

# Digital Shields

## Rethinking Public-Private Partnerships Against Hybrid Threats

BY LEONARD BAUMANN, HERTIE SCHOOL, MASTER OF  
INTERNATIONAL AFFAIRS (ALUMNI)

This paper argues that Europe does not need one main public-private digital shield against hybrid threats. It must have two. To protect its physical infrastructure, Europe needs an attribution-driven, coercive shield, with the state retaining final authority. Information integrity requires the opposite: a legitimacy-preserving shield built on transparency and restraint, because enforcement risks destroying the very openness it is meant to protect. Taking into account the recent Baltic Sea sabotage campaign and also the EU's Foreign Information Manipulation and Interference framework, this paper proposes a differentiated architecture built so that shields remain answerable to democratic oversight.

## TWO SHIELDS, ONE WORD

On December 25, 2024, the tanker *Eagle S* dragged its anchor through the Gulf of Finland, cutting the Estlink 2 power interconnector as well as four data cables. The repairs took nearly six months. A Finnish court later dismissed charges against the captain and two officers for lack of jurisdiction, although that decision was overturned on appeal (Newsweek 2026; ICDS 2026). The *Eagle S* incident was one of over a dozen suspected acts of sabotage against the infrastructure of the Baltic Sea since 2023, most linked to Russia's shadow fleet, which doubles as a sanctions evasion tool and, as many investigators believe, a platform for drone operations and reconnaissance (Carnegie 2025).

During these same years, there was a parallel campaign that was fought with words rather than anchors. The EEAS reframed disinformation as Foreign Information Manipulation and Interference, targeting state-linked operations aimed at destabilizing institutions (Proto et al., 2025). Different method but the same intent: external actors seek to exploit a European asset that is privately controlled while the authority to attribute and deter such attacks remains sovereign.

Many debates fold both problems into one phrase: public-private partnership. This framing is too coarse, and this paper argues that it is also strategically dangerous. The underlying weakness of Europe is not primarily a lack of regulation but a structural mismatch between where authority and control sit: The assets that are under attack are privately financed, owned, and operated, while the power to respond and deter legitimately remains with the state. This mismatch is not a gap that more coordination can close, as it resolves in opposite directions, depending on the domain. The protection of infrastructure depends on the state's monopoly on legitimate coercion: sanctioning owners, boarding vessels, and hardening assets. The integrity of information depends on the opposite instinct:

A state that polices speech too aggressively gives adversaries the very "authoritarian West" narrative that hybrid campaigns exist to establish. Therefore, Europe must have two digital shields, not just one: a legitimacy-preserving shield for information and a coercive shield for infrastructure. A toolkit that is built for just one domain will not just underperform in the other. Its use can actively backfire against European interests. A digital shield that is built on a single template will either under-protect European infrastructure or over-secure European democracy. This essay sets out the reasons why and what a differentiated architecture would look like instead.

## WHY THE PRIVATE SECTOR IS UNABLE TO CARRY THIS ALONE

Around four-fifths of the infrastructure that the EU's 2022 Critical Entities Resilience Directive designates as essential across banking, transport, energy, health, and digital infrastructure is now privately operated or owned (Deloitte 2026). Telecom operators own the cables. The energy utilities run the interconnectors. In the information space, the imbalance runs even deeper: Platforms are not an incidental part of infrastructure but the very battlefield, and their commercial incentives very rarely align with the state's interest in a stable public sphere.

Private operators cannot supply all the capabilities needed to counter hybrid threats. A telecom operator cannot deploy a naval patrol. A platform cannot itself decide, with democratic legitimacy in mind, what counts as foreign interference rather than domestic dissent. Both of these problems need some form of authority that only a state, which is answerable to its public, can hold. Countries, in turn, do not have the commercial data and operational access that private entities have: A coast guard does not know which cable route an operator considers the most exposed, and a ministry does not see the patterns of coordinated accounts that a platform's own

systems can detect in hours. The dependency goes in both directions, which is exactly why the European Democracy Shield calls for a partnership.

However, dependency without differentiation creates box-checking instead of resilience. A partnership that asks a telecom operator to also perform deterrence or asks a ministry to additionally perform forms of content moderation misallocates the capability that each side actually possesses. The main point of a differentiated shield is not simply conceptual tidiness, but that misallocating authority in either direction is itself a vulnerability that a more patient adversary can exploit, whether through testing how long an under-resourced operator takes to notice sabotage, or by testing how quickly a country overreaches into speech regulation and gives the adversary a legitimacy crisis for free.

## INFRASTRUCTURE – THE CASE FOR A COERCIVE BACKSTOP

The Baltic Sea case clearly shows the costs of an undifferentiated approach. The incident reporting was fragmented across national authorities and operators. Legal tools were lagging behind the tactic: The dismissal of the case against Eagle S showed that maritime law was never created to penalize anchor-drag sabotage under flags of convenience. Deterrence was not anticipatory but reactive: NATO's Baltic patrol mission only launched in January 2025, a year into the campaign (ECFR 2025). The European Union's own regulatory response has been similarly slow: By the end of 2024, only four member states had transposed the NIS2 legislation on time, a situation that triggered infringement proceedings against twenty-three others (ECSCO 2026). A directive adopted years after the attack cannot substitute for deterrence in real time.

The institutional response from NATO points in the right direction, even where it remains

incomplete. A critical undersea infrastructure coordination cell, which was established after the Nord Stream sabotage, brings together private operators and military planners: A center at MARCOM was established specifically to deny attackers the cover of plausible deniability, a problem illustrated by the Eagle S case (NATO MARCOM 2024). While the alliance supplies the deterrent posture and also the will to name a perpetrator, the industry supplies the technical picture of where the vulnerabilities lie. What both of them are still missing is speed: The Coordination Cell was established months after Nord Stream, the Maritime Center over a year later, the Baltic Sentry only after many other incidents. A proper shield prepositions coercive capacity before even the first cable is cut, not after the tenth.

What this domain therefore needs is not more information-sharing forums, even if they do help, but a coercive backstop that private operators cannot provide themselves: a coordinated fast-track authority to detain and board vessels of interest, such as the one Finland and Sweden have already improvised in certain cases; possible cost-sharing arrangements so operators are not held liable for sabotage they cannot prevent, which currently disincentivizes the rapid reporting needed to disrupt a hybrid campaign; and not a reactive but a standing allied presence in higher-risk corridors. In this case, the state's coercive authority is not in tension with the partnership. It is the partnership's most important input, the one thing that private industry structurally cannot provide.

The cost of getting this wrong is cumulative, not just one-off. Every month of ambiguous attribution is a month during which the tactic remains cheap for the aggressor but expensive for Europe, as a shadow fleet tanker costs just a fraction of the interconnector it can disable for half a year. A coercive backstop is not just about punishing the last incident but about changing the cost calculation for the next one.

## INFORMATION - THE CASE FOR RESTRAINT

The information domain works inversely. The EU already has various tools in place: a Code of Practice on Disinformation, the EEAS's Rapid Alert System, the Digital Services Act, and also the new European Centre for Democratic Resilience (European External Action Service, 2025; European Commission, 2026b). In theory, this looks like a proper partnership: Platforms report their moderation actions, states share threat warnings, and the Centre is meant to connect it all. However, in practice, it is much weaker than it seems. States will only escalate a warning if they choose to do so, and platforms are not bound to react. Platforms report on themselves, which improves transparency, but still leaves them deciding what counts as manipulation, and the centre itself does not have the power to enforce anything; it can only coordinate.

It may seem tempting to take the infrastructure playbook here as well: harsher rules for platforms, faster takedowns, and quicker judgments about what counts as foreign interference. This, however, would be a mistake. When the cable is cut, it is either cut or not. A controversial post is not so simple: Deciding whether something is an unpopular opinion or a foreign manipulation is a political judgment, not a technical one. A state that allows itself to make decisions quickly and without any oversight becomes the story and hands its opponents exactly the argument they want: that the West silences views it dislikes. This is why the EEAS has moved away from the broader term of disinformation and towards the narrower FIMI to focus only on coordinated foreign interference rather than on the content itself.

So in reality, this domain needs the opposite of what the infrastructure needs: not more speed but more openness. In practice, this means giving independent researchers proper access to platform data and not leaving moderation as an internal black box; making

content decisions time-limited and reversible, rather than final; and allowing the people who assess foreign interference to be separate from anyone with power over ordinary political speech. What Europe actually has going for it is that its institutions can be criticized and checked, while those of its opponents cannot. Giving this up for faster enforcement would trade away the real advantage and strength of Europe in the name of security.

## A DIFFERENTIATED DIGITAL SHIELD

This, in turn, leads to four practical principles, two for each shield. Firstly, plan the response before the actual crisis, not during it. Secondly, protect the operators who report incidents: At the moment, companies underreport suspected sabotage because they fear the financial and legal fallout, which is exactly the wrong incentive when speed matters most. Thirdly, keep the two domains accountable in different ways: fast interdiction powers with parliamentary oversight for infrastructure. Lastly, have built-in expiry dates: The emergency powers, whether they are online or at sea, have to end automatically unless there is fresh evidence that the threat is still active. That renewal should go through parliament and not be decided by the executive alone. Without this, a temporary response to a real threat can quietly turn into a permanent expansion of power, which is itself a win for the kind of adversary this paper is describing.

## CONCLUSION

The public-private partnership has become one of the key phrases in the current European security policy framework. The Baltic sabotage campaign and the EU's FIMI response are not two instances of the same problem. They share a vocabulary and an adversary; that is it. Protecting infrastructure requires the one thing that only the state can provide: attribution and coercive deterrence. Protecting the information space requires the

opposite: transparency, restraint, and appeal rights, as it is the very legitimacy of an open public sphere that is under attack. Treating a shared vocabulary as a common solution has already cost Europe months of delays in the Baltic and leaves its information integrity framework aspirational.

Europe requires two digital shields: one that gives the state enough power to protect and defend its infrastructure, and another that prevents the state from acquiring too much power over information. Built as one shield, the framework will either under-protect Europe or over-secure its democracy. Either failure would hand the initiative to the opponents. Built as two, built on opposite logics and reviewed on a fixed democratic schedule, the shields have a genuine chance of keeping the public sphere open and the cables intact without destroying the distinction between them.

This distinction is this paper's main claim, and it is worth stating it here rather than leaving it implicit in a set of recommendations. A digital shield is not a single instrument that happens to have two applications. It is two instruments that happen to share a name, and Europe's hybrid threat strategy will only work once its institutions stop treating them as one.

## REFERENCES

- ACLED. (2026). Russia's shadow fleet presents a sustained hybrid war threat at sea. <https://acleddata.com/report/russias-shadow-fleet-presents-sustained-hybrid-war-threat-sea>
- Carnegie Endowment for International Peace. (2025). The Baltic Sea at a boil: Connecting the shadow fleet and episodes of sub-sea infrastructure sabotage. <https://carnegieendowment.org/research/2025/06/baltic-russia-maritime-cable-sabotage>
- Center for Strategic and International Studies. (2024). NATO's role in protecting critical undersea infrastructure. <https://www.csis.org/analysis/natos-role-protecting-critical-under-sea-infrastructure>
- Deloitte. (2026). Navigating the EU Critical Entities Resilience Directive. <https://www.deloitte.com/global/en/services/consulting-risk/perspectives/navigating-the-eu-critical-entities-resilience-directive.html>
- European Commission. (2026a). Countering information manipulation. [https://commission.europa.eu/topics/counter-ing-information-manipulation\\_en](https://commission.europa.eu/topics/counter-ing-information-manipulation_en)
- European Commission. (2026b). European Centre for Democratic Resilience. [https://commission.europa.eu/europe-an-centre-democratic-resilience\\_en](https://commission.europa.eu/europe-an-centre-democratic-resilience_en)
- European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2025). European Democracy Shield: Empowering strong and resilient democracies (Joint Communication JOIN(2025) 791 final). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A-52025JC0791>
- European Commission Joint Research Centre. (n.d.). Critical entities resilience. [https://joint-research-centre.ec.europa.eu/projects-and-activities/strengthening-eu-resilience-hybrid-threats-and-critical-entities/critical-entities-resilience\\_en](https://joint-research-centre.ec.europa.eu/projects-and-activities/strengthening-eu-resilience-hybrid-threats-and-critical-entities/critical-entities-resilience_en)
- European Council on Foreign Relations. (2025). Shallow seas and "shadow fleets": Europe's undersea infrastructure is dangerously vulnerable. <https://ecfr.eu/article/shallow-seas-and-shadow-fleets-europes-undersea-infrastructure-is-dangerously-vulnerable/>
- European Cyber Security Organisation. (2026). NIS2 Directive transposition tracker. <https://ecs-org.eu/policy/nis2-directive-transposition-tracker/>
- European External Action Service. (2025). 2024 report on EEAS activities to counter Foreign Information Manipulation and Interference (FIMI). [https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi\\_en](https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en)
- Jamestown Foundation. (2025). Hybrid attacks rise on under-sea cables in Baltic and Arctic regions. <https://jamestown.org/hybrid-attacks-rise-on-undersea-cables-in-baltic-and-arctic-regions/>
- Jermalavičius, T. (Ed.). (2026). The ties that bind: Enhancing security and resilience of critical undersea infrastructure in the Baltic Sea region. International Centre for Defence and Security. [https://icds.ee/static/icds\\_report\\_the\\_ties\\_that\\_bind\\_jermalaviciuseditor\\_april\\_2026.pdf](https://icds.ee/static/icds_report_the_ties_that_bind_jermalaviciuseditor_april_2026.pdf)
- NATO Allied Maritime Command. (2024). NATO officially launches new Maritime Centre for Security of Critical Undersea Infrastructure. <https://mc.nato.int/media-centre/news/2024/nato-officially-launches-new-nmcscui>
- Newsweek. (2026). Alarm raised at Russia's shadow fleet hybrid warfare threat to NATO. <https://www.newsweek.com/alarm-raised-russia-shadow-fleet-hybrid-warfare-threat-na-to-11981779>
- Proto, L., Lamoso-González, P., & Bouza García, L. (2025). The EU's FIMI turn: How the European Union External Action Service reframed the disinformation fight. Media and Communication, 13. <https://www.cogitatiopress.com/mediaandcommunication/article/view/9474>



---

## **AUTHOR**

**Leonard Baumann**

Hertie School, Master of International  
Affairs (Alumni)

---

## **EDITOR**

Bettina Vestring

## **DESIGN**

Luise Rombach



JUNGE **DGAP**