EU CYBER DIRECT

RESEARCH PAPER

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 · October 2026

Authors

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

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

About EU Cyber Direct

EU Cyber Direct – the EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen the rules-based order in cyberspace and build cyber resilient societies. To that aim, the programme conducts research, supports capacity building in partner countries, and promotes multistakeholder cooperation. EU Cyber Direct is implemented by the EU Institute for Security Studies and is funded by the European Union.

Acknowledgements. The authors are grateful to the national authorities of EU member states that reviewed and commented on the draft record of their state's published position, and to the European External Action Service (EEAS) for its guidance and feedback. These contributions have been critical to improving the completeness of this study. The authors also thank Adolfo Moreira for his comments and support.

Disclaimer. The authors alone are responsible for the text and for any inaccuracies that may remain.

Revised edition. Some entries have been clarified and amended following further validation and review of primary sources.

SUGGESTED CITATION

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.

This publication has been produced in the context of the EU Cyber Direct (EU Cyber Diplomacy Initiative) project with the financial assistance of the European Union. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or any other institution.

ISBN 978-92-9462-531-1 · Catalogue number QN-01-26-009-EN-N · DOI 10.2815/7785192

Reproduction is authorised provided the source is acknowledged.

Executive summary

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

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

- **First: we do not lack a definition of active cyber defence, but we have many, carrying several meanings that are each authoritative in its own setting, resulting in the absence of a commonly shared and consistent approach to it.** While the CCDCOE places active cyber defence outside the defended networks, United States doctrine places it inside them, and the United Kingdom uses the label for a domestic programme against everyday cybercrime. In contrast, NATO doctrine does not recognise the category at all. The same split recurs inside the EU: Slovakia defines active defence in statute, on the CCDCOE side of the line, while Ireland names it as a category of military operations without defining it. Around the term has grown a lexicon of hunt forward, persistent engagement, defend forward and national coinages in fifteen languages. These terms name different aspects of the same activity, yet they are often exchanged as synonyms. Officials who agree on active cyber defence may agree on less than they think.
- **Second: member states approach active cyber defence on their own terms, both in how they define it and in where they place it institutionally.** We cluster these approaches across three different models: a ***military model*** with France as its clearest exemplar, an ***intelligence-enabled model*** exemplified by the Netherlands, and a ***police-law model*** which Germany is now legislating and no other member state has attempted. Romania, Italy, Denmark, Poland and Belgium resemble the French model in vocabulary but publish less, while Portugal and Sweden have published fuller statements of what their military cyber operations are for. Slovakia and Czechia place active measures in military intelligence law, with statutory conditions for their use. Spain, Lithuania and Ireland have built institutions ahead of published doctrine, Spain within a hybrid arrangement in which a civil National Cybersecurity Council chaired by the Director of its intelligence service coordinates alongside the military command and the term active cyber defence is used in a protective sense, and Latvia and Slovenia place active or proactive capabilities within military or defence structures but publish little about their operational parameters. Estonia and Finland frame their approach around resilience while pursuing assertive legal diplomacy. Eight member states have yet to publish a position on active cyber defence. One pattern runs through all of them: states readily say which agency is responsible and which vocabulary they use, and understandably say less about where, when, against whom and to what effect they would act.
- **Third**: **member states agree on more than their differences over definitions and institutional placement suggest.** Every published position accepts that international law applies, and no state describes out-of-network activity without binding it to a legal frame in the same document. Military authority is the default, and every published trigger other than the Dutch standing posture is reactive, conditional or procedural. What differs is legal architecture rather than vocabulary, since materially similar activity sits under military, intelligence or police law depending on the state, each with its own oversight.

Drawing on these outcomes, the study concludes that the EU does not need to harmonise capability postures, which remain the sole responsibility of each member state under Article 4(2) TEU. It needs a small set of shared reference points: a minimum disclosure set, a shared vocabulary annex and standing declarations by each member state of the legal basis and the permissible targets of any operations beyond its own networks. The study also finds that reading national cybersecurity strategies alone understates what defence establishments publish, since these concepts sit more often in defence doctrine and in statutes.

Key findings

The 2022 Joint Communication asks member states to invest in active defence capabilities but does not define the term. This study maps how member states approach it, through seven questions: authority, register, locus, target, trigger, effect and legal position.

KEY FINDINGS

1 **Many definitions, none shared.**
The CCDCOE places active cyber defence outside the defended network, United States doctrine places it inside, the United Kingdom applies the label to a domestic programme against cybercrime, and NATO doctrine does not use the category. Related terms – hunt forward, persistent engagement, defend forward and national coinages in fifteen languages – are often used as synonyms. Agreement on the term can mask disagreement on substance.

2 **Three models, each with one clear exemplar.**
A military model (France), an intelligence-enabled model (the Netherlands) and a police-law model (Germany, pending the Bundestag). Most other member states resemble one of them, have built a cyber command before publishing doctrine, or have published no position. States say readily who acts and what they call it; they say far less about where, when, against whom and to what effect.

3 **More common ground than the definitions suggest.**
Every published position accepts that international law applies, and none describes action beyond its own networks without a legal frame. Military authority is the default, and every published trigger other than the Dutch standing posture is reactive, conditional or procedural. The real difference is legal architecture: similar activity sits under military, intelligence or police law, each with its own oversight.

8 of 27
member states have published no position on active cyber defence

15 of 27
have published a national position on international law in cyberspace

19 of 27
publish the legal basis that governs operations beyond their own networks

WHAT THE EU NEEDS

Not harmonised capability postures, which under Article 4(2) TEU remain the responsibility of each member state, but a small set of shared reference points:

- a minimum disclosure set;
- a shared vocabulary annex for EU cyber defence documents;
- standing declarations by each member state of the legal basis and permissible targets of any operations beyond its own networks.

The three models: overview on p. 51, detail in Section 6 · Recommendations: action table on p. 59, detail in Section 9

Contents

Executive summary 3

Key findings 4

List of figures and tables 7

Abbreviations 8

1. Introduction 9

1.1 The policy context 9

1.2 Defining active cyber defence 10

1.3 Study structure 11

2. Research design 12

2.1 Methodology 12

2.2 The analytical dimensions 12

2.3 Conventions of comparison 13

PART I Defining the term: external authorities and related vocabulary 14

3. One term, four diverging reference points 15

3.1 The CCDCOE: outside the defended infrastructure 15

3.2 The United States: inside the network, in real time 16

3.3 The United Kingdom: a domestic protective programme 16

3.4 NATO: no middle category codified 16

3.5 Inside the European Union: the same split in national texts 17

4. The wider lexicon: one family of activity, many names 18

PART II Mapping member states' positions 22

5. Mapping concepts, doctrines and legal frameworks 23

5.1 Authority: institutional and legal basis 24

5.1.1 France: the military model 25

5.1.2 The Netherlands: the intelligence-enabled model 26

5.1.3 Germany: three legal routes at once 27

5.1.4 Romania: the statutory route 29

5.1.5 Military and mixed authority elsewhere: Poland, Italy, Denmark, Spain, Lithuania, Portugal and Sweden 30

5.1.6 The hybrid and intelligence cases, and the states that publish no concept 34

5.2 Register: how states name the activity 37

5.3 Locus and target: where and against whom 40

5.4 Trigger: when action is authorised 42

5.5 Effect: what the activity is intended to do 43

5.6 Legal position: reconciliation with international law 44

PART III Three models of active cyber defence in the Union 46

6. The models 47

The three models at a glance 51

PART IV What this means for the European Union 52

7. Convergence, divergence, and a pattern of disclosure 53
- 7.1 Where the member states converge 53
- 7.2 Where they diverge, and where it matters 54
- 7.3 A pattern of disclosure 55
- 7.4 The minimum disclosure set 56

8. Conclusions and limitations 57
- 8.1 Limitations and items pending verification 57

Recommendations at a glance 59

9. Recommendations 60
- 9.1 A narrative of active cyber defence within responsible state behaviour 60
- 9.2 The EU Declaration on the application of international law 61
- 9.3 A cooperation and coordination mechanism at EU level 62
- 9.4 Joint development and procurement of cyber defence capabilities 63

References 65

Annex A. The authors' working matrix 71

Annex B. Descriptive comparative matrix 74

Annex C. Primary sources by state 77

List of figures and tables

TABLES

Table 1 The seven analytical questions and the terms used to describe them 13

Table 2 The lexicon: terms in circulation and what each one names 20

FIGURES

Figure 1 One term, defined on both sides of the network perimeter 17

Figure 2 The published record, state by state and question by question 23

Figure 3 How many member states answer each question 24

Figure 4 Who acts: the legal family of the acting body 25

Figure 5 How member states name the activity 37

Figure 6 Where member states say they would act, and against whom 41

Figure 7 When action is authorised: distinct kinds of answer 43

Figure 8 What the activity is described as doing 44

Figure 9 National positions on international law in cyberspace 45

Figure 10 The published instruments, 2019 to 2026 48

Figure 11 Where the concepts are published 49

Figure 12 Three legal families, and who oversees each 55

Abbreviations

ACD	Active cyber defence
ACN	Agenzia per la Cybersicurezza Nazionale (Italy)
AIVD	Algemene Inlichtingen- en Veiligheidsdienst (Netherlands)
AJP	Allied Joint Publication (NATO)
ANSSI	Agence nationale de la sécurité des systèmes d'information (France)
BfV	Bundesamt für Verfassungsschutz (Germany)
BKA / BKAG	Bundeskriminalamt / Bundeskriminalamtgesetz (Germany)
BMI	Bundesministerium des Innern (Germany)
BND	Bundesnachrichtendienst (Germany)
BPolG	Bundespolizeigesetz (Germany)
BSI	Bundesamt für Sicherheit in der Informationstechnik (Germany)
CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CEMA	Chef d'état-major des armées (Chief of the Defence Staff, France)
CNO	Computer Network Operations (Denmark)
CNSSI	Committee on National Security Systems Instruction (US)
COMCYBER	Commandement de la cyberdéfense (France)
CTIVD	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (Netherlands)
DCO / OCO	Defensive / offensive cyberspace operation (NATO)
DCO-RA	Defensive cyberspace operation response action (US)
DCS	Defensie Cyberstrategie (Netherlands)
DNSC	Directoratul Național de Securitate Cibernetică (Romania)
FE	Forsvarets Efterretningstjeneste (Denmark)
GG	Grundgesetz (Germany)
IHL	International humanitarian law
KSC	Krajowy System Cyberbezpieczeństwa (Poland)
L2I	Lutte informatique d'influence (France)
LID / LIO	Lutte informatique défensive / offensive (France)
MApN	Ministerul Apărării Naționale (Romania)
MCCE	Mando Conjunto del Ciberespacio (Spain)
MIVD	Militaire Inlichtingen- en Veiligheidsdienst (Netherlands)
NCF	National Cyber Force (UK)
NCKO	Národní centrum kybernetických operací (Czechia)
NCSC	National Cyber Security Centre (UK)
NIST	National Institute of Standards and Technology (US)
SCEPVA	Sovereign Cyber Effects Provided Voluntarily by Allies (NATO)
SIS	Secret Intelligence Service (UK)
SRI	Serviciul Român de Informații (Romania)
TEU	Treaty on European Union
TIB	Toetsingscommissie Inzet Bevoegdheden (Netherlands)
USCYBERCOM	United States Cyber Command
Wbnv	Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Netherlands, draft)
WOC	Wojska Obrony Cyberprzestrzeni (Poland)

1. Introduction

1.1 The policy context

The 2022 Joint Communication on an EU Policy on Cyber Defence states: 'Member States must [...], with urgency and priority, commit to increase investments in full-spectrum cyber defence capabilities, including active defence capabilities. Whilst remaining fully committed to international law and norms in cyberspace, the EU should signal its willingness to use these capabilities in a coordinated way in case of a cyberattack on a Member State'.[1] Similarly, the Council Conclusions that followed call for 'full-spectrum defensive cyber defence capabilities' and encourage 'proactive defensive measures to protect, detect, defend and deter against cyberattacks', while recalling that 'national security, including in the cyber domain, remains the sole responsibility of each Member State, as noted in article 4(2) TEU'.[2] Finally, the more recent EU stocktaking instrument, including the public executive summary of the EU Cyber Census 2025, released in February 2026, tracks implementation of the Policy and does not define active cyber defence either, as one would expect of a tracking exercise. The full Census is EU classified information, a limit recorded in Section 8.[3] While these documents provide clear strategic guidance to strengthen active cyber defence across EU member states, they do not provide a clear definition of what the EU means by it, nor guidance on how it can be operationally achieved.

The absence of a shared definition has not prevented member states from responding to the call by approaching active cyber defence through their own understanding of the term. That diversity is a strength to build on, and it makes a shared reference point all the more useful. In the two years to September 2026 the Netherlands presented a defence cyber strategy announcing a permanent proactive posture of offensive counter-pressure, Germany brought a bill before the Bundestag that would give federal police powers to disrupt attacker infrastructure and opened a constitutional debate in doing so, before introducing a second bill for its intelligence services, and the reference point that European debate has long relied on, the American posture of defending forward, was itself the subject of contested reporting about a stand-down that the Pentagon denied on the record and that a member of Congress later described as a one-day pause.

The words themselves add a further layer. The same family of activity travels under hunt forward, defend forward, persistent engagement, offensive counter-pressure, active cyber defence and a dozen national terms, and these are not competing definitions of one concept but names for different aspects of it. Fixing one term would therefore not settle the matter. The study instead states what each member state has actually said, compares those statements on the same questions, and draws out what the EU can realistically ask of its members as a result.

1 European Commission, & EU High Representative for Foreign Affairs and Security Policy. (2022). Joint communication to the European Parliament and the Council: EU policy on cyber defence (JOIN(2022) 49 final), Introduction. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022JC0049

2 Council of the European Union. (2023). Council conclusions on the EU policy on cyber defence (9618/23), paras. 4, 18. https://www.consilium.europa.eu/media/64526/st09618-en23.pdf

3 European Commission, & EU High Representative for Foreign Affairs and Security Policy. (2026). EU Cyber Census 2025: Executive summary (SWD(2025) 423). Publicly released 20 February 2026, full report EU classified information.

1.2 Defining active cyber defence

The definitional debate is not new. Since at least 2012, when Kesan and Hayes[4] set out the first systematic legal taxonomy of active-defence measures, both the research and policy communities have tried to draw a stable line between passive defence, active cyber defence and offence, notably Lachow[5] and Denning,[6] later with Strawser,[7] by analogy with active air and missile defence, and the Center for Cyber and Homeland Security,[8] which insisted that 'active defense is not synonymous with "hacking back"'. None of these settled the question. Dewar,[9] writing for a CyCon conference itself themed on active cyber defence, opened from the field's 'ill-defined concepts and inconsistently applied terminology' and offered a definition that is itself instructive for our seven analytical questions, because it straddles the locus line on which the later authorities divide: 'ACD is defined here as the proactive detection, analysis and mitigation of network security breaches in real-time combined with the use of aggressive countermeasures deployed outside the victim network'.[10] On the platform commissioning the present study, Herpig and Kuehn[11] argued directly that 'The EU must define what it understands as active cyber defence and how it relates to other cyber policy issues', and Bendiek and Bund[12] have since documented the European shift towards active postures while the legal and political powers for their use remain ill-defined. Against this lineage, the present study claims three things the prior work does not do. It reads the published concepts of all EU member states, document by document, against the same seven analytical questions. It identifies a consistent pattern in what states choose to publish and what they leave unpublished. And it shows, in Section 7, that no state describes action beyond its networks without binding it to a legal frame. In short, the study takes a familiar problem, documents it state by state from the primary record, and points to what can be done about it.

Our approach is likewise complementary to the organisational typology used in the comparative literature. Blessing[13] classifies national cyber forces by organisational structure, distinguishing subordinated, sub-unified and unified models across branch, service and joint forms, and this typology underpins the CCDCOE's comparative work: Štrucl[14] applies it to NATO member states, and the CCDCOE's 2025 study extends the analysis, stating that it 'provides a thorough analysis of cyber force development across all 32 NATO member states, emphasising their distinct methodologies for establishing, organising, and integrating cyber units within their respective military and defence structures'.[15] Those instruments classify how forces are organised, and

4 Kesan, J. P., & Hayes, C. M. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace. Harvard Journal of Law & Technology, 25(2), 429-543.

5 Lachow, I. (2013). Active cyber defense: A framework for policymakers. Center for a New American Security.

6 Denning, D. E. (2014). Framework and principles for active cyber defense. Computers & Security, 40, 108-113.

7 Denning, D. E., & Strawser, B. J. (2017). Active cyber defense: Applying air defense to the cyber domain. In G. Perkovich & A. E. Levite (Eds.), Understanding cyber conflict: Fourteen analogies. Georgetown University Press.

8 Center for Cyber and Homeland Security. (2016). Into the gray zone: The private sector and active defense against cyber threats. George Washington University.

9 Dewar, R. S. (2014). The 'triptych of cyber security': A classification of active cyber defence. In Proceedings of the 6th International Conference on Cyber Conflict (CyCon) (pp. 7-21). NATO Cooperative Cyber Defence Centre of Excellence.

10 Dewar (2014).

11 Herpig, S., & Kuehn, A. (2022, February 25). The EU and responsible active cyber defence. Directions (EU Cyber Direct).

12 Bendiek, A., & Bund, J. (2023). Shifting paradigms in Europe's approach to cyber defence (SWP Comment 2023/C 48). Stiftung Wissenschaft und Politik; Bendiek, A., & Bund, J. (2024). Hardening norms and networks: Europe's cyber defence posture. Intereconomics, 59(4), 198-203.

13 Blessing, J. (2021). The global spread of cyber forces, 2000-2018. In 2021 13th International Conference on Cyber Conflict (CyCon). NATO Cooperative Cyber Defence Centre of Excellence.

14 Štrucl, D. (2021). Comparative study on the cyber defence of NATO member states. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

15 NATO Cooperative Cyber Defence Centre of Excellence. (2025). The evolution of cyber forces in NATO countries. https://ccdcoe.org/uploads/2025/07/The_evolution_of_cyber_forces_in_NATO_countries.pdf

Smeets[16] addresses the adjacent question of how such capability is integrated once built. Our seven analytical questions ask what states say the activity is: where, when, under whose authority, to what effect, in which words, against whom, and under which legal position. A state can be fully classified organisationally while having answered none of our questions, which is precisely the situation of the states that have built commands before publishing doctrine, described in Section 6.

1.3 Study structure

The study addresses four research questions: 1) What do member states mean when they use, or avoid, the term active cyber defence? 2) Where do their published approaches converge, and where do they differ? 3) What does the absence of a published position in many member states imply for cooperation? 4) What could a common framework realistically ask of member states?

Section 2 sets out the methodology we adopted to answer them, including the sources, the seven analytical questions used as a lens to read each state's position, and the conventions of comparison. The study also tested its preliminary outcomes: they were presented to member states, which were invited to respond to a validation survey.

The findings then follow in four parts. Part I (Sections 3 and 4) examines the word itself, through the four reference authorities and the wider lexicon. Part II (Sections 5.1 to 5.6) sets out what member states say. It is organised by the seven analytical questions rather than by country, so that each state appears where its choice is most revealing. Part III (Section 6) groups the material into three models and shows how the remaining states relate to them. Part IV (Sections 7 to 9) draws out what this means for the EU, states the conclusions and their limits, and sets out recommendations for the actors able to act on them.

The proposed working matrix, on which the comparison rests, is in Annex A. Annex B gives the descriptive matrix and Annex C the primary sources by state.

16 Smeets, M. (2018). Integrating offensive cyber capabilities: Meaning, dilemmas, and assessment. Defence Studies, 18(4), 395-410.

2. Research design

2.1 Methodology

The study rests on a reading of primary documents for all twenty-seven member states and four non-EU reference points. These include national cybersecurity and defence cyber strategies, military doctrine, statutes and bills, founding orders of cyber commands, ministerial statements to parliament, and formal national positions on international law in cyberspace. We read them in the original languages wherever they exist, and every foreign-language passage quoted in this study is given verbatim, with our own translation marked as such. Reading published national positions as the evidentiary base, rather than as declaratory gloss, follows the approach taken in the legal literature on state practice in cyberspace.[17]

The analysis proceeded in five stages. The first was an initial mapping. The second was a full re-verification of every claim against the primary text. The third was a test designed to falsify our own central claim and to close gaps through searches in the national languages. The fourth was a review that tested the argument against the prior literature and the most recent EU documents, including the public executive summary of the EU Cyber Census 2025. The fifth was a validation stage, in which the preliminary outcomes were presented to member states, which were invited to respond to a validation survey. The desk stages were complemented by a targeted re-sweep of national legislation portals and armed forces websites, since concepts of this kind are set out in defence doctrine and in statutes more often than in national cybersecurity strategies. Claims that rest on a secondary source, or that could not be verified, are identified as such in the text and again in Section 8, and are not presented as established.

2.2 The analytical dimensions

Rather than begin from any one definition of active cyber defence, which would have prejudged the comparison, we put the same seven analytical questions to each state's documents. Each question corresponds to one dimension of the activity, and together they cover the legal and operational parameters that states need to clarify before they can act together. Table 1 defines the terms used throughout the study and explains why each dimension was chosen.

17 Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent state practice. American Journal of International Law, 112(4), 583-657.

TABLE 1

The seven analytical questions and the terms used to describe them

The same seven questions were put to every state's documents, in the order in which Part II discusses them. Together they cover the legal and operational parameters that states need to clarify before they can act together.

term Widely published term Less often published

TERM	QUESTION	WHAT THE TERM COVERS	WHY WE ASK IT
Authority 19 states	**Who acts, and under which body of law?**	Military, intelligence, police, or a combination	It determines which body oversees the activity and whether prior authorisation or review after the fact applies
Register 27 states, 19 stated	**What vocabulary does the state choose?**	The word offensive, a qualified term such as active or proactive, neutral operational language, purely defensive language, or nothing at all	It shows how a state chooses to present the activity and, as Section 5.2 shows, it is a poor guide to reach
Locus 7 states	**Where does the state say it will act?**	Within its own networks, within partner networks by consent, or in the infrastructure of an adversary or a third party	It is the line on which the four reference authorities divide (Section 3), and it decides whether sovereignty is engaged
Target 5 states	**Against whom is the activity directed?**	State actors, criminal infrastructure, or any system from which an attack originates	It decides whether an operation is law enforcement or interstate conduct, and what escalation risk it carries
Trigger 11 states	**When is action authorised?**	In reaction to an incident, pre-emptively against an imminent threat, or as a standing posture in peacetime	It separates reactive from persistent postures, and it is the parameter closest to operational secrecy
Effect 8 states	**What is the action described as doing?**	Protecting, disrupting or destroying	It shows whether the activity is defensive in practice, whatever it is called
Legal position 15 states	**What has the state said about the international law that governs action beyond its own networks?**	In particular, whether it treats sovereignty as a rule whose breach is a wrongful act	It fixes the legal frame that applies to any operation beyond national networks

Reading the table. Filled terms mark the dimensions that member states publish widely, outlined terms those that fewer publish. Counts are the member states whose published documents answer each question, as in Figure 3, and include Germany's pending bills. The register count covers all twenty-seven: nineteen state a vocabulary and eight have no published position, which is counted as their answer. **Source:** authors, from the working matrix in Annex A.

EU CYBER DIRECT

2.3 Conventions of comparison

Comparative reading of this kind rests on a small number of conventions, which are stated here so that the comparison can be checked against the sources. A document's use of the word offensive is treated as evidence about vocabulary, not about what the capability does. A state whose documents contain the label but describe no actions is recorded as having adopted the label. A state's stated right to respond to unlawful cyberattacks is treated as a legal position, not as an operational trigger, since the two answer different questions. A ministry webpage is treated as a published position but not as doctrine, and the distinction is made explicit in each case. Where a state's documents point in different directions, as Estonia's do, with a resilience-first strategy alongside assertive legal diplomacy, both are described. Where a primary text cannot be retrieved, the state is not characterised on the substantive questions, although institutional facts are recorded where they rest on official statements. The first edition applied this rule to Belgium; this revised edition reads Belgium's Cyber Strategy for Defence and its national Cybersecurity Strategy 2.0 and codes Belgium on that basis. The absence of a published position is

treated as a finding in its own right, with a document that was read and found silent distinguished from a document that could not be obtained. The working matrix in Annex A records the outcome for each state and each question.

PART I

Defining the term: external authorities and related vocabulary

3. One term, four diverging reference points

KEY FINDINGS

1. The four reference authorities disagree on where the activity takes place: the CCDCOE places active cyber defence outside the defended network, United States doctrine inside it, the United Kingdom uses the label for a domestic protective programme, and NATO doctrine has no such category.
2. The same split recurs in national texts inside the Union, so no single meaning is inherited and the EU has room to develop one that suits its own legal order.

We do not lack definitions of active cyber defence, but we can draw on an abundance of them, generating a scattered approach to it. Four reference authorities, the CCDCOE, the United States, the United Kingdom and NATO, use the term, or decline to, in ways that differ on the decisive question of where the activity takes place. None is an EU institution, yet each is a reference point that European debate draws on.

Four bodies of definition are compared here: the glossary of the NATO Cooperative Cyber Defence Centre of Excellence, the United States government glossary maintained by NIST, the United Kingdom's National Cyber Security Centre, and NATO's allied joint doctrine. They are not authorities in the legal sense. None of them binds the Union or its member states, and the EU has adopted none of them. They are treated as the reference definitions for three practical reasons. The first is that they are the definitions European practitioners actually reach for. The Centre of Excellence hosts the Cyber Law Toolkit, whose glossary builds on the Tallinn Manual process on which member states draw, and whose collection of national positions Section 5.6 partly relies on, and NATO's definitions sit in doctrine that twenty-three of the twenty-seven member states have adopted as allies, with their national reservations recorded in the same document. The second is that they are the source of the vocabulary in circulation: defend forward, hunt forward, persistent engagement and active cyber defence all enter European debate from the American and British usages set out below, and EU and national documents borrow them without importing their definitions. The third is that each of the four has written its definition down in a stable and citable form, which is what makes the differences between them demonstrable rather than a matter of impression. The four also happen to cover the Union's principal operational partners, so the divergence between them is not academic: it is the divergence a member state meets when it plans with NATO, with Washington or with London. The sections below take them in turn.

3.1 The CCDCOE: outside the defended infrastructure

The CCDCOE Cyber Law Toolkit glossary, which builds on the Tallinn Manual 2.0 glossary,[18] defines active cyber defence as 'The taking of proactive defensive measures outside the defended cyber infrastructure. A hack-back is a type of active cyber defence'.[19] It defines hack-back as 'A type of active cyber defence, the main purpose of which is to take action against an identified source of a malicious cyber operation. Typically, a hack-back is designed to mitigate the effects of, or stop, the malicious activity, or to gather technical evidence that can be used for attribution purposes', and passive cyber defence as a measure 'that does not involve launching a preventive, pre-emptive, or counter-operation against the source'.[20] On this account, the defining feature of

18 Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations (2nd ed.). Cambridge University Press.

19 NATO Cooperative Cyber Defence Centre of Excellence. (n.d.-a). Glossary. International cyber law: Interactive toolkit. https://cyberlaw.ccdcoe.org/wiki/Glossary

20 CCDCOE (n.d.-a).

active cyber defence is precisely that it reaches beyond one's own networks.

3.2 The United States: inside the network, in real time

United States terminology inverts this. The glossary maintained by NIST, sourcing the Committee on National Security Systems glossary CNSSI 4009-2022, defines active cyber defense as a 'Synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities'.[21] Action outside one's own networks carries a different name: a defensive cyberspace operation response action (DCO-RA) comprises 'Deliberate, authorized defensive measures or activities taken outside of the defended network to protect and defend Department of Defense (DoD) cyberspace capabilities or other designated systems'.[22] The activity the CCDCOE calls active cyber defence is thus, in United States usage, not active cyber defense at all.

3.3 The United Kingdom: a domestic protective programme

The United Kingdom attaches the label to something different again. Active Cyber Defence is the name of an NCSC programme whose stated aim is to 'Protect the majority of people in the UK from the majority of the harm caused by the majority of the cyber attacks the majority of the time', through services aimed at 'high-volume commodity attacks' rather than 'the highly sophisticated and targeted attacks'.[23] The state operating one of Europe's most developed offensive cyber institutions reserves 'active cyber defence' for automated domestic protection.

3.4 NATO: no middle category codified

NATO doctrine contains no active cyber defence category. AJP-3.20, the Allied Joint Doctrine for Cyberspace Operations, defines a defensive cyberspace operation as 'Defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace' and an offensive cyberspace operation as 'Actions in or through cyberspace that project power to create effects which achieve military objectives'.[24] The boundary is drawn tightly: defensive operations 'protect networks and systems, and the information therein, for which NATO has been granted authorised access',[25] and any effects beyond such networks are created only through the Sovereign Cyber Effects Provided Voluntarily by Allies mechanism within operations approved by the North Atlantic Council.[26] The Alliance thus does not codify the intermediate category that EU policy language has opened up. This is not a judgment that the category is incoherent: scholarship reads NATO's binary, and the routing of effects beyond authorised-access networks through national contributions, as a pragmatic compromise reflecting Allies' unwillingness to pool offensive capability.[27]

Taken together, the four authorities place active cyber defence in different places: beyond the defended networks for the CCDCOE, inside them for the United States, in a domestic programme against everyday cybercrime for the United Kingdom, and nowhere for NATO, which leaves the middle ground uncodified. No

21 National Institute of Standards and Technology. (n.d.-a). Active cyber defense. In Computer Security Resource Center glossary. https://csrc.nist.gov/glossary/term/active_cyber_defense

22 National Institute of Standards and Technology. (n.d.-b). Defensive cyberspace operation response action. In Computer Security Resource Center glossary. https://csrc.nist.gov/glossary/term/defensive_cyberspace_operation_response_action

23 National Cyber Security Centre. (n.d.). Introduction to Active Cyber Defence. https://www.ncsc.gov.uk/section/active-cyber-defence/introduction

24 NATO Standardization Office. (2020). AJP-3.20: Allied joint doctrine for cyberspace operations (Edition A, Version 1), Lexicon. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

25 NATO Standardization Office (2020), para. 2.21.

26 NATO Standardization Office (2020), paras. 2.18, 2.23.

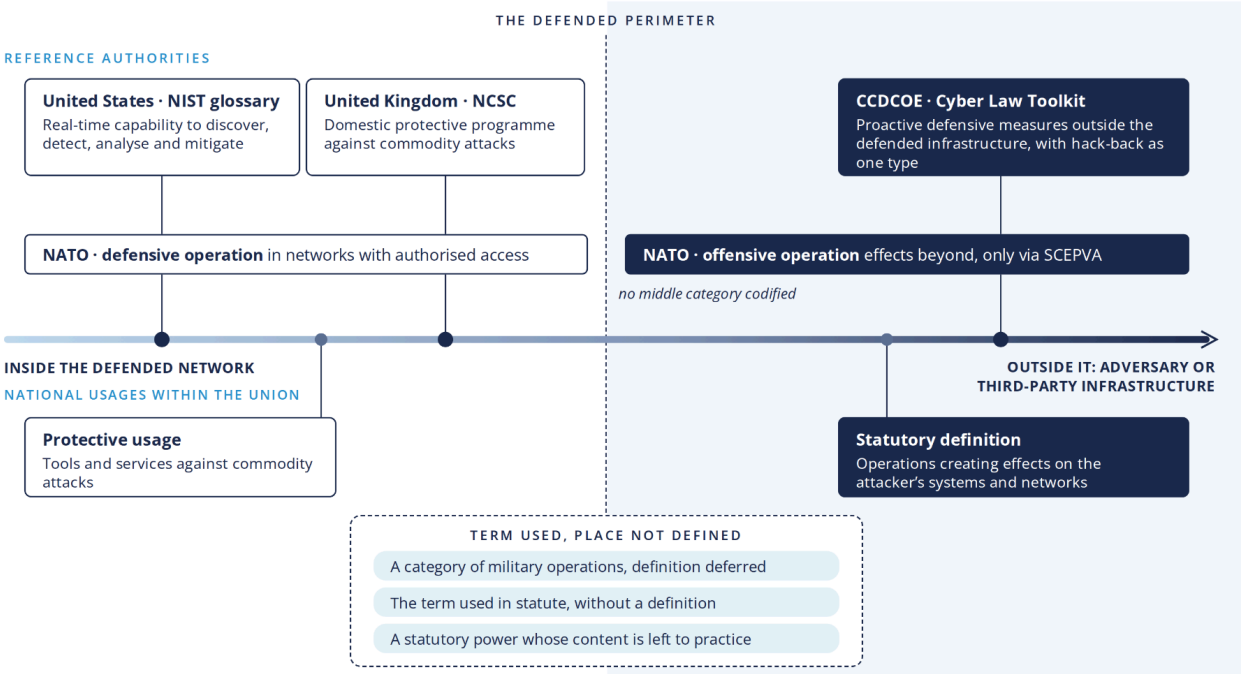
27 Jensen, M. S. (2022). Five good reasons for NATO's pragmatic approach to offensive cyberspace operations. Defence Studies.

single meaning is therefore inherited, and the EU has room to develop one that suits its own legal order. The line on which they divide is not merely terminological: activity conducted outside one's own networks cannot be read by its target as unambiguously defensive, which is why the question of where a state acts carries the weight it does.[28]

FIGURE 1

One term, defined on both sides of the network perimeter

> The reference authorities place active cyber defence on opposite sides of the perimeter, and the few national texts that use the term reproduce the same split.



Source: authors, from CCDCOE (n.d.-a), NIST (n.d.-a, n.d.-b), NCSC (n.d.), AJP-3.20 (2020) and the national texts discussed in Section 3.5. National usages are shown by type, not by state.

EU CYBER DIRECT

3.5 Inside the European Union: the same split in national texts

The variety is not confined to the reference authorities. It recurs inside the EU, in the few national texts that use the term at all. Slovakia is the only member state whose law defines active defence, and it defines it on the CCDCOE side of the line. The Act on Military Intelligence of 2022 gives the Cyber Defence Centre of the Slovak Republic, part of Military Intelligence and the national authority for cyber defence, a power of active defence, which it defines as a 'koordinovaný súbor aktivít, ktoré zahŕňajú detegovanie a analýzu kybernetických útokov a ak je to nevyhnutné, aj následnú reakciu, a to formou operácií vytvárajúcich účinky na útočníkove informačné systémy a siete s cieľom narušiť ich dostupnosť, dôvernosť alebo integritu' [coordinated set of activities comprising the detection and analysis of cyberattacks and, where necessary, a subsequent response in the form of operations creating effects on the attacker's information systems and networks with the aim of disrupting their availability, confidentiality or integrity; authors' translation].[29] Detection and analysis sit inside

28 Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust and fear between nations. Oxford University Press.

29 Národná rada Slovenskej republiky. (2022). Zákon č. 500/2022 Z. z. o Vojenskom spravodajstve [Act No. 500/2022 Coll. on Military Intelligence], adopted 29 November 2022, s. 7, s. 7(5). https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/500/

the definition, but what makes the activity active is the response against the attacker's own systems.

Ireland's Defence Forces leave the question open. Their Cyber Defence Strategy 2024 to 2027 names 'Active Cyber Defence' as one of three main categories of military cyberspace operations for the new Joint Cyber Operations Unit, alongside defensive cyberspace operations and cyberspace intelligence, surveillance and reconnaissance, but does not define it. The strategy's glossary defines instead 'Active Cyber Protection', whose purpose is to 'reduce the harm from commodity cyber-attacks by providing tools and services that protect from a range of attacks',[30] which is close in purpose to the United Kingdom programme described in Section 3.3. The same strategy makes definition a precondition of action, committing the Defence Forces to 'define and implement necessary governance and doctrine required prior to progressing cyberspace operations and active cyber defence'.[31] Latvia, as Section 5.2 records, uses the term in statute without defining it, and Czechia, as Section 5.1.6 sets out, authorises an 'aktivní zásah' [active intervention; authors' translation] in cyberspace without saying in the statute what such an intervention consists of, so that the only public account of its content is the government's description of one it carried out. Four member states therefore reproduce within the EU the variety that Sections 3.1 to 3.4 find among the reference authorities: a statutory definition that places the activity outside the defended network, a military category left undefined beside a protective service of the British type, a statutory use with no definition at all, and a statutory power whose meaning has been supplied by practice rather than by text. Figure 1 sets out both splits side by side.

4. The wider lexicon: one family of activity, many names

KEY FINDINGS

1. Hunt forward, persistent engagement, defend forward and national coinages in fifteen languages name different aspects of one family of activity, yet are often exchanged as synonyms.
2. A member state can answer the EU call for 'active defence capabilities' with internal detection, a takedown service or an out-of-network disruption capability, each supported by an authoritative glossary.

The four reference points are only part of the terminological picture. Around them has grown a wider lexicon in which materially overlapping activity travels under different names, each carrying its own political and legal register. Two United States concepts illustrate how finely the vocabulary slices. Persistent engagement 'shifts DOD and USCYBERCOM's posture in cyberspace from reactive to proactive', with the command stating that it 'actively seeks out threats in cyberspace and eliminates them'.[32] In the terms of our questions it names a moment, the permanent peacetime posture. Hunt forward operations, by contrast, name a locus: defensive teams deployed on a partner's networks at the partner's request, as when 'Estonian and U.S. cyber commands jointly conducted a defensive cyber-operation on Estonian Defence Forces' networks from September 23 to November 6' 2020,[33] with the Department of Defense committing that it 'will continue to conduct hunt forward operations to build cyber resiliency'.[34] A hunt forward operation is formally defensive and consensual, yet it

30 Defence Forces Ireland. (2024). Defence Forces cyber defence strategy 2024-2027. Óglaigh na hÉireann, July 2024. https://www.military.ie/

31 Defence Forces Ireland (2024).

32 U.S. Cyber Command. (2022). Cyber 101: Defend forward and persistent engagement. https://nsarchive.gwu.edu/sites/default/files/documents/semon9-giki0/2022-10-25-USCYBERCOM-Cyber-101-Defend-Forward-Persistent-Engagement.pdf

33 U.S. Cyber Command. (2020, December 3). Estonian, U.S. cyber commands conduct joint defensive cyber operation. https://www.cybercom.mil/Media/News/Article/2433245/

34 U.S. Department of Defense. (2023). Fact sheet: 2023 DoD cyber strategy. https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

places one state's cyber forces inside another state's military networks for weeks, which is exactly the kind of activity other lexicons would file under active cyber defence.

The national terms documented in Sections 5.1 and 5.2 belong to the same family: France's *lutte informatique offensive*, the Netherlands' *permanente proactieve inzet and offensief tegendruk, Germany's aktive Cyberabwehr*, Romania's *capabilități de răspuns ofensiv*, Poland's *pełne spektrum with ofensywne*, Denmark's *Computer Network Operations*, the United Kingdom's *responsible cyber power*, Finland's *response and countermeasures*, Spain's operaciones militares en el ciberespacio and ciberdefensa activa, Sweden's *offensiva and defensiva cyberoperationer*, Lithuania's *kibernetinės erdvės operacijos*, Slovakia's *aktívna obrana*, Czechia's *aktivní zásah*, Portugal's *atividade ofensiva*, Latvia's *aktīvā kiberaizsardzība*, Slovenia's *proaktivno in stalno odzivanje*, and Ireland's *Active Cyber Defence and Active Cyber Protection*. Table 2 provides an overview of the lexicon and locates each term against our seven questions, which makes the underlying pattern visible: the terms are not synonyms and not simply competing definitions of one concept, but names for different cells of the same conceptual space, locus terms, trigger terms, effect terms, and register terms, used interchangeably in policy debate as if they named the same thing.

The consequence for EU policy is practical. A member state can comply with the call to build 'active defence capabilities' by procuring real-time internal detection, by standing up a takedown service against commodity crime, or by developing an out-of-network disruption capability, and each reading is supported by an authoritative glossary. The lexicon compounds the challenge: officials who agree on active cyber defence, hunt forward or proactive engagement may agree on less than they think, because the terms they exchange name different dimensions of the activity.

TABLE 2

The lexicon: terms in circulation and what each one names

The same family of activity travels under many names. The terms are not synonyms: each answers a different subset of the seven analytical questions, which is why officials who exchange them in debate may agree on less than they think.

TERM (ORIGINAL)	USED BY / SOURCE	WHAT IT DENOTES, AS PUBLISHED	WHAT THE TERM NAMES
THE FOUR REFERENCE AUTHORITIES			
Active cyber defence	CCDCOE Cyber Law Toolkit	Proactive defensive measures outside the defended infrastructure, with hack-back a subtype	Adversary infrastructure (locus)
Active cyber defense	United States, CNSSI 4009-2022	Synchronised, real-time discovery, detection, analysis and mitigation	Own networks, real time (locus, trigger)
Active Cyber Defence	United Kingdom, NCSC programme	Automated protection against high-volume commodity attacks	Own networks, protective, criminal targets
Defensive / offensive cyberspace operation	NATO, AJP-3.20	Binary: preserving freedom of action versus projecting power	Protective within authorised access, destructive via SCEPVA
RELATED TERMS			
Hack-back	CCDCOE Cyber Law Toolkit	Action against an identified source of a malicious operation	Adversary infrastructure, disruptive
Defend forward	United States, DoD Cyber Strategy 2023	Disrupting malicious cyber activity before it can affect the homeland	Adversary infrastructure, disruptive
Persistent engagement	United States, US Cyber Command	Proactive posture, continuously seeking out and eliminating threats	Persistent peacetime trigger
Hunt forward operations	United States, US Cyber Command	Defensive operations on a partner's networks, at the partner's request	Partner networks, protective
DCO-RA	United States, CNSSI 4009-2022	Authorised defensive measures taken outside the defended network	Adversary infrastructure, labelled defensive
NATIONAL TERMS			
Lutte informatique offensive (LIO)	France, military doctrine 2019	Effects against adversary systems, autonomous or combined with conventional means	Adversary infrastructure, disruptive to destructive, military
Permanente proactieve inzet, offensief tegendruk	Netherlands, Defence Cyber Strategy 2025	Permanent proactive posture of offensive counter-pressure	Persistent trigger, offensive register
Offensiva och defensiva cyberoperationer	Sweden, Doktrinansats Cyberförsvar 1.1 (2024)	Denial of an adversary's access and manipulation of data, with large parts of the cyber defence active at all conflict and readiness levels	Adversary systems, offensive register, standing posture
Atividade ofensiva	Portugal, Estratégia Nacional de Ciberdefesa 2022	Offensive activity under rules of engagement, authorised from the tactical to the strategic level	Offensive register, effects and authorisation
Capabilități de răspuns ofensiv	Romania, Law 58/2023	Offensive response capabilities against attacks contravening international law	Statutory military mandate, offensive register
Operazioni militari cibernetiche offensive e difensive	Italy, National Cybersecurity Strategy 2022 to 2026	Offensive and defensive military cyber operations, in the cases provided for	Offensive register, conditionality without stated conditions
Computer Network Operations (CNO)	Denmark, Defence Agreements and joint doctrine 2019	Umbrella term for defensive and offensive cyber operations	Offensive register since the 2012 agreement, adversary locus in doctrine
Pełne spektrum działań … ofensywne	Poland, Ministry of National Defence	Full spectrum of activities: defensive, reconnaissance, offensive	Offensive register, no published actions
Aktive Cyberabwehr	Germany, bills pending 2026	Police powers to prohibit systems, redirect traffic, read, delete or alter data	Police authority, danger-aversion trigger

The table continues on the next page.

EU CYBER DIRECT

TABLE 2, CONTINUED

TERM (ORIGINAL)	USED BY / SOURCE	WHAT IT DENOTES, AS PUBLISHED	WHAT THE TERM NAMES
NATIONAL TERMS, CONTINUED			
Aktívna obrana	Slovakia, Act No. 500/2022 Coll., s. 7	Detection and analysis of attacks and, where necessary, operations creating effects on the attacker's systems	Adversary infrastructure, statutory trigger and effect
Aktivní zásah	Czechia, Act No. 289/2005 Coll. as amended 2021	Active intervention in cyberspace, undefined in the statute, with conditions and ministerial consent	Statutory trigger and authority, content supplied by practice
Aktīvās kiberaizsardzības spējas	Latvia, strategy 2023 to 2026 and National Security Law s. 11(5)	Active cyber defence capabilities to be developed, and a ministerial decision on active cyber defence operations	Qualified register, statutory decision procedure
Proaktivno in stalno odzivanje	Slovenia, Medium-Term Defence Programme 2023 to 2028	Proactive and continuous response to cyber threats, and a capability for non-kinetic action	Qualified register, no locus or effect
Active Cyber Defence, Active Cyber Protection	Ireland, Defence Forces Cyber Defence Strategy 2024 to 2027	A category of military cyberspace operations, left undefined, and a protective service against commodity attacks	Undefined category, own networks for the protective service
Responsible cyber power	United Kingdom, National Cyber Force	Contesting and competing with adversaries in cyberspace	Qualified register for out-of-network activity
Response and countermeasures	Finland, Cyber Security Strategy 2024 to 2035	New strategy pillar in the legal register of countermeasures	Reactive trigger
Operaciones militares en el ciberespacio	Spain, Orden DEF/710/2020	Military operations in cyberspace per operational plans in force	Unqualified operational register
Kibernetinės erdvės operacijos	Lithuania, Ministry of National Defence	Cyberspace operations planned and conducted by the new command	Unqualified operational register

EU LEVEL

'Full-spectrum … including active defence capabilities' · EU, JOIN(2022) 49 final. An investment mandate in which the term is left undefined, so it is not located against any of the seven analytical questions.

Reading the table. Each entry is documented verbatim in the body text with its source. The final column states which of the seven analytical questions of Section 2.2 the term answers. **Source:** authors, from the documents quoted in Sections 3 to 6.

EU CYBER DIRECT

PART II

Mapping member states' positions

5. Mapping concepts, doctrines and legal frameworks

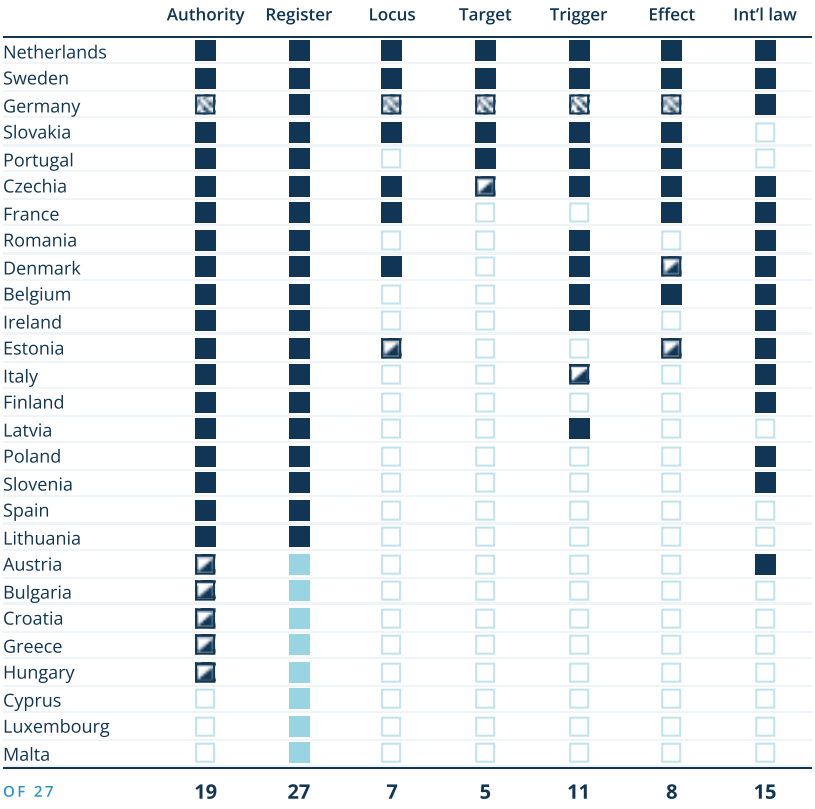
Part II turns from the vocabulary of active cyber defence to the record of the member states themselves. It maps, for all twenty-seven, what their published strategies, doctrines, statutes and official statements say about the activity, read where possible in the national language and coded against the seven questions set out in Section 2.2. The aim is not to rank states or to infer their capabilities, but to establish what each has chosen to put on the public record, and what it has left unsaid.

The sections follow the order of the questions. They begin with the one that in our judgement matters most for cooperation, the legal authority under which a state acts (Section 5.1), move through the vocabulary states use (Section 5.2), where and against whom they would act (Section 5.3), when action is authorised (Section 5.4) and what it is meant to achieve (Section 5.5), and end with the international law positions that bound all the others (Section 5.6). Each section opens with its key findings and includes a summary figure. Reference states outside the EU appear where they illuminate a European choice, and explanations of why a state has chosen as it has are offered as interpretation, distinguished from the documentary findings. Figure 2 sets out the published record state by state and question by question, and Figure 3 shows how many member states answer each question.

FIGURE 2

The published record, state by state and question by question

States readily publish who acts and in what vocabulary. The operational questions are answered by far fewer states, and the pattern holds across the Union.



KEY

- Published answer
- Pending: Germany's bills
- Partial: body named but not its legal family, conditional wording, inward only, or a target named in practice
- Register: no published position, counted as the state's answer
- Not published in the sources reviewed

SIX OF SEVEN IN A SINGLE TEXT

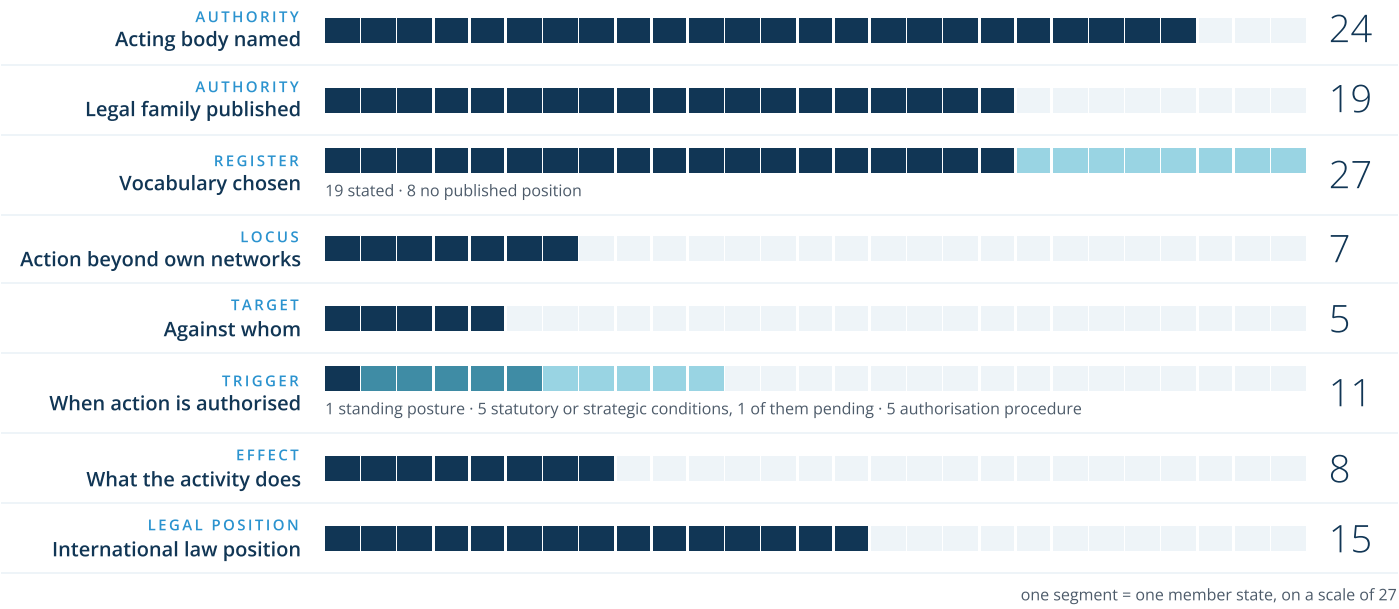
Sweden's doctrinal approach and Slovakia's Act on Military Intelligence. Of the two, Slovakia's alone is law.

Source: authors, Annex A. Questions in the order of Part II. Totals follow Section 7.3. A published authorisation procedure counts as an answer to the trigger question. EU CYBER DIRECT

FIGURE 3

How many member states answer each question

Twenty-four member states name the body that would act. Seven say whether it would act beyond their own networks, and five say against whom.



Source: authors, Section 7.3 and Annex A. Questions in the order of Part II. Operational counts include Germany's pending bills.

EU CYBER DIRECT

5.1 Authority: institutional and legal basis

KEY FINDINGS

1. Military authority is the default; the exceptions, such as the Dutch intelligence route, the German police-law route and the Romanian statute, are deliberate institutional choices with consequences for oversight.
2. The choice of legal basis is not a technicality: it determines who may act, who oversees them and which constitutional constraints apply.

This is the question on which the member states have said most, and on which they differ most consequentially. Each state is coded here by the authority family that governs action beyond its own networks. Germany, which is legislating along more than one route at once, is coded by its novel police-law route and treated in full in Section 5.1.3. Of the nineteen member states whose documents let us answer the question, twelve place the activity under military law or doctrine, four under hybrid arrangements combining intelligence or civil coordinating authorities with military capabilities, two under military intelligence law, and one, in a bill not yet enacted, under police law. Seven of these states, set out in Section 5.3, publish that the activity reaches beyond their own networks. The military default is real, but the exceptions are the interesting cases, because each of them is a deliberate institutional choice with consequences for oversight. Figure 4 shows which body would act in each member state.

FIGURE 4

Who acts: the legal family of the acting body

Military authority is the default: twelve of the nineteen member states that publish a legal family place the activity under military law. The exceptions are deliberate institutional choices.



Military	12	France, Romania, Poland, Italy, Denmark, Lithuania, Portugal, Sweden, Ireland, Latvia, Slovenia, Belgium
Hybrid intelligence–military	4	Netherlands, Estonia, Finland, Spain
Military intelligence *in statute*	2	Czechia, Slovakia
Police *pending*	1	Germany (police bill pending; an intelligence route is also pending, and the armed forces act under existing rules)
Unit named, legal family not published	5	Austria, Bulgaria, Croatia, Greece, Hungary
No acting body published	3	Cyprus, Luxembourg, Malta

Source: authors, Annex A and Section 5.1. One segment = one member state. Belgium's legal family rests on its Cyber Strategy for Defence and Strategic Vision 2025, which give the military cyber capability an offensive mandate. EU CYBER DIRECT

5.1.1 France: the military model

France has published military doctrine for offensive cyber operations since 2019. The Ministry of the Armed Forces describes it as follows: 'La lutte informatique offensive à des fins militaires (LIO) recouvre l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison avec des moyens militaires conventionnels' [Offensive cyber warfare for military purposes (LIO) covers all actions undertaken in cyberspace, conducted autonomously or in combination with conventional military means; authors' translation].[35] The same page states that the cyber weapon aims, 'dans le strict respect des règles internationales, à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données' [in strict compliance with international rules, to produce effects against an adversary system in order to alter the availability or confidentiality of its data; authors' translation].[36] Offensive cyber warfare is thus a military instrument, placed under the Commandement de la cyberdéfense and, through it, under the Chief of the Defence Staff. This is consistent with French constitutional arrangements, under which the President of the Republic is head of the armed forces and the employment of military capabilities is a matter of executive authority, and with a French doctrinal culture that prefers published elements of doctrine to statute. One qualification applies: France's out-of-network military concept sits under COMCYBER, and it is that concept that is described here as military. The wider French architecture is hybrid: military defensive operations (lutte informatique défensive) are planned and organised by COMCYBER in coordination with the civilian ANSSI, which retains its civilian cybersecurity responsibilities, and a separate influence doctrine (lutte informatique d'influence) published in 2021. The military characterisation applies to the out-of-network authority, not to the ecosystem as a whole. The Senate's report on the 2024-2030 military programming law records 4 billion euros programmed for cyber, against 1.6 billion euros under the previous law, together with the personnel build-up towards a target of 5,000.[37] The Ministry's cyber defence pages now state 'Plus de 4 900 cybercombattants et cybercombattantes servent au sein du ministère des Armées. Ils seront plus de 5 500 à l'horizon 2030' [More than 4,900 cyber combatants serve within the Ministry of the Armed Forces; they will number more than 5,500 by 2030; authors' translation],

35 Ministère des Armées. (n.d.-a). La lutte informatique offensive (LIO). https://www.defense.gouv.fr/comcyber/nos-operations/lutte-informatique-offensive-lio

36 Ministère des Armées (n.d.-a).

37 Sénat. (2023). Pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030 (Rapport d'information no. 638, 2022-2023). https://www.senat.fr/rap/r22-638/r22-638_mono.html

[38] which confirms from a primary source the figure of approximately 4,900 previously available only through press reporting.[39] Older pages of the same ministry site still carry 'Plus de 4 000' and, in one case, 3,600, so the headcount is reported here with that caveat. The command has been held since 1 August 2025 by Général de division aérienne Emmanuel Naëgelen, who succeeded Général de corps d'armée Aymeric Bonnemaison.[40]

5.1.2 The Netherlands: the intelligence-enabled model

The Netherlands presented its Defence Cyber Strategy 2025 to parliament on 3 October 2025. The authority to act is constitutional before it is statutory: Defence acts under Article 97 of the Constitution, which charges the armed forces with the defence and protection of the interests of the Kingdom. The intelligence statutes described below govern a narrower question, the terms on which the Defence Cyber Command and the Military Intelligence and Security Service act together, a division set out for parliament in the Minister's letter of 30 May 2024.[41] The accompanying letter states: 'Hiervoor introduceren we een nieuwe koers: een permanente proactieve inzet om meer offensief tegendruk te geven in het cyberdomein' [For this we introduce a new course: a permanent proactive posture to give more offensive counter-pressure in the cyber domain; authors' translation].[42] The strategy applies both in the 'grijze zone tussen oorlog en vrede' [grey zone between war and peace; authors' translation] and in armed conflict, and it also states its own constraint: 'Voor de rechtmatige uitvoering van de DCS benut Defensie de ruimte binnen de bestaande (juridische) kaders van taken en bevoegdheden' [For the lawful implementation of the DCS, Defence uses the room within the existing (legal) frameworks of tasks and powers; authors' translation], with legislative change pursued where legal limits are reached.[43] On escalation the strategy states an intention rather than a constraint: 'Het uitgangspunt daarbij blijft dat Nederland escalatie wil voorkomen' [The starting point remains that the Netherlands wishes to avoid escalation; authors' translation], and this study records it as such.

The enabling legislation predates the strategy. The Temporary Act on investigations by the AIVD and MIVD into countries with an offensive cyber programme was enacted on 13 March 2024, published as Staatsblad 2024, 88, and entered into force on 1 July 2024.[44] The Senate adopted the bill on 12 March 2024.[45] The Act does not create new categories of power. It enables faster and more agile deployment of existing powers under the Intelligence and Security Services Act 2017 and shifts binding oversight for specified powers from prior authorisation by the TIB to review during and after operations by the CTIVD.[46] Two qualifications apply. First, the 'no new powers' characterisation concerns the catalogue of powers, not the intensity of control: during the

38 Ministère des Armées. (n.d.-b). Le Commandement de la cyberdéfense (COMCYBER). https://www.defense.gouv.fr/comcyber/commandement-cyberdefense-comcyber

39 L'Essentiel de l'Éco. (2026). Le Régiment de Cyberdéfense français, en guerre dès sa création. https://lessentieldeleco.fr/7612-le-regiment-de-cyberdefense-francais-en-guerre-des-sa-creation/

40 Ministère des Armées (n.d.-b).

41 Ministerie van Defensie. (2024, May 30). Kamerbrief over de samenwerking tussen het Defensie Cyber Commando en de MIVD (Kamerstuk 33321, nr. 10) [Letter to parliament on cooperation between the Defence Cyber Command and the MIVD].

42 Ministerie van Defensie. (2025b, October 3). Kamerbrief Defensie Cyberstrategie 2025. https://open.overheid.nl/documenten/18553fd0-0941-48e5-a9ea-95054ff1dc05/file

43 Ministerie van Defensie. (2025a). Defensie Cyberstrategie 2025. https://www.defensie.nl/site/binaries/site-content/collections/documents/2025/10/03/defensie-cyber-strategie-2025/Defensie+Cyberstrategie+-+openbaar.pdf

44 Staatsblad van het Koninkrijk der Nederlanden. (2024). Wet van 13 maart 2024, houdende tijdelijke regels over onderzoeken door de AIVD en de MIVD naar landen met een offensief cyberprogramma (Stb. 2024, 88). https://zoek.officielebekendmakingen.nl/stb-2024-88.html; AIVD. (n.d.). Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma. https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen--en-veiligheidsdiensten/wet-op-de-inlichtingen-en-veiligheidsdiensten/tijdelijke-wet-onderzoeken-aivd-en-mivd-naar-landen-met-een-offensief-cyberprogramma

45 Eerste Kamer der Staten-Generaal. (n.d.). Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma (36.263). https://www.eerstekamer.nl/wetsvoorstel/36263_tijdelijke_wet_onderzoeken

46 AIVD (n.d.).

parliamentary process critics argued that replacing binding prior authorisation with review during and after operations weakens the oversight regime, while the government presented it as preserving safeguards at operational speed.[47] Second, the strategy itself is a defence document that frames the armed forces as the acting party, with the intelligence statutes as enablers. The Dutch model is therefore better described as military-led on hybrid legal foundations than as intelligence-led, and it is treated here as hybrid. The strategy remains under active parliamentary scrutiny.

The design of the Dutch posture appears to owe more to institutional history than to strategic preference. The Intelligence and Security Services Act 2017 was itself the subject of public controversy and a consultative referendum before it entered into force, and it created the TIB as a body of prior, binding authorisation precisely to reassure a sceptical public. A defence strategy that wished to act persistently in the grey zone therefore had to be built around that oversight architecture, and the Temporary Act is best understood as the point at which speed of operation and intensity of prior control were rebalanced. The Dutch case shows something the other member states have not yet had to confront: that a persistent posture is, in practice, an oversight question before it is an operational one.

These foundations are themselves now in transition. On 28 August 2026 the government opened a public consultation on a draft Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbnv), whose stated purpose is to replace 'de Wet op de inlichtingen- en veiligheidsdiensten 2017 en de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen' [the Intelligence and Security Services Act 2017 and the Temporary Act on investigations by the AIVD and MIVD into countries with an offensive cyber programme, bulk datasets and other specific provisions; authors' translation], and whose Article 271 repeals both.[48] Three features of the draft are relevant to this study. It generalises the Temporary Act's approach into a threat-based regime in which the use of powers and the accompanying safeguards are tied to the nature of the threat. It merges the two oversight bodies on which the current arrangement rests into a single College van Toetsing en Toezicht with separate review, oversight and complaints sections (Article 160 of the draft), while introducing authorisation by the district court of The Hague for operations concerning lawyers, journalists and parliamentarians (Articles 42 to 44). Its consultation closes on 11 October 2026,[49] so the legal basis of the Union's one published persistent posture is open to comment as this study goes to press. The draft does not alter the account above, which describes the law in force, but it confirms the point that the posture is being built by redesigning oversight, now at the scale of the framework as a whole.

5.1.3 Germany: three legal routes at once

Germany is legislating 'aktive Cyberabwehr' [active cyber defence; authors' translation] along two civilian routes at once, police law and intelligence law, while its armed forces act under the constitutional rules that govern every military deployment. The police-law route came first and is described first. The sequence is documented in official sources: a cabinet decision of 27 August 2025 mandated the bill, the ministerial draft followed on 24 February 2026, the cabinet adopted the government bill on 27 May 2026, and the Bundestag held its first reading on 25 June 2026.

47 Eerste Kamer der Staten-Generaal (n.d.).

48 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties & Ministerie van Defensie. (2026). Wetsvoorstel Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbnv) [Draft bill, public consultation 28 August to 11 October 2026]. https://www.internetconsultatie.nl/wbnv

49 AIVD. (2026, August 28). Start consultatie nieuwe Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten. https://www.aivd.nl/actueel/nieuws/2026/08/28/start-consultatie-nieuwe-wet-bescherming-nationale-veiligheid-door-de-inlichtingen-en-veiligheidsdiensten

[50] The ministry summarises the powers as 'spezifische Cyberabwehrbefugnisse zur Untersagung des Betriebs eines informationstechnischen Systems oder seine Einschränkung oder Unterbindung, zur Umleitung von Datenverkehr … und zum Auslesen, Löschen oder Verändern von Daten in IT-Systemen' [specific cyber defence powers to prohibit, restrict or suppress the operation of an information technology system, to redirect data traffic, and to read out, delete or alter data in IT systems; authors' translation].[51] The bill inserts into the Federal Criminal Police Office Act a new section 8a comprising sections 68a to 68f, and a new section 3a, and into the Federal Police Act a new section 41a. The core power reads: 'Das Bundeskriminalamt darf zur Abwehr einer Gefahr den Betrieb eines informationstechnischen Systems, von dem diese Gefahr ausgeht, untersagen' [To avert a danger, the Federal Criminal Police Office may prohibit the operation of an information technology system from which that danger emanates; authors' translation].[52] Earlier reporting citing a section 62b reflected the superseded ministerial draft, and the numbering in the bill before the Bundestag is 68a to 68f.

The bill is not law, and its constitutional basis is disputed. The government's justification claims federal legislative competence under Article 73 of the Basic Law in conjunction with competence from the nature of the matter, and asserts that 'Die Gefahrenabwehrzuständigkeiten der Länder werden durch die Befugniserweiterung nicht berührt' [The hazard-prevention competences of the Länder are not affected by the extension of powers; authors' translation].[53] The Gesellschaft für Informatik objects that the design 'unterläuft das föderale Kompetenzgefüge des Grundgesetzes. Die Gefahrenabwehr ist nach Art. 30 GG grundsätzlich Ländersache' [undercuts the federal allocation of competences of the Basic Law; hazard prevention is, under Article 30 of the Basic Law, in principle a matter for the Länder; authors' translation].[54] A parliamentary motion opposes the introduction of hack-backs and offensive cyber defence outright, arguing among other things that active cyber defence measures risk amounting to interventions in foreign state information technology infrastructure.[55] The account given here describes the bill as it stood at first reading. It is directed at the attacking systems from which a danger emanates. Whether that extends to systems abroad is the question raised in the parliamentary debate, and it has since been answered explicitly, for a different body, by a second bill. The Bundesrat's opinion did not mount a competence challenge. Its principal objection concerned the absence of a judicial reservation for certain interventions, which the federal government rejected with reference to Federal Constitutional Court rulings of 24 June 2025.[56] The Interior Minister framed the policy in the Bundestag as follows: 'Wer uns zukünftig im Cyberraum angreift, der muss wissen: Wir schlagen zurück und sind in der Lage, die Angreifer in ihrer Infrastruktur zu stören und zu zerstören' [Whoever attacks us in cyberspace in future must know: we strike back and are able to disrupt and destroy the attackers in their infrastructure; authors' translation].[57] The minister's 'zerstören' is a political characterisation, and the bill's own text is the basis for what the powers would permit.

50 Bundesministerium des Innern und für Heimat. (2026, May 27). Aktive Cyberabwehr: Gesetzentwurf nimmt Angreifer ins Visier. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2026/05/cybersicherheit.html; Deutscher Bundestag. (2026a). Entwurf eines Gesetzes zur Stärkung der Cybersicherheit (Drucksache 21/6585). https://dserver.bundestag.de/btd/21/065/2106585.pdf

51 BMI (2026).

52 Deutscher Bundestag (2026a).

53 Deutscher Bundestag (2026a).

54 Gesellschaft für Informatik. (2026, March 16). Stellungnahme zum Referentenentwurf eines Gesetzes zur Stärkung der Cybersicherheit. https://gi.de/fileadmin/GI/Hauptseite/Service/Publikationen/GI_Stellungnahme_Referentenentwurf-Cyberabwehr.pdf

55 Deutscher Bundestag. (2026b). Gegen die Einführung von Hackbacks und offensiver Cyberabwehr (Drucksache 21/6653). https://dserver.bundestag.de/btd/21/066/2106653.pdf

56 Deutscher Bundestag. (2026c). Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung (Drucksache 21/7406). https://dserver.bundestag.de/btd/21/074/2107406.pdf

57 Bundesregierung. (2026, June 25). Bundesinnenminister zur Cybersicherheit im Bundestag. https://www.bundesregierung.de/breg-de/suche/bmi-cybersicherheit-bt-2445290

Germany is the only member state to have proposed placing active cyber defence in police law, and it is not relying on police law alone; neither the police nor the intelligence reform had been enacted at this study's reference date. On 7 September 2026 the federal government introduced a reform of intelligence-services law that would give the Federal Intelligence Service and the Federal Office for the Protection of the Constitution powers of active defence, including in cyberspace.[58] For the Federal Intelligence Service the bill distinguishes immediate defence against imminent dangers encountered in the course of its intelligence work, such as the deletion of victims' data found on the systems of hacker groups, from proactive measures in a specific situation of threat from foreign powers, which may include targeted intrusion into IT systems and the shutting down or disabling of servers used by state hacker groups. Prior control would lie with the Independent Control Council, reporting to the Parliamentary Oversight Panel. Where the police bill leaves the reach abroad unresolved, the intelligence bill is explicit about it: its measures are directed at foreign IT infrastructure.

The armed forces form a third route. The Bundeswehr conducts cyber and information operations through its Cyber and Information Domain Command, and the Ministry of Defence states that its deployment in cyberspace 'unterliegt denselben rechtlichen Voraussetzungen wie jeder andere Einsatz deutscher Streitkräfte' [is subject to the same legal requirements as any other deployment of the German armed forces; authors' translation], with the lawfulness of each operation to be assessed case by case.[59] Military cyber operations therefore rest on the Basic Law and, for deployments, on a mandate of the Bundestag, while military cyber defence at home is provided as administrative assistance. The focus is the protection of the armed forces' own forces and infrastructure, and offensive cyber capabilities are confined to operational contexts under a specific mandate or within NATO-led frameworks.

Germany is therefore the one member state whose published record spans all three authority families this study distinguishes, and the structural reason is the same for each route. German public law has long kept police and intelligence functions apart. Hazard prevention (Gefahrenabwehr) is in principle a competence of the Länder, and the domestic use of the armed forces is tightly constrained by the Basic Law. No single existing body can act against attacker infrastructure across the whole range of cases, and the federal government has responded by extending the powers of each within its own lane: the police against attacking systems in the course of hazard prevention, the intelligence services against foreign infrastructure, and the armed forces within mandated operations. The dispute under Article 30 of the Basic Law attaches to the first of these. The German case is, for the Union, the clearest demonstration that the choice of legal basis is not a technicality: it determines who may act, who oversees them, and which constitutional constraints apply, and in Germany it will do so three times over.

5.1.4 Romania: the statutory route

Romania is the member state whose offensive commitment sits most explicitly in statute. Law No. 58/2023 on the cybersecurity and cyber defence of Romania assigns to the Ministry of National Defence the duties to 'dezvoltă capabilități de răspuns ofensiv, în mod individual sau ca parte dintr-o coaliție ori alianță, utilizabile în caz de atacuri cibernetice care contravin dreptului internațional' [to develop offensive response capabilities, individually or as part of a coalition or alliance, usable in the event of cyberattacks that contravene international law; authors' translation], to 'participă la activități de descurajare în spațiul cibernetic' [to participate in deterrence activities in cyberspace; authors' translation], and to provide the single point of contact with NATO for military cyberspace operations.

58 Deutscher Bundestag. (2026d). Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts (Drucksache 21/7868), 7 September 2026. https://dserver.bundestag.de/btd/21/078/2107868.pdf

59 Bundesministerium der Verteidigung. (n.d.). FAQ: Cyber-Abwehr der Bundeswehr. https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr

[60] The same article requires these activities to be conducted 'cu respectarea dreptului internațional, inclusiv a dreptului internațional umanitar' [in compliance with international law, including international humanitarian law; authors' translation].[61] The national strategy for 2022 to 2027 contains the corresponding commitment to develop 'atât capabilități proactive, care să permită cunoașterea anticipativă a amenințării, cât și capabilități de răspuns ofensiv' [both proactive capabilities allowing anticipatory knowledge of the threat and offensive response capabilities; authors' translation] under an objective titled resilience through a proactive approach and deterrence.[62] Civilian authority sits with the DNSC, critical-infrastructure cybersecurity with the SRI, and the military mandate with the Cyber Defence Command.[63] Romania is the member state that has placed its offensive mandate most explicitly in primary legislation, binding it in the same article to international humanitarian law. This appears to reflect a legislative tradition of setting security competences in statute rather than in doctrine, and it has the practical consequence that Romania's authority basis is the most legible of any member state's, even though the statute says nothing about when the capability would be used or to what effect.

5.1.5 Military and mixed authority elsewhere: Poland, Italy, Denmark, Spain, Lithuania, Portugal and Sweden

The Polish Ministry of National Defence states of its Cyberspace Defence Forces: 'Wojska Obrony Cyberprzestrzeni mają zdolności do realizowania pełnego spektrum działań - od obronnych, przez rozpoznawcze, po ofensywne' [The Cyberspace Defence Forces have the capability to carry out the full spectrum of activities, from defensive, through reconnaissance, to offensive; authors' translation].[64] This remit is also established in statute. Article 15(4)(2) of the Act on the Defence of the Fatherland defines the Cyberspace Defence Forces as a specialist component of the Armed Forces competent to conduct the full spectrum of activities in cyberspace, particularly the proactive protection and active defence of cyberspace elements and resources of key importance to the Armed Forces. The Act further assigns the Commander of the Cyberspace Defence Forces responsibility for conducting activities and operations in cyberspace.[65] The component command was established in 2022 and comprises twelve subordinate units, including two specialist cyberspace-operations units.[66] No published doctrine setting out trigger thresholds or geographic scope for these forces was located across the ministry's public materials. Poland's civilian framework, the Act on the National Cybersecurity System as amended, entered into force on 3 April 2026 and transposes the NIS2 Directive.[67] It is resilience regulation, not an operational mandate. Poland's National Cybersecurity Strategy, adopted in March 2026, expressly refers to proactive protection and active cyber defence, including the disruption of hostile cyber activity before attacks occur. It also envisages more detailed regulation of offensive cyber tools, without establishing a specific operational authorisation threshold. As a strategic objective rather than an operational mandate, it does not alter Poland's coding.[67] That the command was created in the year of Russia's full-scale invasion of Ukraine may explain both the speed of its creation and the ministry's readiness to describe its remit in full-spectrum terms before doctrine had been published.

Italy's National Cybersecurity Strategy 2022-2026 states: 'La Difesa, attraverso le articolazioni specialistiche

60 Parlamentul României. (2023). Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României. https://legislatie.just.ro/Public/DetaliiDocument/265677

61 Parlamentul României (2023).

62 Guvernul României. (2021). Strategia de securitate cibernetică a României, pentru perioada 2022-2027 (Hotărârea de Guvern nr. 1321/2021), sec. 4.4.3. https://legislatie.just.ro/Public/DetaliiDocument/250235

63 Parlamentul României (2023).

64 Ministerstwo Obrony Narodowej. (n.d.). Wojska Obrony Cyberprzestrzeni. https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni

65 Republic of Poland. (2022). Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny [Act of 11 March 2022 on the Defence of the Fatherland]. Original publication: Dz.U. 2022 poz. 655; consolidated text: Dz.U. 2022 poz. 2305, as amended.

66 Ministerstwo Obrony Narodowej (n.d.).

67 Republic of Poland, Ministry of Digital Affairs. (2026). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. https://www.gov.pl/web/baza-wiedzy/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa; Rada Ministrów. (2026). Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, adopted by Resolution No. 92 of 10 March 2026, Monitor Polski, item 309, s. 6.6. https://eli.gov.pl/eli/MP/2026/309/ogl

dedicate, conduce operazioni militari cibernetiche offensive e difensive nei casi previsti' [Defence, through dedicated specialist branches, conducts offensive and defensive military cyber operations in the cases provided for; authors' translation], with the Ministry of Defence defining and coordinating military cyber policy and the intelligence community also conducting cyber operations.[68] Italy publishes neither threshold nor scope.

Denmark's commitment is older than commonly assumed: the Defence Agreement 2013-2017, concluded on 30 November 2012, records that it was 'allerede i Forsvarsforlig 2010-2014 besluttet at afsætte ca. 40 mio. kr. årligt til etablering og drift af en Computer Network Operations (CNO) kapacitet med henblik på at tilvejebringe en kapacitet, der kan gennemføre defensive og offensive militære operationer i cyberspace' [already decided in the Defence Agreement 2010-2014 to allocate approximately DKK 40 million annually for the establishment and operation of a Computer Network Operations capacity, with a view to providing a capacity that can carry out defensive and offensive military operations in cyberspace; authors' translation].[69] The Danish Defence Intelligence Service confirms the umbrella term: 'Defensive og offensive cyberoperationer kaldes under ét Computer Network Operations' [Defensive and offensive cyber operations are collectively called Computer Network Operations; authors' translation].[70] Denmark also has doctrine. The Defence Academy's Værnsfælles Doktrin for Militære Cyberspaceoperationer, of September 2019, defines an offensive cyberspace operation as one 'der har til hensigt at anvende magt i eller gennem en modstanders del af cyberspace' [that intends to apply force in or through an adversary's part of cyberspace; authors' translation] and a defensive one as an operation 'der uden at anvende magt har til hensigt at bevare eller genskabe egen bevægelses- og handlefrihed i cyberspace' [that, without applying force, intends to preserve or restore one's own freedom of movement and action in cyberspace; authors' translation]. The doctrine also states that 'Beslutningskompetencen til at iværksætte CO bør delegeres til det lavest mulige niveau, som operationens vilkår tilsiger' [the competence to decide on launching cyberspace operations should be delegated to the lowest possible level that the conditions of the operation warrant; authors' translation].[71] The intelligence service supplies the political layer: a decision to use its Computer Network Operations capacity to carry out a cyberattack in support of a military operation is taken 'på samme måde, som beslutninger om indsættelse af andre militære magtmidler' [in the same way as decisions on the deployment of other military means of force; authors' translation], with what it calls 'behørig inddragelse af Folketinget' [due involvement of the Folketing; authors' translation].[72] Denmark therefore answers the locus question in doctrine and the decision question twice, at the operational level by delegation and at the political level by parliamentary involvement, while publishing no threshold and no description of effects. Our account of Denmark rests on the 2013-2017 agreement's restatement of a decision taken in the 2010-2014 agreement. The current framework agreement, Aftale om dansk forsvar og sikkerhed 2024-2033 of 28 June 2023, is written in investment and capability terms, and no equivalent Computer Network Operations passage was located in it.[73] The Danish offensive-capability commitment is therefore best read as one of the earlier agreements, which the current framework neither restates nor withdraws. The subsidiary agreements concluded under it were not reviewed and are flagged in Section 8. In Denmark military cyber operations sit with the Defence Intelligence Service. Following the institutional reorganisation of 2024 to 2025, most former civilian national cybersecurity responsibilities were

68 Presidenza del Consiglio dei Ministri, Agenzia per la Cybersicurezza Nazionale. (2022). Strategia nazionale di cybersicurezza 2022-2026. https://www.acn.gov.it/ACN_Strategia.pdf

69 Forsvarsministeriet. (2012). Aftale på forsvarsområdet 2013-2017. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-forsvarsforlig-2013-2017-inkl-bilag-.pdf

70 Forsvarets Efterretningstjeneste. (n.d.). Cyberoperationer. https://www.fe-ddis.dk/da/arbejdsomrade-a/cyberoperationer/

71 Forsvarsakademiet. (2019). Værnsfælles doktrin for militære cyberspaceoperationer (VDMCO) [Joint doctrine for military cyberspace operations], 1st edition. Royal Danish Defence College, September 2019. https://research.fak.dk/esploro/outputs/other/V%C3%A6rnsf%C3%A6lles-Doktrin-for-Milit%C3%A6re-Cyberspaceoperationer/991816060103741

72 Forsvarets Efterretningstjeneste (n.d.).

73 Forsvarsministeriet. (2023). Aftale om dansk forsvar og sikkerhed 2024-2033 [Agreement on Danish defence and security 2024-2033], 28 June 2023. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-aftale-om-dansk-forsvar-og-sikkerhed-2024-2033-aftaletekst-28-06-2023-.pdf

transferred to the authorities responsible for societal safety and emergency preparedness, while the Defence Intelligence Service retained specified operational defensive functions alongside military cyber operations. The earlier concentration of foreign intelligence, national cyber defence and military cyber operations in one institution plausibly explains why the Danish defence agreements could treat offensive capability as a budget line rather than as a doctrinal question.

Spain's Joint Cyberspace Command was created by ministerial order in 2020 as 'el órgano responsable del planeamiento, la dirección, la coordinación, el control y la ejecución de las acciones conducentes a asegurar la libertad de acción de las FAS en el ámbito ciberespacial' [the body responsible for planning, directing, coordinating, controlling and executing actions to ensure the armed forces' freedom of action in the cyberspace domain; authors' translation]. The same order provides that it 'planea, dirige, coordina, controla y ejecuta las operaciones militares en el ciberespacio, de acuerdo con los planes operativos en vigor' [plans, directs, coordinates, controls and executes military operations in cyberspace in accordance with operational plans in force; authors' translation].[74] The order does not use the words offensive, active response, or deterrence, and Spain should not be characterised as offensive on its basis. The command's current public mission statement does use the active register, describing its work as 'ayudando a prevenir y responder de forma eficaz y eficiente a los ciberataques y a enfrentar de forma activa las ciberamenazas' [helping to prevent and respond effectively and efficiently to cyberattacks and to confront cyber threats actively; authors' translation].[75] This is a change of register and not of mandate: the phrase names no locus, no trigger and no effect, and the 2020 order remains the operative instrument. Spain's framework is broader than the military command alone, and its hybrid classification describes this wider institutional arrangement; it does not by itself establish a combined legal authority for operations beyond defended networks, and statements drawn from a draft national strategy are read as emerging proposals rather than adopted doctrine. The Centro Nacional de Inteligencia (CNI) operates under Law 11/2002,[76] and the Centro Criptológico Nacional (CCN), attached to the CNI and regulated by Royal Decree 421/2004, is responsible for the security of the information technology systems of the Administration.[77] Spain's 2019 National Cybersecurity Strategy uses the active register in this protective sense, providing for 'medidas de ciberdefensa activa en el sector público con el objetivo de mejorar las capacidades de respuesta' [active cyber defence measures in the public sector with the aim of improving response capabilities; authors' translation] and for 'medidas de ciberdefensa activa de ciudadanos y pymes' [active cyber defence measures for citizens and small and medium-sized enterprises; authors' translation],[78] while the 2021 National Security Strategy identifies defensa activa [active defence; authors' translation] among the capabilities of national cybersecurity.[79] This usage is close to the protective programme of the United Kingdom described in Section 3.3, and it concerns the protection of systems in Spain rather than action beyond national networks. National coordination in this field rests with the National Cybersecurity Council, a civil collegiate body supporting the National Security Council and chaired by the Secretary of State Director of the CNI,[80] a role the Spanish Ministry of Foreign Affairs has confirmed to the authors. On the authority question, Spain is therefore coded as a hybrid intelligence–military arrangement: a civil coordinating body chaired by the head of the intelligence service sits alongside the Joint Cyberspace Command, while operations in cyberspace remain, on the published record, with the military command.

74 Ministerio de Defensa. (2020). Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa (BOE-A-2020-8638). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-8638

75 Estado Mayor de la Defensa. (n.d.). Mando Conjunto del Ciberespacio (MCCE). https://emad.defensa.gob.es/unidades/mcce/

76 Jefatura del Estado. (2002). Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. https://www.boe.es/eli/es/l/2002/05/06/11/con

77 Ministerio de Defensa. (2004). Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, art. 2. https://www.boe.es/eli/es/rd/2004/03/12/421/con

78 Departamento de Seguridad Nacional. (2019). Estrategia Nacional de Ciberseguridad 2019 (Orden PCI/487/2019, de 26 de abril), línea de acción 1, medida 12, and línea de acción 4, medida 5. https://enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/ES_NCSS_2019_es.pdf

79 Presidencia del Gobierno. (2021). Estrategia de Seguridad Nacional 2021 (Real Decreto 1150/2021, de 28 de diciembre).

80 Ministerio de la Presidencia. (2018). Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad, apartado quinto. https://www.boe.es/buscar/act.php?id=BOE-A-2018-799

Lithuania's Cyber Defence Command began operating on 1 January 2025. The Ministry of National Defence describes a unit that 'planuos ir vykdys kibernetinės erdvės operacijas' [will plan and conduct cyberspace operations; authors' translation], and no official Lithuanian document located for this study uses the term offensive cyber operations.[81] In both of these cases the military institution exists, but the documents that create it describe operations without qualifying them, and the texts support no further characterisation.

Portugal belongs in this group, and its operative documents are defence documents rather than the lapsed civil cybersecurity strategy. The organic law of the armed forces general staff created a Cyberdefence Operations Command responsible for planning, directing, coordinating, controlling and executing 'operações no e através do ciberespaço' [operations in and through cyberspace; authors' translation].[82] The National Cyberdefence Strategy, approved by the Council of Ministers on 20 October 2022, says what those operations are for, and it is the fullest statement of purpose published by any member state outside France, the Netherlands, Sweden and Slovakia. It gives cyberdefence the lead in military action responding to 'ameaças originárias de Estados ou entidades não estatais, direta ou indiretamente, nomeadamente quando sejam promovidas de forma encoberta por Estados' [threats originating from States or from non-state entities, directly or indirectly, in particular when they are promoted covertly by States; authors' translation]. It describes 'operações reativas, preventivas e outras deliberadas' [reactive, preventive and other deliberate operations; authors' translation] whose purpose is, among others, to 'neutralizar, manipular, negar, romper, degradar ou destruir a capacidade de uma entidade em aceder livremente ao ciberespaço' [neutralise, manipulate, deny, disrupt, degrade or destroy an entity's capacity to access cyberspace freely; authors' translation]. And it places offensive activity under a published authorisation structure, providing that it is to be 'regulados por normas próprias, na forma de regras de empenhamento, com autorizações que podem ir do âmbito tático ao estratégico, sendo essas normas autorizadas pelo poder político instituído' [regulated by rules of their own, in the form of rules of engagement, with authorisations that may run from the tactical to the strategic level, those rules being authorised by the established political power; authors' translation].[83]

Portugal therefore answers the locus, effect, target and authority questions, and answers the trigger question as an authorisation structure rather than as a threshold: it says who may authorise action, and at what level, without saying in what circumstances. Its register is the explicit one: 'atividade ofensiva' [offensive activity; authors' translation]. The term ciberdefesa ativa does not appear in the strategy at all. The Portuguese case matters for this study's argument in a second way. A state that a search for cybersecurity strategies would record as having published nothing current turns out to have published, four years before, one of the fuller statements in the Union of what military cyber operations are for.

Sweden requires separate treatment. The national cybersecurity strategy for 2025 to 2029 does assign the armed forces' cyber defence resources a peacetime support role: 'I fredstid kan Försvarsmaktens cyberförsvarsresurser användas för att stödja samhället under kriser eller andra allvarliga händelser' [In peacetime, the Armed Forces' cyber defence resources can be used to support society during crises or other serious events; authors' translation].[84] Read on its own, that sentence supports a defensive coding. It is not the operative document. The Swedish Armed Forces have published a doctrinal approach to cyber defence, Doktrinansats Cyberförsvar, version 1.1, which they deliberately designate a doctrinal approach rather than a formally adopted doctrine and which has applied since 1 December 2024 and issued by the head of the

81 Krašto apsaugos ministerija. (2025). Pradeda veikti Lietuvos kariuomenės kibernetinės gynybos valdyba. https://kam.lt/pradeda-veikti-lietuvos-kariuomenes-kibernetines-gynybos-valdyba/

82 República Portuguesa. (2022). Decreto-Lei n.º 19/2022, de 24 de janeiro, Lei Orgânica do Estado-Maior-General das Forças Armadas [Organic law of the armed forces general staff], art. 41. Diário da República, 1.ª série, n.º 16. https://diariodarepublica.pt/dr/detalhe/decreto-lei/19-2022-178080766

83 Presidência do Conselho de Ministros. (2022). Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro, Estratégia Nacional de Ciberdefesa [National cyberdefence strategy], approved by the Council of Ministers on 20 October 2022. Diário da República, 1.ª série, n.º 211, 2 November 2022. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924

84 Government Offices of Sweden. (2025). Nationell strategi för cybersäkerhet 2025-2029 (Skr. 2024/25:121). https://www.regeringen.se/rattsliga-dokument/skrivelse/2025/03/skr.-202425121

Defence Staff strategy unit, and that document answers six of this study's seven questions in a single text, the seventh, the international law anchor, coming from the position Sweden publishes separately.[85] It distinguishes defensive cyber operations, which 'kan genomföras både i Försvarsmaktens egna system och i system utanför myndigheten' [may be conducted both in the Armed Forces' own systems and in systems outside the agency; authors' translation], from offensive cyber operations, which are directed 'mot system som motståndaren behöver för att genomföra sin verksamhet' [against systems that the adversary needs in order to conduct its activity; authors' translation], and it places the decision on the latter at the military-strategic level: 'Offensiva cyberoperationer beslutas och leds på militärstrategisk nivå' [Offensive cyber operations are decided and directed at the military-strategic level; authors' translation]. On the trigger it states that 'stora delar av cyberförsvaret är aktivt i samtliga konflikt- och beredskapsnivåer' [large parts of the cyber defence are active at all conflict and readiness levels; authors' translation]. The effects named are the denial of an adversary's access and the manipulation of data and information, in support of the Supreme Commander's freedom of action and ultimately of Sweden's sovereign rights, and the counterpart is defined as an antagonist, an actor with both the intent and the capability to act maliciously in or through the cyber domain, covering state, state-sponsored and non-state actors.

The doctrinal approach does not stand alone. The Armed Forces state on their own pages that 'Cyberförsvaret har förmåga att genomföra offensiva och defensiva cyberoperationer' [The cyber defence has the capability to conduct offensive and defensive cyber operations; authors' translation],[86] and the 2024 defence bill carries the same commitment into government policy, undertaking 'en förstärkning av förmågan till defensiva och offensiva cyberoperationer' [a strengthening of the capability for defensive and offensive cyber operations; authors' translation] and describing operations 'i och utanför Försvarsmaktens system och plattformar' [in and outside the Armed Forces' systems and platforms; authors' translation].[87] The defence bill further states that the Armed Forces are responsible for Sweden's offensive cyber capability, with support from the National Defence Radio Establishment (FRA) described as being of central importance. Sweden therefore belongs with France and the Netherlands rather than with Estonia and Finland, and it is the only member state whose published doctrine separates the locus question into three settings at once: its own systems, systems outside the agency that it has been tasked to defend, and the systems of an adversary. That separation is the framework of Section 3 set out in a national document, which is why the Swedish case matters beyond Sweden itself.

5.1.6 The hybrid and intelligence cases, and the states that publish no concept

Estonia's current strategy, Cybersecurity Strategy 2024-2030, is resilience-framed, and a full review of the English text located no offensive-operations passage,[88] while Estonia's operational cooperation is documented on the defensive side: 'Estonian and U.S. cyber commands jointly conducted a defensive cyber-operation on Estonian Defence Forces' networks from September 23 to November 6' in 2020.[89] Finland added a fourth pillar to its strategy in 2024, with the government stating that 'response and countermeasures have been added to the strategy as a completely new area',[90] and the strategy affirming that 'Breaching the sovereignty of a state is

85 Försvarsmakten. (2024). Doktrinansats Cyberförsvar, version 1.1 [Doctrine approach: cyber defence]. Swedish Armed Forces, in force 1 December 2024. https://www.forsvarsmakten.se/globalassets/02-om-forsvarsmakten/myndighetsinformation/dokument/doktriner/doktrinansats-cyberforsvar-1.1.pdf

86 Försvarsmakten. (n.d.). Cyberförsvarssystem [Cyber defence systems]. https://www.forsvarsmakten.se/om-forsvarsmakten/organisation/stridskrafter/cyberforsvar/cyberforsvarssystem/

87 Regeringen. (2024). Totalförsvaret 2025-2030 (prop. 2024/25:34) [Total defence 2025-2030]. Government of Sweden. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/totalforsvaret-2025-2030_hc0334/

88 Ministry of Justice and Digital Affairs. (2024). Cybersecurity strategy 2024-2030: Cyber-conscious Estonia. https://enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

89 U.S. Cyber Command (2020).

90 Finnish Government. (2024a, October 10). Revised cyber security strategy responds to changed security environment [Press release]. https://valtioneuvosto.fi/en/-/1410829/revised-cyber-security-strategy-responds-to-changed-security-environment

a violation of international law. This also applies to cyberspace'.[91] Czechia locates military cyber operations in its Military Intelligence service, whose National Cyber Operations Centre is mandated to conduct 'široké spektrum operací v kyberprostoru' [a broad spectrum of operations in cyberspace; authors' translation].[92] The mandate is not the whole of the Czech record. An amendment of 2021 inserted into the Act on Military Intelligence a power to carry out an 'aktivní zásah v kybernetickém prostoru' [an active intervention in cyberspace; authors' translation], and set conditions for it: the facts established in cyberspace must indicate a threat to important interests of the state, the cyberattack or threat against those interests must be ongoing or 'bezprostředně hrozí' [immediately imminent; authors' translation], and it must not be possible to avert it in cooperation with the armed forces. The service may act 'pouze po předchozím souhlasu ministra obrany' [only with the prior consent of the Minister of Defence; authors' translation].[93] The statute does not say what an active intervention consists of. What it consisted of on one occasion became public on 8 April 2026, when the Ministry of Defence announced that Military Intelligence had joined, in March 2026, an international operation led by the United States Federal Bureau of Investigation against the global infrastructure of compromised network devices abused by APT28, a group the ministry associates with Russian military intelligence, and that it 'provedlo aktivní zásah spočívající v úpravě nastavení části globálně zneužívané infrastruktury' [carried out an active intervention consisting in altering the configuration of part of the globally abused infrastructure; authors' translation].[94] Czechia is therefore not a state that built an institution and published nothing. It has a statutory power of active intervention, with conditions and a ministerial gate, and it is one of the very few member states whose government has publicly described an out-of-network operation that it carried out. That the power sits in an intelligence service appears to reflect the position of Military Intelligence in the Czech security architecture rather than a considered choice between the models set out in Section 6. Belgium inaugurated a Cyber Command in October 2022, which became a fifth service component in 2024 and was renamed the Belgian Cyber Force in July 2025. Its Cyber Strategy for Defence gives the military cyber capability an offensive mandate, under which Defence develops its own cyber effects to support conventional operations or to conduct its own cyber operations, and the national Cybersecurity Strategy 2.0 for 2021 to 2025 commits Defence, during national crises, to deploy its intrusive and offensive capabilities to respond with a cyberattack of its own, to neutralise an attack and identify its perpetrators. Belgium is therefore coded as military in authority and offensive in register, with a conditional trigger and a neutralising effect; neither text says where such an operation would take place or against which category of actor.[95] Belgium's Strategic Vision for Defence 2025 expressly identifies active defence actions (Defend), the development of offensive cyber capabilities (Fight) and the ability to disrupt enemy networks. It does not specify the detailed legal authorisations governing individual external operations.[96]

Slovakia shares the Czech placement and publishes far more. Its Cyber Defence Centre, established within Military Intelligence in 2018, is the national authority for cyber defence under the Act on Military Intelligence of 2022, which defines active defence in the terms quoted in Section 3.5 and sets out when the Centre may conduct it. The conditions are cumulative. There must be a cyberattack on objects of special importance, other

91 Finnish Government. (2024b). Finland's cyber security strategy 2024-2035. https://enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/FI_NCSS_2024_en.pdf

92 Ministerstvo obrany České republiky. (2019). Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR. https://mocr.mo.gov.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/

93 Parlament České republiky. (2021). Zákon č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství [Act No. 150/2021 Coll. amending Act No. 289/2005 Coll. on Military Intelligence], §§ 16f-16g. Sbírka zákonů, §§ 16f and 16g. https://www.e-sbirka.cz/sb/2021/150

94 Ministerstvo obrany České republiky. (2026). Vojenské zpravodajství provedlo aktivní zásah v kybernetickém prostoru [Military Intelligence carried out an active intervention in cyberspace], 8 April 2026. https://mocr.mo.gov.cz/informacni-servis/zpravodajstvi/vojenske-zpravodajstvi-provedlo-aktivni-zasah-v-kybernetickem-prostoru-263230/

95 Incyber News. (2025). Defense at the heart of European cyber commands. https://incyber.org/en/article/incyber-defense-at-the-heart-of-european-cyber-commands/ Belgian Defence. (2019, May). Cyber Strategy for Defence, English version. https://ccdcoe.org/uploads/2018/10/Belgian-Defence-Cyber-Strategy-EN.pdf. Centre for Cyber Security Belgium. (2021). Cybersecurity Strategy Belgium 2.0, 2021-2025, p. 37. https://ccb.belgium.be/

96 La Défense. (2025). Vision stratégique Défense 2025 [Strategic vision for Defence 2025], approved 18 July 2025. Belgian Defence. https://www.mil.be/media/ac5okcnp/strategic-vision-2025-extended.pdf

important objects or critical infrastructure, or a serious cybersecurity incident. The attack or threat against important interests of the state must be one that 'bezprostredne hrozí, nastane alebo trvá' [is imminent, occurs or is ongoing; authors' translation]. Finally, active defence must be 'jediný možný účinný spôsob ich odvrátenia' [the only possible effective means of averting them; authors' translation]. The same conditions of imminence and necessity also permit active defence against attacks on the systems of the Ministry of Defence or of Military Intelligence, and in fulfilment of collective-defence or other binding international treaty obligations, subject to the statutory conditions in §7(7)(b)–(c) and the prior approval requirement under §7(9). The Centre may act only with the prior consent of the Minister of Defence or, in the minister's absence, of a member of the Security Council designated by its chair, and the chair is to be informed without delay of the start and end of any active defence.[97] Read against the seven questions, the statute answers six: who acts, what the activity is called, where it takes place, when it is permitted, what it is meant to do and against whom. It touches the seventh only through its reference to collective-defence or other binding international treaty obligations. After Sweden's doctrinal approach it is the most complete published answer in the Union, and unlike Sweden's it is law.

Beyond the states treated so far, a further group of member states maintains a military or military-intelligence cyber unit while publishing no concept of its own. Croatia's Cyberspace Command was established in 2019 under an amendment to the Defence Act that gives the armed forces competence for action in cyberspace in neutral terms. Hungary's Cyber Operations Command exercises operational-level command of cyber and information operations under a 2022 government decree. Bulgaria maintains a command for communications-information support and cyber defence. Greece maintains a cyber defence directorate under its defence staff, named in the strategy for 2026 to 2030 as the Διεύθυνση Κυβερνοάμυνας, and a Joint Information Technology Corps established by Law 5110/2024.[98] Austria assigned military cyber tasks to Directorate 6 of the General Staff in October 2024, and its Security Strategy of 2024, reviewed for this study, frames cyber in terms of the resilience of constitutional institutions and critical infrastructure without adopting an active or offensive register,[99] while the progress report on its measures catalogue records a cross-cutting defence concept, 'Einsatz im Cyber-Raum' [deployment in cyberspace; authors' translation], completed in 2023 and not published.[100] The official 2025 progress report refers to this concept, but its underlying text was not reviewed as a publicly available primary document. Latvia maintains a National Guard cyber defence unit dating from 2013, which concentrates on defensive cyberspace operations and on support to the armed forces, to CERT.LV and to the military CERT. Slovenia maintains a cyber defence centre dating from 2014. Latvia and Slovenia differ from the rest of this group in naming an active or proactive capability, as Section 5.2 records. Ireland's Joint Cyber Defence Command reached initial operating capability in January 2025 and is to reach full operating capability in January 2028. Its mission is to 'conduct full spectrum cyberspace operations across the cyber domain in order to support Defence Forces operations at home and overseas, and to enhance national cyber defence resilience and contingent capabilities'. Its operations are to be 'directed by the DF Joint Force Commander on consultation with the CHOD', the Chief of Defence, and to be 'subject to Use of Force policy provisions, approved Rules of Engagement (ROE) and National Authority as appropriate', and its Joint Cyber Operations Unit is to conduct defensive cyberspace operations, active cyber defence, and cyberspace intelligence, surveillance and reconnaissance.[101] Ireland is the clearest case in the Union of a state that has named the activity and built the command while expressly deferring the doctrine, which its strategy makes a

97 Národná rada Slovenskej republiky (2022), s. 7(7) to 7(9).

98 Hellenic Republic. (2024). Law 5110/2024, Government Gazette A 75 of 24 May 2024, establishing among other provisions a Joint Information Technology Corps in the Armed Forces.

99 Bundeskanzleramt. (2024). Österreichische Sicherheitsstrategie 2024 [Austrian security strategy 2024]. Republic of Austria. https://www.bundeskanzleramt.gv.at/dam/jcr:941a3cb3-7320-4c31-a4d2-3307f57faad3/sicherheitsstrategie_oesterreich_2024.pdf

100 Bundeskanzleramt. (2025). Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit: Fortschrittsbericht 1/2025 [Measures catalogue of the Austrian cyber security strategy: progress report 1/2025], as at 5 March 2025. https://www.bundeskanzleramt.gv.at/dam/jcr:cdfd1277-9df5-4e65-87bc-bffd0c54ed7b/Massnahmenkatalog_OeSCS_Fortschrittsbericht_1_2025.pdf

101 Defence Forces Ireland (2024).

condition of progressing operations. For Malta and Cyprus no military cyber unit was located. Luxembourg maintains no such command, and its cyberdefence strategy of 2021 defines cyberdefence as the 'moyens mis en place pour mener à bien et exécuter des mesures défensives contre des cybermenaces' [means put in place to carry out and execute defensive measures against cyber threats; authors' translation] and a cyber operation as an 'ensemble d'actions menées dans ou via le cyberespace dans le but de préserver la liberté d'action' [set of actions conducted in or through cyberspace in order to preserve freedom of action; authors' translation].[102] None of these mandates is qualified as offensive, and apart from the authorisation routes of Ireland and Latvia none names a locus, a trigger or an effect: they describe cyber defence, or operations in cyberspace, without saying what the operations would be. The instruments are listed by state in Annex C.

5.2 Register: how states name the activity

KEY FINDINGS

1 Vocabulary is the one question every publishing state has answered, and the one whose answer tells us least.

2 Nine member states use an explicitly offensive register, but a choice of words does not show what a capability does.

The vocabulary a state chooses is the question on which every state that has published anything has given an answer, and the one on which the answer tells us least. Nine member states use the explicitly offensive register: France in the very name of its doctrine, Belgium in the offensive cyber capability its Cyber Strategy for Defence assigns to the armed forces, the Netherlands in 'offensief tegendruk', Romania in 'răspuns ofensiv', Poland in 'ofensywne', Italy in 'operazioni militari cibernetiche offensive', Denmark in 'offensive militære operationer' and in a doctrine that defines them by the application of force, Portugal in 'atividade ofensiva', and Sweden in 'offensiva cyberoperationer'. Polish legislation also uses the qualified term 'aktywna obrona', alongside 'proaktywna ochrona', in defining the statutory remit of the Cyberspace Defence Forces. Germany prefers the qualified 'aktive Cyberabwehr', Finland the legal register of 'response and countermeasures', Spain neutral operational language for its military command and the qualified 'ciberdefensa activa' for protective measures in its cybersecurity strategy, Lithuania neutral operational language, and Estonia defensive framing. Figure 5 sets out the vocabulary each member state has chosen.

FIGURE 5

How member states name the activity

Nineteen member states have chosen a vocabulary. Nine call the activity offensive outright, seven qualify it as active, proactive or a countermeasure, and only Estonia frames it as purely defensive.



Explicitly offensive *e.g. lutte informatique offensive*	9	France, Netherlands, Romania, Poland, Italy, Denmark, Portugal, Sweden, Belgium
Qualified: active, proactive *e.g. aktívna obrana, Aktive Cyberabwehr*	7	Germany (pending), Czechia, Finland (countermeasures), Ireland (undefined), Latvia, Slovakia (defined in statute), Slovenia
Operational, unqualified	2	Spain, Lithuania
Defensive only	1	Estonia
No published position	8	Austria, Bulgaria, Croatia, Cyprus, Greece, Hungary, Luxembourg, Malta

Source: authors, Annex A and Section 5.2. One segment = one member state. A state's use of the word offensive is evidence about vocabulary, not about what the capability does (Section 2.3). EU CYBER DIRECT

102 Direction de la défense. (2021). Stratégie de cyberdéfense du Luxembourg [Luxembourg cyberdefence strategy]. Ministère des Affaires étrangères et européennes, February 2021. https://defense.gouvernement.lu/

Five further member states use the qualified register in their current documents. Czechia, Slovakia and Ireland are discussed in Sections 3.5 and 5.1.6, and Czechia's usage is the barest of the three, a statutory authorisation to carry out an 'aktivní zásah' that the statute leaves undefined. Slovakia is the only member state to define the term, in statute, and Ireland names it as a category of military operations while deferring its definition to doctrine still to be written. The other two, Latvia and Slovenia, use it without defining it. Latvia's cybersecurity strategy for 2023 to 2026 sets out, under its deterrence priority, the tasks of detecting, investigating and disrupting malicious activity in cyberspace and holding offenders to account, 'kā arī attīstīt aktīvās kiberaizsardzības spējas' [and also to develop active cyber defence capabilities; authors' translation], and states separately that the protection of information and of cyberspace in crisis and in war is to be secured 'izmantojot aktīvos un pasīvos aizsardzības pasākumus' [using active and passive defence measures; authors' translation].[103] Latvia therefore joins Germany, Slovakia, Ireland, Poland and Spain in using the term active defence itself, Spain only in a protective sense. The strategy assigns the capability it names no locus, no trigger and no effect, but the term is not confined to the strategy. The National Security Law, as amended in June 2022, provides that 'Aizsardzības ministrs, izvērtējot valsts drošības un aizsardzības intereses, pieņem lēmumu par Nacionālo bruņoto spēku speciālo operāciju īstenošanu ārvalstīs un aktīvās kiberaizsardzības operāciju īstenošanu' [The Minister for Defence, having assessed the interests of national security and defence, shall take the decision on the implementation of special operations of the National Armed Forces abroad and on the implementation of active cyber defence operations; authors' translation].[104] The same provision requires the Minister to coordinate that decision with the Prime Minister and the Minister for Foreign Affairs, and Latvia distinguishes this legal decision-making procedure from the operational development of active cyber defence capabilities, which remains under discussion. Latvia and Slovakia are thus the only member states to have published a statutory procedure for deciding on operations that the law itself calls active defence. Latvia's is placed in the same sentence as special operations abroad, and its strategy treats the capability as one still to be developed. It is the inverse of the pattern in Section 5.1.6, where institutions precede doctrine: in Latvia the law precedes the capability, and it uses the term without defining it. Slovenia's Medium-Term Defence Programme 2023 to 2028 commits the armed forces to develop cyber operations capabilities providing 'proaktivno in stalno odzivanje na kibernetske grožnje' [proactive and continuous response to cyber threats; authors' translation], and to establish a 'zmogljivost za nekinetično delovanje' [capability for non-kinetic action; authors' translation].[105] Neither state says where the capability would be used or against whom, which is the pattern Section 7.3 describes, and in neither case does a published procedure or programme show that a mature operational capability already exists; Slovenia's programme, moreover, places proactive cyber response and non-kinetic action side by side without treating them as one capability.

103 Aizsardzības ministrija. (2023). Latvijas kiberdrošības stratēģija 2023.-2026. gadam [Latvia's cyber security strategy 2023-2026]. https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kiberdro%C5%A1%C4%ABbas%20strat%C4%93%C4%A3ija%202023.-2026.gadam_.pdf

104 Saeima. (2022). Nacionālās drošības likums [National Security Law], section 11(5) as amended 16 June 2022. https://likumi.lv/ta/id/14011-nacionalas-drosibas-likums

105 Ministrstvo za obrambo Republike Slovenije. (2023). Srednjeročni obrambni program Republike Slovenije 2023-2028 [Medium-term defence programme of the Republic of Slovenia 2023-2028], No. 80300-1/2023/10, 31 May 2023. https://www.gov.si/assets/ministrstva/MO/Dokumenti/SOPR_2023-2028_sprejet.pdf Retained in the successor programme: Ministrstvo za obrambo Republike Slovenije. (2025). Srednjeročni obrambni program Republike Slovenije 2026-2031 [Medium-term defence programme 2026-2031], adopted 6 November 2025, p. 26, on proactive and continuous responses to cyber threats. https://www.gov.si/assets/ministrstva/MO/Dokumenti/sopr_26-31_sprejet.pdf

For some member states the qualified 'active defence' register accompanies capability that their documents do not otherwise describe, which suggests that the term can serve to describe capability in a register suited to a state's domestic political context, though the Dutch and French cases show that explicit vocabulary is equally available within the Union. The German trajectory is illustrative, from coalition-agreement scepticism about hack-backs to a bill empowering federal police to disrupt and destroy attacker infrastructure, with 'aktive Cyberabwehr' as the label throughout.[106] A claim that circulates in the commentary should therefore be treated with caution: that vocabulary and capability are inversely related. The record does not support an inversion as a general rule. The Netherlands combines the most expansive published concept in the Union, action in adversary infrastructure as a permanent posture, with the explicitly offensive register, and France names its doctrine offensive. What the record does support is the weaker and more useful claim that register is a poor proxy for reach in either direction: the qualified register is used both by states with the furthest documented reach, the United Kingdom's NCF and Germany's pending federal powers, and by the United States for a purely internal technical capability, while the explicit register is used both by states that document action in adversary infrastructure and by states whose documents describe no actions at all. Inferences from a state's vocabulary to its posture, in either direction, should therefore not be drawn.

Mapping the EU landscape onto the three non-EU reference states, the United States, the United Kingdom and Norway, shows that vocabulary tracks national convention rather than capability: the states with the most developed offensive capability either avoid the term active cyber defence or use it for something else entirely, while usage within the EU is mixed, with the Netherlands and France attaching explicitly offensive vocabulary to their most expansive concepts. The United States describes its posture as defending forward: 'Since 2018, the Department has conducted a number of significant cyberspace operations through its policy of defending forward, actively disrupting malicious cyber activity before it can affect the U.S. Homeland',[107] a posture U.S. Cyber Command frames as persistent engagement that 'shifts DOD and USCYBERCOM's posture in cyberspace from reactive to proactive'.[108] Its formal definition of active cyber defense, meanwhile, is the internal technical one quoted in Section 3. The United Kingdom created the National Cyber Force in 2020 'by building on the previous National Offensive Cyber Programme', drawing together 'personnel from GCHQ, the Ministry of Defence (MOD), including Defence Science and Technology Laboratory (Dstl), and SIS under one unified command', under the banner of responsible cyber power: 'to be a truly responsible cyber power, nations must be able to contest and compete with adversaries in cyberspace'.[109] Its active cyber defence, as shown, is a domestic protective programme. Norway publishes a defensive national strategy[110] and a national position on international law whose countermeasures passage requires that measures 'must be limited to what is considered necessary and proportional, and may only target the State to which the cyber operation or internationally wrongful act can be attributed'.[111]

One episode illustrates how contested even the reference points can be. In early 2025 The Record reported, citing three unnamed sources, that the U.S. Secretary of Defense had ordered Cyber Command 'to stand down from all planning against Russia, including offensive digital actions'.[112] The Pentagon denied it on the record,

106 BMI (2026); Bundesregierung (2026).

107 U.S. Department of Defense (2023).

108 U.S. Cyber Command (2022).

109 National Cyber Force. (2023). Responsible cyber power in practice. https://www.gchq.gov.uk/files/NCF_Responsible_Cyber_Power_In_Practice.pdf

110 Norwegian Ministries. (2019). National cyber security strategy for Norway. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

111 Government of Norway. (2021). National position of Norway on international law in cyberspace. Reproduced in the CCDCOE Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Norway_(2021)

112 Matishak, M. (2025, February 28). Exclusive: Hegseth orders Cyber Command to stand down on Russia planning. The Record. https://therecord.media/hegseth-orders-cyber-command-stand-down-russia-planning

stating that it 'has neither canceled nor delayed any cyber operations directed against malicious Russian targets and there has been no stand-down order whatsoever'.[113] In May 2025 Representative Don Bacon stated publicly that a one-day pause had occurred; its full scope and the underlying orders have not been independently established, and this study reports both accounts.

5.3 Locus and target: where and against whom

KEY FINDINGS

1. Seven member states describe action in adversary or third-party infrastructure; most say very little about where they would act.
2. Whether an operation targets a criminal server or a state actor decides whether it is law enforcement or interstate conduct, and on the published record partners cannot tell which most states intend.

On these two questions the member states have said very little, and the little they have said is worth stating precisely, because the answers decide which body of law an operation falls under. Seven member states describe action in adversary or third-party infrastructure; Romania and Portugal, discussed below, use language that names the activity without fixing its location. France's doctrine speaks of effects against 'un système adverse'. The Netherlands' posture is one of offensive counter-pressure, and its Temporary Act is, by its own title, directed at 'landen met een offensief cyberprogramma', countries with an offensive cyber programme. Romania's statute contemplates offensive response to 'atacuri cibernetice care contravin dreptului internațional'. Slovakia's statute defines active defence by operations creating effects on 'útočníkove informačné systémy a siete', the attacker's information systems and networks. Germany's police bill is directed at the attacking systems from which a danger emanates, while its intelligence bill of September 2026 names foreign IT infrastructure, including the servers of state hacker groups, explicitly. Portugal's cyberdefence strategy speaks of operations 'no e através do ciberespaço' directed at an entity's capacity to access cyberspace; the phrase identifies the domain of an operation, not its location, and does not by itself establish action in an adversary or third-party network, so Portugal's external locus is recorded as not established. Denmark's joint doctrine defines an offensive cyberspace operation as the application of force 'i eller gennem en modstanders del af cyberspace', in or through an adversary's part of cyberspace. Czechia's Military Intelligence has described altering the configuration of attacker-controlled infrastructure outside its own networks. Sweden is the seventh, and its doctrinal approach is the most explicit treatment of the question published by any member state, setting out three loci in a single text: its own systems, systems outside the agency that it has been tasked to defend, and the adversary's systems. One state describes action only on the inward side: Estonia, whose documented operational cooperation took place on its own defence networks with a consenting partner present. Figure 6 shows where each member state says it would act, and against whom.

Against whom is even less often stated. The Dutch statute names countries with an offensive cyber programme. The Defence Cyber Strategy is broader than the statute's title, and contemplates cyber deployment coordinated with every other form of military action, including allied operations and non-military instruments of power, so the statutory category should not be read as the outer limit of the Dutch concept. Romania's Law No. 58/2023 provides for offensive response capabilities in the event of cyberattacks that contravene international law; the provision does not specify the category of actor responsible for an attack or whether a response would take place beyond defended networks, so Romania is recorded as publishing neither a locus nor a target. The German police bill names the attacking systems irrespective of the actor

113 Stars and Stripes. (2025, March 4). Pentagon denies halting cybersecurity operations against Russia. https://www.stripes.com/theaters/us/2025-03-04/cyber-hegseth-pentagon-russia-17031715.html

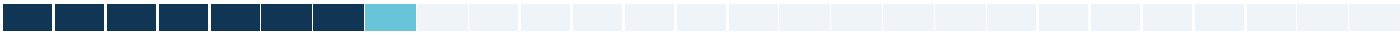
behind them, and the intelligence bill names state hacker groups and other actors in a specific situation of threat from foreign powers. The Slovak statute names the attacker whose attack on specified objects or state interests gives rise to the power, without distinguishing state from non-state authors. The Swedish doctrinal approach defines the counterpart as an antagonist, a category that covers state, state-sponsored and non-state actors. The Portuguese strategy names threats originating from states or from non-state entities, directly or indirectly, and singles out those promoted covertly by states, which is the most precise target statement published by any member state. Czechia, without publishing a target category, has named an actual target, the compromised infrastructure abused by a group it associates with Russian military intelligence. No other member state says. The reference states are instructive by contrast: the United Kingdom's Active Cyber Defence programme is aimed explicitly at high-volume commodity crime, while its National Cyber Force contests state adversaries, and the United States' defend forward posture speaks of 'malicious cyber activity' without distinguishing its authors. Whether an out-of-network operation is directed at a criminal server or at a state actor determines whether it is law enforcement or interstate conduct, which law governs it, and what escalation risk it carries, and on the current published record a partner cannot know which of these most member states intend. Part IV returns to this, because it is the gap that a common framework could most usefully close.

FIGURE 6

Where member states say they would act, and against whom

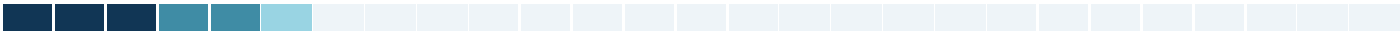
Seven member states say whether they would act beyond their own networks. Five say against whom, and a sixth has named a target only in practice.

LOCUS · WHERE THE STATE SAYS IT WILL ACT



Adversary or third-party infrastructure	7	France, Netherlands, Germany (pending), Denmark, Czechia, Sweden (own, defended and adversary systems), Slovakia
Own and partner networks only	1	Estonia
Not published	19	the remaining nineteen member states

TARGET · AGAINST WHOM THE ACTIVITY IS DIRECTED



State actors and attacker systems	3	Germany (pending), Portugal, Sweden
Attacker systems, actor not specified	2	Netherlands, Slovakia
Named in practice only	1	Czechia (a state-linked group named in one announced operation)
Not published	21	the remaining twenty-one member states

Source: authors, Annex A and Section 5.3. One segment = one member state. Germany's answers come from bills not yet enacted.

EU CYBER DIRECT

5.4 Trigger: when action is authorised

KEY FINDINGS

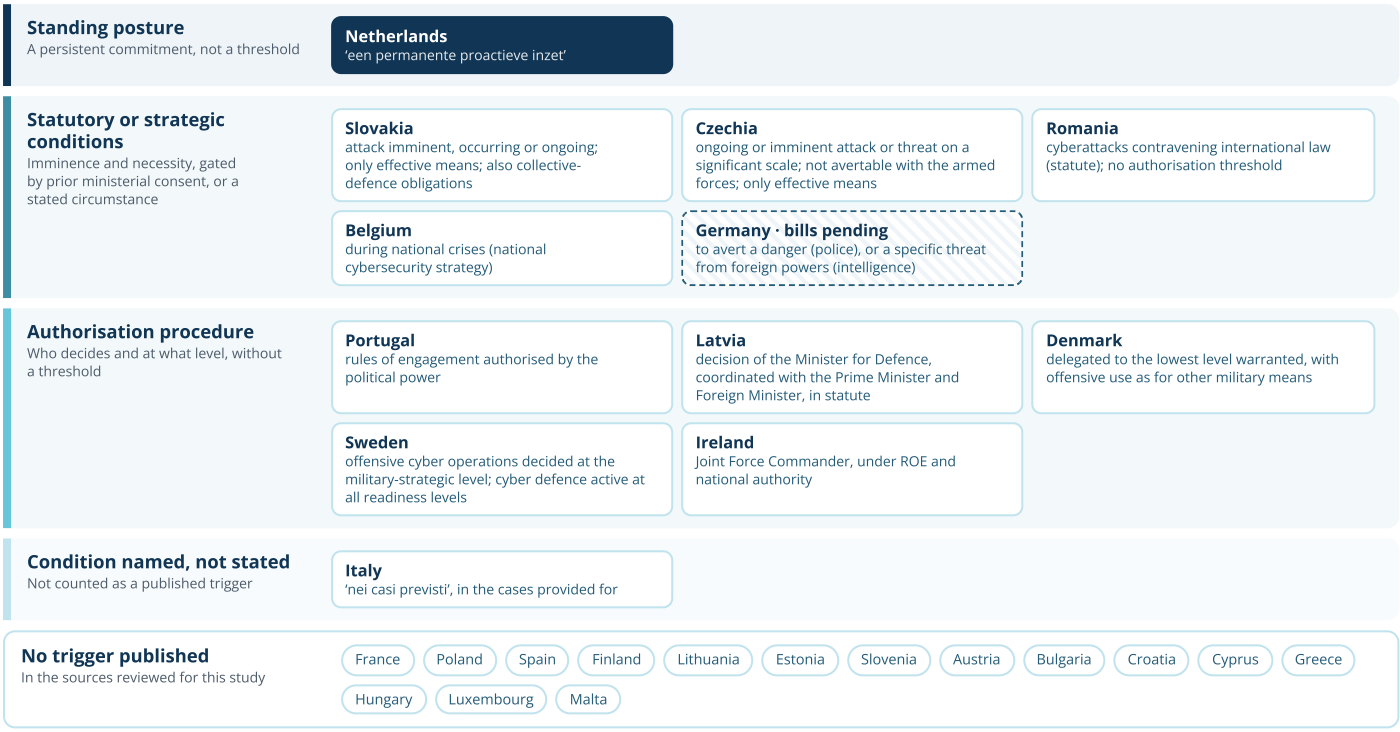
1. The states with the strongest vocabulary say least about triggers: France and Poland publish none, and Romania names only the circumstance.
2. Only the Netherlands commits to a standing posture; every other published trigger is reactive, conditional or a decision procedure.

The trigger is the question on which the states with the strongest vocabulary have said least. Of the nine member states using the offensive register, two publish no operational trigger at all, France and Poland. Romania's statute names the circumstance, cyberattacks that contravene international law, without an authorisation threshold, Belgium's national strategy names national crises, and Italy's 'nei casi previsti', in the cases provided for, names a condition without stating it and is therefore not counted as a published trigger (Figure 7). One state commits to a standing posture: the Netherlands, in 'een permanente proactieve inzet'. Sweden's doctrinal approach states that 'stora delar av cyberförsvaret är aktivt i samtliga konflikt- och beredskapsnivåer', a readiness condition for cyber defence as a whole, and separately places the decision on offensive cyber operations at the military-strategic level; the published material does not establish that offensive operations are continuously conducted, so Sweden is recorded as publishing a decision procedure, not a standing posture. Finland's strategy identifies 'response and countermeasures' as a priority, but the passage does not specify the circumstances or authorisation threshold for an operation, so no trigger is recorded. Latvia publishes not a trigger but a decision procedure: under Section 11(5) of the National Security Law the Minister for Defence decides on active cyber defence operations after assessing national security and defence interests, in coordination with the Prime Minister and the Minister for Foreign Affairs. Slovakia publishes the most fully specified trigger in the Union, and in statute: an attack on specified objects or critical infrastructure, or a serious incident, that is imminent, occurring or ongoing, where active defence is the only effective means of averting it, with the prior consent of the Minister of Defence, and also in connection with collective-defence or other binding international treaty obligations, subject to the statutory conditions in §7(7)(b)–(c) and the prior approval requirement under §7(9). Czechia publishes conditions as exacting as Slovakia's and in the same form: an ongoing or immediately imminent cyberattack or threat to important interests of the state on a significant scale, which cannot be averted in cooperation with the armed forces and for which active intervention is assessed as the only possible effective means, with the prior consent of the Minister of Defence. Germany's two bills, neither yet enacted, would add statutory conditions of their own, permitting police action to avert a danger and intelligence action in a specific situation of threat from foreign powers. Portugal publishes not a threshold but an authorisation structure, with rules of engagement whose authorisations run from the tactical to the strategic level and are themselves authorised by the political power. Denmark publishes a decision rule pointing the other way, delegating the competence to launch cyberspace operations to the lowest level the conditions warrant, while reserving the use of its offensive capacity to the procedure that governs other military means of force. Ireland places the direction of operations with the Joint Force Commander, under rules of engagement. Spain's command acts 'de acuerdo con los planes operativos en vigor', which places the trigger in classified planning rather than in public doctrine. The Union therefore does not face a spectrum of trigger doctrines to harmonise. It faces one published standing posture, two sets of statutory conditions in Slovakia and Czechia, with a third pending in Germany, five published authorisation procedures without thresholds, in Portugal, Latvia, Denmark, Ireland and Sweden, and elsewhere a general absence of published triggers. The absence appears deliberate: the trigger is the parameter closest to operational secrecy, and states have treated it accordingly. Figure 7 groups the published answers by kind.

FIGURE 7

When action is authorised: distinct kinds of answer

The published triggers are not points on one spectrum that could be harmonised. They are different kinds of answer: a standing posture, statutory or strategic conditions and authorisation procedures.



Source: authors, Section 5.4 and Annex A. Rungs describe the form of the published answer, not the permissiveness of the policy.

EU CYBER DIRECT

5.5 Effect: what the activity is intended to do

KEY FINDINGS

1. Only eight member states describe what their capability beyond their own networks does.
2. Where effects are described they range from degrading an adversary system's availability or data to detecting, restricting, disrupting and disabling attackers.

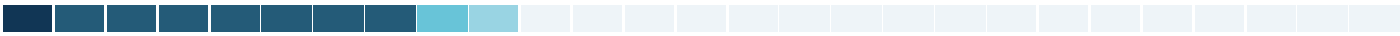
Only eight member states describe what their capability beyond their own networks does. France's doctrine aims to produce effects against an adversary system 'pour en altérer la disponibilité ou la confidentialité des données'. The passage describes disruption and neutralisation, not destruction, and France is coded accordingly. The Netherlands sets out four effects in sequence: to detect aggressive cyber actors in good time, to restrict their freedom of action, to disrupt their activities and to disable their means of attack, which it frames as offensive counter-pressure against persistent attacks. Germany's bill would permit the prohibition of a system's operation, the redirection of traffic, and the reading, deletion or alteration of data. Belgium's national strategy describes a cyberattack of Defence's own to neutralise an attack. Sweden's doctrinal approach names the denial of an adversary's access and the manipulation of data and information, in support of the Supreme Commander's freedom of action and of Sweden's sovereign rights. Slovakia's statute defines active defence by its effect, operations on the attacker's systems 's cieľom narušiť ich dostupnosť, dôvernosť alebo integritu' [with the aim of disrupting their availability, confidentiality or integrity; authors' translation]. Portugal's strategy is the most explicit of all on this question, naming operations intended to neutralise, manipulate, deny, disrupt, degrade or destroy an entity's capacity to access cyberspace freely. Czechia's statute says nothing about effects, but its government has described one: the alteration of the configuration of

attacker-controlled infrastructure, together with the securing of vulnerable devices on Czech territory. Romania, Italy and Poland declare an offensive capability and describe no actions, and are recorded here as having adopted the vocabulary, while Denmark defines its offensive operations by the application of force in an adversary's part of cyberspace but describes no particular effect. Their apparent similarity to France and the Netherlands is a similarity of words, not of documented concept, and the distinction matters for the Union's discussions. Ireland's strategy speaks of effects that achieve commanders' objectives, without saying what they are.[114] The remaining states describe protective activity within their own networks or nothing at all. Figure 8 sets out what each member state says the activity would do.

FIGURE 8

What the activity is described as doing

Eight member states describe what the activity does, from neutralising, restricting and disrupting attackers to destroying their systems. Only Portugal expressly includes destruction; the French passage cited describes disruption.



Disruptive to destructive	1	Portugal
Disruptive *detect, restrict, disrupt, disable*	7	France, Netherlands, Germany (pending), Czechia (as described in one operation), Slovakia, Sweden, Belgium (neutralisation)
Application of force, no specific effect	1	Denmark
Protective, own networks	1	Estonia
Not published	17	the remaining seventeen member states

Source: authors, Annex A and Section 5.5. One segment = one member state. Protective effect within a state's own networks is recorded but not counted as an answer to the effect question.

EU CYBER DIRECT

5.6 Legal position: reconciliation with international law

KEY FINDINGS

1. The 2024 EU Declaration is the first common EU position: a violation of sovereignty is an internationally wrongful act even below the thresholds of intervention or force.
2. The United Kingdom stands apart in rejecting a specific sovereignty rule, a divergence that matters for joint operations with the EU's closest non-EU partner.

The Declaration on a Common Understanding of the Application of International Law to Cyberspace, approved on 18 November 2024, is the first EU-level common position on the subject. On sovereignty it states: 'The violation of the obligation to respect State sovereignty amounts to an internationally wrongful act, even if such a violation does not constitute a prohibited intervention or a prohibited use of force'.[115] On due diligence: 'Due diligence is an obligation of conduct, not of result'. On the use of force: 'Whenever the scale and effects of a cyber operation are comparable to those of a traditional kinetic use of force, it constitutes a use of force within the meaning of Article 2(4) of the UN Charter'. On international humanitarian law: 'The principle of distinction applies irrespective of whether the cyber attack is exercised in an offensive or a defensive context'.

114 Defence Forces Ireland (2024).

115 Council of the European Union. (2024). Declaration on a common understanding of the application of international law to cyberspace (ST 15833/2024). https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf

[116] The last sentence bears directly on this study's subject: under the EU's own position, labelling an operation defensive, active or otherwise changes nothing in its legal assessment. Figure 9 shows which member states have published a national position on international law in cyberspace.

FIGURE 9

National positions on international law in cyberspace

Fifteen member states have published a national position. Slovakia, one of the two states that answer six of the seven questions in a single text, has not.



Published: sovereignty as a rule	5	France, Netherlands, Poland, Estonia, Finland
Published, not analysed here	10	Germany, Romania, Italy, Denmark, Czechia, Belgium, Sweden, Ireland, Slovenia, Austria
No national position located	12	Slovakia, Portugal, Latvia, Spain, Lithuania, Bulgaria, Croatia, Cyprus, Greece, Hungary, Luxembourg, Malta

Source: authors, Annex A, Annex B and Section 5.6. One segment = one member state.

EU CYBER DIRECT

National positions verified for this study align with the Declaration's sovereignty rule in France ('Le principe de souveraineté s'applique au cyberespace' [the principle of sovereignty applies to cyberspace; authors' translation]),[117] Finland ('Finland sees sovereignty as a primary rule of international law, a breach of which amounts to an internationally wrongful act'),[118] the Netherlands, which holds that states may not conduct cyber operations violating another state's sovereignty while noting that 'the precise boundaries … have yet to fully crystallise',[119] and Poland, whose position adds that 'the violation of a state's sovereignty may occur both in the event of an attack against state infrastructure and against private infrastructure'.[120] Estonia has gone furthest on response, advancing the view that 'states which are not directly injured may apply countermeasures to support the state directly affected by the malicious cyber operation'.[121] The United Kingdom stands apart, and its position is recorded not only in speeches but as a formal national reservation to NATO doctrine: 'the UK government does not consider that the current state of international law allows for a specific rule or additional prohibition for cyberspace operations beyond that of a prohibited intervention'.[122] Any EU active cyber defence framework that reaches into foreign networks will therefore be assessed by the EU's own members under a sovereignty rule that the Union's closest non-EU partner does not accept.

116 Council of the European Union (2024).

117 Ministère des Armées. (2019). Droit international appliqué aux opérations dans le cyberespace. https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf

118 Ministry for Foreign Affairs of Finland. (2020). International law and cyberspace: Finland's national positions. https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf

119 Government of the Netherlands. (2019). Appendix: International law in cyberspace [Letter to Parliament]. Reproduced in the CCDCOE Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019)

120 Republic of Poland. (2022). The Republic of Poland's position on the application of international law in cyberspace. https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131

121 Republic of Estonia. (2019). President of the Republic at the opening of CyCon 2019. Reproduced in the CCDCOE Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Estonia_(2019)

122 NATO Standardization Office (2020), Record of Specific Reservations.

PART III

Three models of active cyber defence in the Union

6. The models

KEY FINDINGS

1. Member states fall into three models, each with one clear exemplar: military (France), intelligence-enabled (the Netherlands) and police-law (Germany).
2. Building the institution before publishing the concept is the most common position in the Union, which makes legal interoperability difficult.

Read against the seven questions above, the member states fall into three models, each with a single clear exemplar. They are described as models rather than as types because a model is defined by its institutional logic, not by the number of states that follow it, and because the remaining member states are best understood by how they resemble or depart from them.

The military model. France is its exemplar: offensive cyber operations are a published military doctrine, placed under a joint cyber command and, through it, under executive authority, with the state's international law position published separately and in similar terms. Romania, Italy, Denmark, Poland and Portugal resemble France in placing the capability under military authority and in using the offensive register, but they differ sharply in what they publish: Romania in statute, Italy in a strategy sentence, Denmark in a budget line of a defence agreement and in a joint doctrine, Poland in statute and on a ministry webpage, and Portugal in a national cyberdefence strategy. What unites them is a choice of institution and a choice of words. What separates most of them from France is that France has said what the capability does. Portugal says it too, and in more operational terms than France, while Denmark says where force may be applied without saying to what effect. Sweden belongs in this model as well, and is the only follower whose published doctrinal approach answers every question the model raises, differing from France in publishing a trigger, which France does not.

The intelligence-enabled model. The Netherlands is its exemplar and, within the Union, its only full member: a defence strategy committing to a permanent proactive posture rests on intelligence statutes that were rebuilt around an oversight architecture, and the innovation of the Temporary Act lies in adjusting that oversight rather than in creating powers. The United Kingdom's National Cyber Force, which draws together intelligence and defence personnel under one command, is the closest analogue outside the Union. The model's defining feature is that persistence in peacetime is achieved by redesigning oversight, and its lesson for other member states is that a persistent posture will be an oversight question before it is an operational one. Slovakia is its nearest relative in the Union: its statutory power of active defence sits in military intelligence law, but it is governed by prior ministerial consent rather than by a redesigned oversight architecture, and it is conditional rather than persistent.

The police-law model. Germany is its exemplar and, pending the Bundestag's decision, its only instance anywhere in the Union: powers to act against attacker infrastructure are assigned to the federal police and the Federal Criminal Police Office under the logic of hazard prevention. The model has one advantage that the others lack, in that it keeps offensive cyber action out of both the armed forces and the intelligence services, and one cost that the others do not pay, in that it engages the constitutional allocation of competences and the judicial safeguards attached to police powers. Whether the model survives the legislative process will be settled in the Bundestag.

Three further groups of states relate to these models without following any of them. Spain and Lithuania have built the institution before publishing the doctrine, and Ireland has done so deliberately, making doctrine a published precondition of operations: each has a military cyber command whose founding documents describe operations without qualifying them as offensive or defensive. Spain is the instructive case, because its doctrine exists: PDC-3.20, Doctrina de operaciones en el ámbito ciberespacial, was issued by the defence staff on 28 April 2021 and is cited in the ministry's own teaching material, but it is not published, so what Spain has decided cannot be read. Its framework of national coordination under the National Cybersecurity Council and of protection under the CNI and the CCN, set out in Section 5.1.5, is published but does not concern action beyond national networks. They are the documented core of a larger group: as Section 5.1.6 records, five further member states, Austria, Bulgaria, Croatia, Greece and Hungary, maintain a military cyber unit whose published mandate is equally unqualified, which makes building the institution before publishing the concept the most common position in the Union rather than an exception to the three models. The groups cut across one another: a state may appear here and also among those with no published position on active cyber defence, because the first sorts on institutions and the second on concepts.

Estonia and Finland are resilience-first states whose strategies are defensive in framing even where, as with Estonia's advocacy of collective countermeasures and Finland's new pillar of response and countermeasures, their legal diplomacy is assertive. In these states the assertiveness appears in public statements on international law rather than in the defence documents examined; Estonia's 2019 statement on collective countermeasures was made by President Kersti Kaljulaid. And the remaining member states have for the most part published no position that would allow us to place them at all, although the group of unreviewed states is narrow. Figure 10 dates the published instruments on which these groupings rest.

FIGURE 10

The published instruments, 2019 to 2026

> Twenty of the twenty-six national instruments shown date from 2022 or later. In 2026 alone came two German bills and Czechia's account of an operation carried out.



Source: authors, Sections 3.5, 5.1 and 5.2 and Annex B. Position within a year is approximate. Denmark's capacity decision dates from the Defence Agreement 2010 to 2014.

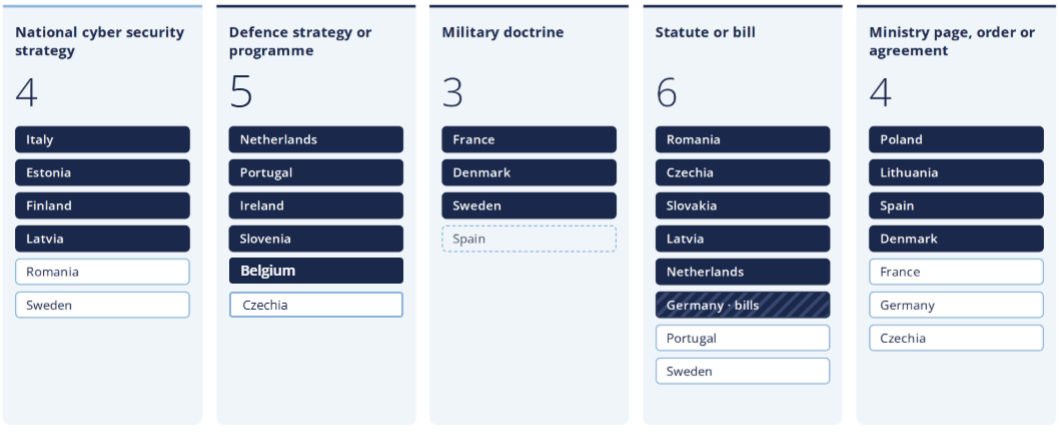
EU CYBER DIRECT

Current strategies have been reviewed in the national language for Austria, Bulgaria, Cyprus, Greece, Ireland, Latvia, Luxembourg, Malta and Slovakia. In each of these except Greece, Ireland, Latvia and Slovakia no active, proactive or offensive term was located, which converts those entries from not verified into reviewed and absent. Greece's strategy for 2026 to 2030 refers to active deterrence in developing national defence cyber capabilities; the phrase does not by itself establish a published mandate for offensive operations or for action beyond defended networks, so Greece's coding is unchanged. For Ireland and Slovakia the term appears in a Defence Forces strategy and in a statute respectively, rather than in the national cybersecurity strategy. Two recent successor strategies do not change the coding: Greece adopted a national cybersecurity strategy for 2026 to 2030 in December 2025,[123] and Czechia a successor approved in September 2025 and effective from 2026.[124] Portugal's 2019 to 2023 cybersecurity strategy has lapsed[125] and its replacement, required by the cybersecurity legal regime adopted in December 2025, had not been adopted at the date of this study.[126] That gap concerns civil cybersecurity only, and Portugal's cyberdefence strategy of 2022, treated in Section 5.1.5, is in force. Latvia and Slovenia, on the strength of the passages quoted in Section 5.2, place active or proactive capabilities within military or defence structures, while leaving their operational scope largely unspecified. Czechia leaves this group altogether: with a statutory power of active intervention and a described operation, it belongs beside Slovakia among the states that place active measures in military intelligence, and Portugal belongs with the military model described above. Slovakia, which names, places and conditions it in statute, belongs with none of these groups and is discussed with the intelligence-enabled model above. What remains unreviewed is narrow: Croatia's standalone national strategy, Hungary's national strategy, and Slovenia's cybersecurity resolution, each recorded in Section 8. Figure 11 shows the kinds of document in which the

FIGURE 11

Where the concepts are published

> The concepts are published mainly in statutes, defence strategies, doctrine and ministry pages. Four states set theirs out in a national cyber security strategy, and none of those four describes action beyond its own networks.



Nineteen member states with substantive published concepts, including Belgium. Numbers count states carrying their concept in each document type, and some use two.

Source: authors, Annexes A and C.

EU CYBER DIRECT

123 National Cybersecurity Authority of Greece. (2025). Εθνική Στρατηγική Κυβερνοασφάλειας 2026-2030 [National cybersecurity strategy 2026-2030], ministerial decision No. 2563 of 16 December 2025. https://cyber.gov.gr/wp-content/uploads/2025/12/ΕΣΚ-2026-2030.pdf

124 Národní úřad pro kybernetickou a informační bezpečnost. (2025). Národní strategie kybernetické bezpečnosti České republiky 2026-2030 [National cyber security strategy of the Czech Republic 2026-2030], approved 3 September 2025. https://nukib.gov.cz/

125 European Commission. (n.d.). National strategy: Cyberspace security 2019-2023 [Portugal]. Better Internet for Kids knowledge hub. https://better-internet-for-kids.europa.eu/en/knowledge-hub/national-strategy-cyberspace-security-2019-2023

126 República Portuguesa. (2025). Decreto-Lei n.º 125/2025, de 4 de dezembro, Regime Jurídico da Cibersegurança [Legal regime for cybersecurity]. Diário da República n.º 234/2025. https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

concepts are published.

On the international law dimension the count is firmer: national positions on the application of international law in cyberspace were confirmed for fifteen member states (Austria, Belgium, Czechia, Denmark, Estonia, Finland, France, Germany, Ireland, Italy, the Netherlands, Poland, Romania, Slovenia and Sweden) through primary documents or the CCDCOE toolkit's compilations. Thirteen of these are analysed in this series' comparative legal study of the positions issued as of April 2024,[127] and the two published since are Belgium's national position of 2025 and Slovenia's position paper of May 2026, while for twelve none was located in the sources searched, among them Spain.[128] This count rests partly on tracker compilations and is stated with that caveat.

The absence of a published position is not evidence of absent capability. The German case shows a state that legislated years after commentators assumed a settled position, and the Danish case shows a political decision taken more than a decade before most observers date it. What the absence of a published framework does make difficult is legal interoperability: a partner cannot align with a framework that has not been stated.

127 Schmitt, M. N., & Vihul, L. (2024). European approaches to the application of international law in cyberspace: A comparative legal analysis. EU Cyber Direct. https://eucyberdirect.eu/research/european-approaches-to-the-application-of-international-law-in-cyberspace-a-comparative-legal-analysis

128 NATO Cooperative Cyber Defence Centre of Excellence. (n.d.-b). National positions. International cyber law: Interactive toolkit. https://cyberlaw.ccdcoe.org/wiki/List_of_articles

The three models at a glance

How member states organise active cyber defence, by institutional logic

	Military model Exemplar: France	**Intelligence-enabled model** Exemplar: the Netherlands	**Police-law model** Exemplar: Germany
Who acts	Armed forces, through a joint cyber command under executive authority	Intelligence and security services, under intelligence statutes	Federal police and the Federal Criminal Police Office, under hazard prevention law
Posture	Offensive cyber operations as published doctrine (France) or doctrinal approach (Sweden); France publishes no trigger, Sweden a decision at the military-strategic level	A permanent proactive posture set out in the defence strategy	Powers to act against attacker infrastructure
Oversight	Executive authority; international law position published separately	A rebuilt oversight architecture, adjusted by the Temporary Act	The judicial safeguards attached to police powers
Defining feature	A choice of institution and of words; France also says what the capability does	Peacetime persistence achieved by redesigning oversight	Keeps offensive action out of the armed forces and intelligence services, at the cost of engaging the constitutional allocation of competences
Followers and relatives	Romania, Italy, Denmark, Poland, Portugal, Sweden	Slovakia and Czechia, in military intelligence law; the UK National Cyber Force outside the EU	None yet; its future rests with the Bundestag

OUTSIDE THE THREE MODELS

Institution before doctrine

A military cyber command whose mandate is published without saying whether operations are offensive or defensive. Spain, Lithuania and Ireland; also Austria, Bulgaria, Croatia, Greece and Hungary. The most common position in the Union.

Resilience first

Estonia and Finland emphasise resilience while also publishing assertive positions on cyber defence and international law.

No published position

Most remaining member states have published nothing that would allow them to be placed.

Groups overlap: a state may have built an institution and still have no published position on active cyber defence. Source: Section 6.

PART IV

What this means for the European Union

7. Convergence, divergence, and a pattern of disclosure

KEY FINDINGS

1. Member states converge on more than the debate suggests: international law applies, out-of-network activity is always paired with a legal frame, military authority is the default and triggers are reactive.
2. States readily disclose who acts and what they call it, but rarely where, when, against whom and to what effect, which is the basis for a minimum disclosure set.

7.1 Where the member states converge

Five points of convergence emerge from the record, and the common ground is larger than the debate suggests. First, a normative floor: every member state with any published position accepts that international law applies to cyber operations, a floor now stated collectively in the 2024 Declaration,[129] and the four member state positions analysed in Section 5.6 that address the question, those of France, the Netherlands, Finland and Poland, accept sovereignty as a primary rule, while the Estonian statement analysed there addresses collective countermeasures rather than the sovereignty rule itself. Second, a legal-pairing norm: no member state claims out-of-network activity without pairing it to a legal frame in the same document. France's doctrine acts 'dans le strict respect des règles internationales',[130] Romania's statute binds its offensive mandate to international humanitarian law,[131] the Dutch strategy operates within existing legal frameworks and legislates where it reaches their limits,[132] and Germany's bill rests its powers on a claimed constitutional competence.[133] The pattern holds equally for the states treated later in Section 5.1: Portugal subordinates offensive activity to rules of engagement authorised by the political power, Slovakia and Czechia set their conditions in statute and gate them on ministerial consent, Denmark ties the use of its offensive capacity to the procedure governing other military means of force, and Sweden places the decision at the military-strategic level. Whatever else divides them, no state asserts a legally unbounded concept. Third, a military default: where an authority basis is published at all, it is military in twelve of nineteen cases (France, Romania, Poland, Italy, Denmark, Lithuania, Sweden, Belgium, Ireland, Portugal, Latvia and Slovenia), against four hybrid arrangements (the Netherlands, Estonia, Finland, Spain), two military-intelligence placements (Czechia and Slovakia) and one pending police-law placement (Germany). The outliers are deliberate design choices, not drift. Fourth, a reactive default on triggers: every published trigger except that of the Netherlands is reactive, conditional or procedural, the Slovak and Czech statutory triggers being the most fully specified of these, so the persistent peacetime posture that dominates the transatlantic debate has, within the EU, one adherent on the published record. Fifth, institutional convergence: the building of military cyber commands proceeds across otherwise different groups, with Spain's joint command reorganised in 2020, Poland's component and Belgium's Cyber Command in 2022, Lithuania's from 2025, and Estonia's Defence Forces cyber command conducting a joint defensive operation with the United States by 2020 at the latest.[134]

129 Council of the European Union (2024).
130 Ministère des Armées (n.d.-a).
131 Parlamentul României (2023).
132 Ministerie van Defensie (2025a).
133 Deutscher Bundestag (2026a).
134 Ministerio de Defensa (2020); Ministerstwo Obrony Narodowej (n.d.); Incyber News (2025); Krašto apsaugos ministerija (2025); U.S. Cyber Command (2020).

7.2 Where they diverge, and where it matters

The divergence that matters is not the one the vocabulary suggests. Register divergence, offensive versus active versus operational versus defensive labels, is the most visible difference between the member states and the least informative, as Section 5.2 showed. Three divergences carry real weight. The first and deepest is the authority-family divergence. Military offensive cyber capabilities are described in France, Romania and Portugal, although their published operational scope differs; comparable activity sits under hybrid constitutional and intelligence law in the Netherlands, under military intelligence law in Czechia and Slovakia, and under police law in Germany's pending bill. Germany, legislating along police and intelligence routes at once while its armed forces act under Bundestag mandates, would carry military, intelligence and police law within a single state. These are not stylistic differences: they determine which oversight body supervises the activity, whether prior authorisation or ex-post review applies, whether a judicial reservation is debated, as in the German Bundesrat exchange,[135] and which body of international law the state itself invokes. A joint operation spanning the three families would run simultaneously under three oversight architectures, as Figure 12 shows. The second is the trigger divergence, which is close to binary: the standing posture of the Netherlands against everyone else. Portugal, Latvia, Denmark and Ireland publish who authorises action rather than when it is warranted, and Section 5.4 sets out what the EU faces in place of a spectrum of trigger doctrines. The third divergence sits at the edge of the EU rather than inside it: every analysed member state position that addresses sovereignty accepts it as a primary rule, while the United Kingdom formally reserves against any rule beyond non-intervention.[136] The sharpest binary divergence over active cyber defence lies outside the EU rather than within it, and any EU framework reaching into foreign networks should be designed with that difference in view. Within the EU the picture is finer-grained than the binary suggests: published European positions differ on the threshold at which a sovereignty violation occurs, including whether it requires effects of a certain gravity, a debate documented in the legal literature,[137] so intra-European agreement on the rule does not yet mean agreement on its application. Finally, the target column deserves its own sentence, because it is the least populated column in the record and the most consequential: among member states, the Netherlands, Portugal, Slovakia and Sweden publish target categories, while Germany does so in two bills not yet enacted and Czechia has named an adversary only in describing an operation after the fact. Romania's statutory provision does not specify a target category. As Section 5.3 sets out, the target type decides which body of law governs an operation, and on current publication partners cannot know which of these most member states intend.

A further divergence is narrower than these and sharper for it, because it concerns a single activity rather than a whole concept: the hunting for an adversary inside networks one already defends. Luxembourg's cyberdefence strategy files that activity as defence, defining cyberdefence as the means put in place to carry out defensive measures against cyber threats and a cyber operation as action in or through cyberspace to preserve freedom of action.[138] The United Kingdom gives the name Active Cyber Defence to a programme of automated protection inside British networks, as Section 3.3 sets out. The CCDCOE, by contrast, would not call protective activity inside one's own infrastructure active cyber defence at all, since on its definition the term begins where the defended infrastructure ends. The same conduct is therefore defence in one national document, active cyber defence in the usage of a close partner, and outside the category altogether on the definition most widely used in European legal practice.

135 Deutscher Bundestag (2026c).

136 NATO Standardization Office (2020).

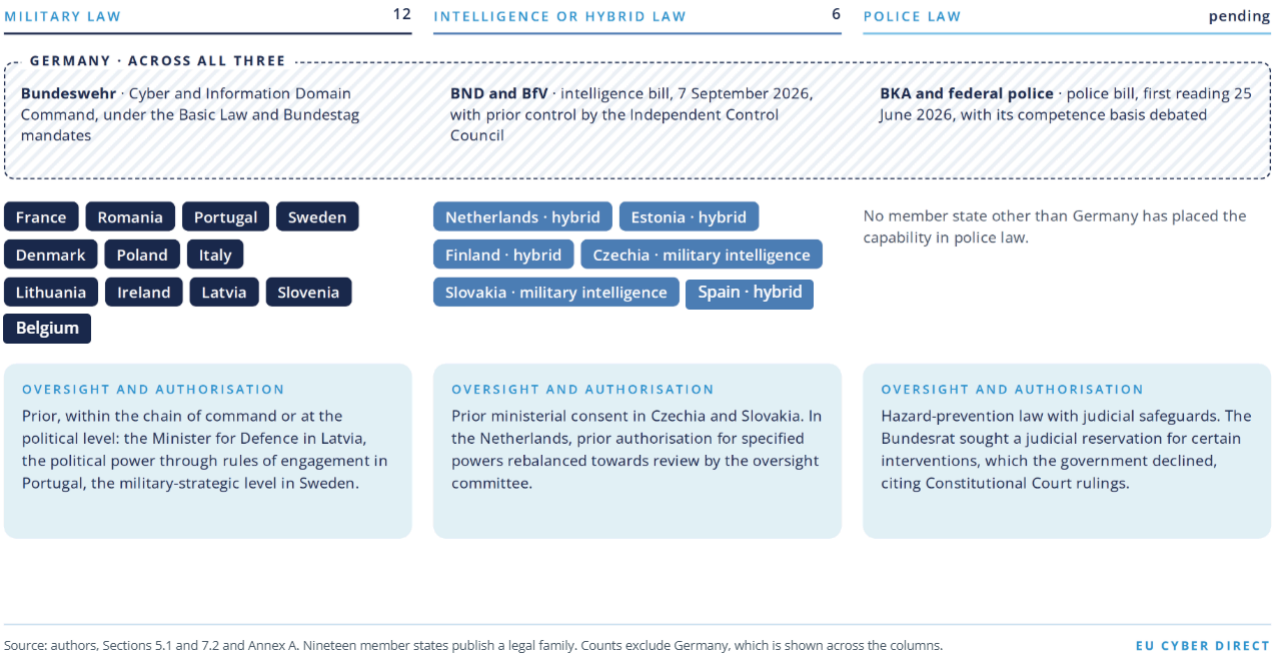
137 Moynihan, H. (2019). The application of international law to state cyberattacks: Sovereignty and non-intervention. Chatham House; Delerue, F. (2020). Cyber operations and international law. Cambridge University Press.

138 Direction de la défense (2021).

FIGURE 12

Three legal families, and who oversees each

> Similar action beyond national networks is placed under three legal families, and the family decides who oversees it and when authorisation is given. Germany's published record spans all three.



Source: authors, Sections 5.1 and 7.2 and Annex A. Nineteen member states publish a legal family. Counts exclude Germany, which is shown across the columns.

EU CYBER DIRECT

Sweden settles the point from inside the EU. Its published doctrinal approach classifies uppsökande verksamhet, the searching or hunting activity conducted within its own systems and within systems it has been tasked to defend, as one of four components of defensive cyber operations, alongside sensor analysis, incident handling and countermeasures.[139] The activity that the United Kingdom labels active is thus, in the fullest published doctrinal approach to cyber defence of any member state, plainly defensive. Neither usage is wrong, because there is no common definition against which either could be measured. Reporting framed around the term alone would therefore yield answers that are hard to add together, which is why the disclosure set recommended in Section 7.4 is framed around the seven questions rather than around the term.

7.3 A pattern of disclosure

Standing back from the individual questions, a consistent pattern appears in what the member states have chosen to publish, and it is the single most useful observation the comparison yields. States readily say which agency is responsible: twenty-four of the twenty-seven name a body, and nineteen publish the legal family under which it acts. Every state that has published anything has chosen a vocabulary. Fifteen have published a position on international law. But when the questions turn operational, the answers thin. Seven states publish that they would act beyond their own networks, eight what the activity would do, and five against whom. On the trigger, one publishes a standing posture, five set statutory or strategic conditions, Germany among them in its pending bills, and five publish an authorisation procedure without a threshold. Two national documents answer six of the seven questions in a single text: Sweden's doctrinal approach and Slovakia's Act on Military Intelligence. In each case the seventh, the international law anchor, is supplied, if at all, by a separately published position, and of the two only Slovakia's is law. This is an understandable pattern: the dimensions that are readily published are institutional and declaratory, and those that are not are the ones

139 Försvarsmakten (2024).

closest to operational planning. It is consistent with the wider finding that states publicise the institutional shell of cyber capacity while withholding its operational content.[140] It is recorded as a description of practice, not as a criticism of it. The state-by-state matrix in Figure 2 should be read in the same spirit: it records whether a question has been answered, not how far-reaching the answer is, so a high count marks transparency rather than assertiveness. Germany's two bills are counted wherever they answer a question, although neither is yet law. Throughout, a published authorisation procedure is counted as an answer to the trigger question, and the register is counted as an answer in its own right. Its implication for the EU is nonetheless significant: any instrument that asks member states to report on their 'active defence capabilities' will collect agencies and vocabularies, not concepts, unless it asks the operational questions by name, and it will have to be judicious about which of those questions it is reasonable to ask.

One alternative reading must be stated rather than assumed away. The operational silences may reflect capability that does not yet exist rather than capability withheld. The barriers to building a military cyber force are high,[141] and a state with a new command and no doctrine may simply not yet have decided the answers. A stronger version of the same reading holds that the effects such operations can reliably achieve are more limited than doctrine implies.[142] The published record cannot distinguish the two, and the two carry different policy implications. The states that have built commands before publishing doctrine are the natural test cases, and the question can only be settled by direct engagement with the states concerned.

7.4 The minimum disclosure set

Read together, the pattern of disclosure, the convergences and the divergences point to a precise and realistic policy target. The questions the EU most needs its member states to answer are exactly the ones that the record shows to carry little sensitivity and to be widely published already on one side, and to be consequential but largely unpublished on the other. Authority basis is already published by nineteen member states, so inviting its declaration codifies existing practice with minimal additional effort. Target type is almost never published and is the dimension that decides which legal regime an operation falls under, so inviting its declaration offers the greatest gain in legal interoperability for the least additional disclosure. A vocabulary statement, saying which of the lexicon's terms a state uses and what it means by them, involves no operational disclosure. By contrast, trigger and effect are operationally sensitive, and the record shows that states treat them as such. Locus needs a distinction the record itself supplies. Specific locus, which systems an operation would touch, is as sensitive as the trigger. Categorical locus, whether a state's concept extends beyond its own networks at all, is already published by seven member states, and it follows from the authority declaration itself: a state that declares which law governs its action beyond its own networks has answered the categorical question in the same breath. It is therefore included in the disclosure set, in that form and no other. What a realistic common framework should not demand is the operationally specific form of locus, the trigger and the effect. This proposal has a lineage to acknowledge: Herpig and Kuehn[143] argued on this study's own commissioning platform that the EU must define active cyber defence, and Herpig's earlier framework proposed safeguards for active cyber defence operations including transparency measures.[144] The minimum disclosure set is narrower and structural rather than operational: it asks states to declare standing facts about authority and target type ex ante, not to account for operations ex post, and it derives its content from the observed publication gradient rather than from normative first principles. Section 9 develops this into the study's recommendations.

140 Kostyuk, N. (2021). Deterrence in the cyber realm: Public versus private cyber capacity. International Studies Quarterly, 65(4), 1151-1162.

141 Smeets, M. (2022). No shortcuts: Why states struggle to develop a military cyber-force. Oxford University Press.

142 Maschmeyer, L. (2021). The subversive trilemma: Why cyber operations fall short of expectations. International Security, 46(2), 51-90.

143 Herpig and Kuehn (2022).

144 Herpig, S. (2021). Active cyber defense operations: Assessment and safeguards. Stiftung Neue Verantwortung.

8. Conclusions and limitations

KEY FINDINGS

1. The challenge for coordination is not a missing definition but a surplus of them.
2. The recommendations are deliberately modest, because the key constraint is mutual legibility, a problem the EU is well placed to solve.

Returning to the study's questions: what member states mean by active cyber defence is now set out, state by state and question by question, in Part II and in the working matrix in Annex A, the implications of divergence and of unpublished positions are the legal interoperability costs described in Section 7, and the pathway to a common framework follows in Section 9. Three conclusions stand. First, the challenge for coordination is not a missing definition but a surplus of them, and the surplus is structured: the authorities disagree on where, when and to what effect the activity takes place, so an EU instrument that invokes active defence capabilities inherits all of their meanings at once. Second, where member states have moved, they have followed three institutional paths, military, intelligence-enabled and police-law, which produce different oversight regimes and different international law exposure for materially similar operations. Third, vocabulary is an unreliable guide to any of this in either direction, and the EU's discussions will be better served by asking members what they mean than by inferring it from what they call it. Beneath these differences the common ground is larger than the debate suggests: every published position accepts that international law applies, and no state describes out-of-network activity without a legal frame.

The recommendations that follow from these conclusions are stated, with their addressees, in Section 9. They are deliberately modest, because a key constraint identified by this study is mutual legibility, a problem the EU is well placed to solve.

8.1 Limitations and items pending verification

The following could not be verified against primary documents and must not be cited from this study as established. First, the cyber provisions of Denmark's Defence Agreement 2010-2014, cited here only through the 2013-2017 agreement's back-reference, and those of the subsidiary agreements concluded under the 2024-2033 framework, together with claims about the oversight mandate of the Danish intelligence oversight body. Second, a successor to Spain's national cybersecurity strategy of 2019, and confirmation that Spain has published no international law position, which is reported here as not located. Third, current-strategy reviews in the national language for Croatia's standalone national strategy, for Hungary and for Slovenia's cybersecurity resolution, the other national reviews having been completed. Croatia's long-term armed forces development plan for 2025 to 2036 was reviewed for this study and names the Cyberspace Command's objectives in terms of cyber defence and situational awareness only. Fourth, any published doctrine of Poland's Cyberspace Defence Forces beyond the ministry webpage quoted. Fifth, the reported passage on 'difesa attiva' [active defence; authors' translation] in the Italian strategy's challenges section, retrieved only via secondary reporting and therefore excluded from the body of this study. Sixth, the precise current French cybercombatant headcount, on which the ministry's own pages remain inconsistent, the most recent giving more than 4,900 with a target of more than 5,500 by 2030. Three further items are recorded with the same caution. Spain's

cyberspace operations doctrine PDC-3.20 is established to exist, and is dated and cited in material the Ministry of Defence hosts, but the doctrine itself is not published and has not been read for this study. An Italian reform reported in August 2026, which would make the Chief of the Defence Staff the authority for a 'spazio cibernetico di interesse nazionale' [cyberspace of national interest; authors' translation], could not be verified in any official source and is therefore not used. The Czech statutory text of the 2021 amendment was read through a legal publisher's reproduction of the Collection of Laws, the official electronic Collection having refused retrieval, while the operation described in Section 5.1.6 rests on the Ministry of Defence's own published account. One limitation is methodological rather than documentary. Sweden's published doctrinal approach to cyber defence and Slovakia's Act on Military Intelligence were not located in the first desk passes, because those passes rested on national cybersecurity strategies rather than on defence doctrine and military intelligence legislation. Both were located before publication and are used here, and the reading was widened in consequence. Entries recording that no locus, trigger, effect or target was published should nonetheless be read as findings about the record this study located, rather than as demonstrations that no such statement exists. The central negative claim about EU-level definition is verified against public EU documents only. The full EU Cyber Census 2025 is EU classified information and could not be checked, so the claim is bounded to the public record. The stand-down episode reported in Section 5.2 was first denied on the record by the Pentagon; in May 2025 Representative Don Bacon stated publicly that a one-day pause had occurred, and its full scope and the underlying orders have not been independently established in the public record. Both statements are reported.

Two developments postdate the body of this study's verification work and are reported at an early stage only: the Dutch draft Wbnv described in Section 5.1.2, whose consultation opened on 28 August 2026 and closes on 11 October 2026, and the German intelligence-services bill of 7 September 2026 described in Section 5.1.3. The account of the Netherlands otherwise describes the law in force as of July 2026, and the final content and parliamentary fate of both texts remain open.

Recommendations at a glance

Eleven voluntary recommendations, each derived from a finding in Section 7 and addressed to the actor able to act on it. Recommendations 4 to 7 together form the minimum disclosure set.

NO.	ACTION	WHO ACTS	INSTRUMENT
9.1 A narrative within responsible state behaviour			
1	Build the narrative on conduct and constraint, not on the label, with a common vocabulary annex	Council, Horizontal Working Party on Cyber Issues, cyber ambassadors	*Council text*
2	State collectively the common ground the published record already shows	Council and member states collectively	*Council text*
9.2 The EU Declaration on international law			
3	Apply the Declaration's rule on labels to cyber defence documents; develop it on the sovereignty threshold	Member states, as authors of the Declaration	*Council text*
4	Publish a national position on international law, and the scope of any unpublished doctrine	The twelve member states without one	*National statement*
9.3 A cooperation and coordination mechanism			
5	Declare the legal authority basis for any operations beyond national networks	Member states individually	*National statement*
6	Declare the target types such operations may be directed against	Member states individually	*National statement*
7	Publish a one-line statement of the term used and what it covers	Member states individually	*National statement*
8	Ask for the underlying facts, not the label, in the Cyber Census	EEAS, Commission	*EU stocktaking*
9	Maintain the Annex A matrix as a shared reference, each state confirming its own row	EEAS, European Defence Agency, EU Cyber Commanders, cyber ambassadors	*Shared reference*
9.4 Joint development and procurement			
10	Specify joint capabilities by function, locus and effect, not by label	European Defence Agency, Commission, member states	*Capability programme*
11	Record which authority and oversight apply in each participating state before a programme proceeds	European Defence Agency, Commission, member states	*Capability programme*

9. Recommendations

The recommendations are organised around the four questions the Union's cyber ambassadors and cyber commanders are themselves asking: how active cyber defence fits within the broader framework of responsible state behaviour, how far the EU Declaration on the application of international law should be developed, what cooperation or coordination mechanism is feasible at EU level, and what joint development and procurement of cyber defence capabilities would require. Each recommendation is derived from a finding of Section 7, names the actor able to act on it, and is voluntary. Because the member states are both the authors of collective instruments and the authors of their own declarations, several recommendations are addressed to the same governments in different capacities. What distinguishes them is the instrument, a Council text, a national statement, or a capability programme, not the group of actors. Taken together the disclosure recommendations constitute the minimum disclosure set developed in Section 7.4. The trigger, the effect and the operationally specific form of locus are deliberately excluded from any disclosure request: the pattern of disclosure shows that member states treat these as sensitive, and a framework asking for them would be unlikely to command consensus. Locus in its categorical form, whether a state's concept reaches beyond its own networks, is included, for the reason given in Section 7.4.

9.1 A narrative of active cyber defence within responsible state behaviour

1

RECOMMENDATION 1 · *To the Council, its Horizontal Working Party on Cyber Issues and the cyber ambassadors*

Build the narrative on conduct and constraint rather than on the label, and give it a common vocabulary annex for EU cyber defence documents.

The annex should adapt the defensive and offensive cyberspace operation categories that the twenty-three allied member states have already accepted in NATO doctrine, with the four non-allied member states adopting them as an EU text rather than by reference, and it should state explicitly that 'active defence' is not a defined EU term. That the NATO pair has no middle category, which Section 3.4 records as a pragmatic compromise rather than a doctrinal judgement, is the property that makes it usable here: an annex whose purpose is to stop a term absorbing several meanings at once should not itself supply a third box. The Union's own Declaration already supplies the principle on which this rests, namely that the principle of distinction applies irrespective of whether a cyber attack is exercised in an offensive or a defensive context, so that calling an operation active changes nothing in its legal assessment. A narrative built on the label would therefore claim something the Union has already said is legally immaterial.

2

RECOMMENDATION 2

State collectively what the record in Section 7.1 already shows individually, because it is the strongest evidence of responsible behaviour the Union has and it requires no state to disclose anything new.

Every member state with a published position accepts that international law applies to cyber operations. No member state claims activity beyond its own networks without binding it to a legal frame in the same document. Authority is military in twelve of the nineteen cases where the legal family is published at all, with the departures from that default being deliberate design choices. Every published trigger other than the Dutch standing posture is reactive or conditional, five further states publishing an authorisation procedure in place of a trigger. A narrative of responsible state behaviour that is anchored in these four findings is defensible against the record, and it can be stated without reopening what any member state regards as operationally sensitive.

9.2 The EU Declaration on the application of international law

3

RECOMMENDATION 3 · *To the member states acting in the Council as the authors of the Declaration*

Carry the Declaration's own rule on labels into the Union's cyber defence documents, and take the Declaration further on the two points on which the positions analysed in Section 5.6 still differ.

The first is the threshold at which a violation of sovereignty occurs, and in particular whether effects of a certain gravity are required, which remains disputed between European positions and is the question on which any operation reaching into another state's networks will turn. The second is the consequence the Union draws from the fact that its closest non-EU partner reserves against the existence of a sovereignty rule at all, which is a divergence the Declaration notes in substance but does not address as a practical matter for joint operations.

4

RECOMMENDATION 4 · *To the twelve member states with no published national position*

Publish one.

Fifteen member states have done so, two of them since the Declaration was adopted, and the positions published are the instrument through which the Declaration acquires content: they state where a state locates the sovereignty threshold, what it accepts on due diligence, and how it reads countermeasures. A national position costs nothing operationally, as the fifteen show, and its absence is the single largest gap in the international law column of the matrix. The same argument applies to doctrine that exists but is unpublished, as in Spain and Austria: a state that has decided and not said imposes the same cost on its partners as a state that has not decided, and publishing the scope and the authority structure, without the operational content, would remove it.

9.3 A cooperation and coordination mechanism at EU level

5

RECOMMENDATION 5 · *To member states individually*

Declare, as a standing statement, which legal authority basis, military, intelligence or law enforcement, governs any cyber operations beyond the state's own networks.

Nineteen member states already publish it, so the declaration codifies existing practice at minimal effort, and it gives partners the single fact that determines which oversight body supervises the activity and which constraints apply to it. The declaration should say, in the same line, whether that authority extends beyond the state's own networks at all, which is the categorical form of the locus question and follows from the authority basis in any event.

6

RECOMMENDATION 6 · *To member states individually*

Declare which target types, criminal infrastructure, state actors, or attacker systems irrespective of the actor behind them, out-of-network operations may be directed against.

This is the least often answered of the seven questions and the most consequential, because it decides whether an operation is law enforcement or interstate conduct, which body of law governs it, and what escalation risk a partner is being asked to share.

7

RECOMMENDATION 7 · *To member states individually*

Publish a one-line vocabulary statement: which term the state uses for activity conducted beyond its own networks, and what it understands that term to cover.

This is the third element of the minimum disclosure set and the cheapest of the three, because it discloses nothing operational, and it is also the element without which the other two cannot be read across states, since, as Sections 3 and 5.2 show, the same activity is filed under opposite registers in different capitals. Section 7.2 shows the cost of leaving it unsaid: one and the same activity, hunting inside networks a state already defends, is filed as defence in a member state's own document and as active cyber defence in the usage of a close partner.

8

RECOMMENDATION 8 · *To the EEAS and the Commission, in the Cyber Census and in any future stocktaking*

Ask for the underlying facts rather than for the label.

A question that asks member states to report their 'active defence capabilities' will collect twenty-seven vocabularies, because, as Sections 3 and 5.2 show, the term means different things in different capitals and two states can describe the same activity in opposite registers. A question that asks instead which authority basis governs operations beyond own networks, which target types are permitted, and which term the state uses and how it defines it, will collect answers that can be compared with one another. The reporting burden is the same, and only the comparability of the result changes.

9 **RECOMMENDATION 9** · *To the EEAS and the European Defence Agency, with the EU Cyber Commanders and the cyber ambassadors*

Maintain the working matrix in Annex A as a standing shared reference, with each member state confirming or correcting its own row, so that it becomes a maintained common instrument rather than a one-off research output.

Because the Commanders and the ambassadors meet under rotating presidencies and hold no secretariat, custody should sit with the EEAS or the Agency, with the two formats reviewing the matrix annually. The same custodian should keep a standing inventory of the instruments the matrix rests on, doctrine, military intelligence statutes and defence agreements as well as strategies, since this study's own experience is that the concepts live in documents that a search for cybersecurity strategies does not return. Both formats already meet regularly under successive presidencies,[145] so the mechanism recommended here is a standing reference document rather than a new body. A coordination mechanism does not require a common capability posture. It requires that partners can read one another's authorities, which is what Recommendations 5 to 9 supply.

9.4 Joint development and procurement of cyber defence capabilities

10 **RECOMMENDATION 10** · *To the European Defence Agency, the Commission and member states in capability planning*

Specify jointly developed or jointly procured cyber capabilities by function, the locus in which they operate and the effect they produce, rather than by the label.

This is specification among the participants in a programme, not public declaration, and it is therefore compatible with the exclusion stated at the head of this section. The 2022 Joint Communication invites investment in 'full-spectrum cyber defence capabilities, including active defence capabilities' without defining the term,[146] so a programme that carries the phrase into its requirements inherits its ambiguity: participating states will build to different specifications while reporting against the same line, and the divergence will surface at the point of use rather than at the point of design.

145 Estado Mayor de la Defensa. (2023). ESP CHOD opens the conference of EU Cyber Commanders, part of the Spanish Presidency of the European Union. https://emad.defensa.gob.es/en/emad/Actividades_del_JEMAD/listado/231024_MCCE_CyberCo.html; European External Action Service. (2024, January 17). Cyber: EU holds informal meetings of Cyber Ambassadors and Commanders [Press release]. https://www.eeas.europa.eu/eeas/cyber-eu-holds-informal-meetings-cyber-ambassadors-and-commanders_en; Cyprus Presidency of the Council of the European Union. (2026). EU Cyber Commanders [Event listing]. https://cyprus-presidency.consilium.europa.eu/en/events/eu-cyber-commanders/

146 European Commission & High Representative (2022).

11 RECOMMENDATION 11 · *To the same addressees*

Record, before a joint programme proceeds, which authority family will operate the capability in each participating state and which oversight applies to it.

As Section 7.2 shows, materially similar activity sits under military law in some member states, intelligence law in others and police law in Germany's pending bill, and Germany alone would span all three. A single jointly procured capability operated under three legal regimes raises questions of accreditation, data handling, classification and the rules under which crews may train and operate together, and these are design questions for the programme rather than questions to be settled by its eventual users. Recording the answer at the outset is also the cheapest way to discover early that a given capability cannot be shared at all.

References

AIVD. (n.d.). Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma. https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen--en-veiligheidsdiensten/wet-op-de-inlichtingen-en-veiligheidsdiensten/tijdelijke-wet-onderzoeken-aivd-en-mivd-naar-landen-met-een-offensief-cyberprogramma

AIVD. (2026, August 28). Start consultatie nieuwe Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten. https://www.aivd.nl/actueel/nieuws/2026/08/28/start-consultatie-nieuwe-wet-bescherming-nationale-veiligheid-door-de-inlichtingen-en-veiligheidsdiensten

Aizsardzības ministrija. (2023). Latvijas kiberdrošības stratēģija 2023.-2026. gadam [Latvia's cyber security strategy 2023-2026]. https://www.mod.gov.lv/sites/mod/files/document/Latvijas%20kiberdro%C5%A1%C4%ABbas%20strat%C4%93%C4%A3ija%202023.-2026.gadam_.pdf

Belgian Defence. (2019, May). Cyber Strategy for Defence, English version. https://ccdcoe.org/uploads/2018/10/Belgian-Defence-Cyber-Strategy-EN.pdf

Bendiek, A., & Bund, J. (2023). Shifting paradigms in Europe's approach to cyber defence (SWP Comment 2023/C 48). Stiftung Wissenschaft und Politik.

Bendiek, A., & Bund, J. (2024). Hardening norms and networks: Europe's cyber defence posture. Intereconomics, 59(4), 198-203.

Blessing, J. (2021). The global spread of cyber forces, 2000-2018. In 2021 13th International Conference on Cyber Conflict (CyCon). NATO Cooperative Cyber Defence Centre of Excellence.

Buchanan, B. (2016). The cybersecurity dilemma: Hacking, trust and fear between nations. Oxford University Press.

Bundeskanzleramt. (2024). Österreichische Sicherheitsstrategie 2024 [Austrian security strategy 2024]. Republic of Austria. https://www.bundeskanzleramt.gv.at/dam/jcr:941a3cb3-7320-4c31-a4d2-3307f57faad3/sicherheitsstrategie_oesterreich_2024.pdf

Bundeskanzleramt. (2025). Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit: Fortschrittsbericht 1/2025 [Measures catalogue of the Austrian cyber security strategy: progress report 1/2025], as at 5 March 2025. https://www.bundeskanzleramt.gv.at/dam/jcr:cdfd1277-9df5-4e65-87bc-bffd0c54ed7b/Massnahmenkatalog_OeSCS_Fortschrittsbericht_1_2025.pdf

Bundesministerium der Verteidigung. (n.d.). FAQ: Cyber-Abwehr der Bundeswehr. https://www.bmvg.de/de/themen/cybersicherheit/cyber-verteidigung/cyber-abwehr

Bundesministerium des Innern und für Heimat. (2026, May 27). Aktive Cyberabwehr: Gesetzentwurf nimmt Angreifer ins Visier. https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2026/05/cybersicherheit.html

Bundesregierung. (2026, June 25). Bundesinnenminister zur Cybersicherheit im Bundestag. https://www.bundesregierung.de/breg-de/suche/bmi-cybersicherheit-bt-2445290

Center for Cyber and Homeland Security. (2016). Into the gray zone: The private sector and active defense against cyber threats. George Washington University.

Centre for Cyber Security Belgium. (2021). Cybersecurity Strategy Belgium 2.0, 2021-2025. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf

Council of the European Union. (2023). Council conclusions on the EU policy on cyber defence (9618/23). https://www.consilium.europa.eu/media/64526/st09618-en23.pdf

Council of the European Union. (2024). Declaration on a common understanding of the application of international law to cyberspace (ST 15833/2024). https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf

Cyprus Presidency of the Council of the European Union. (2026). EU Cyber Commanders [Event listing]. https://cyprus-presidency.consilium.europa.eu/en/events/eu-cyber-commanders/

Defence Forces Ireland. (2024). Defence Forces cyber defence strategy 2024-2027. Óglaigh na hÉireann, July 2024. https://www.military.ie/

Delerue, F. (2020). Cyber operations and international law. Cambridge University Press.

Denning, D. E. (2014). Framework and principles for active cyber defense. Computers & Security, 40, 108-113.

Denning, D. E., & Strawser, B. J. (2017). Active cyber defense: Applying air defense to the cyber domain. In G. Perkovich & A. E. Levite (Eds.), Understanding cyber conflict: Fourteen analogies. Georgetown University Press.

Departamento de Seguridad Nacional. (2019). Estrategia Nacional de Ciberseguridad 2019 (Orden PCI/487/2019, de 26 de abril). https://enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/ES_NCSS_2019_es.pdf

Deutscher Bundestag. (2026a). Entwurf eines Gesetzes zur Stärkung der Cybersicherheit (Drucksache 21/6585). https://dserver.bundestag.de/btd/21/065/2106585.pdf

Deutscher Bundestag. (2026b). Gegen die Einführung von Hackbacks und offensiver Cyberabwehr (Drucksache 21/6653). https://dserver.bundestag.de/btd/21/066/2106653.pdf

Deutscher Bundestag. (2026c). Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung (Drucksache 21/7406). https://dserver.bundestag.de/btd/21/074/2107406.pdf

Deutscher Bundestag. (2026d). Entwurf eines Gesetzes zur Reform des Nachrichtendienstrechts (Drucksache 21/7868), 7 September 2026. https://dserver.bundestag.de/btd/21/078/2107868.pdf

Dewar, R. S. (2014). The 'triptych of cyber security': A classification of active cyber defence. In Proceedings of the 6th International Conference on Cyber Conflict (CyCon) (pp. 7-21). NATO Cooperative Cyber Defence Centre of Excellence.

Direction de la défense. (2021). Stratégie de cyberdéfense du Luxembourg [Luxembourg cyberdefence strategy]. Ministère des Affaires étrangères et européennes, February 2021. https://defense.gouvernement.lu/

Eerste Kamer der Staten-Generaal. (n.d.). Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma (36.263). https://www.eerstekamer.nl/wetsvoorstel/36263_tijdelijke_wet_onderzoeken

Efrony, D., & Shany, Y. (2018). A rule book on the shelf? Tallinn Manual 2.0 on cyberoperations and subsequent state practice. American Journal of International Law, 112(4), 583-657.

Estado Mayor de la Defensa. (n.d.). Mando Conjunto del Ciberespacio (MCCE). https://emad.defensa.gob.es/unidades/mcce/

Estado Mayor de la Defensa. (2023). ESP CHOD opens the conference of EU Cyber Commanders, part of the Spanish Presidency of the European Union. https://emad.defensa.gob.es/en/emad/Actividades_del_JEMAD/listado/231024_MCCE_CyberCo.html

European Commission. (n.d.). National strategy: Cyberspace security 2019-2023 [Portugal]. Better Internet for Kids knowledge hub. https://better-internet-for-kids.europa.eu/en/knowledge-hub/national-strategy-cyberspace-security-2019-2023

European Commission, & EU High Representative for Foreign Affairs and Security Policy. (2022). Joint communication to the European Parliament and the Council: EU policy on cyber defence (JOIN(2022) 49 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022JC0049

European Commission, & EU High Representative for Foreign Affairs and Security Policy. (2026). EU Cyber Census 2025: Executive summary (SWD(2025) 423). Publicly released 20 February 2026, full report EU classified information.

European External Action Service. (2024, January 17). Cyber: EU holds informal meetings of Cyber Ambassadors and Commanders [Press release]. https://www.eeas.europa.eu/eeas/cyber-eu-holds-informal-meetings-cyber-ambassadors-and-commanders_en

Finnish Government. (2024a, October 10). Revised cyber security strategy responds to changed security environment [Press release]. https://valtioneuvosto.fi/en/-/1410829/revised-cyber-security-strategy-responds-to-changed-security-environment

Finnish Government. (2024b). Finland's cyber security strategy 2024-2035. https://enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/FI_NCSS_2024_en.pdf

Forsvarets Efterretningstjeneste. (n.d.). Cyberoperationer. https://www.fe-ddis.dk/da/arbejdsomrade-a/cyberoperationer/

Forsvarsakademiet. (2019). Værnsfælles doktrin for militære cyberspaceoperationer (VDMCO) [Joint doctrine for military cyberspace operations], 1st edition. Royal Danish Defence College, September 2019. https://research.fak.dk/esploro/outputs/other/V%C3%A6rnsf%C3%A6lles-Doktrin-for-Milit%C3%A6re-Cyberspaceoperationer/991816060103741

Försvarsmakten. (n.d.). Cyberförsvarssystem [Cyber defence systems]. https://www.forsvarsmakten.se/om-forsvarsmakten/organisation/stridskrafter/cyberforsvar/cyberforsvarssystem/

Försvarsmakten. (2024). Doktrinansats Cyberförsvar, version 1.1 [Doctrine approach: cyber defence]. Swedish Armed Forces, in force 1 December 2024. https://www.forsvarsmakten.se/globalassets/02-om-forsvarsmakten/myndighetsinformation/dokument/doktriner/doktrinansats-cyberforsvar-1.1.pdf

Forsvarsministeriet. (2012). Aftale på forsvarsområdet 2013-2017. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-forsvarsforlig-2013-2017-inkl-bilag-.pdf

Forsvarsministeriet. (2023). Aftale om dansk forsvar og sikkerhed 2024-2033 [Agreement on Danish defence and security 2024-2033], 28 June 2023. https://www.fmn.dk/globalassets/fmn/dokumenter/forlig/-aftale-om-dansk-forsvar-og-sikkerhed-2024-2033-aftaletekst-28-06-2023-.pdf

Gesellschaft für Informatik. (2026, March 16). Stellungnahme zum Referentenentwurf eines Gesetzes zur Stärkung der Cybersicherheit. https://gi.de/fileadmin/GI/Hauptseite/Service/Publikationen/GI_Stellungnahme_Referentenentwurf-Cyberabwehr.pdf

Government Offices of Sweden. (2025). Nationell strategi för cybersäkerhet 2025-2029 (Skr. 2024/25:121). https://www.regeringen.se/rattsliga-dokument/skrivelse/2025/03/skr.-202425121

Government of Norway. (2021). National position of Norway on international law in cyberspace. Reproduced in the CCDCOE Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Norway_(2021)

Government of the Netherlands. (2019). Appendix: International law in cyberspace [Letter to Parliament]. Reproduced in the CCDCOE Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_Netherlands_(2019)

Guvernul României. (2021). Strategia de securitate cibernetică a României, pentru perioada 2022-2027 (Hotărârea de Guvern nr. 1321/2021). https://legislatie.just.ro/Public/DetaliiDocument/250235

Hellenic Republic. (2024). Law 5110/2024, Government Gazette A 75 of 24 May 2024, establishing among other provisions a Joint Information Technology Corps in the Armed Forces.

Herpig, S. (2021). Active cyber defense operations: Assessment and safeguards. Stiftung Neue Verantwortung.

Herpig, S., & Kuehn, A. (2022, February 25). The EU and responsible active cyber defence. Directions (EU Cyber Direct).

Incyber News. (2025). Defense at the heart of European cyber commands. https://incyber.org/en/article/incyber-defense-at-the-heart-of-european-cyber-commands/

Jefatura del Estado. (2002). Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. https://www.boe.es/eli/es/l/2002/05/06/11/con

Jensen, M. S. (2022). Five good reasons for NATO's pragmatic approach to offensive cyberspace operations. Defence Studies.

Kesan, J. P., & Hayes, C. M. (2012). Mitigative counterstriking: Self-defense and deterrence in cyberspace. Harvard Journal of Law & Technology, 25(2), 429-543.

Kostyuk, N. (2021). Deterrence in the cyber realm: Public versus private cyber capacity. International Studies Quarterly, 65(4), 1151-1162.

Krašto apsaugos ministerija. (2025). Pradeda veikti Lietuvos kariuomenės kibernetinės gynybos valdyba. https://kam.lt/pradeda-veikti-lietuvos-kariuomenes-kibernetines-gynybos-valdyba/

Lachow, I. (2013). Active cyber defense: A framework for policymakers. Center for a New American Security.

La Défense. (2025). Vision stratégique Défense 2025 [Strategic vision for Defence 2025], approved 18 July 2025. Belgian Defence. https://www.mil.be/media/ac5okcnp/strategic-vision-2025-extended.pdf

L'Essentiel de l'Éco. (2026). Le Régiment de Cyberdéfense français, en guerre dès sa création. https://lessentieldeleco.fr/7612-le-regiment-de-cyberdefense-francais-en-guerre-des-sa-creation/

Maschmeyer, L. (2021). The subversive trilemma: Why cyber operations fall short of expectations. International Security, 46(2), 51-90.

Matishak, M. (2025, February 28). Exclusive: Hegseth orders Cyber Command to stand down on Russia planning. The Record. https://therecord.media/hegseth-orders-cyber-command-stand-down-russia-planning

Ministère des Armées. (2019). Droit international appliqué aux opérations dans le cyberespace. https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf

Ministère des Armées. (n.d.-a). La lutte informatique offensive (LIO). https://www.defense.gouv.fr/comcyber/nos-operations/lutte-informatique-offensive-lio

Ministère des Armées. (n.d.-b). Le Commandement de la cyberdéfense (COMCYBER). https://www.defense.gouv.fr/comcyber/commandement-cyberdefense-comcyber

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties & Ministerie van Defensie. (2026). Wetsvoorstel Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbnv) [Draft bill, public consultation 28 August to 11 October 2026]. https://www.internetconsultatie.nl/wbnv

Ministerie van Defensie. (2024, May 30). Kamerbrief over de samenwerking tussen het Defensie Cyber Commando en de MIVD (Kamerstuk 33321, nr. 10) [Letter to parliament on cooperation between the Defence Cyber Command and the MIVD].

Ministerie van Defensie. (2025a). Defensie Cyberstrategie 2025. https://www.defensie.nl/site/binaries/site-content/collections/documents/2025/10/03/defensie-cyber-strategie-2025/Defensie+Cyberstrategie+-+openbaar.pdf

Ministerie van Defensie. (2025b, October 3). Kamerbrief Defensie Cyberstrategie 2025. https://open.overheid.nl/documenten/18553fd0-0941-48e5-a9ea-95054ff1dc05/file

Ministerio de Defensa. (2004). Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional. https://www.boe.es/eli/es/rd/2004/03/12/421/con

Ministerio de Defensa. (2020). Orden DEF/710/2020, de 27 de julio, por la que se desarrolla la organización básica del Estado Mayor de la Defensa (BOE-A-2020-8638). https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-8638

Ministerio de la Presidencia. (2018). Orden PRA/33/2018, de 22 de enero, por la que se publica el Acuerdo del Consejo de Seguridad Nacional, por el que se regula el Consejo Nacional de Ciberseguridad. https://www.boe.es/buscar/act.php?id=BOE-A-2018-799

Ministerstvo obrany České republiky. (2019). Národní centrum kybernetických operací vypracovalo Strategii kybernetické obrany ČR. https://mocr.mo.gov.cz/informacni-servis/zpravodajstvi/narodni-centrum-kybernetickych-operaci-vypracovalo-strategii-kyberneticke-obrany-cr-201906/

Ministerstvo obrany České republiky. (2026). Vojenské zpravodajství provedlo aktivní zásah v kybernetickém prostoru [Military Intelligence carried out an active intervention in cyberspace], 8 April 2026. https://mocr.mo.gov.cz/informacni-servis/zpravodajstvi/vojenske-zpravodajstvi-provedlo-aktivni-zasah-v-kybernetickem-prostoru-263230/

Ministerstwo Obrony Narodowej. (n.d.). Wojska Obrony Cyberprzestrzeni. https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni

Ministrstvo za obrambo Republike Slovenije. (2023). Srednjeročni obrambni program Republike Slovenije 2023-2028 [Medium-term defence programme of the Republic of Slovenia 2023-2028], No. 80300-1/2023/10, 31 May 2023. https://www.gov.si/assets/ministrstva/MO/Dokumenti/SOPR_2023-2028_sprejet.pdf

Ministrstvo za obrambo Republike Slovenije. (2025). Srednjeročni obrambni program Republike Slovenije 2026-2031 [Medium-term defence programme of the Republic of Slovenia 2026-2031], adopted 6 November 2025. https://www.gov.si/assets/ministrstva/MO/Dokumenti/sopr_26-31_sprejet.pdf

Ministry for Foreign Affairs of Finland. (2020). International law and cyberspace: Finland's national positions. https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf

Ministry of Justice and Digital Affairs. (2024). Cybersecurity strategy 2024-2030: Cyber-conscious Estonia. https://enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

Moynihan, H. (2019). The application of international law to state cyberattacks: Sovereignty and non-intervention. Chatham House.

Národná rada Slovenskej republiky. (2022). Zákon č. 500/2022 Z. z. o Vojenskom spravodajstve [Act No. 500/2022 Coll. on Military Intelligence], adopted 29 November 2022, s. 7. https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/500/

Národní úřad pro kybernetickou a informační bezpečnost. (2025). Národní strategie kybernetické bezpečnosti České republiky 2026-2030 [National cyber security strategy of the Czech Republic 2026-2030], approved 3 September 2025. https://nukib.gov.cz/

National Cyber Force. (2023). Responsible cyber power in practice. https://www.gchq.gov.uk/files/NCF_Responsible_Cyber_Power_In_Practice.pdf

National Cybersecurity Authority of Greece. (2025). Εθνική Στρατηγική Κυβερνοασφάλειας 2026-2030 [National cybersecurity strategy 2026-2030], ministerial decision No. 2563 of 16 December 2025. https://cyber.gov.gr/wp-content/uploads/2025/12/ΕΣΚ-2026-2030.pdf

National Cyber Security Centre. (n.d.). Introduction to Active Cyber Defence. https://www.ncsc.gov.uk/section/active-cyber-defence/introduction

National Institute of Standards and Technology. (n.d.-a). Active cyber defense. In Computer Security Resource Center glossary. https://csrc.nist.gov/glossary/term/active_cyber_defense

National Institute of Standards and Technology. (n.d.-b). Defensive cyberspace operation response action. In Computer Security Resource Center glossary. https://csrc.nist.gov/glossary/term/defensive_cyberspace_operation_response_action

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.-a). Glossary. International cyber law: Interactive toolkit. https://cyberlaw.ccdcoe.org/wiki/Glossary

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.-b). National positions. International cyber law: Interactive toolkit. https://cyberlaw.ccdcoe.org/wiki/List_of_articles

NATO Cooperative Cyber Defence Centre of Excellence. (2025). The evolution of cyber forces in NATO countries. https://ccdcoe.org/uploads/2025/07/The_evolution_of_cyber_forces_in_NATO_countries.pdf

NATO Standardization Office. (2020). AJP-3.20: Allied joint doctrine for cyberspace operations (Edition A, Version 1). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Norwegian Ministries. (2019). National cyber security strategy for Norway. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

Parlament České republiky. (2021). Zákon č. 150/2021 Sb., kterým se mění zákon č. 289/2005 Sb., o Vojenském zpravodajství [Act No. 150/2021 Coll. amending Act No. 289/2005 Coll. on Military Intelligence], §§ 16f-16g. Sbírka zákonů. https://www.e-sbirka.cz/sb/2021/150

Parlamentul României. (2023). Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României. https://legislatie.just.ro/Public/DetaliiDocument/265677

Presidencia del Gobierno. (2021). Estrategia de Seguridad Nacional 2021 (Real Decreto 1150/2021, de 28 de diciembre).

Presidência do Conselho de Ministros. (2022). Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro, Estratégia Nacional de Ciberdefesa [National cyberdefence strategy], approved by the Council of Ministers on 20 October 2022. Diário da República, 1.ª série, n.º 211, 2 November 2022. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/106-2022-202899924

Presidenza del Consiglio dei Ministri, Agenzia per la Cybersicurezza Nazionale. (2022). Strategia nazionale di cybersicurezza 2022-2026. https://www.acn.gov.it/ACN_Strategia.pdf

Rada Ministrów. (2026). Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej [Cybersecurity strategy of the Republic of Poland], adopted by Resolution No. 92 of 10 March 2026, Monitor Polski, item 309. https://eli.gov.pl/eli/MP/2026/309/ogl

Regeringen. (2024). Totalförsvaret 2025-2030 (prop. 2024/25:34) [Total defence 2025-2030]. Government of Sweden. https://www.riksdagen.se/sv/dokument-och-lagar/dokument/proposition/totalforsvaret-2025-2030_hc0334/

República Portuguesa. (2022). Decreto-Lei n.º 19/2022, de 24 de janeiro, Lei Orgânica do Estado-Maior-General das Forças Armadas [Organic law of the armed forces general staff], art. 41. Diário da República, 1.ª série, n.º 16. https://diariodarepublica.pt/dr/detalhe/decreto-lei/19-2022-178080766

República Portuguesa. (2025). Decreto-Lei n.º 125/2025, de 4 de dezembro, Regime Jurídico da Cibersegurança [Legal regime for cybersecurity]. Diário da República n.º 234/2025. https://diariodarepublica.pt/dr/detalhe/decreto-lei/125-2025-962603401

Republic of Estonia. (2019). President of the Republic at the opening of CyCon 2019. Reproduced in the CCDCOE Cyber Law Toolkit. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Estonia_(2019)

Republic of Poland. (2022). Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny [Act of 11 March 2022 on the Defence of the Fatherland]. Original publication: Dz.U. 2022 poz. 655; consolidated text: Dz.U. 2022 poz. 2305, as amended.

Republic of Poland. (2022). The Republic of Poland's position on the application of international law in cyberspace. https://www.gov.pl/attachment/3203b18b-a83f-4b92-8da2-fa0e3b449131

Republic of Poland, Ministry of Digital Affairs. (2026). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. https://www.gov.pl/web/baza-wiedzy/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa

Saeima. (2022). Nacionālās drošības likums [National Security Law], section 11(5) as amended 16 June 2022. https://likumi.lv/ta/id/14011-nacionalas-drosibas-likums

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations (2nd ed.). Cambridge University Press.

Schmitt, M. N., & Vihul, L. (2024). European approaches to the application of international law in cyberspace: A comparative legal analysis. EU Cyber Direct. https://eucyberdirect.eu/research/european-approaches-to-the-application-of-international-law-in-cyberspace-a-comparative-legal-analysis

Sénat. (2023). Pour une coordination de la cyberdéfense plus offensive dans la loi de programmation militaire 2024-2030 (Rapport d'information no. 638, 2022-2023). https://www.senat.fr/rap/r22-638/r22-638_mono.html

Smeets, M. (2018). Integrating offensive cyber capabilities: Meaning, dilemmas, and assessment. Defence Studies, 18(4), 395-410.

Smeets, M. (2022). No shortcuts: Why states struggle to develop a military cyber-force. Oxford University Press.

Staatsblad van het Koninkrijk der Nederlanden. (2024). Wet van 13 maart 2024, houdende tijdelijke regels over onderzoeken door de AIVD en de MIVD naar landen met een offensief cyberprogramma (Stb. 2024, 88). https://zoek.officielebekendmakingen.nl/stb-2024-88.html

Stars and Stripes. (2025, March 4). Pentagon denies halting cybersecurity operations against Russia. https://www.stripes.com/theaters/us/2025-03-04/cyber-hegseth-pentagon-russia-17031715.html

Štrucl, D. (2021). Comparative study on the cyber defence of NATO member states. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2022/04/Comparative-study-on-the-cyber-defence-of-NATO-Member-States.pdf

U.S. Cyber Command. (2020, December 3). Estonian, U.S. cyber commands conduct joint defensive cyber operation. https://www.cybercom.mil/Media/News/Article/2433245/

U.S. Cyber Command. (2022). Cyber 101: Defend forward and persistent engagement. https://nsarchive.gwu.edu/sites/default/files/documents/semon9-giki0/2022-10-25-USCYBERCOM-Cyber-101-Defend-Forward-Persistent-Engagement.pdf

U.S. Department of Defense. (2023). Fact sheet: 2023 DoD cyber strategy. https://media.defense.gov/2023/May/26/2003231006/-1/-1/1/2023-DOD-CYBER-STRATEGY-FACT-SHEET.PDF

Annex A. The authors' working matrix

This is the matrix on which the comparison in Parts II and III rests. It records, for each state and each of the seven analytical questions of Section 2.2, what the primary documents allow us to say, together with the kind of document it comes from. 'Not published' means we read the documents and found no answer, 'not verified' means the primary document could not be retrieved, and 'pending' means the answer comes from a bill not yet enacted. The abbreviations in parentheses are our shorthand and are explained in the note below.

State	Evidentiary basis	Authority basis	Declaratory register	Locus of action	Target type	Trigger	Intended effect	International law anchor
France	Doctrine + official page	Military (MIL)	Explicitly offensive (OFF)	Adversary infrastructure (L2)	Not published	Not published	Disruptive (E1)	Sovereignty as rule (SOV)
Netherlands	Strategy + statute	Hybrid intelligence-military (HYB)	Explicitly offensive (OFF)	Adversary infrastructure (L2)	Not restricted by the strategy (SYS)	Persistent, peacetime (T2)	Detect, restrict, disrupt, disable (E1)	Sovereignty as rule (SOV)
Germany	Two bills (pending) + ministry statement	Police, pending (POL); intelligence route also pending, military route under existing rules, see Section 5.1.3	Qualified 'active' (ACT)	Attacking systems (police bill); foreign IT infrastructure (intelligence bill) (L2, pending)	Attacking systems; state hacker groups (SYS/STATE, pending)	Danger aversion (police); specific threat from foreign powers (intelligence) (T1, pending)	Disruptive (E1, pending)	Published, not analysed (PUB)
Romania	Statute + strategy	Military, statutory (MIL)	Explicitly offensive (OFF)	Not specified in the cited provision	Not specified in the cited provision	Cyberattacks contravening international law (T1, circumstance stated; no authorisation threshold)	Not published	Published, not analysed (PUB)
Poland	Statute + official webpage	Military (MIL)	Explicitly offensive (OFF)	Not published	Not published	Not published	Not published	Sovereignty as rule (SOV)
Italy	Strategy	Military (MIL)	Explicitly offensive (OFF)	Not published	Not published	Conditional, 'nei casi previsti'	Not published	Published, not analysed (PUB)
Denmark	Agreement (2013-2017, restating 2010-2014) + joint doctrine	Military (MIL)	Explicitly offensive (OFF)	Adversary's part of cyberspace (L2)	Not published	Decision delegated to the lowest level warranted; offensive use follows the procedure for other military means, with parliamentary involvement	Application of force; no specific effect published	Published, not analysed (PUB)
Spain	Ministerial order + statute + strategy	Hybrid (HYB)	Operational, unqualified (OPS)	Not published	Not published	Not specified in the cited published documents	Not published	None located
Lithuania	Official webpage	Military (MIL)	Operational, unqualified (OPS)	Not published	Not published	Not published	Not published	None located

State	Evidentiary basis	Authority basis	Declaratory register	Locus of action	Target type	Trigger	Intended effect	International law anchor
Czechia	Statute + webpage + government account of an operation	Military intelligence (INT)	Qualified 'active intervention' (ACT)	Attacker-controlled infrastructure outside own networks (L2)	Compromised infrastructure abused by a named state-linked group, named in practice only (SYS/STATE; not counted)	Threat to important state interests on a significant scale; attack ongoing or immediately imminent; not avertable with the armed forces; active intervention the only effective means; prior ministerial consent (T1)	Reconfiguration of abused infrastructure, as described in one operation (E1)	Published, not analysed (PUB)
Portugal	Strategy + organic law	Military (MIL)	Explicitly offensive (OFF)	In and through cyberspace; action beyond defended networks not expressly established (not counted)	States and non-state entities, including covert state promotion (STATE/SYS)	Rules of engagement from tactical to strategic level, authorised by the political power (procedure)	Neutralise, manipulate, deny, disrupt, degrade or destroy (E1/E2)	None located
Belgium	Defence cyber strategy + Strategic Vision 2025 + national strategy	Military (MIL)	Explicitly offensive (OFF)	Not published	Not published	National crises (T1)	Neutralise an attack (E1)	Published, not analysed (PUB)
Estonia	Strategy	Hybrid (HYB)	Defensive only (DEF)	Own and partner networks (L0/L1)	Not published	Not published	Protective (E0)	Sovereignty as rule (SOV)
Finland	Strategy	Hybrid (HYB)	Qualified 'countermeasures' (ACT)	Not published	Not published	Not published	Not published	Sovereignty as rule (SOV)
Sweden	Doctrinal approach + strategy + bill	Military (MIL)	Explicitly offensive (OFF)	Own systems, defended systems, adversary systems (L0/L1/L2)	Antagonist: state, state-sponsored, non-state (SYS/STATE)	Cyber defence active at all conflict and readiness levels; offensive operations decided at the military-strategic level (procedure)	Denial of access; manipulation of data (E1)	Published, not analysed (PUB)
Ireland	Defence Forces strategy	Military (MIL)	Qualified 'active', undefined (ACT)	Not published	Not published	Directed by the Joint Force Commander under ROE and national authority	Not published	Published, not analysed (PUB)

State	Evidentiary basis	Authority basis	Declaratory register	Locus of action	Target type	Trigger	Intended effect	International law anchor
Latvia	Strategy + statute	Ministerial decision for operations; civilian lead for posture (MIL)	Qualified 'active' (ACT)	Not published	Not published	Ministerial decision on national security and defence interests, coordinated with the Prime Minister and the Minister for Foreign Affairs (statutory)	Not published	None located
Slovakia	Statute	Military intelligence, statutory (INT)	Qualified 'active', defined in statute (ACT)	Attacker's information systems and networks (L2)	Attacker systems, actor not specified (SYS)	Attack on specified objects, imminent, occurring or ongoing; only effective means; prior ministerial consent; also collective-defence or other binding treaty obligations (§7(7)(b)–(c); §7(9) approval) (T1)	Disrupt availability, confidentiality or integrity (E1)	None located
Slovenia	Defence programme	Military (MIL)	Qualified 'proactive' (ACT)	Not published	Not published	Not published	Not published	Published, not analysed (PUB)
Remaining EU MS (8): Austria, Bulgaria, Croatia, Cyprus, Greece, Hungary, Luxembourg, Malta	Not applicable	Military cyber unit named for Austria, Bulgaria, Croatia, Greece and Hungary; legal family not published	No published position (SIL); reviewed and absent for six	Not published	Not published	Not published	Not published	None located for seven of these eight; twelve across the EU27
US: defend forward	Strategy	Military (MIL)	Explicitly offensive (OFF)	Adversary infrastructure (L2)	Attacker systems (SYS)	Persistent, peacetime (T2)	Disruptive (E1)	Published, not analysed (PUB)
US: 'active cyber defense'	Glossary (CNSSI)	Not applicable	Qualified 'active' (ACT)	Own networks (L0)	Not applicable	Real time	Protective (E0)	Published, not analysed (PUB)
UK: NCF	Framework document	Hybrid intelligence-military (HYB)	Qualified 'responsible' (ACT)	Adversary infrastructure (L2)	Not published	Persistent, peacetime (T2)	Not published	Non-intervention only (NI)
UK: 'Active Cyber Defence'	Programme document	Not applicable	Qualified 'active' (ACT)	Own networks (L0)	Commodity, criminal (CRIM)	Reactive (T0)	Protective (E0)	Non-intervention only (NI)
NATO: DCO / OCO	Doctrine	Not applicable (Alliance, not a state)	Binary, no middle term	Authorised-access networks; beyond via SCEPVA	Not applicable	Not applicable	Protective (E0) or destructive (E2)	IHL applies

Note. Shorthand: MIL military, INT intelligence, POL police, HYB hybrid; OFF explicitly offensive, ACT qualified active or proactive, OPS unqualified operational, DEF defensive, SIL no published position; L0 own networks, L1 partner networks by consent, L2 adversary or third-party infrastructure; STATE, CRIM and SYS for state actors, criminal infrastructure and attacker systems irrespective of actor; T0 reactive, T1 imminent threat or danger aversion, T2 persistent peacetime posture; E0 protective, E1 disruptive, E2 destructive; SOV sovereignty as a rule, NI non-intervention only, PUB published but not analysed here. Every coded entry is supported by a quotation and citation in Part II. Annex C also lists instruments that were reviewed but not quoted.

Annex B. Descriptive comparative matrix

State	Responsible actor	Legal framework	Terminology in official documents	Geographic scope (as published)	Trigger threshold (as published)	Stated international law position
France	COMCYBER, under CEMA	Military doctrine (2019); LPM 2024-2030	Lutte informatique offensive (LIO); LID; L2I	Effects against adversary systems; autonomous or combined with conventional means	Not published as operational trigger; response right stated in international law position	Published (2019); sovereignty applies to cyberspace
Netherlands	Defensie; AIVD / MIVD	Art. 97 Constitution; Wiv 2017; Temporary Act (Stb. 2024, 88); draft Wbnv	Permanente proactieve inzet; offensief tegendruk	Adversary infrastructure; not restricted to the statutory category	Grey zone between war and peace and armed conflict; escalation avoidance stated	Published (2019); sovereignty rule, boundaries not fully crystallised
Germany	BKA, Bundespolizei, BSI (proposed); BND and BfV (proposed); Cyber and Information Domain Command	BT-Drs. 21/6585 (police law) and BT-Drs. 21/7868 (intelligence law), both pending, with a federal competence dispute ongoing; Basic Law and Bundestag mandate for the armed forces	Aktive Cyberabwehr (bill pending)	Attacking systems; foreign IT infrastructure under the intelligence bill	Danger aversion; specific threat from foreign powers; Bundestag mandate for military operations	Published (2021)
Romania	MApN (Cyber Defence Command); DNSC; SRI	Law 58/2023; Strategy 2022-2027 (HG 1321/2021)	Capabilități de răspuns ofensiv; descurajare	Not specified in the cited provision; 'individually or in coalition or alliance' describes the mode of action	Cyberattacks contravening international law (circumstance; no authorisation threshold)	Published (2021); IHL compliance required by statute
Poland	WOC / DKWOC; CSIRT NASK / GOV / MON	Defence structures; KSC Act as amended (in force 3 Apr 2026, NIS2); Act on the Defence of the Fatherland, Art. 15(4)(2) and Art. 23.	Pełne spektrum: obronne, rozpoznawcze, ofensywne; proaktywna ochrona; aktywna obrona	Not published	Not published	Published (2022); sovereignty covers private infrastructure
Italy	Difesa (specialist branches); ACN; intelligence	National Cybersecurity Strategy 2022-2026	Operazioni militari cibernetiche offensive e difensive	Not specified in strategy	Nei casi previsti (in the cases provided for)	Published (2021)
Denmark	Forsvarets Efterretningstjeneste (FE) / CFCS	Defence Agreements 2010-2014 and 2013-2017; Værnsfælles Doktrin for Militære Cyberspaceoperationer (2019)	Defensive og offensive militære operationer i cyberspace (CNO)	In or through an adversary's part of cyberspace	Decision delegated to the lowest level warranted; offensive capacity used as other military means, with involvement of the Folketing	Published (2023)
Estonia	RIA; Defence Forces Cyber Command (2018)	Cybersecurity Strategy 2024-2030	Resilience-framed; no offensive terminology located	Hosted allied defensive operations on own networks	Not published	Published (2019, 2021); collective countermeasures advanced
Finland	National Cyber Security Director; Defence Forces	Cyber Security Strategy 2024-2035 (10 Oct 2024)	Active cyber defence; response and countermeasures (strategy pillar IV)	Not published	Strategic response priority; no specific operational trigger published	Published (2020); sovereignty a primary rule

State	Responsible actor	Legal framework	Terminology in official documents	Geographic scope (as published)	Trigger threshold (as published)	Stated international law position
Spain	Mando Conjunto del Ciberespacio (EMAD); Consejo Nacional de Ciberseguridad, chaired by the CNI Director (national coordination); CNI and CCN	Orden DEF/710/2020; Law 11/2002 and RD 421/2004 (CNI and CCN); Orden PRA/33/2018 (National Cybersecurity Council); National Cybersecurity Strategy 2019; National Security Strategy 2021.	Operaciones militares en el ciberespacio; no offensive term in founding order; ciberdefensa activa for protective measures (2019 strategy)	Not specified in the cited published documents	Not specified in the cited published documents	No published position located
Lithuania	Cyber Defence Command (from 1 Jan 2025)	Armed forces structure law amendment (2024)	Kibernetinės erdvės operacijos; no offensive term located	Not published	Not published	No published position located
Sweden	Försvarsmakten, with FRA in support; NCSC for civil cybersecurity	Doktrinansats Cyberförsvar 1.1 (doctrinal approach, applied since 1 Dec 2024); prop. 2024/25:34; strategy 2025-2029 (skr. 2024/25:121)	Offensiva och defensiva cyberoperationer; cyberförsvarsresurser	In and outside own systems and platforms; against systems the adversary needs	Cyber defence active at all conflict and readiness levels; OCO decided at military-strategic level; continuous offensive operations not established	Published (2022)
Czechia	Vojenské zpravodajství (NCKO)	Zákon č. 289/2005 Sb. as amended by zákon č. 150/2021 Sb., §§ 16f-16g; Cyber Defence Strategy (2019)	Široké spektrum operací v kyberprostoru; aktivní zásah v kybernetickém prostoru (statute)	Attacker-controlled infrastructure abroad, as described in the operation announced on 8 April 2026	Threat to important state interests on a significant scale; attack ongoing or immediately imminent; not avertable with the armed forces; active intervention the only effective means; prior consent of the Minister of Defence	Published (2024)
Portugal	Comando de Operações de Ciberdefesa, under the Chief of the Defence Staff	Estratégia Nacional de Ciberdefesa (RCM 106/2022); Decreto-Lei n.º 19/2022, art. 41	Atividade ofensiva; operações no e através do ciberespaço	Operations in and through cyberspace; action beyond defended networks not expressly established by the passage cited	Rules of engagement, authorisations from tactical to strategic level, authorised by the political power	No position located
Belgium	Cyber Command (2022); fifth component (2024); Belgian Cyber Force (2025)	Cyber Strategy for Defence; Cybersecurity Strategy Belgium 2.0 (2021-2025)	Offensive cyber capability; cyber effects; intrusive and offensive capabilities	Not published	National crises (national strategy)	Published (2025)
Ireland	Joint Cyber Defence Command (IOC January 2025, FOC January 2028); NCSC for national cybersecurity	Defence Forces Cyber Defence Strategy 2024-2027	Active Cyber Defence (undefined); Active Cyber Protection	Not published	Directed by the Joint Force Commander on consultation with the Chief of Defence; use of force policy, ROE, national authority	Published (2023)

State	Responsible actor	Legal framework	Terminology in official documents	Geographic scope (as published)	Trigger threshold (as published)	Stated international law position
Latvia	National Cyber Security Centre (main institution); Minister for Defence decides on active cyber defence operations; National Guard battalion	Kiberdrošības stratēģija 2023-2026; National Security Law s. 11(5) (2022); National Cyber Security Law (2024)	Aktīvās kiberaizsardzības spējas; aktīvie un pasīvie aizsardzības pasākumi	Not published	Ministerial decision upon assessment of national security and defence interests, coordinated with the Prime Minister and the Minister for Foreign Affairs; capability development under discussion	No published position located
Slovakia	Cyber Defence Centre of the Slovak Republic, within Military Intelligence; national cyber defence authority	Act No. 500/2022 Coll. on Military Intelligence, s. 7 (2022)	Aktívna obrana (defined in statute)	Attacker's information systems and networks	Attack on specified objects or critical infrastructure, or serious incident; imminent, occurring or ongoing; only effective means; prior consent of the Minister of Defence; also collective-defence or other binding treaty obligations (§7(7)(b)–(c); §7(9) prior approval)	No position located
Slovenia	Slovenska vojska; Center za kibernetsko obrambo (2014)	Srednjeročni obrambni program 2023-2028; 2026-2031 (2025)	Proaktivno in stalno odzivanje; zmogljivost za nekinetično delovanje	Not published	Not published	Published (2026)
Remaining EU MS (8)	National CERTs / CSIRTs; some MoD units	Mostly absent or resilience legislation only	Varied or absent; reviewed and no active, proactive or offensive term located for Austria, Bulgaria, Cyprus, Luxembourg and Malta; Greece: see note; Croatia and Hungary not fully reviewed	Own networks where published	Primarily reactive where published	No published position located for seven of these eight (Austria has published)
United Kingdom (ref.)	National Cyber Force (GCHQ, MOD incl. Dstl, SIS)	NCF framework document (2023)	Responsible cyber power (NCF); Active Cyber Defence reserved for domestic protective programme	Not specified in public framework	Contest and compete posture	No standalone sovereignty rule beyond non-intervention (AJP-3.20 reservation)
United States (ref.)	U.S. Cyber Command; NSA	2023 DoD Cyber Strategy; CNSSI 4009-2022	Defend forward; persistent engagement; active cyber defense (internal, technical); DCO-RA (external)	Adversary networks (defend forward)	Disruption before effects reach the homeland	Extensive published positions
NATO (ref.)	Cyberspace Operations Centre; sovereign contributions	AJP-3.20 (2020); SCEPVA mechanism	No active defence category: DCO / OCO binary only	OCO only via SCEPVA in NAC-approved operations	DCO limited to authorised-access networks	International law applies; IHL principles apply to COs

Note. Entries reflect primary documents verified for this study as of 26 September 2026, except where marked. 'Not published' is a verified absence in the reviewed sources, while 'not verified' means the primary source could not be retrieved. Reference rows (UK, US, NATO) are included for comparative anchoring only. Greece's National Cybersecurity Strategy 2026-2030 refers to active protection and active deterrence, without establishing a defined military active-defence operation or external operational mandate.

Annex C. Primary sources by state

The inventory lists, per state, the primary instruments on which the comparison rests. Full bibliographic details of the instruments quoted in Part II are in the reference list. The inventory also records instruments that were reviewed without being quoted.

State	Primary instruments relied on
France	Éléments publics de doctrine militaire de lutte informatique offensive and COMCYBER pages (2019, n.d.); Droit international appliqué aux opérations dans le cyberespace (2019); Sénat, rapport no. 638 (2023).
Netherlands	Defensie Cyberstrategie 2025 and Kamerbrief (2025); Article 97 of the Constitution; Minister's letter of 30 May 2024 (Kamerstuk 33321, nr. 10); Temporary Act, Stb. 2024, 88; Wiv 2017; draft Wbnv (public consultation, 2026).
Germany	Gesetzentwurf BT-Drs. 21/6585 (2026) and Bundesrat exchange BT-Drs. 21/7406; Gesetzentwurf zur Reform des Nachrichtendienstrechts BT-Drs. 21/7868 (2026); Die Linke motion BT-Drs. 21/6653; BMVg on the legal basis of Bundeswehr cyber operations; BMI communications (2026).
Romania	Legea nr. 58/2023; Strategia de securitate cibernetică 2022-2027 (HG 1321/2021).
Poland	Ministry of National Defence WOC page (n.d.); international law position (2022); KSC Act as amended (2026); Act on the Defence of the Fatherland; Strategia Cyberbezpieczeństwa RP, Resolution No. 92 of 10 March 2026 (M.P. item 309), s. 6.6.
Italy	Strategia nazionale di cybersicurezza 2022-2026 (2022).
Denmark	Aftale på forsvarsområdet 2013-2017 (2012), restating the 2010-2014 agreement; Værnsfælles Doktrin for Militære Cyberspaceoperationer, Forsvarsakademiet (2019); FE cyber operations page (n.d.).
Spain	Ley 11/2002; Real Decreto 421/2004; Orden PRA/33/2018 (Consejo Nacional de Ciberseguridad); Estrategia Nacional de Ciberseguridad 2019; Estrategia de Seguridad Nacional 2021 (RD 1150/2021); Orden DEF/710/2020; Mando Conjunto del Ciberespacio mission statement (n.d.); PDC-3.20, Doctrina de operaciones en el ámbito ciberespacial (Estado Mayor de la Defensa, 28 April 2021), established to exist and cited in ministry-hosted material but not published.
Lithuania	Ministry of National Defence announcement, Cyber Defence Command (2025).
Czechia	Zákon č. 289/2005 Sb. o Vojenském zpravodajství, as amended by zákon č. 150/2021 Sb., §§ 16f-16g (aktivní zásah); Ministry of Defence, NCKO and Cyber Defence Strategy communication (2019); Ministry of Defence account of the active intervention of March 2026, published 8 April 2026.
Belgium	Cyber Strategy for Defence (Belgian Defence, English version via CCDCOE); Cybersecurity Strategy Belgium 2.0, 2021-2025 (Centre for Cyber Security Belgium), p. 37; Vision stratégique Défense 2025 (approved 18 July 2025), Annex C of which identifies active defence actions (Defend), offensive cyber capabilities (Fight) and the disruption of enemy networks; institutional facts from official statements.

State	Primary instruments relied on
Estonia	Cybersecurity Strategy 2024-2030; Küberväejuhatuse põhimäärus, confirmed by order of the Commander of the Defence Forces of 3 May 2022; national positions (2019, 2021); USCYBERCOM joint operation release (2020).
Finland	Cyber Security Strategy 2024-2035 (2024); international law positions (2020).
Sweden	Doktrinansats Cyberförsvar, version 1.1, designated a doctrinal approach, applied since 1 December 2024 (Försvarsmakten); Regeringens proposition 2024/25:34, Totalförsvaret 2025-2030; Nationell strategi för cybersäkerhet 2025-2029 (skr. 2024/25:121); Försvarsmakten cyber defence pages.
Austria	Österreichische Strategie für Cybersicherheit 2021; Österreichische Sicherheitsstrategie 2024; Maßnahmenkatalog ÖSCS, Fortschrittsbericht 1/2025, recording an unpublished cross-cutting concept Einsatz im Cyber-Raum (reported as completed in 2023; underlying concept not publicly reviewed); BMLV, Directorate 6 (IKT and Cyber), from 1 October 2024; position paper on cyber activities and international law (2024). Reviewed; no active or offensive term located.
Bulgaria	Cyber-Resilient Bulgaria 2023 (Council of Ministers Decision 301/2021); Ministry of Defence, Command for Communications-Information Support and Cyber Defence. Reviewed; no active or offensive term located.
Croatia	Defence Act as amended, Narodne novine 70/2019; Cyber Security Act, Narodne novine 14/2024; Cyberspace Command (2019); Dugoročni plan razvoja Oružanih snaga 2025-2036, Narodne novine 104/2025, reviewed for this study and naming cyber defence and situational awareness only. Standalone national cybersecurity strategy not reviewed.
Cyprus	Cybersecurity Strategy of the Republic of Cyprus (2020), Digital Security Authority. Reviewed; no active or offensive term located; no military cyber unit located.
Greece	National Cybersecurity Strategy 2020-2025 and 2026-2030 (ministerial decision 2563 of 16 December 2025), the latter read in full; it refers to active deterrence in developing national defence cyber capabilities (Action 4.E.4) but contains no mandate for offensive operations or action beyond defended networks; Law 5110/2024 establishing a Joint Information Technology Corps and a joint cybersecurity operations centre.
Hungary	Government Decree 614/2022 (XII.29.); Hungarian Defence Forces Cyber Operations Command pages. National cybersecurity strategy not reviewed.
Ireland	Defence Forces Cyber Defence Strategy 2024-2027 (July 2024), including the Joint Cyber Defence Command (initial operating capability January 2025); National Cyber Security Strategy 2019-2024 (lapsed; successor in preparation); Commission on the Defence Forces report (2022); position paper on international law (2023).
Latvia	Latvijas kiberdrošības stratēģija 2023.-2026. gadam; Nacionālās drošības likums, s. 11(5), as amended 16 June 2022; Nacionālās kiberdrošības likums (2024), ch. 3 s.4; National Guard cyber defence unit, ministerial order of 30 July 2013.

State	Primary instruments relied on
Luxembourg	Stratégie de cyberdéfense du Luxembourg (2021), Direction de la défense, including its definitions of cyberdéfense and cyber opération; Service de cyberdéfense of the army. Reviewed; no active or offensive term located.
Malta	National Cybersecurity Strategy 2023-2026; published order of battle of the Armed Forces of Malta. Reviewed; no active or offensive term located; no cyber unit listed.
Portugal	Estratégia Nacional de Ciberdefesa, Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro (approved 20 October 2022); Decreto-Lei n.º 19/2022 (organic law of the armed forces general staff), art. 41, establishing the Comando de Operações de Ciberdefesa; Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (lapsed); Decreto-Lei n.º 125/2025 (replacement civil strategy required, not yet adopted).
Slovakia	Zákon č. 500/2022 Z. z. o Vojenskom spravodajstve [Act on Military Intelligence], s. 7, adopted 29 November 2022; Národná stratégia kybernetickej bezpečnosti 2021-2025 (Government Resolution 5/2021); Cyber Defence Centre within Military Intelligence (from 1 April 2018).
Slovenia	Srednjeročni obrambni program 2023-2028 (No. 80300-1/2023/10); Srednjeročni obrambni program 2026-2031 (adopted 6 November 2025), p. 26; Center za kibernetsko obrambo (2014); position paper on international law (May 2026). Cyber security resolution not reviewed.
United Kingdom	Responsible Cyber Power in Practice (2023); NCSC ACD pages (n.d.); AJP-3.20 UK reservation (2020).
United States	2023 DoD Cyber Strategy fact sheet; USCYBERCOM Cyber 101 (2022); NIST/CNSSI glossary entries (n.d.).
Norway	National Cyber Security Strategy (2019); national position (2021).

About EU Cyber Direct

EU Cyber Direct – the EU Cyber Diplomacy Initiative supports the European Union's cyber diplomacy and international digital engagements in order to strengthen the rules-based order in cyberspace and build cyber resilient societies. To that aim, the programme conducts research, supports capacity building in partner countries, and promotes multistakeholder cooperation. EU Cyber Direct is implemented by the EU Institute for Security Studies and is funded by the European Union.

AUTHORS

Dr Andrea Calderaro
EU Cyber Direct – the EU Cyber Diplomacy Initiative
EU Institute for Security Studies (EUISS)
Andrea.Calderaro@iss.europa.eu

Marius Houwen
EU Cyber Direct – the EU Cyber Diplomacy Initiative
EU Institute for Security Studies (EUISS)
Marius.Houwen@iss.europa.eu

EU CYBER DIRECT
The EU Cyber Diplomacy Initiative

Implemented by
euiss
European Union Institute for Security Studies

Funded by the European Union