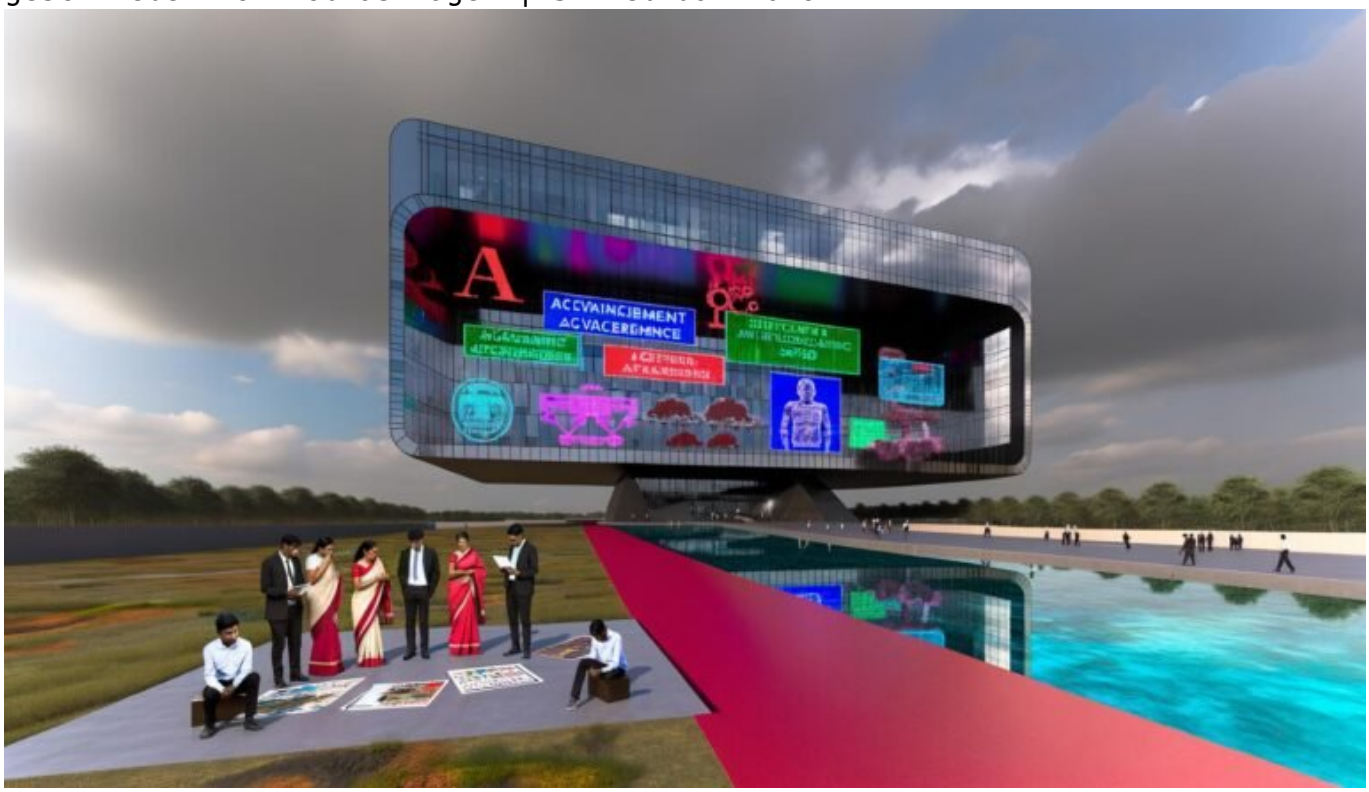
Cyberagentur Kritik Kritik: Mehr Schein als Sein?

Category: Opinion
geschrieben von Tobias Hager | 3. Februar 2026



Cyberagentur Kritik Kritik: Mehr Schein als Sein?

Staatsgeförderte Cyberagentur: Klingt nach digitaler Speerspitze, ist oft nur eine blendende Fassade. Wer glaubt, dass Innovationsförderung made in Germany automatisch Cyber-Exzellenz bedeutet, lebt noch im Märchen vom digitalen Wunderland. In diesem Artikel nehmen wir die Cyberagentur auseinander – technisch, politisch und wirtschaftlich. Fakten statt Pressemitteilungen. Ehrliche Analyse statt PR-Geschwurbel. Willkommen bei der schonungslosesten Kritik, die du zur Cyberagentur je lesen wirst.

- Was ist die Cyberagentur eigentlich – und warum existiert sie wirklich?

- Die größten technischen Versäumnisse und Innovations-Illusionen
- Warum Fördergeld nicht gleich Fortschritt ist: Die Mängel der Vergabe
- Wie viel digitale Substanz steckt wirklich hinter den Projekten?
- Fehlende technologische Tiefe: Von Buzzwords und PowerPoint-Magie
- Politische Spielchen, Intransparenz und das Problem mit der Zielsetzung
- Was ausländische Cyberagenturen besser machen – und warum Deutschland hinterherhinkt
- Konkrete Handlungsempfehlungen statt leere Kritik
- Warum echte Cybersecurity Innovation in Deutschland so schwer ist

Die Cyberagentur ist das Lieblingskind deutscher Digitalpolitik: Mit Steuergeldern gepäppelt, mit Visionen überfrachtet und mit Erwartungen erschlagen. Doch was bleibt übrig, wenn man die Hochglanzfolien beiseitelegt und sich die technischen Details ansieht? Spoiler: Ernüchterung. Wer die Cyberagentur für eine Elite-Schmiede hält, hat die Realität entweder nicht verstanden – oder ignoriert. Während die Agentur sich in Innovationsrhetorik suhlt, bleiben Durchbrüche und echte Cybersecurity-Exzellenz meist auf der Strecke. Die Kritik ist laut, die Mängel offensichtlich – und trotzdem feiert sich das Projekt immer wieder selbst. Zeit für eine schonungslose Inventur.

Was ist die Cyberagentur? Von der Vision zur Realität – und zurück

Die Cyberagentur wurde 2018 als „Agentur für Innovation in der Cybersicherheit“ gegründet – mit großem Tamtam und der Ansage, Deutschland zur globalen Cyber-Supermacht zu machen. Ziel: disruptive Technologien fördern, militärische und zivile Cyberfähigkeiten stärken, und die Bundesrepublik vor digitalen Bedrohungen schützen. Klingt nach einer Mischung aus DARPA und deutschem Mittelstand? Schön wär’s. Die Realität ist weniger heroisch.

Statt waghalsiger Forschung und echter Disruption dominiert Bürokratie. Die Cyberagentur ist ein Hybrid aus Bundesbehörde, Innovations-Labor und Fördertopf, dessen Mandat irgendwo zwischen Verteidigungs- und Innenministerium hin- und herschwappt. Klar, es gibt Projektförderungen, Wettbewerbe und viele bunte Grafiken zu „Zukunftstechnologien“. Aber was hat das wirklich gebracht? Wer sich die Ergebnislisten ansieht, findet jede Menge Pilotprojekte, Studien und Prototypen – aber kaum ein echtes Cyber-Produkt, das im internationalen Vergleich besteht.

Das Grundproblem: Die Cyberagentur will alles sein – Innovationsmotor, Förderbank, Strategieberater, Technologietransferstelle – und verliert sich dabei in politischer Zielkonfusion. Das Ergebnis ist ein Apparat, der zwar viel verspricht, aber selten liefert. Die Versäumnisse sind nicht nur politisch, sondern vor allem technisch. Denn echte Cybersecurity lebt von Tiefe, nicht von PowerPoint.

Die Cyberagentur Kritik setzt genau hier an: Sind die geförderten Projekte wirklich disruptiv? Oder werden hier nur Buzzwords wie Künstliche Intelligenz, Blockchain und Quantencomputing verbraten, um Schlagzeilen zu produzieren? Wer die Ankündigungen analysiert, findet viel heiße Luft und wenig Substanz.

Technische Substanz oder Buzzword-Bingo? Die Innovationsillusion der Cyberagentur

Wer sich die geförderten Projekte der Cyberagentur anschaut, sieht vor allem eines: Innovationsrhetorik und Buzzword-Bingo. Von „Secure Artificial Intelligence“ über „Post-Quantum Cryptography“ bis zu „Resilient Cloud Architectures“ – kein Hype-Begriff der letzten fünf Jahre fehlt. Das Problem: In den seltensten Fällen steckt echte technologische Substanz dahinter.

Viele Projekte bleiben auf Konzept- oder Machbarkeitsstudien-Ebene hängen. Proof-of-Concepts, Whitepapers, Demos – aber keine ausgereiften Produkte, keine skalierbaren Lösungen, keine Open-Source-Initiativen, die den Markt wirklich bewegen. Gerade im Bereich Cybersecurity sind das aber die harten Währungen: funktionierende Protokolle, robuste Implementierungen, nachweisbare Angriffsresilienz.

Die Cyberagentur Kritik wird hier ganz konkret: Die technische Tiefe fehlt, weil die Auswahlprozesse oft eher politisch als technologiegetrieben sind. Hauptsache, das Projekt klingt nach Innovation, erfüllt die Förderkriterien und lässt sich für die nächste Pressekonferenz verwerten. Ob es wirklich ein Sicherheitsproblem löst oder einen technischen Durchbruch bringt, steht auf einem anderen Blatt.

Wer echte Cybersecurity-Innovation will, braucht Fachleute, die verstehen, wie Exploits, Zero-Day-Angriffe, Penetrationstests und Kryptographie auf Protokollebene funktionieren. Doch die Reviews und Auswahlgremien der Cyberagentur sind oft mit Generalisten besetzt, die sich von schicken PowerPoint-Folien beeindrucken lassen. Das Ergebnis: Mehr Schein als Sein.

Fördergeld-Vergabe: Warum staatliche Mittel selten zu

technologischem Fortschritt führen

Geld ist im Prinzip genug da: Der Etat der Cyberagentur liegt im zweistelligen Millionenbereich. Doch die Art und Weise, wie Fördermittel vergeben werden, ist ein Paradebeispiel für deutsche Digitalpolitik: Viel Papierkram, wenig Risiko, geringe technische Due Diligence. Die Vergabekriterien sind so vage, dass sich fast jedes Projekt irgendwie in die Förderraster pressen lässt.

Das Problem bei der staatlichen Förderung: Sie fördert selten echte Disruption, sondern vor allem Projekte, die den Beamtenapparat nicht überfordern. Wer zu radikal denkt, zu nah am Markt agiert oder zu technisch argumentiert, wird ausgebremst. Lieber ein weiteres Blockchain-Konzeptpapier als ein echtes, implementiertes Zero-Knowledge-Proof-System, das Angreifer wirklich ins Schwitzen bringt.

Cyberagentur Kritik heißt deshalb auch: Die Förderlogik ist nicht auf technische Exzellenz, sondern auf politische Risikominimierung ausgelegt. Das Ergebnis? Viel Mittelmaß, wenig Durchbrüche. Die nationale Cybersicherheitslandschaft bleibt abhängig von Importtechnologien, weil echte Eigenentwicklungen zu selten gefördert werden – oder im Sumpf aus Bürokratie und politischen Zielkonflikten versanden.

Was müsste sich ändern? Ganz einfach: Technische Tiefe muss Vorrang vor politischer Bequemlichkeit haben. Auswahlgremien brauchen echte Security-Experten, nicht nur Verwaltungserfahrung. Fördermittel sollten an messbare technische Meilensteine geknüpft sein – und nicht an die Fähigkeit, ein besonders gefälliges Antragspapier zu schreiben.

Transparenz, Zielsetzung, Vergleich: So machen es andere Cyberagenturen besser

Ein Blick ins Ausland zeigt, wie es gehen kann. Die US-amerikanische DARPA ist das Benchmark-Modell: Hier entscheiden technische Experten, welche Projekte gefördert werden – und zwar nach dem Innovationsgehalt, nicht nach Pressetauglichkeit. Funding gibt es für echte „Moonshots“, nicht für PR-Schaumschlägerei. Die Ergebnisse sprechen für sich: Viele der wichtigsten Internet- und Sicherheitstechnologien der letzten 30 Jahre stammen aus dem DARPA-Kosmos.

Auch Israel und Großbritannien setzen bei ihren Cyberagenturen auf technologische Exzellenz und Transparenz. Offene Calls, Peer-Reviews durch Fachleute, regelmäßige technische Audits und ein Fokus auf Open Source sind

Standard. Im Vergleich dazu wirkt die deutsche Cyberagentur wie ein Innovations-Playground für den politischen Mittelbau – mit wenig externem Review, kaum offenen Daten und einer auffällig geringen Erfolgsquote bei echten Durchbrüchen.

Die Cyberagentur Kritik muss deshalb auch die Transparenz ansprechen. Wo sind die offenen Ergebnisberichte? Was ist aus den geförderten Projekten geworden? Welche Technologien wurden tatsächlich in die Praxis übernommen, welche landeten im Schubladen-Archiv? Wer hier nach konkreten Antworten sucht, findet oft nur Schweigen – oder wohlformulierte Ausflüchte.

Was bleibt, ist der Eindruck: Die Cyberagentur hat ein Transparenzproblem und ein Zielproblem. Ohne klare, technisch messbare Zielvorgaben und echte externe Reviews bleibt sie ein digitaler Selbstzweck – finanziert vom Steuerzahler, aber mit fragwürdigem Nutzen.

Cyberagentur Kritik: Handlungsempfehlungen für echte Cybersecurity-Innovation

Die Probleme der Cyberagentur sind kein Naturgesetz. Mit den richtigen Maßnahmen ließe sich aus dem Laden tatsächlich ein Innovationsmotor machen. Wie das geht? Hier die Schritt-für-Schritt-Liste für eine Cyberagentur, die ihren Namen verdient:

1. Echte technische Peer-Reviews implementieren
   Projekte müssen von anerkannten Security-Experten geprüft werden, nicht von Verwaltungsbeamten.
2. Fördermittel an technische Meilensteine koppeln
   Kein Geld für Konzeptpapiere, sondern für funktionierende Prototypen, offene Code-Reviews und nachweisbare Angriffsresilienz.
3. Transparenz-Offensive starten
   Veröffentlichung aller Projektergebnisse, vollständige Open-Data-Reports, regelmäßige Audits durch externe Fachleute.
4. Open Source und Community-Förderung priorisieren
   Wer echte Sicherheit will, muss offene Standards und quelloffene Software fördern – nicht Blackbox-Lösungen großer Konzerne.
5. Internationale Benchmarks einführen
   Jedes geförderte Projekt muss sich mit dem internationalen Stand der Technik messen, nicht mit dem deutschen Mittelmaß.
6. Politik raus aus der Technik
   Die Cyberagentur muss von technischen, nicht von politischen Zielen geleitet werden. Alles andere ist Innovationsverhinderung.

Wer diese Punkte umsetzt, macht aus der Cyberagentur mehr als einen Fördertopf mit schönem Namen. Es geht um digitale Souveränität, echte Innovationskraft und den Aufbau von Cyber-Kompetenz, die ihren Namen verdient.

Fazit: Cyberagentur Kritik – Zeit für radikale Ehrlichkeit

Die Cyberagentur ist ein Paradebeispiel dafür, wie gute Absichten in deutschen Digitalprojekten oft an Bürokratie, politischer Zielverirrung und technischer Oberflächlichkeit scheitern. Die Kritik ist berechtigt: Es fehlt an messbaren Erfolgen, an technischer Tiefe und an Transparenz. Wer die Agentur für eine echte Cybersecurity-Eliteschmiede hält, glaubt an Märchen.

Doch Kritik allein reicht nicht. Was die Cyberagentur jetzt braucht, ist ein radikaler Kurswechsel: Technische Exzellenz statt Buzzword-Bingo, offene Ergebnisse statt PR-Geklingel, und echte Innovation statt Fördertourismus. Nur dann kann Deutschland im globalen Cyberwettbewerb bestehen. Bis dahin bleibt die Cyberagentur: Mehr Schein als Sein.