Critical Infrastructure and the Cognitive Domain: Cyberattacks as Instruments of Coercion across Maritime, Energy and Digital Networks

Andrea Caligiuri
Associate Professor of International Law and
Director of CiRAM (*Centro interdipartimentale di Ricerca sull'Adriatico e il Mediterraneo*),
University of Macerata

1. Conceptual Framework

The protection of critical infrastructure has become a central issue in contemporary security policy. As global economic systems become increasingly interconnected through digital technologies, infrastructures sustaining trade, energy supply and communications have acquired strategic importance. Ports, electricity grids and submarine cables now constitute key nodes within a complex network supporting the global economy.

At the same time, digitalisation has introduced new vulnerabilities. Cyberattacks targeting infrastructure have emerged as a central feature of geopolitical competition. Such operations do not necessarily aim at physical destruction, but rather to disrupt economic activity, influence public confidence or shape decision-making processes. In this sense, cyberattacks increasingly operate within the cognitive domain.

The cognitive domain may be defined as the sphere in which perceptions, beliefs and expectations are formed and translated into decisions by political authorities, economic actors and societies. It refers to the processes through which information is internalised and acted upon. Within this domain, disruptions and uncertainties generated by cyber operations acquire strategic significance by shaping risk perception and influencing behaviour.

The cognitive domain thus operates as a mediating layer between technical disruption and strategic effect. Cyberattacks do not automatically produce cognitive consequences; their impact depends on how disruption is perceived and interpreted. This aligns with classical theories of coercion, particularly those developed by Thomas Schelling, according to which strategic value lies in influencing expectations and choices.

This article argues that cyber operations targeting critical infrastructure should be understood as forms of "systemic coercion".

2. Cyberattacks and Systemic Risks

The vulnerability of critical infrastructure has been illustrated by major cyber incidents. The NotPetya attack in 2017 demonstrated how operations targeting logistics networks may generate cascading disruptions across global supply chains, including the shutdown of Maersk's terminals.

Energy infrastructure has also proven vulnerable. The Stuxnet malware demonstrated the capacity to manipulate industrial control systems, while the Colonial Pipeline ransomware attack in 2021 disrupted fuel supply networks and generated public concern.

In Europe, the sabotage of the Nord Stream pipelines in 2022 highlighted the vulnerability of offshore energy infrastructure and intensified debates on protection.

These dynamics involve both state and non-state actors. While similar techniques may be employed, their implications differ depending on attribution and intent. State-attributable operations may be interpreted as strategic coercion, whereas non-state activities may nonetheless generate comparable systemic effects.

These cases show that cyberattacks may produce consequences extending beyond immediate disruption. In interconnected systems, attacks on a single node may generate cascading economic and political effects. Their strategic impact lies less in disruption itself than in their capacity to generate uncertainty and shape expectations, functioning as instruments of indirect coercion.

3. Subsea Cables as Strategic Chokepoints: Vulnerability, Control and Cognitive Effects

Subsea communication cables constitute the physical backbone of the global digital economy. Today, more than ninety-nine per cent of international data traffic—including financial transactions, governmental communications and internet services—is transmitted through fibre-optic cables located on the seabed. These infrastructures connect continents and enable the functioning of global financial markets, digital services and international communications. Their strategic relevance has also prompted specific recent EU action on the security and resilience of submarine cable infrastructures, including the EU Action Plan on Cable Security (JOIN(2025) 9 final), which introduces a coordinated European approach to submarine cable protection based on prevention, detection, response and deterrence.

Despite their importance, submarine cable systems exhibit several structural vulnerabilities. Public debates often focus on the physical cables located on the seabed, yet the most critical points in the network are frequently located on land. Cable landing stations, where submarine cables connect to terrestrial infrastructure, represent particularly sensitive nodes within global digital communication networks and function as critical chokepoints through which large volumes of international data traffic pass.

Because cable landing stations are located within the territory of coastal states, they fall under national jurisdiction and domestic regulatory frameworks. This situation creates an important interaction between the international legal regime governing submarine cables and domestic legal frameworks regulating telecommunications infrastructure. Coastal states therefore exercise considerable control over these strategic nodes of global connectivity.

The legal protection of submarine cables has long been recognized under the law of the sea. The United Nations Convention on the Law of the Sea (UNCLOS), in addition to establishing a legal framework governing their installation depending on the maritime zones concerned, also defines a framework relating to their protection. In particular, Articles 113–115 require States to adopt domestic legislation criminalizing the intentional or negligent damage of submarine cables on the high seas and provide rules on liability and repair.

However, this framework remains primarily oriented towards physical damage and does not adequately address vulnerabilities arising from cyber interference with the digital systems that manage contemporary cable networks. As submarine cable systems have become increasingly integrated with digital routing platforms, network management software and data centres, this regulatory gap has become more significant. This evolution

suggests that existing law of the sea provisions may no longer fully capture the security challenges affecting contemporary maritime digital infrastructures.

In practice, many vulnerabilities in submarine cable systems arise from the terrestrial components of the network. Network management platforms, routing systems and data centres associated with cable landing stations may all represent potential targets for cyberattacks. Disruptions affecting these systems may interrupt international communications without causing visible damage to the submarine cable itself.

Beyond their operational implications, these vulnerabilities also have a distinct strategic dimension. The disruption – or even the credible threat of disruption – of submarine cable systems may function as a form of signalling, conveying information about an actor's capabilities to penetrate and manipulate critical nodes of global connectivity. At the same time, the exposure of such vulnerabilities may contribute to deterrence dynamics by shaping expectations about the potential costs of escalation.

More importantly, cyber operations targeting cable infrastructure may operate as instruments of coercion. By generating uncertainty regarding the reliability of communication flows, such actions may influence the behaviour of governments, markets and private operators. In highly interconnected digital systems, the anticipation of disruption may be as consequential as disruption itself, as it affects trust in infrastructure and alters decision-making processes across multiple sectors.

Subsea cable infrastructures thus exemplify how critical infrastructure may be leveraged not only for disruption, but as a means of exercising cognitive and economic coercion through the manipulation of uncertainty and trust in global connectivity systems.

4. International Law and the Grey Zone of Cyber Competition

Cyberattacks targeting critical infrastructure raise fundamental questions within international law, as they challenge the adequacy of existing legal categories to capture forms of coercion that operate without physical force yet produce strategically significant constraints on state autonomy. The prohibition of the use of force under Article 2(4) of the UN Charter remains a cornerstone of the contemporary legal order. However, traditional interpretations of this principle were developed primarily with reference to kinetic military operations.

Within contemporary legal scholarship, cyber operations are often assessed through the scale and effects test. Yet many cyber operations targeting critical infrastructure are deliberately designed to remain below this threshold, operating within the so-called grey zone between peace and armed conflict.

This raises the question whether such operations may nevertheless fall within the prohibition of intervention in the internal affairs of a State. According to the prevailing view, prohibited intervention presupposes coercion with respect to matters falling within the target State's *domaine réservé*. Traditionally, coercion has been understood as interference bearing on the State's freedom of choice in the exercise of its sovereign functions.

However, this understanding may be insufficient to capture the strategic logic of contemporary cyber operations targeting critical infrastructure. In highly interconnected systems, influence may be exerted not through direct compulsion, but through the manipulation of systemic conditions shaping decision-making processes.

Cyber operations that generate significant and foreseeable disruptions to critical infrastructure may alter market behaviour, affect public confidence and constrain the

range of viable policy options available to a state. In such circumstances, coercion may arise not from the imposition of a specific course of action, but from the structured limitation of alternatives within the decision-making environment.

This form of influence may be conceptualized as "systemic coercion", understood as the deliberate shaping of a state's decision-making environment through the generation of systemic uncertainty affecting critical infrastructures. This form of influence remains distinct from mere persuasion insofar as it operates through the deliberate creation of constraints that significantly affect the target State's range of policy options.

On this basis, this article proposes a functional understanding of coercion centred on its effects on decision-making autonomy. Cyber operations targeting critical infrastructure may amount to prohibited intervention where three cumulative conditions are met: (i) the operation produces or risks producing systemic disruption in sectors essential to state functioning; (ii) such disruption is reasonably foreseeable and attributable to the acting entity; and (iii) the resulting uncertainty or instability materially constrains the target state's capacity to freely determine its sovereign choices.

Such an approach does not require direct compulsion, but instead focuses on whether the operation effectively reshapes the decision-making environment in a manner comparable, in functional terms, to traditional coercion, as reflected in prevailing interpretations of the principle of non-intervention. It thus offers a doctrinally grounded framework for assessing cyber operations that operate within the grey zone, while demonstrating that forms of systemic coercion may arise even in the absence of direct compulsion, where the manipulation of infrastructure-dependent uncertainty effectively constrains state autonomy in functional terms.

These legal and conceptual developments also have important implications for governance. If coercion may operate through systemic uncertainty, then resilience cannot be understood solely in technical terms. Regional and international cooperation becomes essential to manage risks across interconnected infrastructures, promote information-sharing and ensure coordinated responses.

Such approaches highlight that infrastructure security is not only a matter of protection, but also of governance and trust. By stabilizing expectations and reinforcing confidence in the reliability of critical systems, governance mechanisms can mitigate the cognitive and systemic effects of cyber disruptions. In this sense, resilience involves not only safeguarding infrastructure, but also limiting the conditions under which systemic coercion can be exercised.

5. Final Remarks

The interaction between cyberattacks, critical infrastructure and the cognitive domain reflects a broader transformation in contemporary security dynamics. Infrastructure systems that sustain global connectivity are no longer merely assets to be protected, but rather strategic arenas through which influence can be exercised.

The strategic significance of cyber operations lies not only in their capacity to disrupt systems, but in their ability to generate systemic uncertainty. It is this uncertainty that shapes perceptions, alters risk calculations and ultimately influences economic behaviour and political decision-making processes.

This analysis suggests that contemporary strategic competition increasingly unfolds through the manipulation of expectations and systemic stability rather than through direct physical destruction. Cyberattacks against critical infrastructure can therefore operate as

instruments of indirect coercion, capable of producing strategic effects without crossing traditional legal thresholds.

These developments challenge existing legal and policy frameworks, which remain largely oriented towards physical damage and kinetic threats. Addressing these challenges requires not only enhanced technical resilience, but also a conceptual shift towards recognizing systemic coercion as a central feature of contemporary cyber competition.

Recognizing systemic coercion as a legally relevant category may thus require a recalibration of the non-intervention principle, capable of capturing forms of constraint that operate through systemic interdependence rather than direct compulsion.

Bibliography

- BURNETT, Douglas R.; BECKMAN, Robert and DAVENPORT, Tara M., *Submarine Cables: The Handbook of Law and Policy*, Brill, 2014
- KELLO, Lucas, *The Virtual Weapon and International Order*, Yale University Press 2017
- ROSCINI, Marco, *Cyber Operations and the Use of Force in International Law*, Oxford, 2014
- SCHELLING, Thomas C., *Arms and Influence*, Yale University Press, 1966
- SCHMITT, Michael N., (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed., Cambridge University Press, 2017
- ZETTER, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*, Crown, 2014