Cyberagentur Kritik Kommentar: Zwischen Hoffnungen und Zweifeln

Category: Opinion
geschrieben von Tobias Hager | 2. Februar 2026

Cyberagentur Kritik Kommentar: Zwischen Hoffnungen und Zweifeln

Die Cyberagentur – das große Versprechen, Deutschlands digitale Verteidigung endlich auf das nächste Level zu heben, feiert munter Budgetrekorde, brüstet sich mit “strategischer Autonomie” und verteilt auf LinkedIn die immer gleichen Innovationsfloskeln. Was wirklich bleibt? Skepsis, offene Baustellen und eine digitale Landschaft, die noch immer mehr nach PowerPoint als nach Cyberpower aussieht. Dieser Kommentar seziert, warum die Cyberagentur mehr ist als ein politisches Feigenblatt – aber weniger als die erhoffte digitale Speerspitze. Willkommen beim Realitätscheck zwischen PR-Gelaber und echter Cyberkompetenz.

- Die Cyberagentur als Prestigeprojekt – Anspruch, Hype und Realität
- Warum strategische Autonomie mehr Buzzword als Substanz ist
- Kritische Analyse der Projekte, Transparenzdefizite und Entscheidungswege
- Die Rolle der Cyberagentur im deutschen Innovations-Ökosystem
- Fehlende Durchschlagskraft bei Forschung, Transfer und Marktdurchdringung
- Technische Herausforderungen: Security, KI, Post-Quantum – und wie viel davon wirklich ankommt
- Schwächen bei Personal, Agilität und Kollaboration mit der Industrie
- Schritt-für-Schritt: Was sich ändern muss, damit aus Hoffnung keine Leerstelle wird
- Kritischer Ausblick: Zwischen Systemfehler und letzter Chance

Die Cyberagentur ist das Lieblingskind der deutschen Digitalpolitik: Einmal ordentlich Budget, ein paar schicke Claims zu “Disruption” und “Souveränität” – und schon glaubt man, beim globalen Cyberwettrüsten mitspielen zu können. Doch hinter der Fassade brodelt es: Zu wenig echte Innovation, zu viel Verwaltung, zu viele Stakeholder ohne Skin in the Game. Während andere Nationen Cyberfähigkeiten als militärisch-strategische Assets begreifen, bleibt Deutschland beim Innovations-Mikado: Viel Ankündigung, wenig Risiko, kaum Resultate. Das Resultat ist ein System, das zwar Projekte beauftragt, aber selten echten Impact generiert – und dabei so transparent ist wie ein Blackbox-Mandat.

Wer sich ernsthaft mit der Cyberagentur beschäftigt, wird schnell merken: Die Erwartungen von außen sind gigantisch, das politische Versprechen noch größer, aber die Wirklichkeit ist ein Flickenteppich aus Pilotprojekten, Forschungsförderung und vielstufigen Abstimmungsrunden. Das ist in etwa so disruptiv wie ein Faxgerät in der Cloud. Und der eigentliche Witz: Während die Cyberagentur öffentlichkeitswirksam von “Gamechanger-Innovationen” spricht, fehlt es intern an personellen Ressourcen, technischem Know-how und Entscheidungsfreude. Willkommen im deutschen Cyber-Realismus.

Cyberagentur als Leuchtturm: Anspruch, Wirklichkeit und der deutsche Sonderweg

Die Gründung der Cyberagentur wurde als Wendepunkt gefeiert: Endlich Schluss mit zersplitterten Zuständigkeiten, endlich Fokus auf disruptive Forschung im Bereich Cybersecurity. Das Ziel: Deutschland technologisch unabhängig machen, kritische Infrastrukturen absichern, militärische Cyberfähigkeiten aufbauen. Der Anspruch? Hoch. Die Realität? Ernüchternd. Die Cyberagentur ist in der Theorie eine “Agentur für Innovation in der Cybersicherheit” – de facto ist sie eine Mischung aus Forschungsträger, Thinktank und Fördermitteldealer.

Statt echter strategischer Autonomie bleibt es häufig beim Buzzword-Bingo. “Souveränität” klingt nett, aber wie viel davon ist wirklich da? Die meisten

Projekte basieren auf existierenden Frameworks, Open-Source-Komponenten oder Importtechnologien. Selbst bei KI oder Post-Quantum-Security ist Deutschland maximal Mitspieler, nicht Taktgeber. Die Cyberagentur kann daran wenig ändern, solange sie mehr PowerPoint als Prototypen produziert.

Was auffällt: Der deutsche Sonderweg in Sachen Cyberagentur ist geprägt von Kompromissen. Zwischen Verteidigungsministerium, Forschungsministerium, Innenministerium und Kanzleramt wird um Kompetenzen gerungen – die Folge sind lange Entscheidungswege, wenig Agilität und eine Kultur der Absicherung statt Risikobereitschaft. Wer wirklich disruptive Ergebnisse will, bekommt stattdessen ein Innovations-Gemischtwarenladen mit zu vielen Köchen und zu wenig Output.

Die Cyberagentur könnte der Leuchtturm sein, an dem sich Deutschlands digitale Ambitionen messen. Was fehlt, ist der Mut, aus der Komfortzone zu gehen – und das Verständnis, dass Cyberinnovation nicht durch Gremien entsteht, sondern durch technologische Exzellenz, klare Roadmaps und echte Kollaboration mit der Industrie.

Strategische Autonomie: Buzzword oder technologische Substanz?

Mantraartig wird bei jeder Pressekonferenz der Begriff “strategische Autonomie” bemüht. Gemeint ist damit nichts anderes als die Fähigkeit, Schlüsseltechnologien unabhängig von Drittstaaten zu entwickeln und zu betreiben. Klingt nach digitaler Selbstbestimmung, ist aber in der Praxis oft Wunschdenken. Woran liegt das? An den Lieferketten, am fehlenden Zugang zu Halbleitern, an der Abhängigkeit von US-Clouds, an fehlenden eigenen Standards – und, ganz ehrlich, am Know-how-Defizit bei echten Cutting-Edge-Technologien.

Die Projekte der Cyberagentur sind ein Spiegel dieser Misere. Ob KI-gestützte Angriffserkennung, Post-Quantum-Verschlüsselung oder autonome Security-Automation – die meisten Entwicklungen greifen auf existierende Frameworks aus den USA oder Asien zurück. Eigene Standards? Selten. Eigene Hardware? Noch seltener. Von “Autonomie” bleibt oft nur die Illusion, am Ende doch unabhängig zu sein, solange man die Komponenten zumindest selbst zusammenbauen darf.

Das hat direkte Auswirkungen auf die Cybersicherheit kritischer Infrastrukturen und staatlicher Systeme. Wer heute glaubt, mit ein paar deutschen Start-ups und Forschungskooperationen die technologische Souveränität zu erreichen, unterschätzt die Komplexität globaler Lieferketten und die Dominanz internationaler Tech-Konzerne. Der Begriff “strategische Autonomie” ist im aktuellen Setting der Cyberagentur mehr PR-Label als reale Zielsetzung – und das ist gefährlich, weil es falsche Sicherheit suggeriert.

Was wäre nötig? Eine echte, eigenständige Technologieentwicklung, mehr Investitionen in Halbleiter, Betriebssysteme, sichere Cloud-Infrastrukturen und vor allem ein radikaler Bruch mit der “Wir kaufen, was wir nicht bauen können”-Mentalität. Solange aber die Cyberagentur an den politischen Leinen hängt, wird aus dem Buzzword selten Substanz.

Projektportfolio, Transparenz & Entscheidungswege: Zwischen Fortschritt und Blackbox

Wer sich das Projektportfolio der Cyberagentur ansieht, stößt auf eine bunte Palette: KI zum Schutz kritischer Infrastrukturen, Post-Quantum-Kryptografie, automatisierte Angriffsabwehr, Prototypen für sichere Kommunikationsnetze. Klingt nach Fortschritt, ist aber oft Proof-of-Concept und selten marktreif. Das Problem: Es fehlt an Transparenz, welche Projekte tatsächlich realen Impact haben, wie die Auswahlprozesse ablaufen und nach welchen Kriterien gefördert wird.

Die Entscheidungswege sind ein Lehrstück deutscher Verwaltungskunst. Ein Innovationsantrag wandert durch mehrere Gremien, wird bewertet, priorisiert, erneut evaluiert und vielleicht irgendwann beauftragt. Wer hier auf Agilität setzt, wird eines Besseren belehrt. Die Folge: Time-to-Market tendiert gegen Null, und disruptive Themen verhungern im Genehmigungsmarathon. Wie viele der Cyberagentur-Projekte haben es bisher in die breite Umsetzung geschafft? Die Bilanz ist ernüchternd.

Auch die Zusammenarbeit mit Wirtschaft und Forschung ist kompliziert. Zwar werden öffentliche Ausschreibungen gemacht, aber der Prozess ist schwerfällig, die Anforderungen oft praxisfern. Viele relevante Player aus der deutschen Tech-Szene sind längst abgewandert oder kooperieren lieber mit internationalen Clustern. Und selbst wenn ein Projekt erfolgreich ist, bleibt die Frage: Wer übernimmt den Transfer in die Fläche? Hier fehlt es an klaren Verantwortlichkeiten, an Technologietransfer-Mechanismen und an echtem Ownership.

Für den Innovationsstandort Deutschland ist das ein Armutszeugnis. Die Cyberagentur muss lernen, Projekte schneller, transparenter und wirkungsorientierter zu steuern. Andernfalls bleibt sie eine teure Blackbox ohne messbaren Mehrwert.

Technische Herausforderungen: Security, KI, Post-Quantum –

und die Lücke zur Wirklichkeit

Im Cyberagentur-Hype liest sich alles wie ein Auszug aus dem Gartner Hype Cycle: KI everywhere, autonome Systeme, Post-Quantum-Security, Offensive Cyber Capabilities. Der Unterschied zwischen Slideware und echter technischer Exzellenz zeigt sich aber beim Blick in die Details. Wo stehen wir wirklich?

Security by Design ist das erklärte Ziel – die Realität sind Proof-of-Concepts mit begrenzter Skalierbarkeit. Viele Projekte kranken daran, dass sie zwar technisch interessant sind, aber entweder nicht den Sprung in die Praxis schaffen oder an regulatorischen Hürden scheitern. Beispiel Post-Quantum-Kryptografie: Der Bedarf ist riesig, die Lösungen sind international längst in Entwicklung, aber die deutsche Beteiligung ist marginal. Die Cyberagentur fördert, aber sie gestaltet nicht federführend.

Im Bereich Künstliche Intelligenz werden Projekte zur Angriffserkennung, automatisierten Verteidigung und Threat Intelligence gefördert. Die Algorithmen stammen meist aus internationalen Open-Source-Projekten oder werden von externen Partnern implementiert. Eigene KI-Kompetenz? Kaum vorhanden. Die Folge: Deutschland bleibt Konsument, nicht Entwickler. Bei offensiven Cyberfähigkeiten bewegt sich die Cyberagentur ohnehin auf politischem Minenfeld – zwischen vager Absichtserklärung und realer Umsetzung klafft eine gewaltige Lücke.

Die technische Realität ist, dass die meisten Projekte zwar Buzzword-kompatibel, aber selten “state of the art” sind. Wer echte Innovation will, muss nicht nur fördern, sondern auch entwickeln, testen, iterieren – und vor allem Fehler zulassen. Das aber ist (noch) nicht Teil der Cyberagentur-DNA.

Schritt-für-Schritt: Was müsste sich ändern, damit die Cyberagentur relevant wird?

Die Cyberagentur steht am Scheideweg: Entweder sie wird zum echten Treiber technologischer Innovation – oder sie bleibt ein teures Experiment mit minimalem Impact. Was müsste passieren? Hier die wichtigsten Schritte, die den Unterschied machen könnten:

- 1. Technisches Know-how radikal erhöhen: Mehr Tech-Experten, weniger Verwaltung. Die Agentur braucht CTOs, Security-Architekten, KI-Forscher – keine Karriere-Beamten.
- 2. Entscheidungswege verkürzen: Weniger Gremien, mehr Ownership. Klare Verantwortlichkeiten, schnelle Go/No-Go-Entscheidungen, agiles Projektmanagement nach DevOps-Standards.
- 3. Transparenz herstellen: Offenlegung der Projekte, der Kriterien und der Roadmaps. Wer fördert was, warum und mit welchem Ziel? Keine Blackbox, sondern messbare KPIs.

- 4. Zusammenarbeit mit der Industrie stärken: Offene Calls, echte Partnerschaften mit deutschen Tech-Firmen, Start-ups und Forschungseinrichtungen. Technologietransfer muss zur Kernaufgabe werden.
- 5. Fehlertoleranz und Iteration zulassen: Innovation braucht Experimente, Scheitern und Lernen. Proof-of-Concepts dürfen nicht in der Schublade verschwinden, sondern müssen skaliert oder eingestellt werden.
- 6. Fokus auf Schlüsseltechnologien: Eigene Initiativen zu Halbleitern, Post-Quantum, souveränen Clouds und Betriebssystemen. Nicht alles fördern, sondern gezielt investieren.
- 7. Monitoring und Impact-Tracking etablieren: Regelmäßige Audits, Impact-Analysen und öffentlich einsehbare Fortschrittsreports. Ohne messbaren Mehrwert bleibt alles bloße Förderung.

Diese Schritte sind kein Hexenwerk, aber sie erfordern Mut zur Veränderung. Wer die Cyberagentur heute nur als politischen Selbstzweck begreift, wird den digitalen Rückstand nicht aufholen. Es geht um nicht weniger als die digitale Zukunft des Landes.

Kritischer Ausblick: Systemfehler oder letzte Chance?

Die Cyberagentur steht exemplarisch für den deutschen Umgang mit Digitalisierung: Viel Anspruch, wenig Umsetzung, noch weniger Mut zu echten Experimenten. Zu viele Stakeholder, zu viele Kompromisse, zu wenig technologische Tiefe. Die Gefahr: Das Projekt verkommt zum nächsten Feigenblatt der Digitalpolitik – teuer, öffentlichkeitswirksam und letztlich irrelevant für die reale Cyberverteidigung.

Doch die Chance bleibt. Mit den richtigen Reformen, einer Fokussierung auf technische Exzellenz und einer neuen Fehlerkultur könnte die Cyberagentur tatsächlich zum Gamechanger werden. Dafür braucht es aber einen radikalen Bruch mit der bisherigen Praxis: Weg von der Verwaltung, hin zu einer echten, agilen Tech-Agentur mit Durchschlagskraft. Sonst bleibt vom großen Cyberversprechen am Ende nur ein weiterer Punkt auf der langen Liste deutscher Digitalprojekte – ambitioniert gestartet, wirkungslos gelandet.

Die Hoffnung stirbt zuletzt, aber sie braucht endlich handfeste Resultate. Die Cyberagentur muss liefern – ohne Ausreden, ohne PR-Gelaber, ohne endlose Abstimmungsrunden. Sonst bleibt sie das, was sie heute ist: ein Kommentar auf dem Weg zum digitalen Nirgendwo.