Cyberresiliente Gesellschaft – Untersuchung des menschlichen Faktors im Cyberraum

Petra Welscher, Joline Wochnik, Fabian Schrumpf und Nicole Selzer

Gliederung

1. Die Cyberagentur

Cybersicherheit als Pfeiler für die digitale Souveränität von Übermorgen?

Auftrag der Agentur für Innovation in der Cybersicherheit GmbH (kurz: Cyberagentur) ist das Vorantreiben von disruptiver Forschung im Bereich der Cybersicherheit und diesbezüglicher Schlüsseltechnologien mit einem zukunftsgerichteten Zeithorizont von 10-15 Jahren. Die Cyberagentur wurde 2020 als GmbH des Bundes mit dem Ziel gegründet, zur digitalen Souveränität Deutschlands beizutragen und die innere und äußere Sicherheit Deutschlands zu stärken.

Um dieses Ziel zu erreichen, wird disruptive Forschung identifiziert, finanziert und evaluiert. Dabei steht allem voran die Bereitschaft der Cyberagentur, als Auftraggeberin bei Forschungsaufträgen ein hohes Risiko des Scheiterns zu akzeptieren. Gesellschafterin der Cyberagentur ist die Bundesrepublik Deutschland, welche durch das Verteidigungsministerium sowie das Innenministerium vertreten wird. Daher legt die Cyberagentur ihren Forschungsfokus auf die zukünftigen Bedarfe derjenigen, die tagtäglich für die innere und äußere Sicherheit arbeiten. Dazu zählen unter anderem Behörden und Organisationen mit Sicherheitsaufgaben, Bundeswehr und Nachrichtendienste.

In ihrer Rolle als Auftraggeberin vergibt die Cyberagentur cybersicherheitsbezogene Forschungsvorhaben in der anwendungsorientierten Grundlagenforschung (Technologiereifegrad 1-4). Die Cyberagentur schaut mit einem holistischen Blick auf das Thema der Cybersicherheit, was sich in den Themenschwerpunkten der derzeit drei Abteilungen – Schlüsseltechnologien, Sichere Systeme, Sichere Gesellschaft – widerspiegelt. Zu den *Schlüsseltechnologien* zählen u. a. Kryptologie, Quantencomputing, Künstliche Intelligenz und Autonome Intelligente Systeme. Bei den *Sicheren Systemen* sind u. a. Cybersicherheit in der Bundesverwaltung, Schutz kritischer Infrastrukturen, Cybersicherheit in schwierigen Umgebungen und Sichere Hardware und Lieferketten verortet. Zur *Sicheren Gesellschaft*, zählen u. a. Digitale Identitäten, Mensch-Maschine-Interaktion, der Cyberbefähigte Staat sowie die Cyberresiliente Gesellschaft. Thematisch werden die Aktivitäten der Cyberagentur vom internen Innovations- und Wissensmanagement durch kontinuierliche Trend- und Szenarioanalysen mitbestimmt.

So will die Cyberagentur durch die Vergabe disruptiver Forschungsprojekte einen maßgeblichen Beitrag zur technologischen Souveränität Deutschlands im Cyber- und Informationsraum leisten.

2. Der Themenschwerpunkt „Cyberresiliente Gesellschaft“

Die „Cyberresiliente Gesellschaft“ ist als einer von fünf Themenschwerpunkten in der Abteilung *Sichere Gesellschaft* angesiedelt. Im Gegensatz zu der in der Forschungslandschaft häufig anzutreffenden technischen Fokussierung, legt der Themenschwerpunkt besonderes Augenmerk auf den menschlichen Faktor der Cybersicherheit. Dabei wird der Mensch als Einzelwesen sowie auch die Gesellschaft als Ganzes adressiert. Kernaspekte der vorangetriebenen Programme sind daher die (soziotechnische) Cyberresilienz, Cybersicherheit, Cyberkriminalität, Desinformation und digitale Befähigung.

Die Konzeption der Programme erfolgt dabei bedarfsträgerorientiert. So werden zukünftig gesehene Bedarfe bereits im Vorfeld von Behörden und weiteren Bedarfsträgern der Cyberagentur an diese herangetragen und bilden die Grundlage von Programmideen. Auf diese Weise sollen gesetzgeberische Bedarfe antizipiert und Handlungsoptionen für Strafverfolgungsbehörden und die Bundeswehr entworfen werden. Zur Konkretisierung der Ideen werden

Literaturrecherchen durchgeführt und Expertinnen und Experten auf dem entsprechenden Gebiet interviewt.

Die entwickelten Empfehlungen, welche aus den Programmen des Themenschwerpunktes „Cyberresiliente Gesellschaft" resultieren, können beispielsweise Maßnahmen zur Unterstützung der Cybersicherheit und zur Bekämpfung von Cyberkriminalität betreffen.

Mit den Programmen verfolgt der Themenschwerpunkt die Zielrichtung, disruptive Grundlagenforschung voranzutreiben sowie die gesamtgesellschaftliche Cyberresilienz zu stärken.

3. Projektvergabe

Die Cyberagentur nutzt zur Vergabe von Forschungsprojekten neben klassischen Vergabeverfahren zu großen Teilen innovative Verfahren, welche meist einen wettbewerblichen Charakter aufweisen. So werden Programme oft als vorkommerzielle Auftragsvergaben (PCP) ausgeschrieben. Bei PCP handelt es sich um ein spezifisches, durch die EU-Kommission entwickeltes, Verfahren für die Beschaffung von Forschungs- und Entwicklungsleistungen, das eine wettbewerbsorientierte Forschung und Entwicklung in Phasen vorsieht.[1]

Das PCP-Verfahren kann durch den jeweiligen Auftraggeber individuell konzipiert werden. Für die Cyberagentur hat sich folgender Verfahrensablauf bewährt: Zunächst reichen interessierte Forscherinnen und Forscher bzw. Forschungsverbünde Konzepte ein. Anhand von Bestenauslese wird anschließend bestimmt, welcher bzw. welche Forschungsverbünde ihre Konzepte als konkrete Projekte umsetzen können. Die Programme der Cyberagentur werden immer deutschlandweit auf der Vergabeplattform des Bundes (www.evergabe-online.de) veröffentlicht. Bei oberschwelligen Verfahren erfolgt die Ausschreibung zusätzlich auf der europäischen Vergabeplattform TED (www.ted.europa.eu). Der Wert, ab dem ein Verfahren als oberschwellig gilt, liegt momentan bei 221.000 €.

---

[1] *Selzer et al.* (2023), S. 91.

4. Aktuelle Programme

Zum derzeitigen Stand (Q4 2024) hat der Themenschwerpunkt „Cyberresiliente Gesellschaft" drei Programme ausgeschrieben. Weitere Programme sind in Planung. Bei den Programmen handelt es sich jeweils, dem Scope der Cyberagentur entsprechend, um Grundlagenforschung mit einem Planungshorizont von 10-15 Jahren.

4.1 Zukünftige Cyberkriminalität

Das Programm „Zukünftige Cyberkriminalität" (Abk.: zCK) setzt sich aus den zwei Teilprogrammen „Mustererkennung und -analyse" und „Zukunftsanalyse" zusammen.

Im ersten Teilprogramm sollen Muster hinsichtlich der Angriffsziele, -weise und -durchführung von Cyberkriminalität identifiziert und analysiert werden. Dabei sollen nicht nur technische Muster, sondern insbesondere auch solche Strukturen betrachtet werden, die auf kulturellen und strukturellen Bedingungen beruhen.

Kulturelle und strukturelle Bedingen, welche soziale, wie auch technische Aspekte einbeziehen können, finden sich z. B. in der Akzeptanz neuartiger Technologien, dem Cybersicherheitsgefühl, der Angst vor Cyberkriminalität, aber auch dem technologischen Entwicklungsstand und Verbreitungsgrad, dem Ausprägungsgrad des Cybersicherheitsniveaus sowie dem Ausbildungsstand bezüglich Cyberhygiene wieder. Weitere relevante Bedingungen können rechtliche Rahmenbedingungen, Sprache und Kulturdimensionen, beispielweise nach *Hofstede*[2] (Machtdistanz, Unsicherheitsvermeidung, etc.) sein.

Das Erkennen und Analysieren der Muster soll es ermöglichen, frühzeitig globale Entwicklungen der Cyberkriminalität zu erkennen und Vorhersagen zu treffen, wann bestimmte Erscheinungsformen von anderen Staaten auf Deutschland und Europa übergreifen. Auf diese Weise soll ein Frühwarnradar für Cyberkriminalität erforscht werden.

Das zweite Teilprogramm hat eine Zukunftsanalyse zum Gegenstand. Hier sollen solche Technologien identifiziert werden, welche die Cyberkriminalität in den nächsten 10-15 Jahren voraussichtlich beeinflussen werden. So sollen empirisch fundierte Vorhersagen in Bezug auf die mögliche Entwicklung der

---

[2] *Hofstede* (2001).

Cyberkriminalität getroffen werden. Ein weiteres Ziel dieses Teilprogrammes ist es, neben dynamischen Faktoren auch etwaige stabile Faktoren zu identifizieren, d. h. solche Bedingungen zu erkennen, die trotz der schnellen Veränderungen der Technologien und der Cyberkriminalität über die Zeit voraussichtlich konstant bleiben. Die Zukunftsanalyse soll neben der Berücksichtigung technischer Faktoren ebenfalls besonderen Fokus auf kulturelle und strukturelle Bedingungen in Deutschland legen.

Das Programm zCK wurde am 19. Februar 2024 als PCP-Verfahren ausgeschrieben. Gegenwärtig arbeiten pro Teilprogramm jeweils drei Forschungsverbünde ein Langkonzept aus, welches bis zum 28. Februar 2025 einzureichen ist. Im Anschluss an die Evaluation wird pro Teilprogramm jeweils eine Auftragnehmerin bzw. ein Auftragnehmer ausgewählt, welche bzw. welcher das Langkonzept umsetzen wird. Für das Teilprogramm 1 stehen der Auftragnehmerin bzw. dem Auftragnehmer 36 Monate zur Verfügung. Im Teilprogramm 2 erfolgt die Umsetzung in 24 Monaten.

4.2 Schäden durch Cyberkriminalität

Die Annehmlichkeiten, welche die digitale Welt der Gesellschaft, der Wirtschaft und dem Staat bietet, nehmen mit steigender Konnektivität zu. Neben diesen Annehmlichkeiten steigen damit einhergehend allerdings auch die Gefahren sowie das Ausmaß potenzieller Schäden.

Ziel des Forschungsvorhabens „Schäden durch Cyberkriminalität“ (Abk.: SCK) ist die Entwicklung eines Modells, das Metriken und Methodiken vereint, um ganzheitlich materielle wie immaterielle Schäden der Cyberkriminalität zu erfassen. Ganzheitlich bedeutet in diesem Kontext, die möglichst vollständige, umfassende und vorausschauende Betrachtung des Schadensbildes der einzelnen Erscheinungsformen durch Cyberkriminalität anhand möglichst vieler Einzelaspekte und Zusammenhänge. Das Modell soll systematisch, reproduzierbar und überprüfbar die verschiedenen Arten und das Ausmaß von Schäden durch Cyberkriminalität kurz-, mittel-, und langfristig sowie Kaskadeneffekte empirisch erfassen und robust gegenüber Veränderungen der Kriminalitätslandschaft sein, um zukünftige Formen von Cyberkriminalität frühzeitig bewerten zu können. Der Fokus des Programmes liegt auf Auswirkungen der Cyberkriminalität in Deutschland unter der möglichen Referenz anderer Länder.

Die Ergebnisse des Programmes sollen verwendet werden, um das Cybersicherheitsniveau samt Veränderungen und Entwicklungen der Bundesrepublik Deutschland präzise einschätzen zu können und so eine strategische Ausrichtung von Cybersicherheitsmaßnahmen, ggf. die Priorisierung bestehender und die Initiierung neuer Maßnahmen sowie die effiziente Allokation von Ressourcen zu ermöglichen.

Ausschreibungsstart des Programmes SCK war der 26. Juni 2024. Derzeit erstellen die Teilnehmenden Kurzkonzepte für ihr potenzielles SCK-Projekt. Nach Abgabe und Evaluation dieser Kurzkonzepte erstellen die drei am besten bewerteten Teilnehmenden ein detaillierteres Langkonzept. Anschließend bekommt einer der Teilnehmenden die Möglichkeit das ausgearbeitete Konzept innerhalb von 42 Monaten umzusetzen.

4.3 VeNIM

Digitale Multimediainhalte werden täglich auf Webseiten, Blogs und auf sozialen Medien geteilt. Das Erkennen der Integrität und Authentizität der rezipierten Inhalte sowie deren Grad der Veränderung und Manipulation stellt für die meisten Nutzerinnen und Nutzer eine große Herausforderung dar.

Das Programm „Umsetzung eines Vertrauenskonzepts für eine nachhaltige Informations- und Medienarchitektur“ (Abk.: VeNIM) nimmt sich genau dieser Herausforderung an. Leistungsgegenstand ist ein Konzeptpapier, welches die Beschreibung einer holistischen Vertrauensarchitektur für Multimediainhalte (Audio, Bild, Video und Text) sowie umsetzbare Empfehlungen zur Realisierung dieser bietet.

Es sollen grundlegende Fragen zur Ausgestaltung sowie den Anforderungen einer solchen Architektur beantwortet werden. Diese soll es ermöglichen, die Integrität, Authentizität sowie die Urheberschaft von Multimediainhalten verschiedenster Art zu prüfen und nachzuvollziehen. Im Zentrum des Programmes steht dabei die Frage, wie eine skalierbare, generische Architektur gestaltet sein muss, die die zuverlässige Überprüfung und Nachverfolgung der Authentizität, Integrität und Urheberschaft multimedialer Inhalte erlaubt und dabei gleichzeitig durch niedrige Einstiegshürden für Nutzerinnen und Nutzer ohne umfassende technische Kenntnisse einfach nutzbar ist sowie Personen mit berechtigtem Interesse an Anonymität wirksam schützt.

Für das Unterschwellenprogramm VeNIM wurde im Wege der Bestenauslese ein Projektentwurf ausgewählt und am 12. August 2024 beauftragt. Die

Fertigstellung des Konzeptpapiers ist für Mitte Dezember geplant. Die Erkenntnisse aus VeNIM sollen in ein folgendes Forschungsprogramm zur Realisierung einer Vertrauensarchitektur für Medieninhalte einfließen.

5. Ausblick

Die Bereiche, mit denen sich der Themenschwerpunkt „Cyberresiliente Gesellschaft" befasst, verändern sich einhergehend mit der Schnelligkeit der technologischen Entwicklungen sehr dynamisch. Auf Grund dessen sind wir bemüht stets neue Forschungslücken in den vielseitigen Bereichen der Cyberresilienz, Cybersicherheit, Cyberkriminalität sowie Desinformation zu identifizieren. Um diese Lücken frühzeitig schließen zu können und damit die Gesellschaft sowie die Bedarfsträger der Cyberagentur gegen zukünftige Bedrohungen besser aufzustellen, arbeiten wir mit Nachdruck an neuen Ideen und sind immer an einem Austausch mit der Forschungslandschaft über zukünftige Entwicklungen und Forschungslücken interessiert.

Literatur

Hofstede, G. (2001): Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. Thousand Oaks: Sage.

Selzer, N./Andresen, K./Hummert, C. (2023): Die Mission der Cyberagentur in Halle – im Fokus: die Cyberresiliente Gesellschaft. KriPoZ, 23(2), S. 89-92.