying rationale of the cyber sanctions regime should be clearly outlined.[6] This should include a determination of whether the sanctions are intended to *coerce* targets to change their behaviour, *constrain* their activities or access to resources, and/or *signal* to the target and other would-be cyber criminals activities in cyberspace that the sanctioning power will not tolerate.[7] Such a logic should be inherent in the sanctions planning process as well as in the communications surrounding their use. Research by the TSC suggests that sanctions, at least in the UN context, are most likely to be effective in the sphere of signalling, with constraining and coercing achieving lower success rates.[8] In the case of cyber sanctions, the perpetrators of attacks may be less concerned about being 'named and shamed' as part of a retaliatory response. Furthermore, as cyber criminals are unlikely to subscribe to the same types of norms as the senders of the sanctions, the stigmatising or isolating impact of the cyber sanctions regime may be more limited as compared to other regimes: indeed, becoming the target of such measures could be conceived by such malicious actors as 'a badge of honour.' Nevertheless, while the targets of sanctions in the cyber domain might not be dissuaded, other actors might well be. This occurs in a context where potential criminals may be deterred if consequences are to be expected as a result of certain actions. In light of the above, constraining malicious actors' access to required resources or seeking to coerce their behaviour may be more productive strategies given the uniqueness of the cyber ecosystem.

Is the coordination with other foreign policy instruments ensured?

EU sanctions should always be contextualised in terms of the bloc's wider foreign and security policy strategies and activities. Sanctions must always be combined with other policy tools if they are to succeed in some way. In the case of cyber sanctions, and as already foreseen by the Cyber Diplomacy Toolbox (CDT), this could include dialogue, trade talks, diplomacy, law enforcement, collaboration with other countries and multilateral institutions, cooperation with the private sector and, in some instances, covert counterattacks and military deterrence. A better understanding of how these various instruments interact is needed in order to improve our insights into how sanctions work in

[5] Erica Moret and Patryk Pawlak, "The EU Cyber Diplomacy Toolbox: Towards a Cyber Sanctions Regime?", *EUISS Brief* no. 24, July 12, 2018.

[6] Francesco Giumelli, "How EU Sanctions Work: A New Narrative," *EUISS Chaillot Paper* no. 129, May 2013,

[7] Francesco Giumelli, "New Analytical Categories for Assessing EU Sanctions". *The international Spectator: Italian journal of international affairs*, vol. 45, no. 3 (2010): pp. 131–144.

[8] TSC, 2018, *op. cit.*

practice. At the same time, creating links between different policy instruments and considering their interactive effects is key in order to avoid potential unintended consequences of sanctions.

Does the choice of specific sanctions support the stated objectives?

When the EU employs cyber sanctions, it is worth keeping in mind that certain types of sanctions can be more effective than others, and the way in which different foreign and security policy tools are combined also plays a crucial role in their success. Diplomatic sanctions, for example, tend to be less effective due to the fact that they do not generate immediate economic consequences.[9] Similarly, travel bans and asset freezes – two of the most common forms of EU targeted restrictive measures – can be easily circumvented, especially in the absence of other foreign policy and security measures.[10] The UN experience has also demonstrated that there is a certain threshold of measures beyond which the effectiveness of sanctions diminishes.[11] For instance, an optimal level appears to be that which targets key export commodities (apart from oil), or sizeable companies that affect entire sectors of a targeted economy. On the other hand, sanctions consisting of only one measure (such as flight restrictions, or individual sanctions measures, taken alone) are never effective.[12]

Is the timing and longevity of the sanctions adequate?

In general terms, sanctions applied over a shorter timespan have been shown to be more effective than long-term measures that allow the target to develop alternative commercial relationships, generate domestic substitutes for sanctioned goods or engage in sanctions-busting activities through the use of middlemen and front companies. In the case of UN sanctions, some 40% of assessed 'successes' in altering the behaviour of a target have tended to occur in the first 12 months of a sanctions regime. In around 60% of cases that are deemed 'failures', the sanctions regimes exceeded three years. As such, sanctions regimes should be designed to be flexible and should be regularly reviewed and adapted to changing conditions. This is particularly relevant for the cyber domain, where quicker adaptation of sanctions will certainly be required. Furthermore, particularly in cyberspace, sanctions that can be enacted quickly and without warning would have higher chances of success, as they would not allow the target to prepare alternative courses of action. As pointed out in a previous EUISS publication on this topic, '[u]nexpectedness can be achieved by contingency planning, short deliberations, quick implementation, the engagement of unexpected (non-traditional) sanction imposers, and the use of instruments (new types of sanctions or restrictive measures) that have not been used before'.[13]

[9] Clara Portela, "The EU's 'Sanctions Paradox'," in *Stiftung Wissenschaft und Politik (SWP Comments)*, 18, 2007, pp. 1-8.

[10] Ibid.

[11] Thomas Biersteker and Marcos Tourinho, "Have UN Targeted Sanctions Worked?" in Sebastian von Einsiedel and George Lopez (eds.), *The Sanctions Enterprise: Assessing a Quarter-Century of UN Action for Peace, Security and Human Rights* (Cambridge: Cambridge University Press, forthcoming).

[12] Ibid.

[13] Iana Dreyer and José Luengo-Cabrera (eds.), "On Target? EU Sanctions as Security Policy Tools", *EUISS Report* no. 25, September 2015.

Do the sanctions demonstrate a detailed understanding of the target?

Obtaining a detailed understanding of targets is a particular challenge given the anonymity that characterises the cyber domain. In the case of sanctions imposed against state actors, factors such as their political and economic stability, level of democratic freedoms, membership in international organisations, global economic and commercial interconnectivity, and degree of resilience to vulnerabilities are all vital considerations in crafting sanctions with an increased chance of meeting their stated aims.[14] If the targeted entity is an individual, company or a website, then a detailed understanding of its financing and resourcing, as well as connections to wider networks and motivations, is essential prior to sanctions imposition. Depriving a targeted entity of its main sources of revenue can be a highly effective way of constraining activities in which it is engaged and which are deemed unacceptable to sanctioning powers.[15]

Are the foreseen capabilities and resources sufficient?

Considerable levels of expertise, sufficient investment and advanced capabilities are necessary in the efficient imposition, enforcement and monitoring of sanctions. This is likely to be particularly valid in the technically sophisticated and fast-changing cyber domain. Nevertheless, cyber expertise within member states varies broadly at present. Furthermore, sanctions practice in the EU, as well as in the UN, has historically been marred by under-resourcing, under-staffing and sub-optimal transfer of institutional knowledge.[16] This has improved somewhat in recent years with investments in sanctions capabilities in the European External Action Service (EEAS) and the European Commission as well as in the competent authorities of various member states. The recent involvement of the member states and the Commission in the working group on cyber issues is an example of how awareness and the culture of cybersecurity can be improved. Nevertheless, staff turnover means that EU officials and seconded national experts from EU member states may only work on sanctions or cyber policies for a limited period of time, then move on to different jobs. This inevitably has an impact on institutional memory and hence the effectiveness of the entire sanctions regime.

Do the existing mechanisms for coordination and information-sharing work?

The effectiveness of sanctions in the EU can be affected by the degree of political support from individual member states and different departments within sanctioning authorities. The EU's requirement for consensus among all member states has, on occasion, led to sanctions being diluted.[17] The pace of reaching agreements on sanctions can also vary depending on the preferences and interests of individual member states. Moreover, there may also exist barriers and silos between relevant teams working on sanctions in EU institutions,[18] which presents difficulties for coordination with other sanctioning powers (such as the US). These drawbacks could be mitigated by mechanisms or groupings to coordinate and monitor joint

[14] Thomas Biersteker and Peter A. G. van Bergeijk, "How and When do Sanctions Work? The Evidence", in Iana Dreyer and José Luengo-Cabrera (eds.), "On Target? EU Sanctions as Security Policy Tools," *EUISS Report* no. 25, September 2015.

[15] Ibid.

[16] Mikael Eriksson, *Targeting Peace: Understanding UN and EU Targeted Sanctions* (Farnham: Ashgate, 2010)

[17] Erica Moret, Evidence provided to the UK House of Lords EU External Affairs Sub-Committee on post-Brexit sanctions policy and defence/security cooperation with the EU, July 2017, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/eu-external-affairs-subcommittee/brexit-sanctions-policy/written/70456.pdf.

[18] Ibid.

working in this field, something which is not currently well-developed at the global level.[19]

Sanctions also often depend on the sharing of intelligence and other sensitive forms of information between state actors. This is of particular relevance for cyber sanctions, where certainty about attribution, and adherence to the principles of necessity and proportionality are key conditions for the legality of countermeasures adopted under international law.[20] Despite this, global efforts to confront cyber threats are currently hampered by issues such as reluctance to share sensitive information linked to cyber capabilities or vulnerabilities. Efficient cooperation and information-sharing between EU organisations (including the Hybrid Fusion Cell, Europol's EC3, the EU CSIRT network and ENISA) will positively influence the EU's ability to identify targets and craft proportionate sanctions in response.

How is multilateral engagement and coordination with partners ensured?

Studies show that the effectiveness of sanctions can be augmented when various major economic and political powers work together to avoid creating economic gaps that can be exploited by third parties, for evasion or trade diversion. This is particularly the case regarding financial sanctions or embargoes on particular commodities.[21] In the context of cyber sanctions, the US is the only other sanctioning power that has so far imposed its own restrictions. Nevertheless, others are likely to follow suit, which could enhance the effectiveness of the EU's own measures, particularly if measures are coordinated strategically and judiciously. This might include traditional sanctioning partners, such as Canada, Japan and Australia, non-EU European neighbours which traditionally align with EU restrictive measures (such as Iceland, Norway, Switzerland and Ukraine) or collaboration through other regional and *ad-hoc* groupings, such as the G7.

Are the mechanisms for cooperation with industry in place?

Close collaboration exists between the EU and the banking sector in the realm of targeted financial sanctions and compliance of financial institutions. This type of cooperation between the EU and the private sector could serve as a basis for developing a similar network on cyber sanctions.

Close cooperation with the private sector and technical communities through exchanges of information and good practices is of pivotal importance to ensure that the EU's cyber sanctions are sufficiently targeted, up-to-date and in line with the latest technological developments. This is especially relevant with regard to compliance, where the private sector can help shed light on the activities of targeted actors.

Is there a clear communication strategy?

Clear communication about the precise objectives of a given sanctions regime should be prioritised, especially given the potential reputational, economic and legal risks and costs that the imposition of a sanctions regime entails. In the cyber sanctions context, such costs may include a potential deleterious impact on domestic firms, a rise in corruption and criminality, in addition to a heightened probability of retaliation. Clear communication of purposes could also diminish 'rally-around-the-flag'

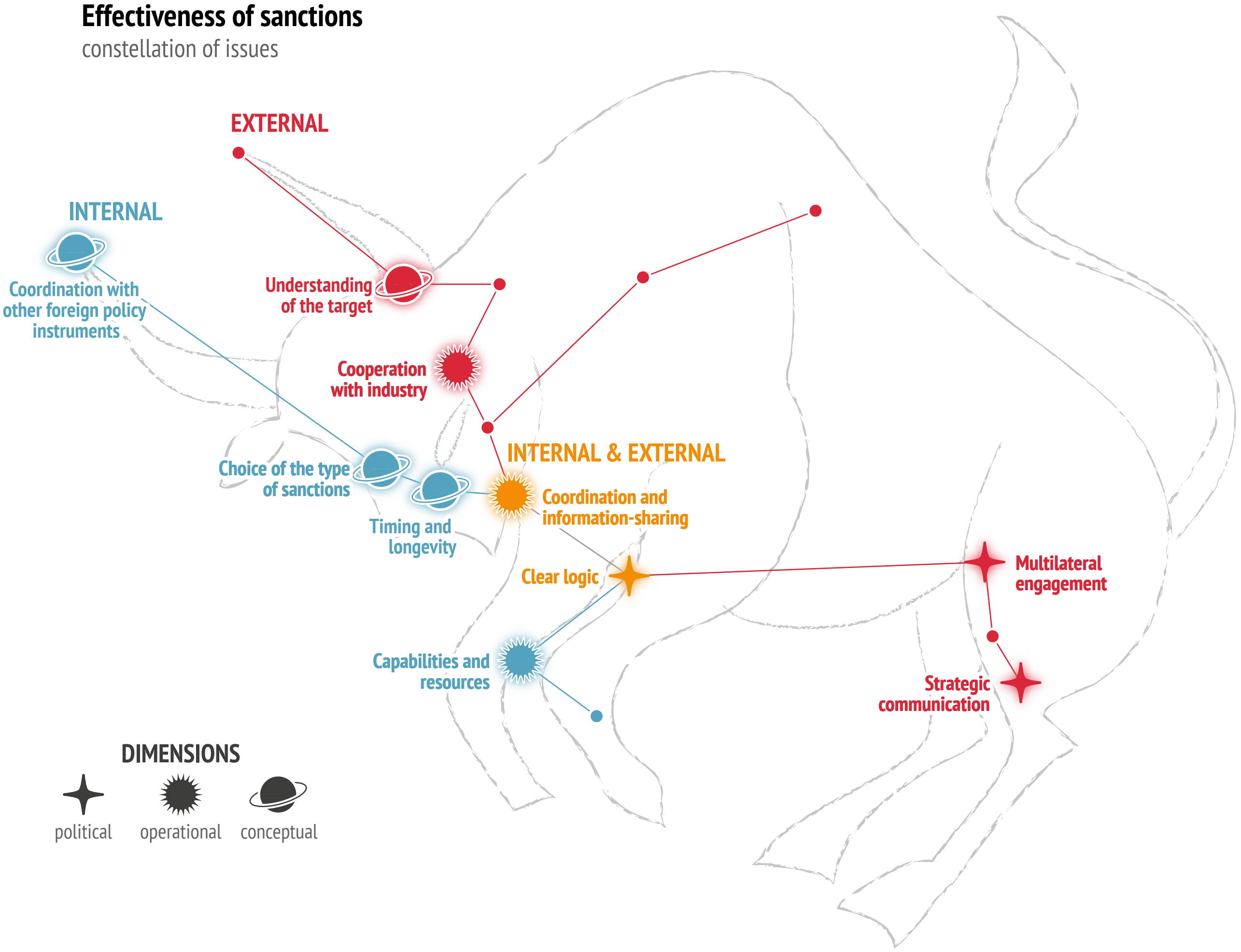
[19] Erica Moret and Fabrice Pothier, "Sanctions After Brexit," *Survival: Global Politics and Strategy*, vol. 60, no. 2, (2018): pp. 179-200.

[20] Erica Moret and Patryk Pawlak, *op. cit.*

[21] Thomas Biersteker and Peter A. G. van Bergeijk, *op. cit.*

Effectiveness of sanctions

constellation of issues


EXTERNAL
INTERNAL
Coordination with other foreign policy instruments
Understanding of the target
Cooperation with industry
Choice of the type of sanctions
Timing and longevity
INTERNAL & EXTERNAL
Coordination and information-sharing
Clear logic
Multilateral engagement
Capabilities and resources
Strategic communication
DIMENSIONS
political
operational
conceptual

effects, where the government of the target of sanctions (i.e. an individual or corporate entity) garners popular support, or the strengthening of ties between the targeted entity and third countries or groups that may be deemed hostile to the senders of sanctions. The EU as a sanctioning power should also carefully consider the role played by the threat of adopting sanctions, given that a threat can sometimes have as, if not more, important an impact as the imposition of the sanctions themselves.[22] Companies and individuals also need to be properly and adequately informed on a continuous basis by those imposing sanctions, otherwise they will tend to change their operations in order to de-risk, which might inadvertently affect the effectiveness of policies in place. In general, poor communication undermines the legitimacy of the sending power and the effectiveness of the sanctions regime as a whole by reducing the number of actors, be they other countries or entities, willing to implement remedial measures or revert to an acceptable course of action.

[22] Ibid.

CONCLUSIONS

The issues raised in this chapter and the proposed questions suggest that valuable lessons can be drawn from the sanctions regimes established in other policy areas. However, they cannot be applied automatically and need to be adjusted for the cyber context. Imposing sanctions in the cyber world presents a few differences from the imposition of conventional sanctions that are worth highlighting. First, sanctions in the cyber domain are more likely to deter states, but they are less likely to deter individuals from acting in the name of states. Second, the implementation and enforcement of sanctions in cyberspace require more developed skills than 'conventional' sanctions. These should be either acquired by states and/or drawn from the private sector. Third, sanctions in the cyber world are likely to fall short of the initially stated objective (e.g. a change in behaviour), which can increase their unintended effects (e.g. the target of the sanctions adopts an even more aggressive posture). Consequently, sanctions need to be designed in a way that allows for timely adjustments and changes. Special provisions for a cyber sanctions regime might need to be considered in order to address this matter. Thus, in principle, the effectiveness of sanctions in the cyber world can be assessed with a similar logic to that applied to sanctions in the 'conventional' world. However, due to the rapidly changing nature of the problem/actors and the absence of borders in cyberspace, a sufficient level of effectiveness can be reached only if international cooperation is enhanced both in terms of depth and quality.

The checklist presented above points to a number of issues that can be organised according to their thematic focus (i.e. conceptual, operational and political) as well as the target audience (i.e. internal and external – see diagram on previous page). In order to better understand the drivers behind the success and failure of a specific sanctions regime and to ensure its effectiveness, it is important to properly identify and assess the assumptions and concepts underpinning the design of the regime (e.g. interaction with other foreign policy tools, type of sanctions used, or a deep understanding of the target), its operational aspects (e.g. coordination and information-sharing mechanisms, capabilities and resources), as well as the political choices involved (e.g. logic of intervention, strategic communication). At the same time, each of these aspects is addressed to internal or external audiences driven by different motivations: political buy-in, better understanding of potential consequences for the parties involved, and awareness of the required resources and capabilities, among others. The subsequent chapters of this *Chaillot Paper* seek to help the reader navigate these complex questions and issues.