EU CYBER DIRECT

STUDY EXECUTIVE SUMMARY

DEFINING 'ACTIVE DEFENCE' IN CYBERSPACE

A comparative analysis of EU member states: concepts, doctrines and legal frameworks

Dr Andrea Calderaro
Marius Houwen

EU Cyber Direct, European Union Institute for Security Studies · Research paper, October 2026

Why this study

The 2022 Joint Communication on an EU Policy on Cyber Defence calls on member states to invest in 'full-spectrum cyber defence capabilities, including **active defence capabilities**'. It sets a clear strategic direction but does not define active cyber defence or say how member states should strengthen it. The Council Conclusions of May 2023 and the public record of the EU Cyber Census 2025 leave the same question open.

To help fill this gap, the study explores whether and how member states approach active cyber defence themselves, and how they define it. It examines the strategies, doctrines, statutes and legal frameworks of all 27 member states through seven analytical questions. The findings show where approaches converge and where they differ, and offer a practical basis for **shared planning and mutual legibility** across the EU.

SEVEN ANALYTICAL QUESTIONS

1. **Authority:** Who acts, and under which body of law?
2. **Register:** What vocabulary does the state choose?
3. **Locus:** Where does the state say it will act?
4. **Target:** Against whom is the activity directed?
5. **Trigger:** When is action authorised?
6. **Effect:** What is the action described as doing?
7. **Legal position:** What has the state said about the international law that governs action beyond its own networks?

KEY FINDINGS

- **Many definitions, none shared:** several meanings, each authoritative in its own setting, and no common EU approach.
- **Three models:** military (France), intelligence-enabled (the Netherlands) and police-law (Germany).
- **More agreement than definitions suggest:** every published position accepts international law and a legal frame.
- **A consistent disclosure pattern:** states name the agency and vocabulary, less often where, when, against whom and to what effect.

RECOMMENDATIONS
FOUR PRIORITIES FOR THE EU

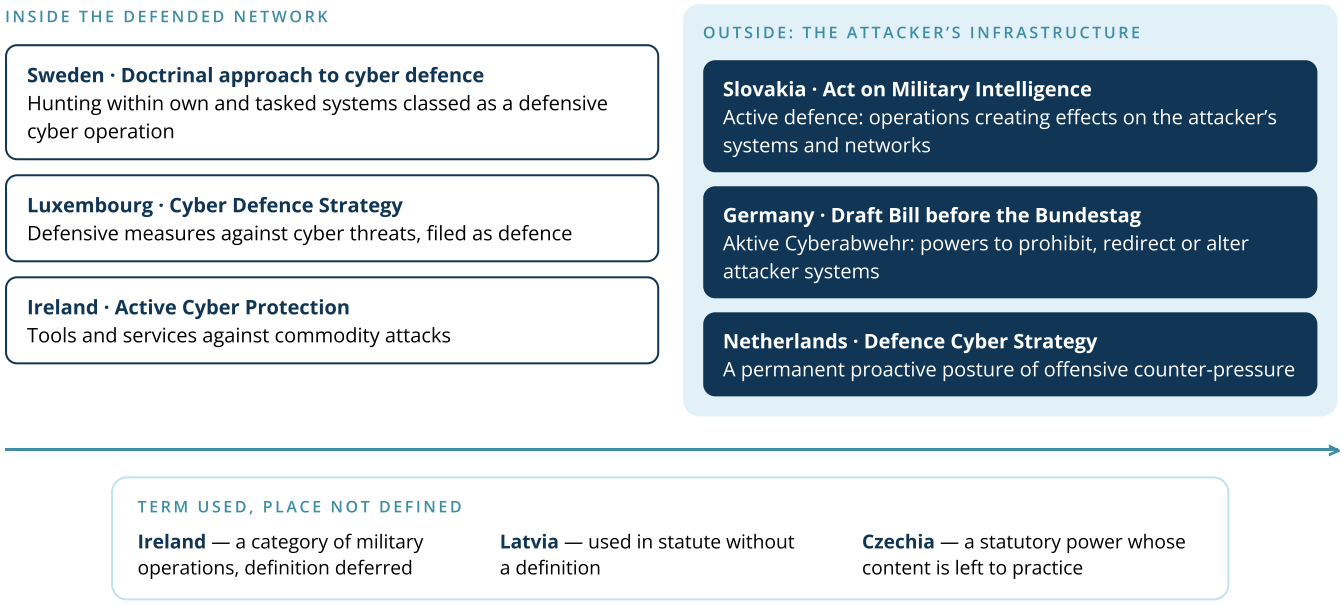
1. Frame active cyber defence by conduct and constraint, not the label, with a shared vocabulary
2. Develop the EU Declaration on international law; twelve states to publish a national position
3. Each state declares its legal basis, targets and term; the EU maintains a shared matrix
4. Specify joint capabilities by function, recording authority and oversight in advance

Funded by European Union
Implemented by euiss European Union Institute for Security Studies

One term, both sides of the perimeter

The EU's own texts leave 'active cyber defence' open, and the member states that use the term place it on **opposite sides of the network perimeter**. Figure 1 sets national usages on one axis, from inside the defended network to the attacker's infrastructure. The same conduct — hunting for an adversary inside one's own networks — is plainly defensive in Sweden's doctrinal approach, while Slovakia's statute reserves active defence for effects on the attacker's systems.

FIGURE 1 Where member state texts place the activity



Source: authors, from the national texts discussed in Sections 3.5, 5.2 and 7.2.

One family of activity, many names

National terms in fifteen languages name different cells of the same space — locus, trigger, effect and register — yet are exchanged as synonyms. **Officials who agree on active cyber defence may agree on less than they think.**

lutte informatique offensive · *offensief tegendruk* · *aktive Cyberabwehr* · *pełne spektrum* · *Computer Network Operations* · *offensiva cyberoperationer* · *aktívna obrana* · *aktivní zásah* · *atividade ofensiva* · *aktīvā kiberaizsardzība* · *proaktivno in stalno odzivanje* · *capabilități de răspuns ofensiv*

BENEATH THE TERMS: THE COMMON GROUND

1 **Normative floor**
International law applies, in every published position.

2 **Legal pairing**
No out-of-network activity without a legal frame.

3 **Military default**
Twelve of nineteen published authority bases are military.

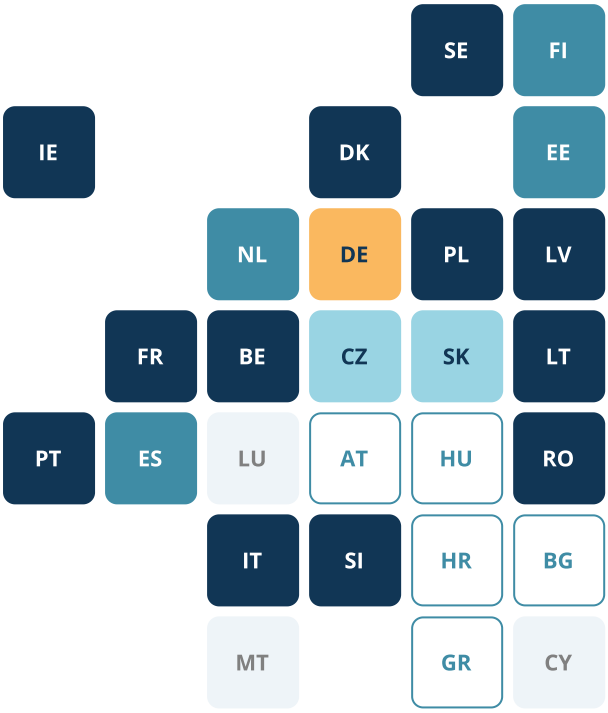
4 **Reactive triggers**
Only the Netherlands publishes a standing posture; every other trigger is conditional or procedural.

5 **Institutions**
Cyber commands built across every group.

Who acts, and under which law

Figure 2 codes each state by the legal family governing action beyond its own networks — the question on which states say most and differ most. **Military authority is the default**; the exceptions are deliberate institutional choices with consequences for oversight.

FIGURE 2 Legal authority for action beyond national networks



12 **Military law or doctrine**
France, Romania, Poland, Italy, Denmark, Lithuania, Portugal, Sweden, Ireland, Latvia, Slovenia, Belgium

4 **Hybrid: intelligence and military**
The Netherlands, Estonia, Finland, Spain

2 **Military intelligence law**
Czechia, Slovakia — statutory conditions, prior ministerial consent

1 **Police law, bill pending**
Germany; an intelligence-services bill is also pending

5 **Unit named, legal family not published**
Austria, Bulgaria, Croatia, Greece, Hungary

3 **No acting body published**
Cyprus, Luxembourg, Malta

Schematic tile map, one tile per member state. Belgium is coded on its Cyber Strategy for Defence (2019) and Strategic Vision 2025, which give the military cyber capability an offensive mandate. Source: authors, Section 5.1 and Annex A.

Three models, three oversight architectures

Three models stand out, each with one clear exemplar. Figure 3 shows how the legal basis decides **who acts and who reviews**; a joint operation spanning the three would run under all three architectures at once.

FIGURE 3 One activity, three legal families

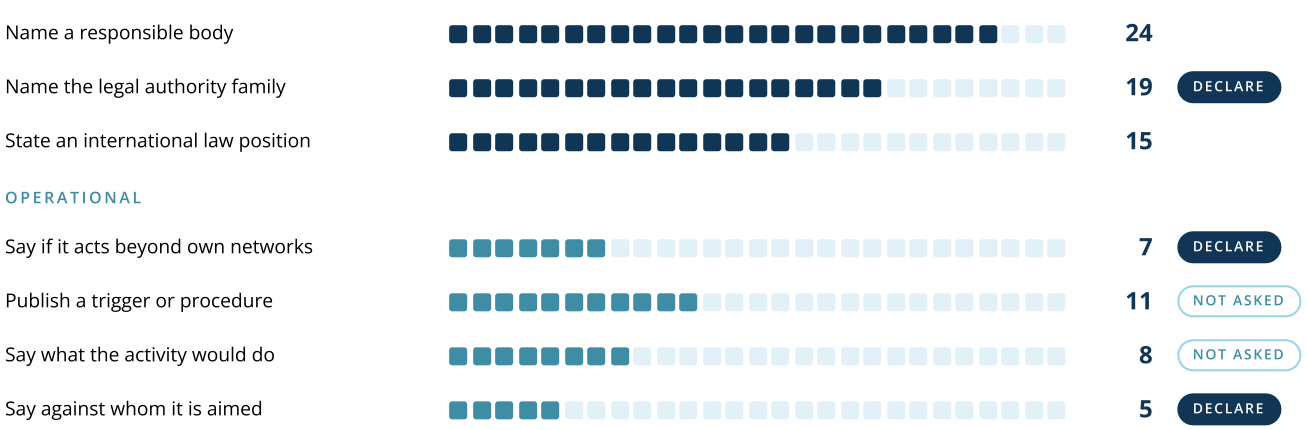
	MILITARY MODEL France Doctrine published 2019	INTELLIGENCE-ENABLED MODEL The Netherlands Temporary Act 2024, strategy 2025	POLICE-LAW MODEL Germany Bill at first reading, June 2026
WHO ACTS	**Armed forces, through a joint cyber command** Offensive cyber operations as published doctrine	**Intelligence and security services** Under intelligence statutes; a permanent proactive posture	**Federal police and Federal Criminal Police Office** Under hazard prevention law, against attacker infrastructure
WHO REVIEWS	**Executive authority** International law position published separately	**A rebuilt oversight architecture** Adjusted by the Temporary Act, not new powers	**Judicial safeguards of police powers** Engages the constitutional allocation of competences
FOLLOWERS	**Romania, Italy, Denmark, Poland, Portugal, Sweden** Same institution and register; Portugal and Sweden publish fuller statements, the others less	**Slovakia and Czechia** In military intelligence law; UK National Cyber Force outside the EU	**None yet** Its future rests with the Bundestag

Source: authors, Section 6.

A pattern of disclosure

Figure 4 counts the states whose documents answer each question. States readily say **which agency is responsible** and under which law; when the questions turn operational, the answers thin; these are the dimensions closest to operational planning.

FIGURE 4 Member states that publish an answer, of 27



One square, one member state. Trigger: one standing posture, five statutory or strategic conditions, five authorisation procedures; German bills counted. Source: authors, Section 7.3 and Annex A.

The minimum disclosure set

National security, including in the cyber domain, remains the sole responsibility of each member state, as noted in Article 4(2) TEU. As marked in Figure 4, together with a national position on international law (Recommendation 4), the EU can invite each state to **declare its legal authority basis**, which also answers whether it acts beyond its own networks, its **permissible target types** and, in one line, **the term it uses and what it covers**. Trigger, effect and specific locus are deliberately left out.

RECOMMENDATIONS: FOUR PRIORITIES FOR THE EU

9.1 · NARRATIVE
Responsible state behaviour
1 Adopt a shared vocabulary annex
2 State the common ground collectively

9.2 · INTERNATIONAL LAW
The EU Declaration
3 Apply the rule on labels; develop the sovereignty threshold
4 Twelve states: publish a national position

9.3 · COORDINATION
An EU-level mechanism
5–7 Declare legal basis, target types and vocabulary
8 Ask the Cyber Census for facts
9 Maintain a shared EU matrix

9.4 · CAPABILITIES
Joint development
10 Specify by function, locus and effect
11 Record authority and oversight first

ABOUT THE AUTHORS

Dr Andrea Calderaro
Director, EU Cyber Direct
EU Institute for Security Studies (EUISS)
Contact: Andrea.Calderaro@iss.europa.eu

Marius Houwen
Deputy Director, EU Cyber Direct
EU Institute for Security Studies (EUISS)
Contact: Marius.Houwen@iss.europa.eu

Scan to download the full report

SUGGESTED REFERENCE

Calderaro, Andrea & Houwen, Marius (2026) *Defining 'Active Defence' in Cyberspace: A Comparative Analysis of EU Member States: Concepts, Doctrines and Legal Frameworks*. Research paper, EU Cyber Direct, October 2026. ISBN 978-92-9462-531-1 · DOI 10.2815/7785192

EU CYBER DIRECT
The EU Cyber Diplomacy Initiative

Funded by European Union

Implemented by euiss European Union Institute for Security Studies