



EUROPÄISCHE
KOMMISSION

Straßburg, den 7.7.2026
COM(2026) 577 final

**MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN
RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND
DEN AUSSCHUSS DER REGIONEN**

Aktionsplan für Cybersicherheit und künstliche Intelligenz

1. Einführung

Künstliche Intelligenz (KI) an vorderster Front der Entwicklung markiert einen Wandel im Bereich der Cybersicherheit. Grenz-KI-Modelle (d. h. die fortgeschrittensten verfügbaren oder in der Entwicklung befindlichen KI-Modelle) bringen verbesserte Fähigkeiten zur Stärkung der Abwehrbereitschaft und zur Verbesserung der Erkennung von Bedrohungen und der Reaktion darauf mit sich, wodurch **beispiellose Möglichkeiten zur Verbesserung der Cyberresilienz** geschaffen werden. Mit der Weiterentwicklung dieser Fähigkeiten¹ wird die KI es den Cybersicherheitsteams ermöglichen, schneller und in größerem Maßstab zu arbeiten, wodurch Organisationen in die Lage versetzt werden, neu auftretenden Bedrohungen wirksamer zu begegnen. Gleichzeitig **können fortgeschrittene KI-Fähigkeiten, die bereits heute verfügbar sind**, auch in Form von Open-Source-Software, **bereits genutzt werden, um die Cyberresilienz der EU zu stärken**².

KI ist bereits zu einem **entscheidenden Element der Bedrohungslage** geworden und ermöglicht automatisiertere, skalierbarere und ausgefeiltere offensive Cyberoperationen, einschließlich Cyberkriminalität³. Während die Fähigkeiten auf Grenzniveau derzeit auf eine kleine Zahl von KI-Modellen und -Systemen konzentriert sind (d. h. Modelle und Systeme, die eine Vielzahl von Aufgaben erfüllen können und die sich dem aktuellen Stand der Technik annähern, diesen erreichen oder darüber hinausgehen)⁴, verringert sich die Lücke bei der Leistungsfähigkeit mit fortschreitender Verbesserung von Open-Source-Modellen. Infolgedessen dürften die tatsächlichen Grenzfähigkeiten im Laufe der Zeit immer zugänglicher werden, auch für böswillige Akteure wie Cyberkriminelle, die diese Fähigkeiten für komplexere Angriffe nutzen können.

Die EU tritt wohlgerüstet in dieses neue Paradigma ein. In den letzten Jahren hat sie die Grundlagen dafür geschaffen: die rechtliche und operative Basis für das Thema Cybersicherheit im KI-Zeitalter. In der **KI-Verordnung** wird der weltweit erste rechtsverbindliche Rahmen für das Management von Risiken festgelegt, die sich aus KI-Systemen und -Modellen ergeben, einschließlich systemischer Risiken der fortgeschrittensten KI-Modelle mit allgemeinem Verwendungszweck wie Risiken des Cybermissbrauchs⁵. Die **Cyberresilienz-Verordnung**, die bis Ende 2027 in vollem Umfang anwendbar sein soll, befasst sich mit der Sicherheit der Lieferketten, indem für Software- und Hardwareprodukte auf dem EU-Markt konzeptionsintegrierte Sicherheit (Security by Design) und Schwachstellenmanagement während des gesamten Lebenszyklus vorgeschrieben werden⁶. Gemeinsam tragen die KI-Verordnung und die Cyberresilienz-Verordnung dazu bei, dass KI-Modelle und -Systeme sowie Produkte mit digitalen Elementen unter Berücksichtigung der Sicherheit entwickelt und gepflegt werden. Parallel dazu bildet die **NIS-2-Richtlinie**⁷

¹ Jüngste Untersuchungen des britischen AI Security Institute deuten darauf hin, dass die fortgeschrittensten KI-Modelle bei kontrollierten Cybersicherheitstests in der Lage sind, immer längere Aufgaben ohne menschliche Hilfe zu erledigen. Die geschätzte Dauer der Aufgaben, die sie bewältigen können, hat sich über einen Zeitraum von Monaten und nicht von Jahren verdoppelt, und die jüngsten Ergebnisse deuten darauf hin, dass sich dieses Tempo noch beschleunigen könnte.

² „AI is changing the economics of vulnerability discovery. Defenders should adapt now“ (KI verändert die wirtschaftlichen Aspekte der Aufdeckung von Schwachstellen. Verteidiger sollten sich jetzt anpassen), CERT-EU, April 2026.

³ ENISA, *ENISA Threat landscape 2025*, Oktober 2025.

⁴ Gemäß der Begriffsbestimmung in Artikel 2 Absatz 4 der vorgeschlagenen Verordnung über Cloud- und KI-Entwicklung (COM(2026) 502 final).

⁵ Verordnung (EU) 2024/1689.

⁶ Verordnung (EU) 2024/2847.

⁷ Die Richtlinie (EU) 2022/2555 deckt elf Sektoren mit hoher Kritikalität (Energie, Verkehr, Banken, Finanzmarktinфраstruktur, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von

zusammen mit der **Verordnung über die digitale operationale Resilienz im Finanzsektor**⁸ einen risikobasierten Rahmen für die Cybersicherheit kritischer Sektoren. Diese Rechtsvorschriften bilden einen soliden Rahmen, der bei wirksamer Umsetzung gegenüber technologischen Entwicklungen und Bedrohungen robust ist. Die **Cybersolidaritätsverordnung** ergänzt diesen Rahmen durch operative Mechanismen zur Unterstützung der Mitgliedstaaten bei der Abwehrbereitschaft gegenüber, Erkennung von und Reaktion auf schwerwiegende Sicherheitsvorfälle und Sicherheitsvorfälle großen Ausmaßes⁹. Zusammen tragen diese Maßnahmen zu den Zielen der **Strategie für eine Union der Krisenvorsorge**¹⁰ und der **ProtectEU-Strategie**¹¹ bei.

Fortgeschrittene KI-gestützte Cyberfähigkeiten sind auch ein entscheidender Faktor für die Gewährleistung der Sicherheit unserer Union. Während diese Fähigkeiten, die über verschiedene Modelle, einschließlich offener Modelle, verfügbar sind, bereits die Cyberresilienz der EU erhöhen können, werden Grenzfähigkeiten hauptsächlich außerhalb der EU entwickelt, und ihre Verfügbarkeit wird häufig durch intransparente, im Ausland bestimmte Prozesse entschieden. Die Kenntnis dieser Fähigkeiten und der Zugang zu ihnen sind daher nicht nur eine Frage der digitalen Resilienz, sondern auch der technologischen Souveränität Europas. Um diese Souveränität zu wahren, muss die EU sicherstellen, dass die Einführung fortgeschrittener KI-gestützter Cybersicherheitsfähigkeiten keine neuen strategischen Abhängigkeiten schafft. Gleichzeitig muss Europa seine Resilienz erhöhen, um mit dieser sich rasch wandelnden Bedrohungslage Schritt zu halten.

Die EU hat bereits **strategische Schritte unternommen, um die Abhängigkeit von kritischen Technologien zu verringern und die in der EU entwickelten Fähigkeiten zu stärken**. Über die Programme Horizont Europa und Digitales Europa finanziert die EU bereits die Entwicklung fortgeschrittener KI-gestützter Cyberfähigkeiten, und der Fonds des Europäischen Innovationsrats ist zu einem wichtigen Investor in technologieintensive Unternehmen in Europa geworden und hat unter anderem Investitionen in Start-ups und Scale-ups im Bereich Cybersicherheit und KI-Technologie getätigt¹². Darüber hinaus würde die kürzlich vorgeschlagene **Verordnung zur Cloud- und KI-Entwicklung**¹³ die Kapazitäten der Rechenzentren in der EU und die Autonomie der EU in den Bereichen Cloud und KI erweitern und die breitere Einführung von KI – einschließlich von Cyber-Tools und -Anwendungen – unterstützen. Sie würde die EU in die Lage versetzen, auf kritische Cloud- und KI-Kapazitäten vertrauen zu können, und so die Abhängigkeiten hinsichtlich geopolitischer und sicherheitsbezogener Risiken verringern. Der Vorschlag baut auf der **Strategie „KI anwenden“** und dem **Aktionsplan für den KI-Kontinent** auf, und darin wird insbesondere die Notwendigkeit anerkannt, Große Herausforderungen zur Unterstützung und zum Ausbau von Grenz-KI einzuführen.

IKT-Diensten, öffentliche Verwaltung und Weltraum) sowie sieben weitere kritische Sektoren (Post- und Kurierdienste; Abfallbewirtschaftung; Produktion, Herstellung und Handel mit chemischen Stoffen; Produktion, Verarbeitung und Vertrieb von Lebensmitteln; verarbeitendes Gewerbe/Herstellung von Waren; Anbieter digitaler Dienste und Forschung) ab.

⁸ Verordnung (EU) 2022/2554.

⁹ Verordnung (EU) 2025/38.

¹⁰ JOIN(2025) 130 final.

¹¹ COM (2025) 148 final.

¹² Sifted, 20. März 2026: Europe's most active deep tech investors in 2025; Bericht des EIC über die erzielte Wirkung (2025).

¹³ COM(2026) 502 final.

Aufbauend auf diesen soliden Grundlagen **muss die EU nun weitere Maßnahmen ergreifen, um die unmittelbaren zugrunde liegenden Probleme und Chancen anzugehen, die die KI im Bereich der Cybersicherheit mit sich bringt.**

Dieser Aktionsplan bietet eine **erste und gezielte Antwort, um die Mitgliedstaaten und Organisationen in der Union bei der Bewältigung dieser neuen Realität zu unterstützen.**

Erstens wird die EU, um eine sichere und verantwortungsvolle Einführung von Grenz-KI zu gewährleisten, ihre Kapazitäten zur Bewertung von Grenz-KI vor ihrer Freigabe ausbauen, auch im Bereich der Cybersicherheit. Dadurch werden ein strenges externes Bewertungsverfahren und erstklassige KI-Bewertungskapazitäten in der EU gefördert. Die EU wird auch den Zugang zu fortgeschrittenen KI-gestützten Cyberfähigkeiten für europäische Akteure erleichtern und die Bemühungen unterstützen, verfügbare KI-Modelle für Anwendungsfälle im Bereich der Cybersicherheit zu testen.

Zweitens wird die EU ihre Bemühungen zur Unterstützung von kritischen Sektoren und KMU bei der Vorbereitung auf KI-gestützte Cyberbedrohungen beschleunigen, unter anderem durch die Umsetzung der wesentlichen Elemente der Cybersicherheit. Unter Nutzung des gesamten Spektrums der verfügbaren KI wird die EU deren Nutzung unterstützen, um die Cyberresilienz zu stärken und die kritischsten Schwachstellen zu beheben.

Drittens wird die EU ihre Fähigkeit zur Entwicklung und Einführung KI-gestützter Lösungen ausbauen, indem sie ein europäisches Ökosystem im KI-Bereich fördert und ihre eigenen Kapazitäten für Grenzentwicklungen weiter stärkt. Um Letzteres zu erreichen, werden dringend umfangreiche Kapitalinvestitionen erforderlich sein, um Europas eigene Kapazitäten im Bereich der Grenz-KI aufzubauen und europäische Lösungen zu fördern, die unseren Bedürfnissen entsprechen.

Schließlich wird die EU im Rahmen dieser Ziele mit gleichgesinnten Partnern zusammenarbeiten, um einen vertrauenswürdigen und sicheren globalen Ansatz für Grenz-KI und Cybersicherheit zu fördern.

2. Säule 1: Sichere, zugängliche und einsetzbare Grenz-KI für die europäische Cybersicherheit

Da fortgeschrittene KI-gestützte Cyberfähigkeiten in naher Zukunft als Waffe gegen unsere kritische Infrastruktur und unsere Gesellschaft eingesetzt werden könnten, muss die EU vorrangig für eine frühzeitige Sensibilisierung für diese Fähigkeiten sorgen, stärkere technische Kapazitäten zur Bewertung ihrer Risiken aufbauen, Möglichkeiten zur Erprobung ihres Potenzials für den Einsatz im Bereich der Cybersicherheit finden und klarere Zugangswege für legitime Cybersicherheitszwecke in Europa festlegen. Zu diesem Zweck wird die EU aufbauend auf dem durch die KI-Verordnung geschaffenen Rechtsrahmen die europäischen Kapazitäten für die Bewertung vor der Freigabe ausbauen, einen gemeinsamen europäischen Ansatz für den Zugang fördern und Testbemühungen koordinieren, damit Grenz-KI für die Cybersicherheit in Europa sicher zugänglich ist und genutzt werden kann.

2.1. Bewertung und Minderung der von Grenz-KI ausgehenden Risiken

In der KI-Verordnung sind Anforderungen an die Cybersicherheit von **KI-Systemen** festgelegt¹⁴, und **Anbieter der fortgeschrittensten KI-Modelle mit allgemeinem**

¹⁴ Gemäß Anhang III der KI-Verordnung gelten KI-Systeme, die in kritischen Infrastrukturen verwendet werden, als hochriskant und unterliegen besonderen Bestimmungen, auch in Bezug auf die Cybersicherheit.

Verwendungszweck sind verpflichtet, systemische Risiken, einschließlich des Missbrauchs von KI im Cyberbereich, zu bewerten und zu mindern¹⁵.

Ab dem 2. August 2026 wird die Kommission die in der KI-Verordnung vorgesehenen Aufsichts- und Durchsetzungsbefugnisse ausüben, um eine wirksame Aufsicht über KI-Systeme sowie über KI-Modelle mit allgemeinem Verwendungszweck, einschließlich Modelle, die systemische Risiken im Zusammenhang mit der Cybersicherheit bergen, sicherzustellen¹⁶. Diese Aufsicht umfasst die Bewertung der von den Anbietern ermittelten Risiken im Zusammenhang mit Modellfähigkeiten und der von ihnen ergriffenen Maßnahmen zur Minderung dieser Risiken. Diese Anforderungen stehen weiterhin in einem angemessenen Verhältnis zu den Fähigkeiten der betreffenden Technologie.

Die Aufsichts- und Durchsetzungsbefugnisse werden durch das **Wissenschaftliche Gremium, das das Büro für künstliche Intelligenz der Kommission berät, sichere Meldekanäle und den Verhaltenskodex für KI mit allgemeinem Verwendungszweck** unterstützt.

2.2. Steigerung europäischer Exzellenz bei der Bewertung von Grenz-KI vor der Freigabe

Um die sichere und verantwortungsvolle Einführung von KI für die Cybersicherheit in der EU zu fördern, müssen die Regulierungsmaßnahmen durch **verbesserte europäische Bewertungskapazitäten** ergänzt werden. Mit der Weiterentwicklung der KI-Fähigkeiten und angesichts der Tatsache, dass systemische Risiken nicht nur im Cyberbereich auftreten können¹⁷, erweist sich die Durchführung externer Bewertungen als bewährtes Verfahren zur Gewährleistung der Sicherheit von Grenz-KI im Einklang mit Ansätzen, die in anderen risikobehafteten Wirtschaftszweigen eingeführt wurden. In der KI-Verordnung wird auch hervorgehoben, wie wichtig eine durch externe Unternehmen durchgeführte **Bewertung vor dem Einsatz** ist, um systemische Risiken zu bewerten und gegebenenfalls zu mindern. Bislang haben die meisten führenden Einrichtungen, die als externe Unternehmen Bewertungen vor dem Einsatz von KI-Modellen durchführen, ihren Sitz außerhalb der EU. Angesichts ihrer zunehmenden Bedeutung ist es dringend erforderlich, dass ein Teil dieses Bewertungsfachwissens und der damit verbundenen Infrastruktur innerhalb der EU besteht.

Die EU muss daher das verfügbare Fachwissen ausbauen, um ein glaubwürdiges und wettbewerbsfähiges Ökosystem von externen Bewertern zu schaffen, die fortgeschrittene KI-Fähigkeiten und Risikominderung bewerten und so das Vertrauen in den KI-Governancerahmen der EU stärken. Zu diesem Zweck wird die Kommission **Kriterien für externe Bewerter für die Zwecke des Verhaltenskodex für KI mit allgemeinem**

¹⁵ In der KI-Verordnung wird ein systemisches Risiko als ein Risiko definiert, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können (Artikel 3 Nummer 65 der KI-Verordnung).

¹⁶ Zu den Durchsetzungsbefugnissen gegenüber Anbietern von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko, die die Bestimmungen über die Minderung systemischer Risiken nicht einhalten, gehören die Anforderung von Informationen über das Modell, die Anforderung des Zugangs zu dem Modell zur Durchführung von Bewertungen, die Anforderung von Risikominderungsmaßnahmen und letztlich die Verhängung von Geldbußen von bis zu 3 % des weltweiten Jahresumsatzes oder die Aufforderung an einen Anbieter, die Bereitstellung auf dem Markt zu beschränken, das Modell zurückzunehmen oder zurückzurufen.

¹⁷ Beispielsweise ist die Biologie ein weiterer Bereich, in dem die Fähigkeiten von KI-Modellen mit allgemeinem Verwendungszweck kontinuierlich zunehmen und missbraucht werden könnten, was ein Risiko für die öffentliche Gesundheit und die öffentliche Sicherheit darstellen könnte.

Verwendungszweck vorschlagen und die Entwicklung eines breiteren Bewertungsökosystems fördern. Dazu gehört auch die Erleichterung eines sinnvollen Austauschs zwischen Bewertern und einschlägigen Sachverständigen, um die Bewertungsmethoden zu verbessern und die Qualifikationsanforderungen zu klären.

Was die **Bewertung von KI-Modellen speziell für die Cybersicherheit** betrifft, so kann Europa in diesem Bereich potenziell mit erstklassigen Cybersicherheitsexperten eine Führungsrolle übernehmen. Angesichts der Dringlichkeit solcher Bewertungen sollte die EU dieses Fachwissen nutzen und ausbauen. Um dieses Ziel zu erreichen, wird die Kommission eine gezielte Aufforderung zur Einreichung von Vorschlägen für den **Aufbau einer EU-Bewertungskapazität für KI-Modelle** veröffentlichen, **die auch Cybersicherheit umfassen muss**. Diese Kapazität würde einen wichtigen Beitrag zu dem im Entstehen begriffenen Ökosystem in der EU leisten und auf neuem Know-how im Bereich der KI-Bewertung in den Mitgliedstaaten aufbauen. Sie wird auch die Regulierungstätigkeiten der Kommission unterstützen, die über das Büro für künstliche Intelligenz durchgeführt werden¹⁸, indem sie eine europäische Option für die Bewertung von KI-Modellen und ihrer Risikominderungsmaßnahmen durch externe Bewerter bietet. Sie wird Informationen für das Risikomanagement der Anbieter liefern, indem die Fähigkeiten der Modelle und die Wirksamkeit der Risikominderungsmaßnahmen der Modellanbieter unabhängig bewertet werden¹⁹.

Diese europäische Kapazität wird Anbieter von KI-Modellen mit allgemeinem Verwendungszweck bei der Einhaltung der einschlägigen Verpflichtungen aus der KI-Verordnung und des Verhaltenskodex für KI-Modelle mit allgemeinem Verwendungszweck unterstützen²⁰. Sie wird ein glaubwürdiges und strenges externes Bewertungsverfahren sicherstellen. Erstklassige Bewertungsfähigkeiten in der EU werden auch zum Verständnis potenzieller systemischer Risiken beitragen, unter anderem im Bereich der Cybersicherheit, aber auch in der Biotechnologie und anderen Bereichen, indem Frühwarnsignale ausgegeben werden, wenn Risiken ermittelt werden.

2.3. Erleichterung des Zugangs zu fortgeschrittenen KI-gestützten Cyberfähigkeiten in der EU

Der Zugang zu Grenz-KI mit fortgeschrittenen Cyberfähigkeiten wird zunehmend durch anbieterspezifische und oft außereuropäische Entscheidungen geregelt, wobei einige Anbieter den Zugang beschränken, um Risiken des Missbrauchs durch **strukturierte Zugangsprogramme** (z. B. stufenweise Modellfreigaben) zu bewältigen. Eine solche Beschränkung kann zwar aus Sicherheitsgründen gerechtfertigt sein, doch mangelt es dieser Praxis häufig an Transparenz in Bezug auf die Kriterien, anhand deren bestimmt wird, welche Organisationen, einschließlich Unternehmen, Zugang erhalten und über welches Verfahren der

¹⁸ Im Kapitel über Sicherheit und Gefahrenabwehr des Verhaltenskodex für KI mit allgemeinem Verwendungszweck werden Anbieter verpflichtet, Modellbewertungen auch durch angemessen qualifizierte unabhängige externe Bewerter durchzuführen (Anlage 3.5). Diese Berichte werden dann die Regulierungstätigkeiten des Büros für künstliche Intelligenz unterstützen, da die Anbieter verpflichtet sind, dem Büro für künstliche Intelligenz alle verfügbaren Berichte über externe Bewertungen zusammen mit dem Modellbericht vorzulegen (Maßnahme 7.4).

¹⁹ Die mit dieser Kapazität durchgeführten Bewertungen unterscheiden sich von den Bewertungen, die auf der in Abschnitt 2.4 genannten Testplattform durchgeführt werden. Die Plattform wird hauptsächlich für das Testen von Cybersicherheitsanwendungen von KI-Modellen genutzt, während der Schwerpunkt der Kapazität auf der Bewertung und Minderung systemischer Risiken liegen wird, um die Einhaltung des Verhaltenskodex zu unterstützen.

²⁰ Bei der Kapazität wird es sich nicht um eine Konformitätsbewertungsstelle handeln, und sie wird die Einhaltung der Vorschriften nur durch ihre Bewertungen unterstützen.

Zugang gewährt wird. Dies kann die Fähigkeit europäischer Akteure, einschließlich der zuständigen Behörden und der Betreiber kritischer Infrastrukturen, beeinträchtigen, diese KI-Fähigkeiten zeitnah zu nutzen und ihre Resilienz zu stärken.

Ein koordinierter Ansatz der EU ist dringend erforderlich, um den einschlägigen **öffentlichen und privaten Akteuren in Europa** den sicheren und unverzüglichen Zugang zu einer solchen Grenz-KI zu erleichtern. Zu diesem Zweck wird die EU einen dem neuesten Stand der Technik entsprechenden, risikobasierten Prozess mit klaren Kriterien fördern, der darauf ausgelegt ist, Missbrauchsrisiken wirksam zu mindern.

Die Kommission wird in Abstimmung mit der Agentur der Europäischen Union für Cybersicherheit (ENISA) einen **europäischen Konzeptentwurf für den strukturierten Zugang zu fortgeschrittenen KI-Fähigkeiten für Cybersicherheitszwecke** als Leitfaden ausarbeiten, in dem dargelegt wird, wie Anbieter von KI mit fortgeschrittenen Cyberfähigkeiten europäischen Organisationen, einschließlich Unternehmen, Zugang gewähren und so deren Minderung von Cyberrisiken unterstützen können.

Dieser Leitfaden wird die **Kriterien** enthalten, die bei der Gewährung des Zugangs zu KI mit fortgeschrittenen Cyberfähigkeiten für europäische Akteure **berücksichtigt werden sollten**. Der Konzeptentwurf sollte einschlägige Kriterien für verschiedene Arten von Organisationen (z. B. EU-Organen, Behörden der Mitgliedstaaten, Betreiber kritischer Infrastrukturen, Cybersicherheitsanbieter und Forschungseinrichtungen) umfassen und beschreiben, wie diese Akteure identifiziert würden. Darüber hinaus sollte er Sicherheitskriterien umfassen, damit der im Rahmen des Konzeptentwurfs gewährte Zugang kein unangemessenes Risiko darstellt, sowie **einen Mechanismus zur Straffung der Gewährung des Zugangs** für zugangsberechtigte Stellen. Dieser Mechanismus sollte auch eine frühzeitige **Unterrichtung** durch die Anbieter über geplante Programme für den vertrauenswürdigen Zugang sowie den Wissensaustausch zwischen EU-Organisationen, denen Zugang zu einem bestimmten Modell oder System gewährt wurde, erleichtern.

Mit dem Konzeptentwurf werden zwar **keine neuen Verpflichtungen für Anbieter eingeführt**, aber die Ziele des Verhaltenskodex für KI mit allgemeinem Verwendungszweck werden unterstützt, indem mögliche Maßnahmen zur Risikominderung ermittelt werden, die das **Management systemischer Risiken** ergänzen können, das von Anbietern von KI-Modellen mit allgemeinem Verwendungszweck mit systemischem Risiko umzusetzen ist^{21,22}. Durch die Bereitstellung eines **europäischen Referenzrahmens** wird der Konzeptentwurf als Grundlage für die weitere internationale Zusammenarbeit dienen.

Der Konzeptentwurf sollte **Notfallmaßnahmen für den Fall umfassen, dass der Zugang zu KI mit fortgeschrittenen Cyberfähigkeiten eingeschränkt oder entzogen wird**, um die Maßnahmen festzulegen, die auf EU-Ebene durchzuführen sind, wenn der Zugang zu einem einschlägigen Modell oder System von einem Anbieter oder einer Behörde eines Drittlands eingeschränkt oder entzogen wird. Darüber hinaus wird die Kommission, wenn ein zeitnaher Zugang zu Grenz-KI für die allgemeine Verwendung erforderlich ist, in Zusammenarbeit mit den Mitgliedstaaten die mögliche Nutzung verfügbarer Finanzierungsinstrumente, einschließlich der gemeinsamen Auftragsvergabe, prüfen, um einen **gemeinsamen Zugang zu solchen Modellen oder Systemen** zu erhalten.

²¹ Im Einklang mit Artikel 55 Absatz 1 Buchstabe b der KI-Verordnung.

²² So wird beispielsweise im Kapitel über Sicherheit und Gefahrenabwehr des Verhaltenskodex der KI mit allgemeinem Verwendungszweck unter Maßnahme 5.1 die „stufenweise Gewährung des Zugangs zum Modell“ als Beispiel für eine Risikominderung genannt.

2.4. Testen von KI mit fortgeschrittenen Cyberfähigkeiten für eine zeitnahe und sichere Einführung von KI im Bereich der Cybersicherheit

Der Zugang zu sicherer und vertrauenswürdiger Grenz-KI muss mit dem Testen ihrer Fähigkeiten für den Einsatz bei Cybersicherheitsoperationen wie der Überprüfung und Behebung von Schwachstellen und der Reaktion auf Sicherheitsvorfälle einhergehen. Um die Vorteile der KI nutzen zu können, müssen Betreiber kritischer Infrastrukturen und Behörden rasch verstehen, wie KI mit fortgeschrittenen Cyberfähigkeiten unter realistischen Cybersicherheitsbedingungen abschneidet, bevor sie in sensiblen Umgebungen eingesetzt wird. Diese Tests sollten in **sicheren und kontrollierten Umgebungen** durchgeführt werden.

Um Synergien auf europäischer Ebene zu schaffen, werden die **ENISA** und die **Gemeinsame Forschungsstelle der Europäischen Kommission (JRC)** in Zusammenarbeit mit anderen einschlägigen Kommissionsdienststellen und Einrichtungen der Union wie dem CERT-EU, Europol und sektoralen Behörden sowie den Mitgliedstaaten daher eine **sichere Testplattform für KI für Anwendungsfälle im Bereich der Cybersicherheit** einrichten²³. Die Plattform wird es den Teilnehmern ermöglichen, ihre eigenen Modell-Zugangsschlüssel gemäß den gemeinsamen Sicherheits- und Vertraulichkeitsvorschriften zu verwenden, wobei jeder Teilnehmer seine eigenen Kosten trägt, seine eigenen Tools verwendet und die Verantwortung für seine Testmethoden trägt. Die ENISA sollte in Abstimmung mit der JRC den Zugang zur Testplattform regeln und die Ergebnisse zusammenfassen.

Diese sichere europäische Testplattform wird es auch ermöglichen, **den Einsatz fortgeschrittener KI-Cyberfähigkeiten in den Systemen kritischer Infrastrukturen zu testen**, ohne die reale Infrastruktur einem Risiko auszusetzen („Cyber-Ranges“²⁴). Im Rahmen dieser Initiative wird der **Anpassung und Ausweitung bestehender Cyber-Ranges** Vorrang vor der Duplizierung von Umgebungen eingeräumt. Insbesondere gilt: Während neue Cyber-Ranges nur in Sektoren entwickelt werden, in denen solche Fähigkeiten derzeit nicht verfügbar sind, könnte die Industrie diese Initiative sektorübergreifend unterstützen, indem sie bestehende Umgebungen bereitstellt, die durch spezielle Zusagen integriert werden sollen. Vorbehaltlich geltender Vertraulichkeitsvorschriften können die Akteure der beitragenden Industrie aggregierte Informationen aus einschlägigen Testtätigkeiten erhalten.

Der Schwerpunkt der Nutzung dieser Umgebung wird auf dem Testen von KI zur Stärkung der Cyberresilienz liegen, und die Nutzung hat nicht zum Ziel, KI-Modelle mit allgemeinem Verwendungszweck im Hinblick auf die Einhaltung der KI-Verordnung zu bewerten²⁵. Mit der Nutzung werden operative Erfahrungen mit dem Einsatz von KI für die Cyberresilienz gefördert und beschleunigt, einschließlich Erkennung, Sichtung, Erkenntnissen über Bedrohungen und Reaktion, um Angreifern einen Schritt voraus zu sein. Um ein hohes Maß an Cybersicherheit in der gesamten Union zu gewährleisten, wird die **ENISA** auf der

²³ Eine bestehende, von der JRC verwaltete Plattform könnte aufgerüstet werden, um diese Art von Tests zu ermöglichen.

²⁴ Cyber-Ranges sind sichere und kontrollierte Umgebungen, die in simulierter Form digitale Systeme, Netze oder Infrastrukturen reproduzieren. Sie ermöglichen Tests unter realistischen Bedingungen und stellen gleichzeitig sicher, dass in dieser Umgebung durchgeführte Tätigkeiten keine Auswirkungen auf reale Systeme oder Dienste haben.

²⁵ Tests von KI im Hinblick auf die Cyberresilienz haben zum Ziel, die operative Eignung eines KI-Modells oder eines KI-Systems für die Wahrnehmung einer bestimmten Cybersicherheitsaufgabe zu verstehen, während die Bewertung von KI-Modellen zur Unterstützung der Einhaltung der KI-Verordnung zum Ziel hat, eine Bewertung der Risiken, die sich aus dem Modell ergeben, und der Wirksamkeit der vom Modellanbieter umgesetzten Risikominderungsmaßnahmen vorzunehmen. Das Testen von KI im Hinblick auf die Cyberresilienz unterscheidet sich daher von der Bewertung von KI-Modellen zur Unterstützung der Einhaltung der KI-Verordnung und erfordert andere Fähigkeiten und Ressourcen.

Grundlage ihres Wissens **Leitlinien und Ratschläge für die sichere Nutzung verfügbarer KI-Modelle und -Systeme** für das breitere Ökosystem herausgeben und pflegen.

Leitaktionen:

- **Leitaktion 1** – Die Kommission wird die Einrichtung einer EU-Bewertungskapazität für KI-Modelle unterstützen, die die Cybersicherheit umfassen muss (2027).
- **Leitaktion 2** – Die Kommission wird in Abstimmung mit der ENISA einen europäischen Konzeptentwurf für den strukturierten Zugang zu fortgeschrittenen KI-Fähigkeiten für Cybersicherheitszwecke erstellen, um sicherzustellen, dass europäische Organisationen sicher und zeitnah auf diese Fähigkeiten zugreifen können (4. Quartal 2026).
- **Leitaktion 3** – Die ENISA und die Gemeinsame Forschungsstelle der Europäischen Kommission (JRC) werden eine sichere Testplattform für KI mit fortgeschrittenen Cyberfähigkeiten für Anwendungsfälle im Bereich der Cybersicherheit entwickeln, um die zeitnahe und sichere Einführung von KI im Bereich der Cybersicherheit zu fördern (4. Quartal 2026).

3. Säule 2: Vorbereitung des Cyber-Ökosystems der EU auf das KI-Zeitalter

Da fortgeschrittene KI-Cyberfähigkeiten zunehmend zugänglich und weithin eingesetzt werden, muss die EU gewappnet sein, einerseits gegen ihren möglichen Missbrauch gegen ihre Wirtschaft und Gesellschaft vorzugehen und sie andererseits sicher für die Cyberresilienz zu nutzen. KI kann die Aufdeckung von Schwachstellen mit einem hohen Automatisierungsgrad und in größerem Umfang beschleunigen und gleichzeitig das Fachwissen, die Zeit und die Ressourcen verringern, die böswillige Akteure für technisch ausgereifte Angriffe benötigen. Die unmittelbare Priorität besteht darin, dass die EU ihre Vorsorge stärken und kritische Sektoren bei der Anpassung an diese Bedrohungen unterstützen muss. Dazu gehört die Integration verfügbarer KI-Lösungen in Cybersicherheitsoperationen, wobei das gesamte Spektrum von KI-Modellen, insbesondere Open-Source-Modelle, genutzt wird und gleichzeitig die Anstrengungen zur Ermittlung und Behebung der kritischsten Schwachstellen beschleunigt werden. Die ENISA ist in einer einzigartigen Position, um diesen Übergang des Cyber-Ökosystems der EU in das KI-Zeitalter zu unterstützen.

3.1. Anwendung der Grundlagen der EU im Bereich der Cybersicherheit und Abwehrbereitschaft

In dieser neuen Technologie- und Sicherheitslandschaft sind die **Grundlagen der Cybersicherheit und die Abwehrbereitschaft heute wichtiger denn je**, und die bestehenden Cybersicherheits-Tools und -Instrumente der EU müssen in vollem Umfang genutzt werden.

Der EU-Rechtsrahmen für Cybersicherheit, insbesondere die **NIS-2-Richtlinie²⁶ und die Verordnung über die digitale operationale Resilienz im Finanzsektor**, bietet eine solide Grundlage für die Abwehrbereitschaft kritischer Infrastrukturen gegen alle Arten von Cybersicherheitsrisiken, auch im Zusammenhang mit KI. Diese Vorschriften müssen daher von

²⁶ In der NIS-2-Richtlinie wird das Grundniveau für Risikomanagementmaßnahmen im Bereich der Cybersicherheit festgelegt und werden wesentliche und wichtige Einrichtungen, die in 18 kritischen Sektoren tätig sind, verpflichtet, ihre Netz- und Informationssysteme zu schützen und Auswirkungen von Sicherheitsvorfällen zu verhindern und zu minimieren.

den Mitgliedstaaten dringend umgesetzt und durchgeführt werden. Darüber hinaus müssen die Mitgliedstaaten die Risiken fortgeschrittener KI bei ihrer Aufsichtstätigkeit berücksichtigen. Ebenso sollten Betreiber in kritischen Sektoren und Finanzunternehmen ihren Rahmen für das Risikomanagement überprüfen und an die neuen Gegebenheiten anpassen, KI-gestützte Cyberangriffe mit höherer Häufigkeit und in größerem Umfang antizipieren und die Time-to-Patch (Zeitspanne für die Schließung von Sicherheitslücken) verkürzen, indem sie den Patch-Zyklus beschleunigen und in der Lage sind, rasch Patches für komplexe Systeme zu erstellen.

Um die Abwehrbereitschaft weiter zu stärken, sollten die Einrichtungen konsequent **grundlegende Cyberhygienemaßnahmen** anwenden und eine Netz- und Systemhärtung umsetzen (unter anderem gegebenenfalls durch Zero-Trust-Ansätze). Sie sollten zudem damit beginnen, **bereits verfügbare KI-Fähigkeiten**, auch in Form von Open-Source-Modellen, zu **nutzen**, um Schwachstellen zu erkennen und die Erkennung und Prävention von Cyberangriffen zu verbessern. Die **Einrichtungen der Union** können mit Unterstützung des CERT-EU und unter Anleitung des Interinstitutionellen Cybersicherheitsbeirats (IICB) in dieser Hinsicht mit gutem Beispiel vorangehen, um die allgemeine Cyberabwehr der Union im Einklang mit der Verordnung über die Cybersicherheit der Einrichtungen der Union²⁷ zu stärken. Die Mitgliedstaaten werden ferner nachdrücklich aufgefordert, die Umwandlungsmöglichkeiten der **EU-Cybersicherheitsreserve** in vollem Umfang zu nutzen, um die Resilienz gegenüber KI-gestützten Cyberbedrohungen zu erhöhen, unter anderem durch Schwachstellensuchen, automatisierte Penetrationstests und Risikoüberwachung und mit Unterstützung für Patching-Empfehlungen.

Darüber hinaus sind, wie in der **Cyberresilienz-Verordnung** zum Ausdruck kommt, die ab dem 11. Dezember 2027 in vollem Umfang gelten wird, Entwicklungsverfahren mit konzeptionsintegrierter Sicherheit, ein systematisches Schwachstellenmanagement, zeitnahes Patching und sichere Codierungsverfahren – einschließlich Ansätzen, mit denen ganze Kategorien von Schwachstellen behoben werden, wie z. B. die speichersichere Software-Entwicklung – nach wie vor von wesentlicher Bedeutung. KI-spezifische Cybersicherheitsrisiken, einschließlich Daten- und Modellvergiftung, Adversarial Attacks und Prompt Injections, müssen im Einklang mit den einschlägigen Bestimmungen der KI-Verordnung ebenfalls sorgfältig bewertet und gemindert werden.

Um diese Bemühungen zu unterstützen, wird die **ENISA** in Zusammenarbeit mit den europäischen Aufsichtsbehörden und anderen einschlägigen Einrichtungen der Union **geeignete Leitlinien, Empfehlungen, Ratschläge und bewährte Verfahren** zur Verfügung stellen und pflegen, **die es Akteuren ermöglichen, den Schutz vor KI-gestützten Bedrohungen aufrechtzuerhalten**²⁸, **und die die sichere Integration von KI-Tools in Cybersicherheitsoperationen fördern**. Bei diesen Leitlinien und Ratschlägen sollten auch die Bedürfnisse von KMU berücksichtigt werden, die am stärksten von Angriffen bedroht sind. Gegebenenfalls könnten diese Bemühungen durch sektorspezifische Initiativen und Kooperationsmechanismen in Bereichen wie Finanzen, **Verkehr**, Energie, Agrar- und Ernährungswirtschaft, Gesundheitswesen²⁹ und Raumfahrt verstärkt und bereichert werden.

²⁷ Verordnung (EU, Euratom) 2023/2841.

²⁸ Ein Beispiel für solche Beratung ist der **Blog-Eintrag** des CERT EU: *AI is changing the economics of vulnerability discovery. Defenders should adapt now* (KI verändert die wirtschaftlichen Aspekte der Aufdeckung von Schwachstellen. Verteidiger sollten sich jetzt anpassen), 21. April 2026.

²⁹ Europäischer Aktionsplan für die Cybersicherheit von Krankenhäusern und Gesundheitsdienstleistern (COM(2025) 10 final).

Mit fortschreitender Weiterentwicklung der Technologien und der damit verbundenen Risiken werden **eine kollektive Lageerfassung und ein strukturierte Weitergabe von Informationen über KI-gestützte Cybersicherheitsbedrohungen** über die einschlägigen Netze der Union, sowohl auf horizontaler als auch auf sektoraler Ebene, von entscheidender Bedeutung sein, um die Lageerfassung zu stärken. Die ENISA sollte prüfen, wie die Zusammenarbeit mit KI-Anbietern unterstützt werden kann, um die Weitergabe von Erkenntnissen über Bedrohungen zu verbessern.

Ebenso sollten die Mitgliedstaaten bestehende Strukturen auf Unionsebene im Bereich der Cybersicherheit nutzen, um die **Abwehrbereitschaft kritischer Infrastrukturen zu bewerten**, indem sie insbesondere in der NIS-Kooperationsgruppe und gegebenenfalls mit dem mit der KI-Verordnung eingesetzten KI-Gremium zusammenarbeiten.

3.2. Beschleunigung des Patching-Prozesses: Verbesserung des Schwachstellenmanagements für die Entdeckung mit KI-Geschwindigkeit

Die unmittelbare Herausforderung für die Cyberabwehr der EU besteht darin, **bestehende Schwachstellen zu beheben, bevor sie in großem Maßstab ausgenutzt werden können**. Da die KI die Zeit verkürzt, die böswillige Akteure benötigen, um Schwachstellen auszunutzen, müssen die einschlägigen Einrichtungen auch ihre Fähigkeit beschleunigen, Schwachstellen schnell genug zu analysieren, zu priorisieren und Patches zu ihrer Behebung zu erstellen und anzuwenden, um ihre Ausnutzung zu verhindern.

Die bestehenden Verfahren zur Behandlung von Schwachstellen müssen verbessert werden, damit sie im Zeitalter der KI-gestützten Entdeckung wirksam sind. Die ENISA sollte sicherstellen, dass die europäischen Infrastrukturen und Dienste für das Schwachstellenmanagement, darunter die Datenbank der Europäischen Union für Schwachstellen (EUVD) und die im Rahmen der Cyberresilienz-Verordnung eingerichtete einheitliche Meldeplattform, im Zeitalter der KI-gestützten Entdeckung von Schwachstellen zweckmäßig sind, und gemeinsam mit den Mitgliedstaaten die Interoperabilität zwischen europäischen, nationalen und globalen Plattformen und Datenbanken für Schwachstellen stärken.

Mit steigender Zahl von Schwachstellenberichten müssen Hersteller entscheiden, welche Mängel in den Produktlinien zuerst behoben werden müssen, während die Nutzer – insbesondere wesentliche und kritische wichtige Einrichtungen – entscheiden müssen, welche Aktualisierungen zuerst implementiert werden sollen, oft mit begrenzten Ressourcen. Organisationen müssen sich auf klare EU-weite, risikobasierte Leitlinien stützen können, die auf die Cyberresilienz-Verordnung und die NIS-2-Richtlinie abgestimmt sind, um dazu beizutragen, Patches für die Schwachstellen bereitzustellen, bei denen die Risiken am größten sind.

Im Rahmen ihrer Verpflichtungen gemäß der NIS-2-Richtlinie **sollten die Mitgliedstaaten auch die nationalen Strategien für die koordinierte Offenlegung von Schwachstellen aktualisieren**, um gegen die KI-gestützte Ausnutzung von Schwachstellen vorzugehen. Die NIS-Kooperationsgruppe sollte ihre Leitlinien für die Umsetzung der koordinierten Offenlegung von Schwachstellen überarbeiten, und zudem sollte die EU überprüfen, ob die ISO/IEC-Normen, die den Rahmen für die koordinierte Offenlegung von Schwachstellen zugrunde liegen, angesichts der derzeitigen Bedrohungen weiterhin ihren Zweck erfüllen. Die internationale Zusammenarbeit ist in dieser Hinsicht ebenfalls von entscheidender Bedeutung, da diese Praktiken weltweit geprägt werden.

Schließlich endet die Sicherung kritischer Infrastrukturen nicht mit der Offenlegung von Schwachstellen oder der Freigabe von Patches. Die größere Herausforderung besteht darin, **diese anzuwenden**. Mit beschleunigter Aufdeckung von Schwachstellen durch KI wird der Engpass bei der Anwendung von Patches akuter. Mit Unterstützung der ENISA sollten die Mitgliedstaaten bestehende Netze wie die NIS-Kooperationsgruppe nutzen, um diese Herausforderung, die von hervorragender Dringlichkeit ist, zu bewältigen.

3.3. Praktische Umsetzung: Behebung der wichtigsten Schwachstellen

Die EU muss nicht nur Wissen darüber aufbauen, wie KI die Cyberresilienz stärken kann; sie muss **dieses Wissen dort anwenden, wo der Bedarf am dringendsten ist**. Die Herausforderung besteht daher nicht nur darin, Schwachstellen schneller zu erkennen, sondern sie auch zu analysieren, zu beheben und die großmaßstäbliche Anwendung von Patches zu koordinieren. **Kritische Open-Source-Software ist aufgrund der hohen Durchdringung kritischer Infrastrukturektoren der richtige Ort, um rasch zu handeln**. Berichten zufolge enthalten 98 % der gesamten Codebasis Open-Source-Software, wobei die Industrie für kritische Infrastrukturen durchschnittlich etwa 80 % der Codebasen mit hohem oder kritischem Risiko aufweist³⁰.

Die **Open-Source-Strategie der EU**³¹, die als Teil des Pakets zur technologischen Souveränität veröffentlicht wurde, umfasst eine Reihe von Maßnahmen zur Erhöhung der Sicherheit und zur Unterstützung der Pflege kritischer Open-Source-Komponenten. In diesem Zusammenhang wird die Kommission mit der ENISA, den Mitgliedstaaten³² und Open-Source-Gemeinschaften zusammenarbeiten, um einige speziell auf den Cyber- und KI-Bereich ausgerichtete Maßnahmen zu erproben.

Die **ENISA wird in Zusammenarbeit mit der Kommission, den Mitgliedstaaten und Open-Source-Gemeinschaften** die in der Strategie vorgesehene Erfassung kritischer Open-Source-Komponenten beschleunigen und auf der Grundlage einer vorläufigen Liste, die sich auf vereinbarte Kriterien stützt, eine **Kampagne für die Resilienz kritischer Open-Source-Komponenten**, die für kritische Infrastrukturen relevant sind, durchführen. Die Ergebnisse der Kampagne werden in die Umsetzung des Open-Source-Pflegeinstruments einfließen. Die Kampagne wird aus einem freiwilligen Sponsoring-Programm bestehen, um Open-Source-Projekte mit Organisationen abzustimmen, die bereit sind, eng mit den Projektbetreuern zusammenzuarbeiten, um die Pflege und Sicherheit der Open-Source-Projekte zu unterstützen. Sponsoren können Mitgliedstaaten, Einrichtungen der Union wie das CERT-EU, Betreiber kritischer Infrastrukturen, Hersteller und andere öffentliche oder private Einrichtungen sein, die in der Lage sind, Unterstützung zu leisten, indem sie beispielsweise den Betreuern von Open-Source-Projekten qualifizierte Personen oder KI-Modelle und -Tools zur Verfügung stellen. Die Mitgliedstaaten und andere berechnigte Nutzer können die Unterstützung privater vertrauenswürdiger Anbieter im Rahmen der **EU-Cybersicherheitsreserve** in Anspruch nehmen, um nach Schwachstellen im Zusammenhang mit Open-Source-Abhängigkeiten in kritischen Infrastrukturen zu suchen. Darüber hinaus wird die ENISA einen **Dienstleistungskatalog mit KI-gestützten Diensten** erstellen, um das Patching und die Behebung von Open-Source-Schwachstellen zu unterstützen.

³⁰ Blackduck, 2026 *Open Source Security and Risk Analysis Report*: z. B. für Luft- und Raumfahrt, Automobilindustrie, Verkehr, Logistik – 87 %; verarbeitendes Gewerbe 88 %; Gesundheitswesen 88 %; Energie 89 %; Internet- und Software-Infrastruktur 80 %.

³¹ COM(2026) 503 final.

³² Insbesondere gegebenenfalls in Abstimmung mit dem Konsortium für eine europäische Digitalinfrastruktur (EDIC) für digitale Gemeingüter.

Open-Source-Betreuer werden von dem Sponsoring-Programm und dem Dienstleistungskatalog profitieren können, um – beschleunigt durch die Entwicklung von KI-Modellen – die Geschwindigkeit und Wirksamkeit ihrer Arbeit zu erhöhen und Cyberrisiken zu verringern. Durch die Initiative werden die bestehende Open-Source-Governance und die bestehenden Arbeitsabläufe gestärkt, und die Initiative wird als Prüfzentrum für die umfassenderen Bemühungen Europas um KI-gestützte Behebung von Schwachstellen dienen, wodurch das operative Know-how der Union weiter verbessert wird. Sie wird dazu beitragen, die Cyberresilienz in allen Sektoren, einschließlich kritischer Infrastrukturen und KMU, zu stärken. Eine erste Pilotkampagne wird 2026 eingeleitet und später ausgeweitet, wenn sie sich als erfolgreich erweist, auch im Zusammenhang mit der Open-Source-Strategie.

Leitaktionen

- **Leitaktion 4 – Die ENISA wird in Zusammenarbeit mit den einschlägigen Einrichtungen der Union Leitlinien, Empfehlungen, Ratschläge und bewährte Verfahren zum Schutz vor KI-gestützten Bedrohungen und für die sichere Integration von KI in Cybersicherheitsoperationen herausgeben (ab dem 3. Quartal 2026).**
- **Leitaktion 5 – Die Kommission, die Mitgliedstaaten, die ENISA und die Industrie werden zusammenarbeiten, um bestehende Verfahren und Tools für das Schwachstellenmanagement an das KI-Zeitalter anzupassen (ab dem 3. Quartal 2026).**
- **Leitaktion 6 – Die ENISA wird in Zusammenarbeit mit der Kommission, den Mitgliedstaaten, den Open-Source-Gemeinschaften, Einrichtungen der Union und der Industrie ein erstes Pilotprojekt einer Kampagne für die Resilienz kritischer Open-Source-Systeme einleiten, um das Patching zu beschleunigen, unter anderem durch den Einsatz von KI (4. Quartal 2026).**

4. Säule 3: Ausbau der europäischen KI-Fähigkeiten im Cyberbereich

In einem Kontext, in dem sowohl defensive als auch offensive Cyberoperationen zunehmend auf fortgeschrittener KI beruhen, wird die Fähigkeit, KI-gestützte Cybersicherheitslösungen zu entwickeln und einzuführen, zu einem strategischen Faktor für Cyberresilienz und -souveränität. Insbesondere in sensiblen Anwendungsfällen muss die EU in der Lage sein, sich auf souveräne KI-Fähigkeiten zu verlassen, die den erforderlichen Sicherheitserfordernissen, auch im Verteidigungsbereich, gerecht werden. Die EU muss nun europäische Anbieter, einschließlich disruptiver Innovatoren, in die Lage versetzen, solche fortgeschrittene KI in Europa zu entwickeln, einzuführen und zu skalieren. Ergänzend zu ihrer Investitionsstrategie im Cyber- und KI-Bereich muss die EU ihr Technologieökosystem konsolidieren, um den dringendsten operativen Cybersicherheitsbedarf zu decken, Investitionen in die Entwicklung und Einführung europäischer Grenz-KI-Fähigkeiten zu fördern und die Kompetenzen zu entwickeln, die für ihren sektorübergreifenden Einsatz erforderlich sind.

4.1. Stärkung des europäischen Ökosystems KI-gestützter Cybersicherheitslösungen

Da KI bereits für böswillige Zwecke genutzt wird, müssen Organisationen beim Einsatz verfügbarer KI-gestützter Cybersicherheitslösungen schneller handeln als Angreifer, um kritische Infrastrukturen sektorübergreifend zu schützen. Die EU muss den europäischen Markt dazu anregen, solche Tools in der erforderlichen Geschwindigkeit und Größenordnung zur Verfügung zu stellen, und die Einführung in unsere kritische Infrastruktur fördern.

Die EU tätigt bereits erhebliche Investitionen zur **Unterstützung der Forschung und Entwicklung einheimischer fortgeschrittener KI-gestützter Cybersicherheitstechnologien** und für die Cybersicherheit von KI; insbesondere werden im Rahmen der Programme Horizont Europa und Digitales Europa 200 Mio. EUR bis zum Ende des derzeitigen mehrjährigen Finanzrahmens investiert. So werden beispielsweise Ende 2026 drei Vorzeigeprojekte im Rahmen von Horizont Europa eingeleitet, um die Entwicklung, das Training und das Testen von KI für Überwachungs-, Erkennungs-, Reaktions- und Selbstheilungsfähigkeiten in digitalen Prozessen und Systemen gegen Cyberangriffe, einschließlich KI-gestützter Adversarial Attacks, sowie die Entwicklung generativer KI-Tools und -Technologien für die kontinuierliche Überwachung, Einhaltung von Vorschriften und die automatisierte Behebung von Schwachstellen zu unterstützen. Die EU finanziert auch den gesamten KI-Fähigkeitenzyklus im Bereich der Strafverfolgung, von der Forschung bis zur Testung, Validierung und operativen Einführung im Rahmen von Horizont Europa, dem Fonds für die innere Sicherheit, Digitales Europa und CERIS. Ebenso investiert die EU über den Europäischen Innovationsrat (EIC), unter anderem durch Direktinvestitionen aus dem EIC-Fonds, in europäische technologieintensive Cybersicherheits- und KI-Unternehmen; diese Investitionen betreffen 2026 und 2027 auch einschlägige Technologien mit doppeltem Verwendungszweck und strategische Verteidigungstechnologien³³. Konkret wird die Kommission bis Ende 2026 ermöglichen, dass Investitionen des EIC-Fonds in Cyber- und KI-Technologieunternehmen getätigt werden, als Teil von Investitionen in Höhe von 100 Mio. EUR in Start-ups und Scale-ups im Bereich der strategischen Verteidigungstechnologie, und sie wird 2027 eine ähnliche Unterstützung fortsetzen. Der Scaleup Europe Fund wird noch im Jahr 2026 seine erste Investition in die Wachstumsphase strategischer Unternehmen tätigen. Aufbauend auf der internationalen Digitalstrategie der EU werden die EU und die Mitgliedstaaten auch das Tech-Business-Angebot der EU nutzen, um die Einführung von KI- und Softwarelösungen zu unterstützen.

Ergänzend zu diesen Investitionen sollte die Union bestrebt sein, den **Wissensaustausch über fortgeschrittene KI-gestützte Cybersicherheitsfähigkeiten gegen groß angelegte Cyberangriffe, bei denen KI eingesetzt wird, weiter zu beschleunigen**. Heute verfügt die EU über ein reichhaltiges Ökosystem und eine reiche Wissensbasis in Wissenschaft, Industrie und Regierung, aber KI-gestützte Lösungen für die Cybersicherheit sind nach wie vor fragmentiert, in operativen Umgebungen unzureichend getestet und weit davon entfernt, sektorübergreifend in großem Maßstab eingesetzt zu werden³⁴. Ein Beispiel ist die automatisierte Behebung von Schwachstellen, die einer der größten operativen Engpässe für die Cybersicherheit im KI-Zeitalter ist: Heute schreitet die KI-gestützte Aufdeckung von Schwachstellen schneller voran als die KI-gestützte Behebung dieser Schwachstellen, und dadurch entsteht ein strukturelles Ungleichgewicht zum Vorteil der Angreifer. Als Reaktion auf Aufforderungen zur Bewältigung der von offensiver KI ausgehenden Bedrohungen³⁵ wird die Kommission daher mit Unterstützung des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) und in Zusammenarbeit mit der ENISA eine spezielle **Große Herausforderung für die KI-gestützte Behebung von Schwachstellen** auf den Weg bringen. Die Große Herausforderung, die europäische Cybersicherheits- und KI-Unternehmen, Forschungseinrichtungen, Betreiber kritischer Infrastrukturen und Open-Source-Gemeinschaften im Rahmen dieser gemeinsamen Aufgabe zusammenbringt, wird die Entwicklung eines KI-Systems unterstützen, das in der Lage ist, Cybersicherheitsteams während des gesamten Zyklus der Schwachstellenbehebung zu unterstützen. Durch die

³³ [The EIC Fund – Europäischer Innovationsrat – Europäische Kommission](#).

³⁴ [Public Letter of Support for a European Grand Challenge in AI and Security – Google Docs](#).

³⁵ Ebenda.

Verknüpfung von Forschung und praktischer Einführung wird die Große Herausforderung es ermöglichen, vielversprechende Lösungen in realistischen operativen Umgebungen zu testen und letztlich Organisationen in ganz Europa zur Verfügung zu stellen, was dazu beiträgt, die operativen Engpässe zu verringern, die einer zeitnahen Behebung von Schwachstellen im Wege stehen. Interessierte Mitgliedstaaten werden aufgefordert, diese Bemühungen um den Wissensaustausch zu unterstützen.

4.2. Aufbau europäischer Grenzfähigkeiten

Während bestehende KI-Modelle und -Systeme mit Cybersicherheitsfähigkeiten bereits erhebliche Möglichkeiten für Cybersicherheitsmaßnahmen bieten, haben durch Grenz-KI gestützte Cyberfähigkeiten auch erhebliche Auswirkungen auf die technologische Souveränität, Sicherheit und Verteidigung Europas. Daher muss die EU **eigene souveräne Grenz-KI-Fähigkeiten mit allgemeinem Verwendungszweck entwickeln**, um das Risiko neuer Abhängigkeiten von einer mittlerweile kritischen strategischen Ressource mit einem zunehmenden Potenzial für einen doppelten Verwendungszweck, der weit über den Bereich der Cybersicherheit hinausgeht, zu mindern. Dies stellt eine umfassendere sektorübergreifende Herausforderung für unsere Wirtschaft und Gesellschaft dar, die die Kommission bei ihrer Weiterentwicklung weiterhin genau beobachten und angehen wird.

Die Kommission hat bereits konkrete Schritte unternommen, um wichtige europäische Akteure bei der Entwicklung von Grenz-KI-Fähigkeiten zu unterstützen.

- Kürzlich wählte die Kommission ein Projekt im Rahmen der Großen Herausforderung für Grenz-KI aus, mit der der Zugang zu EuroHPC-Rechenkapazitäten gewährt und die Entwicklung eines europäischen fortgeschrittenen Open-Source-KI-Modells unterstützt werden³⁶.
- Im Rahmen der Ressource für KI-Wissenschaft in Europa (RAISE) finanziert die Kommission ein Netz von Grenz-KI-Labors, um die Forschung auch in diesem Bereich voranzubringen.
- Im Rahmen von Horizont Europa finanziert die Kommission Maßnahmen, um eine sichere KI im größeren Maßstab auf den Weg zur Grenz-KI zu bringen.
- Die Kommission wird weiterhin mit Frankreich und Deutschland zusammenarbeiten, um eine gemeinsame Initiative (die „Europäische Initiative für Grenz-KI“) zu schaffen, die Forschungs- und Innovationsarbeiten durchführen, Talente anziehen und Spin-offs erleichtern soll.
- Die Kommission nutzt technische Beratung über das Forum für Grenz-KI³⁷.

Diese ersten Schritte bilden eine wichtige Grundlage, doch **ist ein Paradigmenwechsel hinsichtlich der Ambitionen und Ressourcen erforderlich**, um die Ziele Europas für die Grenz-KI in eine dauerhafte souveräne Kapazität und einen Wettbewerbsvorteil zu verwandeln. Angesichts des beispiellosen Umfangs der Ressourcen, die für die Entwicklung von Grenz-KI erforderlich sind, erfordern Grenzprojekte einen kooperativen Ansatz auf Unionsebene. In der vorgeschlagenen Verordnung über Cloud- und KI-Entwicklung werden sie als vorrangige Projekte eingestuft, und es werden Rechenressourcen der Union zugewiesen,

³⁶ Commission selects EUROPA consortium as the winner of the Frontier AI Grand Challenge, a project to build European open-source frontier AI model in all 24 EU languages (Die Kommission wählt das EUROPA-Konsortium als Gewinner der Großen Herausforderung für Grenz-KI aus, ein Projekt zum Aufbau eines europäischen Open-Source-Grenz-KI-Modells in allen 24 EU-Sprachen) | Gestaltung der digitalen Zukunft Europas.

³⁷ Commission seeks experts for forum on Frontier AI (Kommission sucht Experten für das Forum für Grenz-KI) | Gestaltung der digitalen Zukunft Europas.

als Ergänzung zu den von den Mitgliedstaaten zugewiesenen Ressourcen. **Bestehende KI-Fabriken und künftige Gigafabriken** sollten genutzt werden, um als Teil einer souveränen europäischen KI- und Cybersicherheitsinfrastruktur zu dienen, die Rechenleistung, Daten und Konnektivität umfasst, und um die EU als einen führenden KI-Kontinent zu positionieren. Eine solche Konnektivität ist eine Voraussetzung für die vertrauenswürdige Weitergabe KI-fähiger Datensätze, die grenzüberschreitende Bündelung von Ressourcen, den sicheren Betrieb kontrollierter Umgebungen sowie die Entwicklung, Erprobung und Einführung von und den Zugang zu robusten, vertrauenswürdigen und leistungsstarken Cyber-KI-Fähigkeiten. Einschlägige KI-Fabriken mit Schwerpunkt auf dem Cyberbereich sollten den Zugang zu hochwertigen KI-fähigen Datensätzen, die von öffentlichen Daten bis hin zu sensiblen Industrie-³⁸ und Cybersicherheitsdaten reichen, durch vertrauenswürdige, gesicherte und resiliente Datenweitergabemechanismen erleichtern und die Entwicklung und Validierung von KI-Modellen in einer kontrollierten, rechenschaftspflichtigen und überprüfbaren Umgebung durch ihre Datenlabors unterstützen.

Die Kommission wird zudem die Entwicklung souveräner europäischer KI-Cyberfähigkeiten, auch für die Verteidigung, durch den Europäischen Fonds für Wettbewerbsfähigkeit unterstützen, um sicherzustellen, dass Europa besser gerüstet ist, um seine strategischen Interessen zu schützen und kritische Abhängigkeiten zu verringern. In diesem Zusammenhang wird die Kommission mit den einschlägigen Agenturen, einschließlich der ENISA und der Europäischen Verteidigungsagentur (EDA), sowie den Mitgliedstaaten eine spezielle Arbeitsgruppe einrichten, um die Sicherheitsrisiken im Zusammenhang mit der Einführung von Grenz-KI-Modellen in kritischen Verteidigungssystemen und Systemen mit doppeltem Verwendungszweck anzugehen.

Die Entwicklung souveräner Grenzfähigkeiten wird einen **Investitionsbedarf in Höhe von Hunderten Milliarden Euro** mit sich bringen, der nur teilweise aus öffentlichen Mitteln gedeckt werden kann. Dies erfordert dringend die Mobilisierung großer Mengen an privaten Investitionen, insbesondere Risikokapital und Beteiligungskapital, um innovative europäische Lösungen zu entwickeln und zu skalieren. Ohne Rechenleistung, Modelle und Dateninfrastruktur wird Europa zwangsläufig ein gefährdeter Nutzer von Grenz-KI-Systemen bleiben, die anderswo hergestellt werden und von anderen Akteuren plötzlich abgeschaltet werden können – mit enormen wirtschaftlichen und (Cyber-)Sicherheitsauswirkungen. Die Kosten für den Aufbau eigener Grenz-KI-Kapazitäten für Europa können zwar sehr hoch sein, aber die Kosten für den Verzicht auf den Aufbau dieser Kapazitäten können noch höher sein und mit zunehmender Fähigkeitslücke bei der KI von Jahr zu Jahr steigen.

Mit ihrem Paket zur technologischen Souveränität vom 3. Juni 2026 hat die Kommission **Konsultationen mit den Mitgliedstaaten, der EIB-Gruppe und anderen wichtigen Interessenträgern zu dem Vorschlag eingeleitet, eine neue europäische Eigenkapitalkapazität einzurichten**, die ein Portfolio groß angelegter Beteiligungsinvestitionen in Spitzentechnologien und Infrastrukturen verwaltet, die für unsere technologische Souveränität von entscheidender Bedeutung sind – einschließlich digitaler Technologien wie Grenz-KI, aber auch Technologien für saubere Energie, Biotechnologie und potenziell Verteidigungstechnologien. Der Hauptvorteil dieses Mechanismus bestünde darin, einen dringend benötigten Eigenkapital-„Koinvestitionsanker“ zu schaffen, der große Mengen privater Investitionen anzieht, indem er mit auf EU-Ebene bereits bestehenden Finanzierungsinstrumenten wie dem Scaleup Europe Fund zusammenarbeitet oder in diese investiert. Diese neue strategische Technologie-Eigenkapitalfazilität wäre ein Impulsgeber bei

³⁸ Vorbehaltlich der Einhaltung der geltenden Rechtsvorschriften, einschließlich des EU-Wettbewerbsrechts.

der Reaktion auf diese letzte Forderung nach großen EU-Investitionen in Grenz-KI. Was das Instrument InvestEU des Europäischen Fonds für Wettbewerbsfähigkeit betrifft, so könnte ein solcher Mechanismus zu einer wichtigen Einrichtung für strategische, umfangreiche Eigenkapitalinvestitionen für fortgeschrittene Technologien und Infrastrukturen werden.

4.3. Verbesserung der Cybersicherheitskompetenzen für das KI-Zeitalter

Der Erfolg Europas wird nicht allein durch Technologie bestimmt werden. Die Fähigkeit, fortgeschrittene KI bei Cybersicherheitsoperationen wirksam und sicher einzusetzen, wird auch von der **Verfügbarkeit qualifizierter Fachkräfte** abhängen, **die in der Lage sind, KI-Modelle mit fortgeschrittenen Cyberfähigkeiten zu verstehen und sicher zu nutzen** und KI-spezifische Risiken zu bewältigen. Da Cybersicherheitsteams zunehmend fortgeschrittene KI integrieren werden, könnte dies die bestehende Qualifikationslücke im Bereich der Cybersicherheit weiter verschärfen. Die EU muss daher ihre Arbeitskräfte im Bereich der Cybersicherheit stärken, indem sie sie mit den richtigen KI-Kompetenzen für die Cybersicherheit ausstattet.

Die **EU-Akademie für Cybersicherheitskompetenzen**, in der die Industrie, Ausbildungsanbieter und akademische Einrichtungen zu konkreten Zusagen und Partnerschaften für Cybersicherheitsschulungen zusammenkommen, bietet den richtigen Rahmen, um diesem Bedarf auf Unionsebene gerecht zu werden. Die Kommission wird dieses wachsende Ökosystem gemeinsam mit den Mitgliedstaaten nutzen, um im Rahmen der Akademie für Cybersicherheitskompetenzen eine spezielle Maßnahme zur Entwicklung von Schulungsprogrammen für Cybersicherheitsfachkräfte einzuleiten, in denen diese lernen, KI-Tools zu nutzen. Außerdem sollten potenzielle Synergien mit der bevorstehenden Akademie für KI-Kompetenzen ausgelotet werden. Darüber hinaus wird die ENISA den **europäischen Rahmen für Cybersicherheitskompetenzen** aktualisieren, indem sie KI-bezogene Kompetenzen in bestehende Berufsprofile integriert und erforderlichenfalls neue Rollen festlegt.

Leitaktionen:

- **Leitaktion 7 – Die Kommission wird mit Unterstützung des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) und in Zusammenarbeit mit der ENISA eine Große Herausforderung der EU auf den Weg bringen, um einen Beitrag zur Skalierung europäischer KI-gestützter Cybersicherheitslösungen zu leisten (4. Quartal 2026).**
- **Leitaktion 8 – Die Kommission wird gemeinsam mit den Mitgliedstaaten bestrebt sein, Zugang zu den Rechenkapazitäten von KI-Fabriken zu gewähren, um verfügbare fortgeschrittene und Grenz-KI-Modelle für die Cyberresilienz auf souveräner Rechenleistung zu testen, zu trainieren und einzuführen.**
- **Leitaktion 9 – Die Kommission wird mit den Mitgliedstaaten und der Industrie (im Rahmen der Akademie für Cybersicherheitskompetenzen) zusammenarbeiten, um Schulungsmodule für Cybersicherheitsfachleute zum Einsatz von KI für die Cybersicherheit zu entwickeln (4. Quartal 2026).**

5. Zusammenarbeit mit gleichgesinnten Partnern im Hinblick auf ein globales Konzept für die Cybersicherheit im KI-Zeitalter

Die Auswirkungen von KI auf die Cybersicherheit sind naturgemäß global, da KI-Modelle und -Systeme, Software-Lieferketten und Open-Source-Ökosysteme grenzüberschreitend funktionieren. Die Freigabe eines KI-Modells mit Cyberfähigkeiten, das in einem Land entwickelt wurde, kann erhebliche Auswirkungen auf die Sicherheit kritischer Infrastrukturen und Unternehmen in der ganzen Welt haben. Regierungen, internationale Organisationen und die Industrie stehen daher vor **einer gemeinsamen Herausforderung, und die internationale Zusammenarbeit ist von entscheidender Bedeutung**, um eine Fragmentierung zu vermeiden, die Interoperabilität zwischen vertrauenswürdigen Partnern zu fördern und die Anstrengungen zur Minderung der mit KI verbundenen Cybersicherheitsrisiken zu bündeln.

Die EU sollte bei der Gestaltung globaler Verfahren für vertrauenswürdige KI und Cyberresilienz eine Führungsrolle übernehmen und dabei den **Regulierungsrahmen** der Union **im KI- und Cyberbereich** nutzen. Insbesondere ist eine engere Zusammenarbeit zwischen gleichgesinnten Partnern erforderlich, um sicherzustellen, dass Grenz-KI-Fähigkeiten weiterhin sowohl sicher als auch für vertrauenswürdige Anwendungen verfügbar sind, und um gleichzeitig ihren Missbrauch durch böswillige Akteure zu verhindern. Dieser Aktionsplan ist auch ein Aufruf an unsere internationalen Partner, sich an den Anstrengungen zu beteiligen, die Auswirkungen der vorgeschlagenen Maßnahmen auf die Sicherheit von KI und die Cyberresilienz zu verstärken.

Die Kommission wird diese Ziele insbesondere in bilateralen und multilateralen Foren verfolgen. Sie wird sich weiterhin aktiv **in der G7 engagieren, um ihren Ansatz zu fördern**, unter anderem durch die **Arbeitsgruppen Digital und Technologie sowie Cybersicherheit**, um die Arbeit an einem gemeinsamen Verständnis der Cybersicherheitsrisiken, die sich aus fortgeschrittenen KI-Fähigkeiten ergeben, zu unterstützen. Die Kommission wird die Zusammenarbeit der G7 im Bereich von Normen und bei der Bewertung dieser Modelle fördern. Sie ersucht ferner die G7-Mitglieder und andere internationale Partner, sich an den Bemühungen zur Unterstützung der Sicherheit von Open-Source-Software zu beteiligen und im Hinblick auf die Anpassung der Verfahren für das Schwachstellenmanagement zusammenzuarbeiten. Die EU wird sich auch weiterhin in den Vereinten Nationen engagieren.

Auf bilateraler Ebene wird die EU den Austausch mit Partnerländern über fortgeschrittene KI und Cybersicherheit vertiefen, unter anderem durch digitale Partnerschaften, digitale Dialoge oder Cyberdialoge, und wird gegebenenfalls der Modellbewertung, dem Schutz kritischer Infrastrukturen, der Minderung von Schwachstellen und einer verbesserten Cyberresilienz als Kernbereiche der Zusammenarbeit Vorrang einräumen.

Darüber hinaus ist das **Netz für Messung, Bewertung und Wissenschaft fortgeschrittener KI, das vom britischen AISI koordiniert wird** und eng mit den Sicherheitsinstituten der Partnerländer und dem **Büro für künstliche Intelligenz der Kommission** zusammenarbeitet, eine wichtige Plattform für die Entwicklung gemeinsamer Methoden für die Bewertung von Grenz-KI-Modellen, den Austausch bewährter Verfahren und die Unterstützung einer vertrauenswürdigen internationalen Zusammenarbeit im Bereich der KI-Sicherheit.

Die Kommission wird auch einen strukturierten Dialog zwischen Regierungen und führenden Grenz-KI-Entwicklern anregen, um gemeinsame Ansätze für die Sicherheit, Bewertung und verantwortungsvolle Einführung von Grenz-KI zu fördern.

Schließlich wird die EU angesichts der genannten Auswirkungen auf die europäische und nationale Sicherheit den bestehenden Austausch mit der **NATO** über Chancen und Risiken im

Zusammenhang mit Grenz-KI-Fähigkeiten im Cyberbereich verstärken, unter anderem durch die Nutzung des künftigen NATO-Exzellenzzentrums für künstliche Intelligenz.

6. Fazit

Dieser Aktionsplan stellt die Fortsetzung nachhaltiger und koordinierter europäischer Anstrengungen dar. Da sich die Entwicklung fortgeschrittener KI-Fähigkeiten weiter beschleunigen wird und neue Chancen und Risiken entstehen werden, wird die Kommission die Umsetzung des Aktionsplans regelmäßig bewerten und die Maßnahmen erforderlichenfalls anpassen, um sicherzustellen, dass er wirksam zur Entwicklung eines sicheren und resilienten europäischen Ökosystems für das KI-Zeitalter beiträgt.