DETERRENCE IN CYBERSPACE: QUESTIONING THE CONCEPT

EU CYBER DIRECT

15 November 2019, Scotland House, Rond-Point Schuman 9, Brussels

Concept note

Deterrence is a core idea of international politics. It has dominated the western strategic discourse for decades and has now become the new big buzzword in the realm of cyber. Most debate on cyber deterrence focuses on whether conventional or nuclear models of deterrence are applicable to cyberspace, and whether deterrence by punishment or denial, or some combination thereof, works better given the particularities of cyber (Nye 2017). But as deterrence studies enter their "fourth wave" (Lupovici 2010), after establishing deterrence as a strategy, modelling it with game theory, and theory refinement through empirical studies, it is useful to stress that deterrence effectiveness remains an elusive concept; we have no widely accepted causal model of deterrence to draw on in cyber because in deterrence there are always too many variables at play (Freedman 2004). There is, in other words, no consensus what actually does the deterring; deterring effects are contextually specific and have to do as much with norms and taboos as with the potential use of weapons. In debating abstract scenarios, it is often underappreciated that, if deterrence is defined as "dissuading someone from doing something by making them believe that the costs to them will exceed their expected benefit" (Nye 2017, 45), deterrence success depends on how the adversary chooses to respond to threat: "One cannot say 'I hereby deter you' but one can say 'you deterred me'" (Vuori 2016, 24), which makes all the difference in practice. Conventionally seen as the realm of signaling, this premise calls not only for capacities, weapons, threat credibility and pressure, but also for fine-tuned political skills that rely on contextual knowledge about the one to be deterred.

The reasons to resort to deterrence are as much strategic as they are political and include limiting strategic alternatives, the mobilization of political support, and the maintenance of self-identity (Lupovici 2016). As the European Union starts to chart its course on cyber deterrence, these considerations are crucial for a more tangible engagement in cyber politics and weaving an EU narrative of deterrence which reflects its own normative position. How does EU, for example, understand the use of cyber deterrence vis-à-vis its norms-driven cyber diplomacy, specifically with regard to two dilemmas: the precarious balance between stabilizing and escalatory effects of deterrence policies, and the risk of perceiving norms as tools of coercion.

Implementing organisations

ISS European Union Institute for Security Studies

G | M | F The German Marshall Fund of the United States
STRENGTHENING TRANSATLANTIC COOPERATION

Stiftung Neue Verantwortung

This project is funded by the European Union.

There may be a stated preference for deterrence by denial which emphasizes defence and resilience capacities over the militarized approach of deterrence by punishment, but what is it exactly that EU actually wants to deter. Are the social and political costs of deterrence worthy the price, including to the EU's identity as an autonomous cyber actor invested in rule-based and inclusive international order? To address these questions, we should pay more attention to the politics of deterrence, and its perceived origins and effects. In order to do so, the workshop brings a range of academics with expertise across different policy domains where deterrence has been applied to discuss possibilities for the EU to craft a dynamic narrative that reflects its normative standing and ambition in cyber diplomacy.

Deterrence in the EU: state of play

Deterrence and response to cyber-attacks are clearly listed as the motivation for putting the cyber sanctions regime in place. The Joint Communication 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' of 13 September 2017 states that 'effective deterrence means putting in place a framework of measures that are both credible and dissuasive for would-be cyber criminals and attackers' (European Commission, 2017). Consequently, the Joint Communication defines concrete measures to support such approach: a) identifying malicious actors by improving capacity to identify those responsible for cyber-attacks, b) stepping up the law enforcement response, including by facilitating cross-border access to electronic evidence, establishing common forensic standards, and promoting the Council of Europe Convention on Cybercrime; c) public-private cooperation against cybercrime; d) stepping up the political response, including through the implementation of the cyber diplomacy toolbox; and e) building cybersecurity deterrence through the Member States' defence capability, including concrete cyber defence within the framework of a "Permanent Structured Cooperation" (PESCO) and further integrating cybersecurity and defence into Common Security and Defence Policy (CSDP).

References

- European Commission, *The Joint Communication Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450 final, Brussels, 13 September 2017.
- Lawrence Freedman (2004) *Detterence*, Cambridge: Cambridge University Press.
- Amir Lupovici (2010) "The Emerging Fourth Wave of Deterrence Theory - Toward a New Research Agenda", *International Studies Quarterly* 54 (3):705-32.
- Amir Lupovici (2016) *The power of deterrence: emotions, identity and American and Israeli wars of resolve*, Cambridge: Cambridge University Press.
- Joseph Nye (2017) "Deterrence and Dissuasion in Cyberspace", *International Security* 41 (3):44-71. doi: 10.1162/ISEC_a_00266.
- Juha Vuori (2016) "Dettering Things with Words: Detterence as a Speech Act", *New Perpectives* 24 (2):23-50.