



CENTRE FOR
CYBERSECURITY
BELGIUM

Cyber on steroids, game changer, or light at the end of the tunnel?

BE-CYBER 22/9/2026

Pieter Byttebier – Head of International Relations CCB

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister



Frontier AI and the world

Wat als Mythos uw bank, ziekenhuis of, godbetert, een kerncentrale hackt?

AI heeft een turbo gezet op de race tussen cybercriminelen en cybersecurity. Kritieke bedrijven moeten zich wapenen tegen een aanval waarvan ze niet weten hoe die eruit zal zien. "Het wordt een boksring waarin de ene AI-agent met de andere vecht."

Ze zijn niet moeilijk te herkennen, die telefoonjes in gebouwen Nederlands of met een Hollandse accent die beweren dat er iets mis is met uw bankkaart. Het zijn oplichters die gestolen of op internet geverste nummers opbellen om uw bankgegevens te stelen.

Maar wat als datzelfde telefoonje in uw vermomde dialect gebreit, met de boodschap dat uw kaart is misbruikt tijdens uw citytrip naar Amsterdam vorig weekend?

Spreekbuisen kunnen elk dialect nabootsen en het doen en laten van veel mensen op sociale media volgen. Een AI-agent kan die data combineren en automatisch mensen opbellen op een veel gekookt manier dan nu het geval is bij doorname phishing.

Die evolutie is al bezig, zegt Steven Vyncker, de ceo van Spirit, dat actief is in cybersecurity voor bedrijven. Van dag belken robots al mensen op in het Vlaams en ze stellen de vragen. Wie tracht, wordt daarin doorgevoerd met een echte persoon die doorgaat met phishing. "Ze n het doet niet en na een telefoonsje, maar dat is de bedoeling."

De opkomst van AI brengt de cybercriminaliteit in een stroomversnelling en dat moet niet alleen in een tijd voren komen, maar ook in de toekomst.

toegang krijgen tot Mythos. Onder meer de Belgische effectenruimte Euronext zal zijn cybersecurity kunnen afbreken aan Mythos.

Maar de rapporten die over die tests gepubliceerd worden, zijn niet van aard om de mensen te kalmeren. Vorige week nog meldde An Braspel dat Claude Mythos Personeel in korte tijd meer dan tienduizend e-mails of berichten kwade berichten in de software van de vijf deelnemende partijen heeft gevonden. Dat zijn e-mails en berichten die digitale inbrekers of hackers kunnen openen. Het gaat om e-mails die in berichten als Microsoft, Cisco, CrowdStrike of J.P. Morgan. Nog

"Cyberveiligheid is niet iets wat je erbij neemt omdat het wettelijk moet, maar een absolute noodzaak. En ze zal fundamenteel onze manier van werken veranderen"

Fabrice Wynants
Verantwoordelijke cybersecurity Cigalea

meer geavanceerde cyberaanvallen een van de grootste risico's, zegt de Belgische Nationale Bank aan in haar Financial Stability Report. "Technologische vooruitgang, in het bijzonder door AI, maakt onbekend, andere en complexere aanvallen mogelijk, zowel door staatsgevoerde als onafhankelijke spelers." Banken ontwikkelen doorgaans hun eigen software, maar er is een groeiende tendens om pakketten aan te kopen of uit te besteden aan externe IT-bedrijven. "Wat tot kleine onderbrekingen kan leiden", waarschuwt de Nationale Bank. "Wat meer meelidert financiële instellingen op een groenverantwoordelijke wijze IT-providers kiezen, kan een cyberaanval op zijn speler een systemische impact hebben en meerdere banken tegelijk verspillen."

De eerste regel in cyberveiligheid is dat je niet al te veel vertrouwt over je beveiligingsmaatregelen en banken houden zich daaraan. De communicatie van individuele banken en de sectorale instelling is afhankelijk van zijn algemeenheid. "Cyberveiligheid van een bank is en blijft prioriteit nummer een", kan Isabelle Marchand van Fitch Ratings zeggen. "Ze hebben een goed fundament en passen zich voortdurend aan nieuwe technologische veranderingen aan. Dat moet ook de andere kant op."

functies en de aanval schijnt een gat in de verdediging te vinden. Omdat het bij de ene aanval Meit en AZ Monica ingeheld is in een breed ziekenhuisnetwerk van de stad Antwerpen, ging de algemene mening de groenverantwoordelijke zijde onderuit. Maar wat als pakweg het UZ Leuven of meerdere ziekenhuizen tegelijk worden getroffen?

"Ziekenhuizen zijn potentiële doelwitten", waarschuwt bijeen, die onder meer voor het UZ Leuven werkt. "Wie een samenleving wil ontrouwen, legt een ziekenhuis plat. Je moet niet alleen de zorg, maar ook het gebied van de mensen dat het systeem kan beschermen. Angst aanjagen, dat is waar vijanden van het Westen op uitkomen."

LE SOIR

ent **Pourquoi ?** Opinions Podcasts Politique Société Monde

Quand les IA piratent : soulèvement des machines ou coup de com' ?

Des agents IA d'OpenAI ont piraté les infrastructures de Hugging Face. OpenAI s'est empressé de communiquer sur cet « incident » impressionnant. Pourtant, les machines n'ont fait que ce qu'on attendait d'elles.

OpenAI, Anthropic et Google travaillent à la création d'un organe de supervision des risques IA

15 sept. 2026 à 19:11 • 2 min

Partager

Écouter

OpenAI, Anthropic et Google DeepMind travaillent à la création d'un organe de supervision des risques liés à l'intelligence artificielle (IA), a indiqué OpenAI à l'AFP mardi, alors que se multiplient les appels à mieux contrôler les dérives de l'IA.

LIVE Trump kondigt AI-eenheid in leger aan en wil 'AI-tsaar': "We staan voor op de rest, en dat wil ik zo houden"



● CCB first technical findings

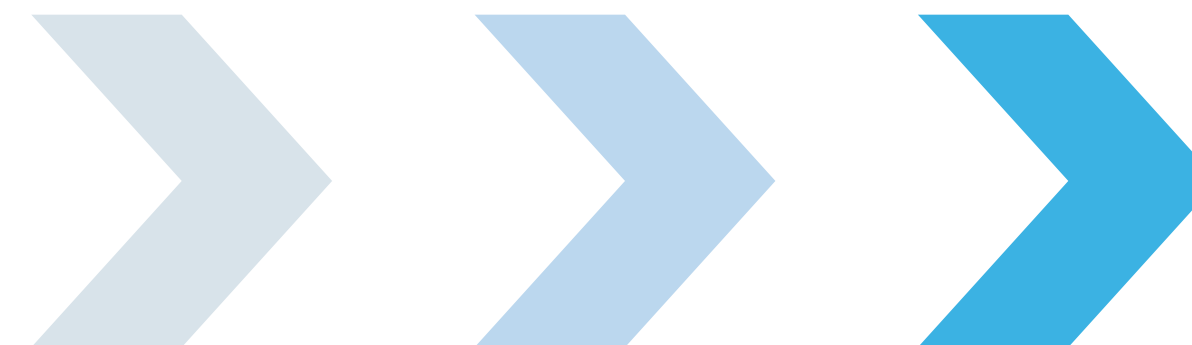
- CCB experts tested (safeguarded) versions of these tools
- Initial conclusion: **“hacking on steroids”**
- Combine **Expert** knowledge, advanced **Tools** and **Compute power (*)**
- Those without these capabilities face a **growing strategic risk**

“hacking on steroids”

Limited tests already show
incredible potential.

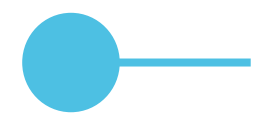
Why Frontier AI matters

- Cybersecurity is entering a **new paradigm**, and game changing months
- Frontier AI enables reasoning **beyond classic scanners**
(flaws as old as 27 years)
- **Vulnerabilities** can be found faster and deeper
(2026: Discovery of thousands of unpatched zero-days across major OS and browser)
- **A race** to find weaknesses before hostile actors do
(Equivalent capability is expected in adversarial hands within 4-6 months)



**From scanning
to reasoning**

Find weaknesses faster than hostile actors do.



Project Glasswing: Vulnerability Findings



Anthropic's AI-assisted vulnerability program — headline figures, as of the May 2026 update

10,000+

high/critical vulnerabilities found across partners

in the first month of the program

23,019

total findings across 1,000+ open-source projects

6,202 estimated high or critical severity

90.6%

true-positive rate on reviewed findings

of a 1,752-finding sample checked by 6 independent firms;

10x increase in bug finding rate

oWhen using Claude Mythos

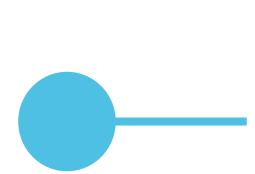
530 → 75 → 65

High/critical → patched → public advisories
bugs disclosed
To maintainers

patching is the current bottleneck, not discovery

27-year old bug

Openbsd bug was found that went unnoticed for decades

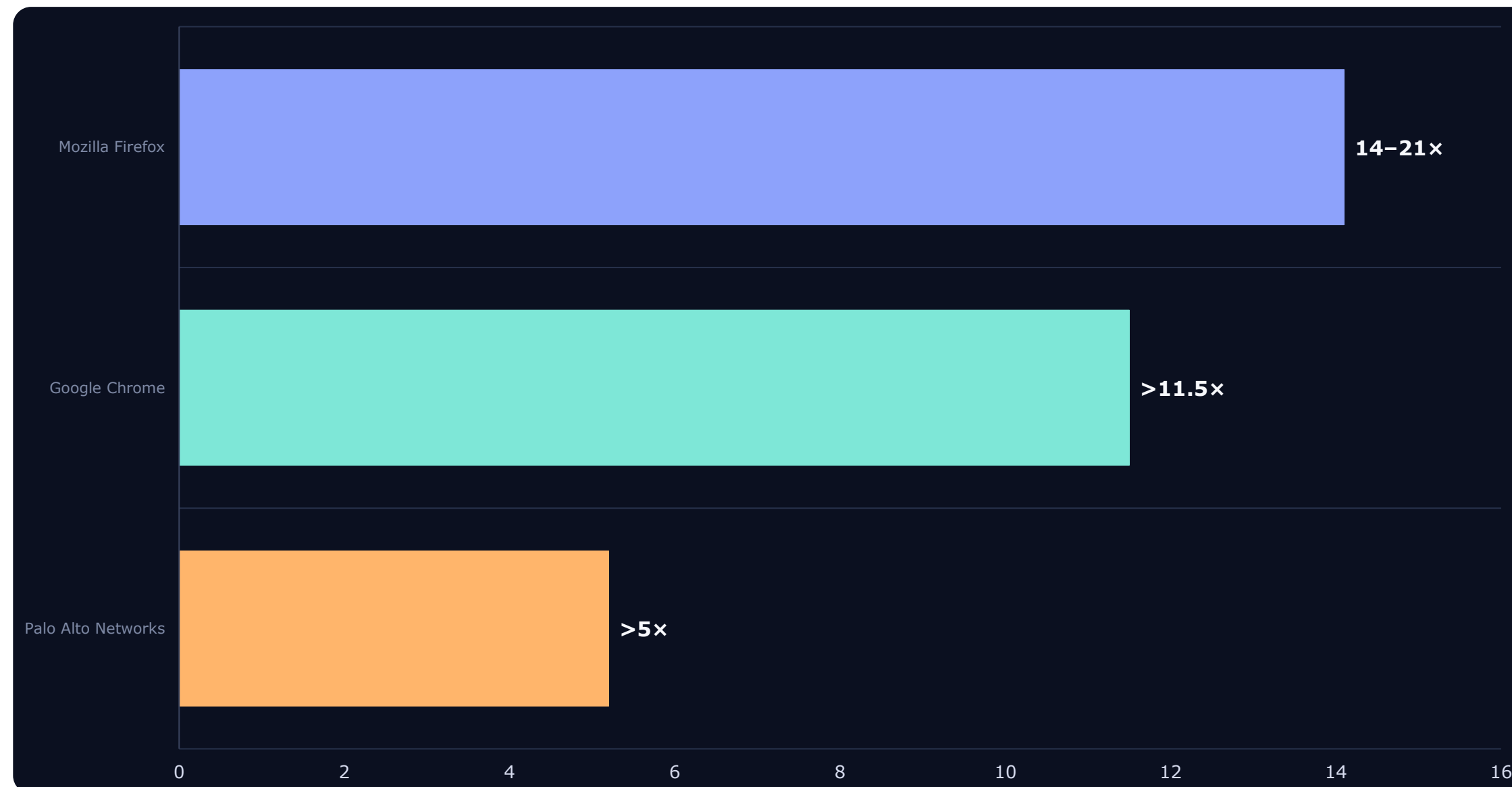


Frontier AI has sharply increased security fixes



Three production case studies show at least 5×, and often more than 10×, the previous patch volume

Conservative increase versus each organization's prior baseline



Baselines differ: monthly Firefox fixes, fixes per Chrome release, and monthly Palo Alto CVEs. The chart uses the lower bound where a range is reported.

What was patched

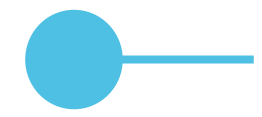
271 AI-identified vulnerabilities fixed in Firefox 150

1,072 security bugs fixed in Chrome 149–150; LLMs generated candidate fixes for most vulnerabilities

75 issues covered by 26 CVEs; patches shipped for all important findings after AI scans

Additional evidence of scale

CodeMender: 72 upstream security fixes. Codex Security: 70,000 findings marked fixed by reviewers. Glasswing: 2,100+ enterprise vulnerabilities and 75 high- or critical-severity open-source bugs patched.



Frontier AI Is Already Increasing Patch Volumes

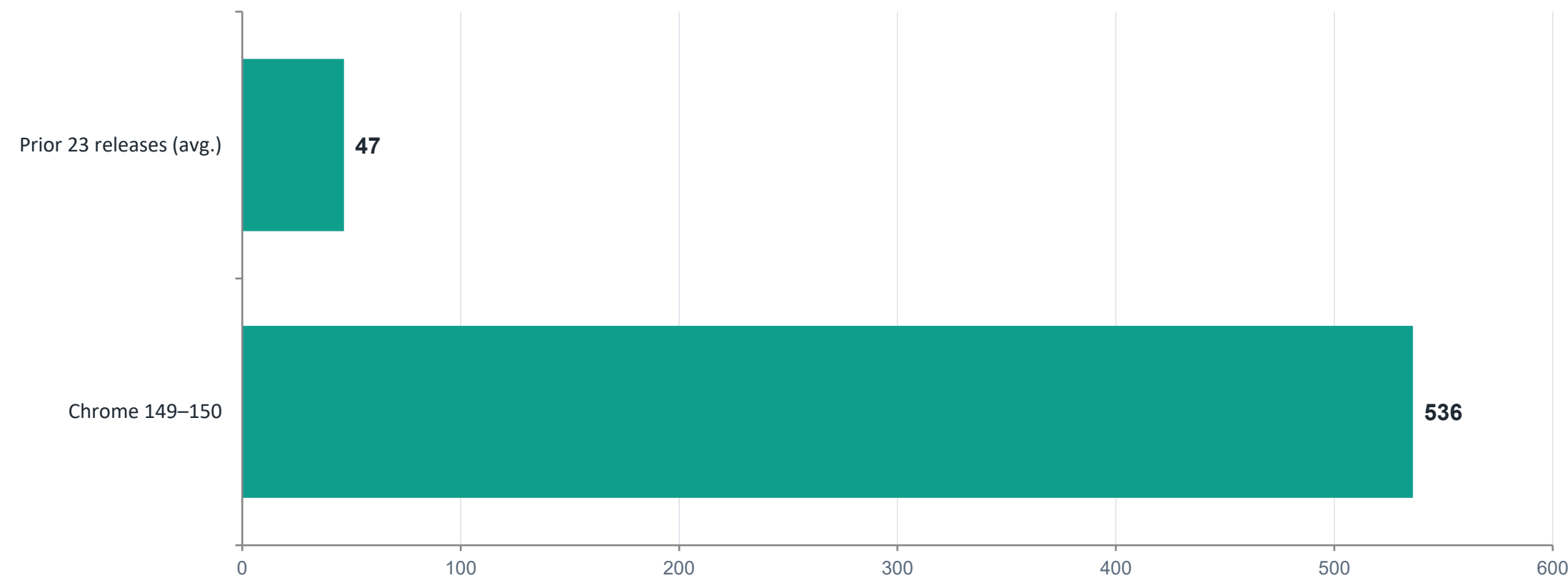


Independent evidence from Google and Microsoft supports the signal seen in Project Glasswing

>11.5×

increase in security fixes per Chrome release

Chrome 149–150 fixed 536 security bugs, more than the previous 23 releases combined (<46.6/release average). Google says LLMs now generate candidate fixes for most vulnerabilities.



Average security bugs fixed per release

INDEPENDENT CORROBORATION

72 security fixes upstreamed by Google DeepMind's CodeMender in six months

Microsoft Patch Tuesday

Microsoft expects releases to keep “trending larger.” It reports that advanced AI is surfacing additional issues and that many internally discovered fixes now come from AI-assisted tooling.

Glasswing adds scale, not sole proof

Claude Code security users patched 2,100+ vulnerabilities in three weeks. Project Glasswing’s open-source program reported 75 of 530 disclosed high/critical bugs patched to date.

— Strategic context

- Frontier AI is now on the international agenda (G7, AI Summit, Davos)
- The market is dominated by **US and Chinese** players
- Enormous challenges for **Open-Source Software**
- **Europe** risks falling behind, is **focused on regulation**
- Belgium needs **a national, pragmatic approach**
- Hard choices on sovereignty? (Short term challenges vs long term goals)

US

CN

EU

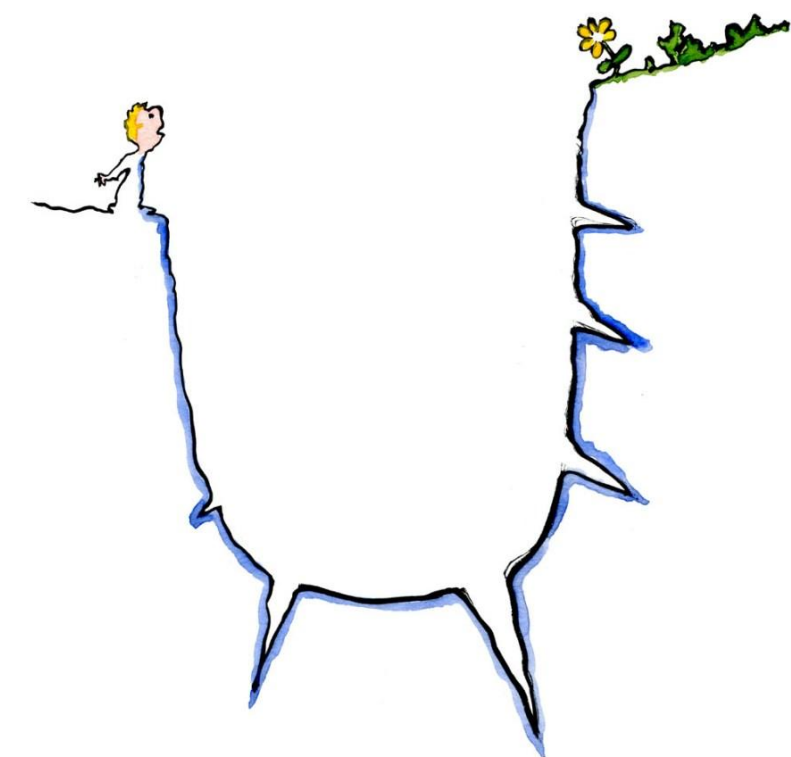
National capability is needed to avoid strategic dependence.

● Our future...



?

- Global
- Belgium



Sometimes you have
to go through worse
to get to better

Frits Ahlefeldt

—

Enter CCB Frontier AI Hub

● Cybersecurity of, due or with AI?

1) Cybersecurity of AI systems

2) Countering cyber attacks due to AI

3) Cybersecurity with AI

CCB tests AI

- To protect our organisation
- To strengthen our own processes (incl. threathunts, detection, etc)
- To help companies compare
- To be a centre of expertise

CCB Frontier AI Hub **Purpose**

- Bring together **Frontier AI providers, Essential Services & CCB**
- Learn how new Frontier AI models can find vulnerabilities
- Explain the Belgian / CCB approach
- Protect our most Essential Services ASAP

1

Learn

What these models can mean for you

2

Share

Knowledge and experience

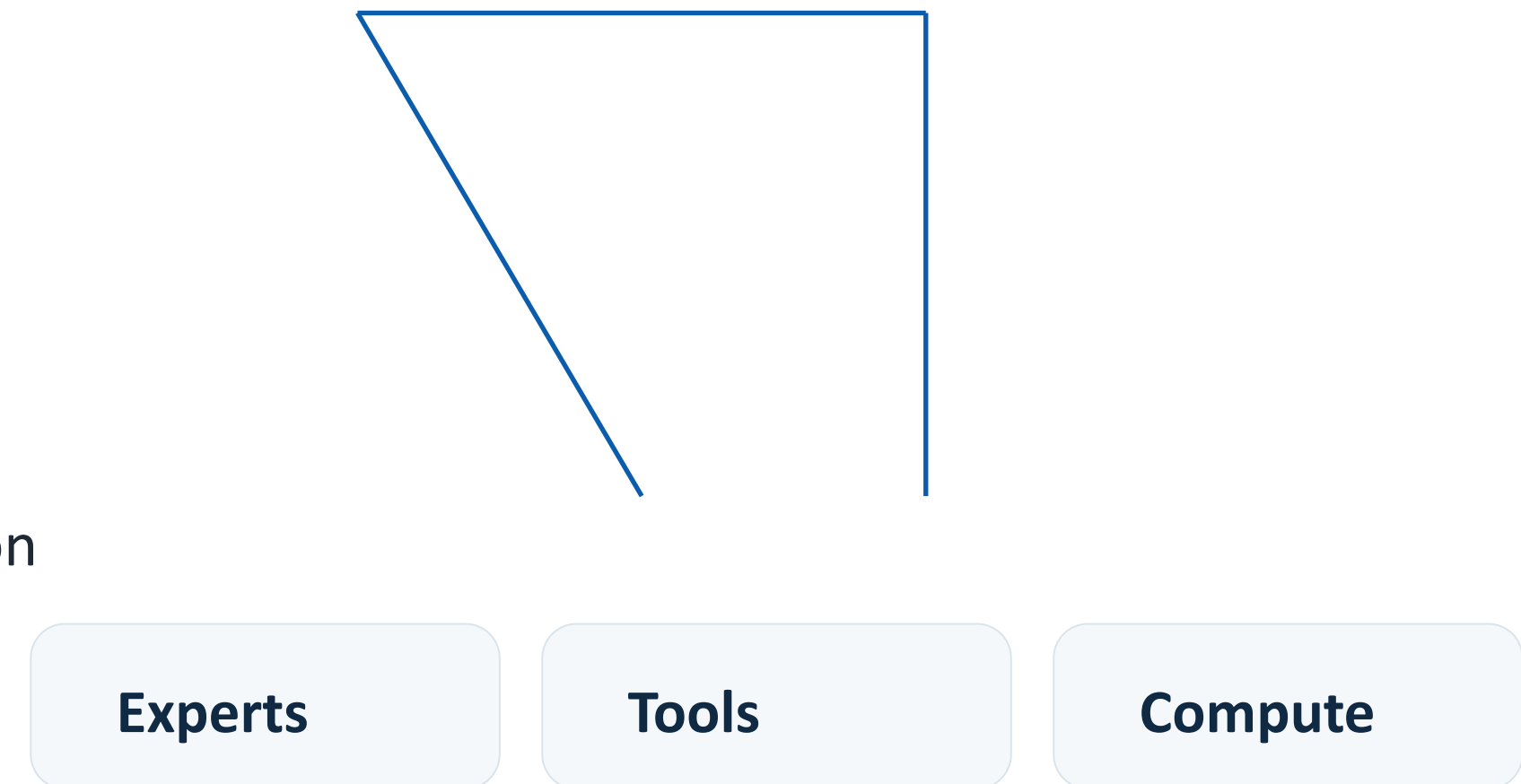
3

Protect

National Essential Services

● The CCB Frontier AI Hub concept

- A **Collaborative environment** hosted and coordinated by CCB
- **Frontier AI providers** bring tools and compute
- **Essential operators** test critical software and systems
- **CCB brings expertise**, trust and national strategy & coordination



Effective capability requires all three.

CCB Hub Approach

- **Hub Exchange Sessions: end of July – Nov 2026**
- CCB Frontier AI HUB – **NIS2 Guide** & public Guidelines
- 2027 : Quarterly Connect and Share Events (> 4000 NIS2 entities)

Offerings already discussed

- OpenAI -*GPT 5.5-Cyber & 5.6 (?)*
- Microsoft MDASH -*Multi-model Agentic Scanning Harness*
- Aikido (BE)-*Aikido's AI-powered security agent harness*
- Google - *CodeMender on Gemini Enterprise Agent Platform*
- Aisle (CZ / USA)
- Anthropic – Mythos 5
- Mistral (FR)

1 Finance

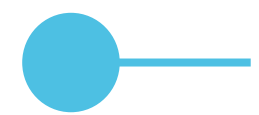
2 Energy

3 Telecom

4 Transport

5 Government

Initial list based on essential operators and CCB operational experience. (50)

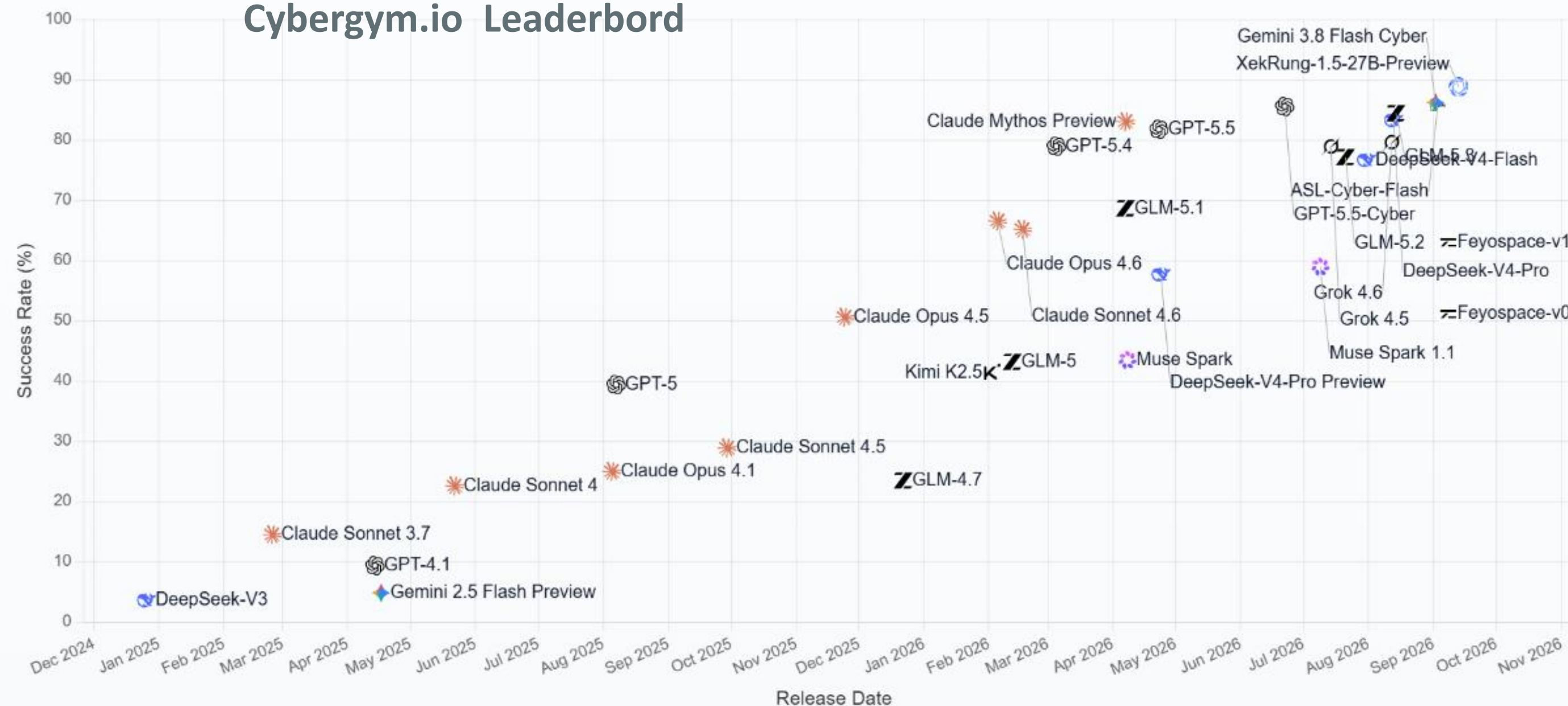


Mythos is not the only model

Beginner CTF Challenge Performance by Model (2.5M token budget)



Cybergym.io Leaderbord

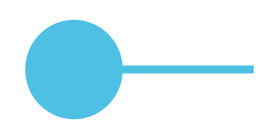


Start now!

It's a race between
you and your
attacker, and they
have left already

—

And EU?



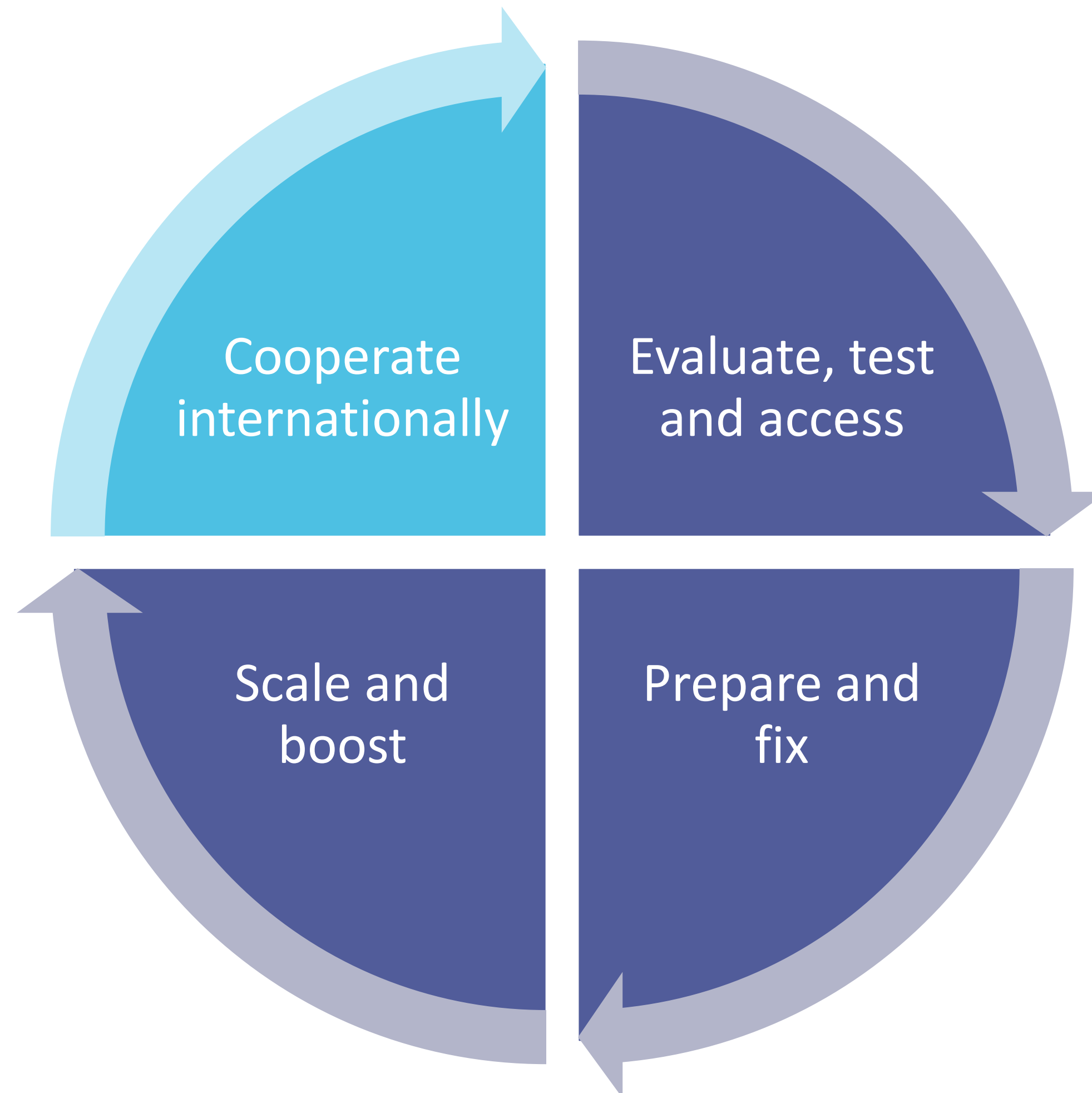
Frontier AI & EU

Money and a Plan

- **Funding** via Digital Europe Plan & Horizon Europe
- **EU Action Plan** on Cybersecurity and Artificial Intelligence
 - 7 July 2026
- **Enforcing** Regulation (AI Act, CRA)



●— Structure of the Action plan





EU Action Plan on Cybersecurity and AI



European Commission Communication COM(2026) 577 final, 7.7.2026 — 3 pillars, 9 Key Actions

1

Pillar 1

Making Frontier AI Safe, Accessible and Deployable for EU Cybersecurity

Key Action 1: Commission supports establishment of an **EU evaluation capacity for AI models** that must include cybersecurity (2027)

Key Action 2: Commission, with ENISA, defines a **European Blueprint for structured access to advanced AI** capabilities for cybersecurity purposes (Q4 2026)

Key Action 3: ENISA and the Joint Research Centre (JRC) develop a **secure testing platform** for AI with advanced cyber capabilities (Q4 2026)

2

Pillar 2

Preparing the EU's Cyber Ecosystem for the Age of AI

Key Action 4: ENISA, with relevant Union entities, issues **guidance, recommendations, advisories** and best practices on protection against AI-powered threats (as of Q3 2026)

Key Action 5: Commission, Member States, ENISA and industry **cooperate to make vulnerability management** practices and tools fit for the AI Age (as of Q3 2026)

Key Action 6: ENISA, with the Commission, Member States, open source communities, Union entities and industry, launches a first **pilot Critical Open Source Resilience Campaign** (Q4 2026)

3

Pillar 3

Scaling European AI Capabilities for Cyber

Key Action 7: Commission, with the European Cybersecurity Competence Centre and ENISA, launches an **EU Grand Challenge** to scale European AI-powered cybersecurity solutions (Q4 2026)

Key Action 8: Commission, jointly with Member States, aims to make **AI Factories'** compute capacity available to test, train and deploy AI models for cyber resilience on sovereign compute

Key Action 9: Commission works with Member States and industry, under the Cybersecurity Skills Academy, to develop AI-for-cybersecurity **training modules** (Q4 2026)

*

Collaborate with like minded partners:

Promote EU approach in G7; Bilateral Exchanges; Support UK AISI; NATO & UN; Encourage dialogue between govts & AI providers

● NEW FUNDING OPPORTUNITIES

DIGITAL EUROPE PROGRAMME - deadline 14 January 2027			BUDGET PER PROJECT	DURATION
DEP 11	Cybersecure tools, technologies and services relying on AI	15 MIL	3-5M EUR	36 MONTHS
	Strengthening cybersecurity capacities of European SMEs with cybersecure AI-powered solutions	20 MIL	3-5M EUR	
	Coordinated preparedness testing and other preparedness actions	15 MIL	1,5M EUR	
	Regional Cable Hubs	5 MIL	2,5M EUR	
	Strengthening EU cybersecurity capacities & capabilities in line with legislative requirements	20 MIL	3-5M EUR	
	Dual-use technologies	10 MIL	3-5M EUR	

THE SECURE PROJECT - deadline January 2027				
	2nd open cascade funding call for EU SMEs	11,5 MIL		

● Join us

Want to learn more about
DEP AI CALLS?



JOIN OUR WEBINAR
Sept 23, 10-11.30



Want to share experiences on your use of AI for
Cybersecurity?





CENTRE FOR CYBERSECURITY BELGIUM



Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Rue de la Loi / Wetstraat 18 - 1000 Brussels

www.ccb.belgium.be

