Die Mission der Cyberagentur in Halle – im Fokus: die Cyberresilliente Gesellschaft

von Dr. Nicole Selzer,
Prof. Dr. Katja Andresen und
Prof. Dr. Christian Hummert *

Abstract
Die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) wurde im Jahr 2020 mit dem Ziel gegründet, innovative high-risk und high-reward Forschung im Bereich der Cybersicherheit und diesbezüglicher Schlüsseltechnologien zu fördern. Ziel der Agentur ist es, die digitale Souveränität Deutschlands und der EU sicherzustellen. Die Cyberagentur verfolgt dabei nicht nur technologische Ansätze, sondern erkennt auch die Bedeutung der Einbettung dieser technologischen Innovationen in ein sozio-technisches Ökosystem an. Der Cluster „Sichere Gesellschaft" befasst sich mit den gesellschaftlichen Aspekten der Cybersicherheit und der Themenschwerpunkt „Cyberresiliente Gesellschaft" insbesondere mit dem menschlichen Faktor von Cybercrime und Cybersicherheit.

The Agentur für Innovation in der Cybersicherheit GmbH – "Innovation for Cybersecurity" (Cyberagentur) was founded in 2020 with the goal to fund innovative, high-risk and high-reward research in cybersecurity and associated scientific research fields. It thus seeks to ensure the digital sovereignty of Germany and the EU. Besides the Cyberagentur's pursuance of technological solutions it also recognizes the importance of embedding these technological innovations into a socio-technical ecosystem. The cluster "secure society" focuses on the societal aspects of cybersecurity and the unit "cyberresilient society" is specifically related to the human factor of cybercrime and cybersecurity.

I. Die Agentur für Innovation in der Cybersicherheit

Die Agentur für Innovation in der Cybersicherheit (kurz Cyberagentur) wurde im Jahr 2020 durch die Bundesregierung gegründet. Sie hat die Aufgabe disruptive Forschungsvorhaben im Bereich der Cybersicherheit zu finanzieren. Dabei nimmt sie einen ressortübergreifenden Blick auf die Innere und Äußere Sicherheit ein. Die Cyberagentur soll des Weiteren Innovationen zu einem sehr frühen Zeitpunkt identifizieren und beauftragen: Sie hat dabei einen Horizont von zehn bis 15 Jahren, was im Bereich der Cybersicherheit sehr lange ist. Die Agentur wurde bewusst nicht als Behörde, sondern als GmbH gegründet, um ihr mehr Freiheiten an die Hand zu geben.

Das Beteiligungsmanagement der vollständigen Inhouse-Gesellschaft des Bundes liegt gemeinsam beim Bundesministeriums der Verteidigung und dem Bundesministeriums des Inneren und für Heimat. Der Sitz der Cyberagentur ist in Halle an der Saale.

Im Rahmen der Strategieentwicklung bis zum März 2022 wurden 15 sogenannte Leitplankenthemen durch die Forscherinnen und Forscher der Cyberagentur identifiziert, die drei thematische Cluster bilden. Das sind:

- Sichere Gesellschaft
- Sichere Systeme und
- Schlüsseltechnologien.[1]

Der Cluster Sichere Gesellschaft soll insbesondere den Blick weg vom reinen IT-System nehmen und den Menschen mehr in das Zentrum der Betrachtung rücken. Es gibt ein Spannungsfeld zwischen IT-Sicherheit und Gesellschaft, das in beide Richtungen wirkt. Neue Technologien können Auswirkungen auf die Gesellschaft haben, wie dies zum Beispiel durch die Einführung von Sozialen Netzwerken erfolgt ist. Auf der anderen Seite hat auch die Gesellschaft durch gesellschaftliche Zwänge oder die gefühlte Sicherheit, Auswirkungen auf die Cybersicherheit. Zu den Leitplankenthemen des Clusters Sichere Gesellschaft zählt die Cyberagentur:

- Cyberbefähigter Staat
- Cyberresiliente Gesellschaft
- Digitale Identitäten
- Digitaler Verbraucherschutz
- Mensch-Maschine-Interaktion

Der Cluster Sichere Systeme befasst sich mit klassischen Fragen der Cybersicherheit, insbesondere mit der Absicherung von IT-Systemen. Dabei ist der Systembegriff bewusst relativ weit gefasst. Das heißt, der Schwerpunkt liegt auf dem Zusammenwirken von Hard- und Software oder dem Einfluss von Lieferketten auf die Systemsicherheit. Systeme sind hier mehr als Systeme von Systemen zu verstehen. Die Schwerpunktthemen die dem Cluster Sichere Systeme zugeordnet sind, lauten:

- Cybersicherheit der (Bundes-)Verwaltung
- Cybersicherheit in schwierigen Umgebungen

* *Prof. Dr. Christian Hummert* ist Forschungsdirektor und Geschäftsführer der Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) in Halle (Saale). *Prof. Dr. Katja Andresen* ist Leiterin der Abteilung „Sichere Gesellschaft" in der Cyberagentur und *Dr. Nicole Selzer* ist Forschungsreferentin in dieser Abteilung.

[1] Strategie der Cyberagentur 2022-2025, online abrufbar unter: https://www.cyberagentur.de/wp-content/uploads/2022/03/20220311-Praesentation-Forschungsstrategie-CA-kurz-fin-1.pdf (zuletzt abgerufen am 22.3.2023).

- Interoperabilität: Digitalisate & Data Fusion
- Sichere Hardware & Lieferketten
- Schutz kritischer Infrastrukturen

Eine weitere Aufgabe der Cyberagentur ist es solche Schlüsseltechnologien zu betrachten, die Auswirkungen auf die Cybersicherheit in zehn bis 15 Jahren haben werden. Hier werden oft intuitiv die Quantentechnologie und der Einsatz von KI als Beispielthemen genannt. Im Bereich der Schlüsseltechnologien werden innerhalb der Cyberagentur die folgenden Themenbereiche adressiert:

- Autonome intelligente Systeme
- Cybersicherheit durch KI & für KI
- Cybersicherheit durch Quantentechnologie
- Kommunikation der Zukunft
- Kryptologie

1. Auftrag

Die Cyberagentur ist mit dem Zweck gegründet worden wagnisbehaftete Forschung und bahnbrechende Innovationen im Bereich der Cybersicherheit und diesbezüglicher Schlüsseltechnologien für die Innere und Äußeren Sicherheit anzustoßen, um einen Beitrag zur technologischen Souveränität Deutschlands im Cyber- und Informationsraum zu leisten. Dabei ist die Cyberagentur selbst keine Forschungseinrichtung, sondern beauftragt Forschung.

Wagnisbehaftete Forschung bedeutet, dass ein hohes, bahnbrechendes Innovationspotenzial besteht, aber auch eine hohe Wahrscheinlichkeit des Scheiterns (high-risk/ high-impact). Es sollen also solche Projekte beauftragt werden, die Schwierigkeiten haben eine Finanzierung auf dem Markt zu finden, die bei Gelingen die Cybersicherheit aber grundlegend ändern würden. Bei solchen Fragen muss der Staat als Mittelgeber einspringen. Dies geschieht analog zu ähnlichen Agenturen im Ausland, wie der US-amerikanischen DARPA, die häufig als Vorbild für die Cyberagentur genannt wird.

Die Mission der Cyberagentur ist:

- Ambitionierte Projekte zu beauftragen und voranzutreiben, die in den nächsten zehn bis 15 Jahren Innovationssprünge für mehr Schutz und Freiheit im Cyber- und Informationsraum versprechen.
- Am Bedarf der Inneren und Äußeren Sicherheit orientiert und eng mit den entsprechenden Bedarfsträgern zusammen zu arbeiten.
- Als treibende Kraft einer offenen Innovations- und Wagniskultur einzustehen und für ein lebendiges Ökosystem zur Förderung von Cybersicherheitstechnologien zu sorgen.

2. Herangehensweise

Die Forschungsstrategie der Cyberagentur enthält die folgenden Grundsätze:[2]

- Die Cyberagentur beauftragt anwendungsbezogene Grundlagenforschung. Das heißt, dass keine Forschungsfragen beantwortet werden, bei denen noch keine mögliche Anwendung für die Sicherheitsbehörden des Bundes ableitbar ist. Wegen des weiten Horizonts finanziert die Cyberagentur Forschung von Technologiereifegrad (TRL)[3] eins bis vier.
- Grundsätzlich identifiziert und beauftragt die Cyberagentur Forschungsvorhaben aus verschiedenen Wissenschaftsdomänen. Es ist die Überzeugung der Agentur, dass wahre Innovation vor allem im Austausch zwischen verschiedenen Disziplinen entsteht.
- Auch wenn die Cyberagentur keine eigene Forschung vorantreibt, sondern als Projektträger agiert, unterhält sie doch eine eigene Beurteilungs- und Evaluationsfähigkeit. Es ist Grundsatz der Forschungsstrategie Forschungsprojekte bei den Auftragnehmern eng zu begleiten und fortlaufend zu evaluieren. Dies ist auch notwendig, um immer wieder Quality Gates zu haben an denen die stark risikobehaftete Forschung abgebrochen werden kann, wenn kein Vertrauen mehr besteht, das Projekt zum Erfolg zu führen.
- Die Cyberagentur hat den Anspruch als Plattform für Wissen und Erfahrungen im Bereich der Cybersicherheit zu agieren. Deshalb wird sie ihr Wissen den Sicherheitsbehörden der Bundesrepublik Deutschland zur Verfügung stellen und darüber hinaus aktiv Ökosysteme im Bereich der Cybersicherheitsforschung unterstützen.
- Grundsätzlich arbeitet die Agentur für Innovation in der Cybersicherheit nachfragegetrieben, das heißt, dass andere Behörden (sogenannte Bedarfsträger) sie beauftragen können spezifische Forschungsprojekte zu finanzieren. Auf der anderen Seite betreibt die Cyberagentur Aufwand im Bereich der Trend- und Szenarioanalysen und kann angebotsorientiert den Sicherheitsbehörden Projekte vorschlagen.
- Die Projektausschreibungen der Cyberagentur sind grundsätzlich offen, dass bedeutet, dass sich Hochschulen, Universitäten, Forschungseinrichtungen, Industrieunternehmen, KMUs oder Startups gleichermaßen auf die Ausschreibungen bewerben können. Dabei agiert die Agentur bewusst Startup freundlich.
- Zur Stärkung der digitalen Souveränität der Bundesrepublik erwirbt die Agentur bei allen Projekten zumindest einen Teil der IP. So kann sie darauf hinwirken, dass die finanzierten Technologien auch in Deutschlang genutzt werden.

[2] Strategie der Cyberagentur 2022-2025 (Fn. 1).

[3] TRL 1: Beobachtung und Beschreibung des Funktionsprinzips, TRL 2: Beschreibung und Anwendung einer Technologie, TRL 3: Nachweis der Funktionstüchtigkeit einer Technologie, TRL 4: Versuchsaufbau im Labor, ISO 16290:2013.

- Die Projektergebnisse werden der Bundesregierung vollumfänglich zur Verfügung gestellt. Bei jedem Projekt wird geprüft, ob die Ergebnisse transparent veröffentlicht werden können, oder ob hier Sicherheitsinteressen berührt werden und die Projekte als Verschlusssache eingestuft werden.

Die Agentur für Innovation in der Cybersicherheit bemüht sich um den Einsatz von innovativen Verfahren in der Vergabe von Forschungsprojekten. Die Beauftragung solcher Projekte kann beispielsweise im Rahmen eines klassischen Vergabeverfahrens erfolgen, als vorkommerzielle Auftragsvergabe (PCP) oder auch als Challenge.[4]

Um den high-risk/high-impact-Gedanken zu gewährleisten, kommen vor allem Beauftragungsverfahren mit wettbewerblichem Aufbau in Frage. Eine Beauftragung mehrerer Auftragnehmer zur Beantwortung der Forschungsfrage reduziert das Risiko, verhindert im Erfolgsfall das Bilden von Monopolen und erhöht die Wahrscheinlichkeit, aus mehreren, konkurrierenden Ansätzen den oder die besten herauszuarbeiten.

Genau für diesen Fall hat die EU-Kommission das Pre-Commercial Procurement (PCP) entwickelt.[5] Hierbei handelt es sich um ein spezifisches Verfahren für die Beschaffung von Forschungs- und Entwicklungsleistungen, dass eine wettbewerbsorientierte Forschung und Entwicklung in Phasen vorsieht. Voraussetzung für das PCP ist die Erfüllung des Ausnahmetatbestandes des § 116 Abs. 1 Nr. 2 GWB sowie ein großes Marktpotential, das heißt, es sind mehrere potenzielle Anbieter verfügbar.

Markus Schaupp und *Prof. Dr. Michael Eßig* haben 2017 die Vor- und Nachteile der vorkommerziellen Auftragsvergabe im Vergleich zur Innovationspartnerschaft beleuchtet und hierbei für das PCP-Verfahren u.a. die folgenden Vorteile herausgestellt:[6]

- Lock-in-Effekte werden vermieden, indem mehrere Teilnehmer an verschiedenen Lösungsentwicklungen forschen, was die Chance erhöht, dass ein Teilnehmer die Problemstellung lösen kann;
- Durch den Wettbewerb zwischen Anbietern unterschiedlicher Lösungsansätze im Forschungs- und Entwicklungsprozess, werden im Vergleich bspw. zur Innovationspartnerschaft wirtschaftlichere und qualitativ hochwertigere Produkte wahrscheinlicher;
- Durch die parallele Bearbeitung wird ein Innovationsimpuls gesetzt, der es zudem ermöglicht ein Ökosystem aus mehreren Akteuren mit entsprechender Expertise zu fördern, die zueinander in einem Qualitätswettbewerb stehen. Hierdurch werden auch monopolistische Lösungen verhindert;
- Das Risiko für Fehlentwicklung ist aufgrund des Wettbewerbs in der Entwicklungsphase geringer, wodurch nicht nur inkrementelle Verbesserungen wahrscheinlich sind, sondern radikale Ansätze und Innovationen möglich werden, die Ziel der Cyberagentur sind;
- Der Zugang für KMUs, die auch als Treiber von Innovationen bezeichnet werden, wird erleichtert (z. B. Vertragsvolumen zu Anfang niedrig, keine strikten Ausschluss- und Eignungskriterien). Zudem können sie in der Projektphase wachsen, sodass sie bei der eigentlichen Beschaffung mit Großunternehmen konkurrieren können;
- Der Anreiz ist höher, das Kosten-Leistungs-Verhältnis im Zuge der späteren kommerziellen Beschaffung weiter zu optimieren;
- Die Beschaffung fällt nicht unter das GPA (Government Procurement Agreement der WTO) und damit können die Teilnehmer dazu angehalten werden, die Leistungen in Europa durchzuführen;
- Die Eigentumsrechte verbleiben (auch) bei den Teilnehmern, wodurch niedrigere Kosten für die Beschaffung zu erwarten sind.

II. Abteilung Sichere Gesellschaft

Die fünf Leitplankenthemen im Cluster Sichere Gesellschaft werden organisatorisch in einer von drei Forschungsabteilungen bearbeitet. Informationssysteme als sozio-technische Systeme werden in den kommenden Jahren einen weiteren technologischen Wandel erfahren. Die Komplexität in der Architektur wird steigen ebenso der Grad der Vernetzung im Cyberraum. Der Cyberraum ist dabei einerseits ein entscheidender Faktor für Innovationen und bestimmend für das wirtschaftliche Handeln, aber eben auch Ausgangspunkt für bekannte und neuartige Bedrohungen, die das gesellschaftliche Leben massiv gefährden können. Eine sichere Gesellschaft ist dann auch eine digitale Gesellschaft, die sich über die Abwesenheit von Cyberterror und Cyberwar als „sicher“ definiert.

Die Zielstellung der Abteilung besteht darin, die digitale Gesellschaft vor dem Hintergrund der beispiellosen Transformation und wachsender (globaler) Abhängigkeiten und hybrider Bedrohungen in ihrer digitalen Souveränität zu stärken, somit ein selbstbestimmtes, sicheres Handeln im Cyberraum zu fördern.

III. Themenschwerpunkt Cyberresiliente Gesellschaft

Angesichts der zunehmenden Vernetzung und Digitalisierung unserer Welt sind bereits heute Cyberangriffe eine wachsende Bedrohung für Gesellschaft, Wirtschaft und

[4] Ausschreibungen online abrufbar unter: https://www.cyberagentur.de/ausschreibungen/ (zuletzt abgerufen am 22.3.2023).

[5] COM(2007) 799 final, 14.12.2007 (PCP Communication); e-Commercial Procurement, Shaping Europe’s digital future (europa.eu), online abrufbar unter: https://digital-strategy.ec.europa.eu/en/policies/pre-commercial-procurement (zuletzt abgerufen am 22.3.2023); Toolkit - European Assistance for Innovation Procurement – eafip, online abrufbar unter: https://eafip.eu/toolkit/ (zuletzt abgerufen am 22.3.2023).

[6] Vgl. *Schaupp/Eßig*, Vorkommerzielle Auftragsvergabe vs. Innovationspartnerschaft, 2017, S. 23 f.

den Staat als Ganzes. Es ist daher ein Verständnis für die Bedeutung der Cybersicherheit und die Bereitschaft erforderlich, in die notwendige Ausbildung, die notwendigen Ressourcen und Technologien zu investieren, um die Widerstandsfähigkeit gegenüber Cyberbedrohungen zu stärken. Nur durch eine proaktive und ganzheitliche Herangehensweise können wir uns gegen die wachsende Bedrohung durch Cyberangriffe wappnen und eine zukunftsfähige, resiliente Gesellschaft aufbauen.

In puncto Cybercrime und Cybersecurity zählt dabei nicht nur die technologische Perspektive, sondern auch der menschliche Faktor, rechtliche Rahmenbedingungen und Wertevorstellungen. Aufgrund dessen beschäftigt sich die Cyberagentur im Themenschwerpunkt „Cyberresiliente Gesellschaft“ mit kriminologischen, rechtlichen und ethischen Fragestellungen. Diese Perspektive ist wichtig, um sicherzustellen, dass die Entwicklung von Technologien im Einklang mit den Interessen der Gesellschaft erfolgt und die Cyberresilienz angesichts des rasanten technologischen Fortschritts gestärkt wird. Cyberresilienz im Kontext der Cyberagentur meint, die Stärkung der Widerstandsfähigkeit der Gesellschaft gegenüber Cyberbedrohungen der Zukunft. Ziel ist es, die Gesellschaft derart zu wappnen, dass sie in der Lage ist sich gegen künftige Formen von Cybercrime zu schützen, Risiken zu antizipieren und geeignete Maßnahmen zu ergreifen, um Angriffen vorzubeugen, diese abzuwehren oder im Worst Case schnell auf Cyberangriffe reagieren zu können, den Betrieb aufrechtzuerhalten, Systeme wiederherzustellen und Schäden zu minimieren.

Eine cyberresiliente Gesellschaft erfordert die Zusammenarbeit verschiedener Akteure – auf gesellschaftlicher, wirtschaftlicher und staatlicher Ebene. Um das Themenfeld entsprechend aufzubauen, über Forschungsvorhaben und Abläufe zu informieren, die Community zu erweitern und Forschungslücken zu identifizieren, werden derzeit Interviews mit Wissenschaftlerinnen und Wissenschaftlern, Vertreterinnen und Vertretern von Strafverfolgungsbehörden und Unternehmen geführt. Neben Literaturrecherchen und der Teilnahme an relevanten Konferenzen, richtet die Cyberagentur vom 10. bis 13. September 2023 auch zwei Veranstaltungen – die Human Factor in Cybercrime Conference[7] und das Network-Event { Cyber : Crime || Security || Society }[8] – aus, um dem notwendigen Community-Building in diesem Bereich Rechnung zu tragen.[9] Idealerweise führt diese Vernetzung zu künftigen Kooperationen bei Ausschreibungen der Cyberagentur. Die anvisierten Forschungsprojekte im Themenfeld „Cyberresiliente Gesellschaft“ zielen darauf ab, die kriminologische Cybersicherheitsforschung zu stärken, um den Bedarf des Gesetzgebers zu antizipieren, Handlungsoptionen zu entwerfen, die Strafverfolgungsbehörden zu wappnen und Maßnahmen zur Unterstützung der Cybersicherheit und Cyberresilienz der Gesellschaft zu entwickeln und zur Bekämpfung zukünftiger Formen von Cyberkriminalität beizutragen. Im Sommer 2023 ist eine erste Ausschreibung in diesem Themenschwerpunkt anvisiert.

7 www.hfc-conference.com.
8 https://www.cyberagentur.de/cyber-css/.
9 Siehe hierzu tiefergehend *Selzer*, Kriminalistik 4/2023.