Zimmermann, Verena; Haunschild, Jasmin; Unden, Marita; Gerber, Paul; Gerber, Nina

Sicherheitsherausforderungen für Smart-City-Infrastrukturen

Wirtschaftsinformatik & Management

Provided in Cooperation with:
Springer Nature

Suggested Citation: Zimmermann, Verena; Haunschild, Jasmin; Unden, Marita; Gerber, Paul; Gerber, Nina (2022) : Sicherheitsherausforderungen für Smart-City-Infrastrukturen, Wirtschaftsinformatik & Management, ISSN 1867-5913, Springer Fachmedien Wiesbaden GmbH, Wiesbaden, Vol. 14, Iss. 2, pp. 119-126, https://doi.org/10.1365/s35764-022-00396-5

Sicherheitsherausforderungen für Smart-City-Infrastrukturen

Viele Städte entwickeln sich hin zu einer „Smart City“. Der Trend birgt einerseits vielfältige Potenziale für Effizienz, Nachhaltigkeit und Sicherheit. Auf der anderen Seite ergeben sich neue Herausforderungen für den Schutz städtischer Infrastrukturen und der darin befindlichen Daten vor Ausfällen und (Cyber-)Angriffen, die in ihrer Komplexität bisher nur wenig untersucht sind.

Verena Zimmermann, Jasmin Haunschild, Marita Unden, Paul Gerber und Nina Gerber

Wirtschaftsinformatik & Management 2022 • 14 (2): 119–126
https://doi.org/10.1365/s35764-022-00396-5
Angenommen: 14. Januar 2022
Online publiziert: 23. März 2022

Verena Zimmermann[1] (✉)
verena.zimmermann@tu-darmstadt.de

Jasmin Haunschild[2]
haunschild@peasec.tu-darmstadt.de

Marita Unden[1]
marita.unden@tu-darmstadt.de

Paul Gerber[1]
paul.gerber@tu-darmstadt.de

Das Konzept der Smart City wird von der Grundidee geleitet „Kommunen funktionsfähig zu halten und durch den Einsatz von Technik effizienter und nachhaltiger zu machen“ [6, S. 4, 1]. Das Smart-City-Konzept birgt eine Reihe von Potenzialen und Möglichkeiten für neue Services: Zum einen kann die Digitalisierung als Reaktion auf wachsende Strukturen und Datenmengen in städtischen Infrastrukturen betrachtet werden, die von Einzelpersonen nicht mehr manuell zu verarbeiten sind. Zusätzlich bieten Smart-City-Dienstleistungen wie z. B. digitale Bürgerservices [3] und intelligente Parkplatzlokalisation [4] Vorteile in Bezug auf Effizienz, Nachhaltigkeit und Komfort. Durch den Einsatz von Sensoren können Anomalien oder Gefahren frühzeitig erkannt und Rettungskräfte durch vernetzte Kommunikationstechnologien effizient zur Steigerung der öffentlichen Sicherheit beitragen.

Auf der anderen Seite birgt die Entwicklung hin zu Smart Cities auch ungelöste Herausforderungen: Die Erhebung und Verknüpfung von Daten führt nicht nur zu Vorteilen für die Nutzenden, sondern auch zu relevanten Debatten um Datenschutz und das Recht auf informationelle Selbstbestimmung. Die Digitalisierung von Daten kritischer Infrastrukturen birgt zudem neue Angriffs- und Ausfallpotenziale.

Cyberangriffe auf digitalisierte Infrastrukturen oder technische Probleme können zu gravierenden Einschränkungen der Versorgung mit lebenswichtigen Gütern oder der öffentlichen Sicherheit führen [7]. Die Einbindung einer großen Anzahl von Infrastrukturen, Organisationen und Informationen führt außerdem zu einer Vielzahl von Stakeholdern mit unterschiedlichen Interessen. Diese reichen von Politik und Verwaltung über die Betreibenden kritischer Infrastrukturen bis hin zu den Bürger:innen, die Informationen über technische Geräte liefern oder städtische Angebote nutzen.

Um nachhaltige und sichere Lösungen für Smart Cities zu entwickeln, sollte daher die Komplexität der Smart City ganzheitlich betrachtet und alle städtischen Stakeholdergruppen mit ihren unterschiedlichen Anforderungen an (Cyber-)Sicherheit einbezogen werden. Ganzheitliche Untersuchungen dieser zunehmenden Verknüpfungen zwischen Infrastrukturen und Stakeholdern sind bisher rar bei gleichzeitig steigender Relevanz für die Gestaltung von städtischen Infrastrukturen und Prozessen, die zukünftig Bestandteil von Smart Cities sein werden [7]. Ziel dieser Untersuchung war es daher, zunächst sicherheitskritische Szenarien im Smart-City-Kontext, offene Herausforderungen und mögliche Lösungsansätze zu identifizieren. Ein besonderes Augenmerk lag dabei auf der Interaktion verschiedener Stakeholdergruppen und Infrastrukturen sowie auf den Wechselwirkungen der Sicherheitskonzepte Betriebssicherheit/Unfallsicherheit (Safety) und Angriffssicherheit (Security).

Methodischer Ansatz

Zur Exploration von sicherheitskritischen Szenarien im Smart-City-Kontext wurde eine Kombination aus vorwiegend quantitativer Expert:innenbefragung und qualitativen Interviews gewählt. Für beide me-

Nina Gerber[1]
nina.gerber@tu-darmstadt.de

[1]*Forschungsgruppe Arbeits- und Ingenieurpsychologie (FAI), Institut für Psychologie, Technische Universität Darmstadt, Darmstadt, Deutschland*

[2]*Wissenschaft und Technik für Frieden und Sicherheit (PEASEC), Fachbereich Informatik, Technische Universität Darmstadt, Darmstadt, Deutschland*

Zusammenfassung

- Trend der Digitalisierung städtischer Infrastrukturen hin zu Smart Cities
- Großes Potenzial von Smart Cities für Effizienz, Komfort, Nachhaltigkeit und Sicherheit
- Herausforderungen für Datenschutz und Sicherheit bei Unfällen (Safety) sowie Angriffsfällen (Security)

thodischen Ansätze wurden Vertreter:innen verschiedener Stakeholdergruppen im Smart-City-Kontext rekrutiert. Dazu gehörten:

- Expert:innen für Stadtentwicklung und Digitalisierung (z. B. Digitalstadt Darmstadt)
- Betreibende sicherheitskritischer Infrastrukturen (z. B. Stromnetzbetreibende, Verkehrsverbände),
- Expert:innen für Safety und Security (z. B. Polizei, Feuerwehr, Fachleute für Cybersicherheit)
- Expert:innen für Recht und Datenschutz (z. B. Rechtswissenschaftler:innen)
- Bürger:innenvertretung (z. B. Politik, Stiftungen, Vereine)

Expert:innenbefragung

Die Onlinebefragung umfasste $N = 31$ Expert:innen, die sich wie folgt auf verschiedene Stakeholdergruppen verteilten: Safety und Security: 15 (48 %); Infrastrukturbetreibende: 7 (23 %); Stadtentwicklung und städtische Digitalisierung: 7 (23 %), Bürger:innenvertretung: 2 (6 %).

Die Expert:innen sahen die Gründe für einen Ausfall in erster Linie in Safety-Beeinträchtigungen wie technischem Versagen, Fehlern und Unfällen, organisatorischen Problemen sowie Naturereignissen. Erst darauf folgten Securityaspekte, besonders Cyberangriffe aus dem In- oder Ausland und Cyberkriminalität. Physische Angriffe durch Krieg und Terrorismus oder betriebsinterne Sabotage wurden dagegen als irrelevant eingeschätzt (siehe **Abb. 1**). Als attraktive Ziele wurden dabei besonders Behörden und Verwaltung, gefolgt von kritischen Infrastrukturen gesehen, erst darauf folgten Unternehmen oder Einzelpersonen. Kriminelle Netzwerke und Geheimdienste anderer Staaten werden für wahrscheinliche Angreifergruppen gehalten, gefolgt von Hacktivist:innen und individuell handelnden Kriminellen. Ausländische Militäreinheiten oder terroristische Gruppen werden dagegen als irrelevant eingeschätzt. Es fiel auf, dass Expert:innen für Stadtentwicklung und städtische Digitalisierung Hacktivismus für deutlich relevanter hielten.

Als Motivation für einen Angriff wurde besonders finanzieller Gewinn, die Ausspähung vertraulicher Informationen sowie politische Beweggründe gesehen. Über alle Fragen hinweg wichen die Expert:innen für Bürger:innenvertretung in ihren Einschätzungen von den anderen Gruppen ab. Da diese Gruppe nur durch zwei Personen vertreten wurde, kann dieser Befund nur als Hinweis für weitere Forschung gedeutet werden.

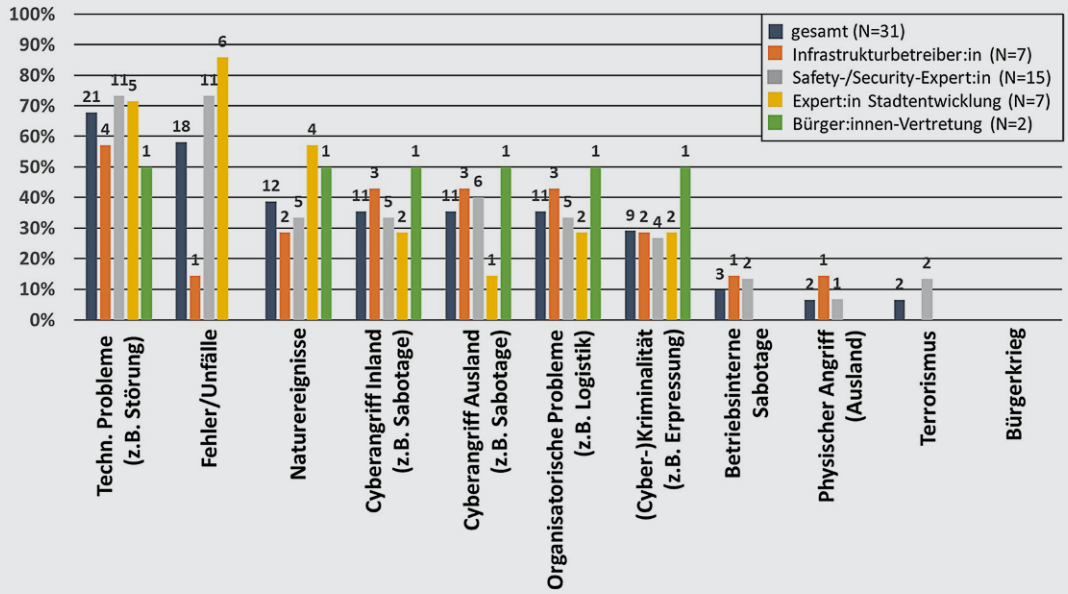
Expert:inneninterviews

In einem zweiten Schritt wurden sieben Interviews mit zehn freiwilligen Expert:innen aus der Stichprobe der Befragung geführt. Daraus werden exemplarisch drei sicherheitsrelevante Szenarien mitsamt der skizzierten Herausforderungen und Lösungsansätze beschrieben. Diese wurden aus der Basis der Interviews gewählt, da sie verschiedene Themenbereiche abdecken und zusätzlich Interaktionen zwischen Infrastrukturen bzw. Stakeholdern adressieren.

Szenario 1: Smart Grids und die Rolle des „Prosumers“

In einem Interview mit einem Stromnetzexperten wurden die zunehmende Digitalisierung von Stromnetzen und daraus resultierende Chancen und Herausforderungen thematisiert.

Abb. 1 Einschätzung der Gründe für einen Infrastrukturausfall in % nach Stakeholdergruppe (y-Achse), absolute Werte oberhalb der Balken (x-Achse), Mehrfachnennung möglich



Beschreibung. Die schwierige Speicherung von Strom hat zur Folge, dass zu jedem Zeitpunkt genau die Menge an Strom produziert werden muss, die aktuell von den Verbrauchern benötigt wird. Dabei müssen Erzeugung und Verbrauch in einer kontinuierlichen Balance gehalten werden, um Über- oder Unterbelastungen von Teilen des Stromnetzes zu vermeiden. Sogenannte Smart Grids nutzen dafür eine intelligente Vernetzung und Steuerung [5].

Dies ist aus Sicht des Experten notwendig: *„Wir gehen hin zu immer kleineren, weit verteilten Energiequellen, Solaranlagen auf den Dächern von Privathäusern, Windparks und Ähnliches und die werden natürlich, damit man die kontrollieren kann, eben auch immer stärker digitalisiert, […] das kann man als Mensch nicht mehr handeln, das heißt, ich brauche digitalen Support"*.

Neben einer optimierten Energienutzung vereinfacht dies auch die Einbindung von „Prosumern". Ehemals passive Konsument:innen haben vermehrt die Möglichkeit, z. B. über Solaranlagen selbst produzierten Strom ins Netz einzuspeisen oder zukünftig über smarte Haushaltsgeräte zielgerichtet zu verbrauchen, um eine erhöhte Nachfrage zu decken oder Energiespitzen abzubauen.

Herausforderungen. Damit gehen aber auch Herausforderungen einher: Der Experte schilderte, dass mit dem Stromnetz eine lange gewachsene, weit verzweigte und teils ungeschützte physische Infrastruktur, z. B. bestehend aus Strommasten und Leitungen, digitalisiert wird. Die Digitalisierung selbst bietet zudem die Möglichkeit von Cyberangriffen auf Stromnetze: *„wenn ich digitalen Support habe, habe ich eine Schnittstelle für Cyberangriffe"*. Als Beispiele nannte der Experte einen Cyberangriff auf das Stromnetz der Ukraine 2015 [2] sowie die zukünftige Möglichkeit z. B. durch Zugriff auf Ladestationen von Elektroautos eine Netzüberlastung herbeizuführen.

Ein großflächiger Stromausfall kann verheerende Konsequenzen durch eine *„kaskadierende Wirkung über die Infrastrukturen hinweg"* haben. So könnte durch einen Stromausfall auch die Versorgung mit Wasser, Nahrung und medizinischen Hilfsmitteln lebensbedrohlich beeinträchtigt sein. Nach Ansicht des Experten ist es dabei weniger entscheidend, ob der Ausfall durch einen Unfall oder einen Angriff ausgelöst wurde. *„Der wichtige Teil passiert danach"*, weil *„die Konsequenz einfach die gleiche ist oder die gleiche sein kann"*, schilderte der Experte. Dies verdeutlicht die Bedeutung der beiden Aspekte Unfall- bzw. Betriebs- und Angriffssicherheit im Bereich des Stromnetzes.

Lösungsansätze. Großes Potenzial sah der Experte insbesondere im Bereich der Resilienz von Stromnetzen. Da-

bei komme zukünftig vor allem der Rolle der Bürger:innen als Prosumer und der *„damit einhergehenden Verantwortlichkeitsveränderungen“* als Produzent eine hohe Bedeutung zu. Prosumer könnten aktiv dazu beitragen, eine durch Ausfälle oder Angriffe erzeugte Instabilität des Stromnetzes abzumildern und so Stromausfälle zu verhindern. Neben technischen und rechtlichen Rahmenbedingungen wäre es aus Sicht des Experten wichtig, dass die Bürger:innen sich ihrer Verantwortung bewusst werden, sich im Krisenfall *„resilient“* zu verhalten und ihre stromkonsumierenden oder -erzeugenden Geräte zur Nutzung durch die Steuerzentralen anzubieten. Durch Wissen über das Thema könnten Bürger:innen eher gewillt sein *„jetzt keinen Strom zu verbrauchen, aber allen Strom, den mein Solarpanel produzieren kann, quasi an das Netz abzugeben, weil es einfach notwendig ist in dieser Notfallsituation“*, so der Experte.

Im Fall eines akuten Stromausfalls könnten verschiedene Stakeholder zusätzlich zur Abmilderung der Konsequenzen beitragen. Der Vorschlag des Experten mithilfe einer infrastrukturübergreifenden Simulation die *„Erfahrbarmachung von Konsequenzen“* zu ermöglichen, könnte dazu beitragen, Bürger:innen zum Mitwirken und Vorsorgen zu motivieren. Beispielsweise könnten sie geeignete Vorräte anlegen, denn *„wenn ich natürlich so eine Simulation sehe und begreife, dass das gar kein unrealistisches Szenario ist […] und was das bedeutet, dann bin ich vielleicht ein bisschen mehr geprimt […] mir doch ein paar Kisten mehr Wasser […] hinzustellen“*.

Szenario 2: Verknüpfung von Cybersicherheit und Privatsphärenschutz

In einem Interview beleuchtete eine Privatsphärenexpertin die Herausforderungen, die sich aus der zunehmenden Digitalisierung, auch im öffentlichen Raum, für den Schutz der Privatsphäre der Bürger:innen ergeben.

Beschreibung. Der Privatsphärenschutz der Bürger:innen ist gerade in Smart Cities ein relevantes Thema. So könnten an öffentlichen Plätzen Sensoren Daten von Bürger:innen erheben, ohne dass diese in adäquater Weise über die Datenerfassung aufgeklärt wurden oder dieser zugestimmt haben.

Hier könnten sich zwei Konflikte zwischen Privatsphärenschutz und Sicherheit ergeben: Einerseits besteht ein Dilemma zwischen dem Bedürfnis der einzelnen Bürger:innen nach Nichterfassung ihrer Daten bei gleichzeitigem Bedürfnis nach erhöhter Betriebssicherheit (Safety) z. B. durch die Erfassung von Verkehrsdaten.

Kernthesen

- Entwicklung nachhaltiger und sicherer Smart-City-Lösungen notwendig
- Unterschiedliche Anforderungen und Erwartungen von Stakeholdergruppen an Sicherheit und Privatsphäre
- Wechselwirkungen zwischen Betriebs- und Angriffssicherheit in städtischen Infrastrukturen

Andererseits ist die Angriffssicherheit (Security) aus Sicht der Expertin Voraussetzung für die Gewährleistung von Privatsphärenschutz: *„[…] ist ja schön, wenn ich quasi einstellen kann, ich möchte nicht, dass Daten gesammelt werden […], aber wenn es dann ein Leak gibt, dann war es das ja auch mit meiner Privacy“*.

Herausforderungen. Die größte Herausforderung besteht aus Sicht der Expertin in der Überforderung der Bürger:innen bei der Aufgabe, die eigenen erfassten Daten zu überblicken sowie bei der jeweiligen Auseinandersetzung mit informierten Einwilligungen zur Datenerfassung und -verarbeitung: *„[…] Menschen sagen, Privatsphäre ist ihnen wichtig aber gleichzeitig fühlen sie sich halt total überfordert, weil, wenn man […] auf eine Website geht, soll man ständig irgendwelchen Cookie Consents zustimmen und man liest sich das eigentlich nicht durch und [hat] auch keine Ahnung welche Geräte, welche Apps, welche Daten sammeln“*.

Dieses Problem gewinnt im Kontext von digitalisierten, „smarten“ Umgebungen wie Smart Homes zunehmend an Relevanz, wenn die Nutzer:innen den Überblick darüber verlieren, welche Geräte welche Daten erfassen. Das gilt insbesondere als Gast in einem fremden smarten Zuhause oder an einem öffentlichen Ort:

„[…] wenn ich halt in 'nen Zuhause von jemand anderem gehe, weiß ich im Zweifelsfall auch nicht, […] [ob] der Kühlschrank gerade 'ne Kamera hat oder ähm keine Ahnung Alexa mithört, während wir uns unterhalten und ähnlich gilt das ja dann für den öffentlichen Raum.“ Dies beschrieb die Expertin wie folgt: *„Also wenn irgendwo Daten gesammelt werden, ohne dass ich das weiß, beziehungsweise einfach auf einmal an so vielen Orten und Momenten gesammelt wird, dass ich einfach keine Chance mehr habe, ständig dem zu widersprechen oder zuzustimmen.“*

Lösungsansätze. Als vielversprechende Lösungsoption skizzierte die Expertin die Entwicklung eines digitalen Pri-

vatsphärenassistenten, der die Privatsphärenpräferenzen der Bürger:innen erfasst und bei Anfragen von Diensten und Geräten entsprechend verwaltet. Dieser Assistent könnte mobil auf dem Smartphone als eigene Anwendung zur Verfügung stehen und die Bürger:innen in ihrem Alltag begleiten oder auf bestimmten Geräten vorinstalliert sein und somit automatisch allen Anwender:innen zur Verfügung stehen. Diese Lösung bietet laut Expertin zusätzlich Vorteile hinsichtlich der Inklusion von Bürger:innen: *„[…] wenn du halt so 'n Assistenten hast, bei dem du halt sagen kannst ‚mach das alles für mich', dann wäre es halt auch zugänglicher für Menschen die vielleicht sich nicht so viel damit beschäftigen können oder wollen"*.

In Fällen, in denen der Assistent auf Eingaben der Bürger:innen angewiesen ist, um auf entsprechende Situationen der Datenerfassung, z. B. auf öffentlichen Plätzen, zu reagieren, bestünde ein weiterer Vorteil darin, dass diese aktiv auf den Umstand und Zweck der Datenerhebung hingewiesen werden: *„[…] da kann man es natürlich mitnutzen, um Bewusstsein zu schaffen, […] aber auch Aufklärung wofür das sinnvoll sein kann"*.

Anbieter für einen solchen Assistenten könnte nach Aussagen der Expertin eine Universität oder eine Initiative wie z. B. der Chaos Computer Club (CCC) sein. Sie verwies dabei auf eine von ihr durchgeführte Studie: Während nichtkommerzielle Institutionen wie Ministerien oder NGOs das Vertrauen potenzieller Nutzer:innen in Bezug auf Privatsphärenschutz genießen, werden erfahrenen kommerziellen Anbietern wie Google größere Kompetenzen im Bereich IT-Sicherheitsschutz (Security) zugeschrieben. Staatliche Institutionen oder private Initiativen, wie Universitäten oder der CCC, die über ein *„gewisses Renommee im Bereich Datenschutz"* verfügen, und denen gleichzeitig Kompetenzen im Bereich IT-Sicherheit zugetraut werden, könnten eine entsprechende Lösung darstellen. Hierbei sei es wichtig, dass der Assistent kostenfrei ist, denn *„Leute [sagen] zwar ‚mir ist Privatsphäre wichtig', aber im Endeffekt sind sie oft dann doch nicht bereit dafür wirklich zu zahlen"*.

Szenario 3: Das staatliche Sicherheitsparadox

Ein Interview mit einer Expertin für Friedens- und Konfliktforschung beschäftigte sich mit dem Einfluss internationaler Akteure auf die (Cyber-)Sicherheit städtischer Infrastrukturen sowie dem Umgang mit bekannten Sicherheitslücken. Zu den genannten Akteuren zählten sowohl staatliche Akteure als auch nichtstaatliche Gruppierungen wie Hacktivist:innen oder Terrorist:innen.

Beschreibung. Grundsätzlich kann Cybersicherheit besonders dadurch erhöht werden, dass Schwachstellen im Programmiercode erkannt und gemeldet werden, sodass Lücken geschlossen werden und Verbraucher:innen durch Aktualisierungen ihre Geräte und Daten sichern können. Andernfalls können die Schwachstellen durch sogenannte Exploits ausgenutzt werden, um Systeme auszuspionieren oder zu manipulieren.

Herausforderungen. Nach Aussage der Expertin bauen Staaten zunehmend auch im militärischen Bereich ihre Cyberkapazitäten aus. Eine Herausforderung bestehe darin, dass diese Kapazitäten unter anderem zur Nutzung von Schwachstellen gegen andere Staaten eingesetzt werden, *„die entweder geleakt werden, das ist schon passiert, oder dass die auch von anderen Akteuren ehm Hackern entdeckt werden und dann auf dem Schwarzmarkt verkauft werden"*. Die Schwachstellen würden nicht unbedingt frei veröffentlicht, sondern als Cyberwaffe aufbewahrt.

Daraus kann sich ein Paradox entwickeln, insofern als Staaten sich zunächst Exploits zurückbehalten *„um potenziell die nationale Sicherheit zu erhöhen"*, es *„aber gleichzeitig dann eben Security-Implikationen hat, wenn andere Akteure, die man eigentlich nicht so geplant hatte, Zugriff dazu bekommen"*. Gleichzeitig reduzierten Exploits die Sicherheit anderer Staaten, die fürchten müssten, mithilfe dieser angegriffen zu werden. Als Reaktion bauten diese gegebenenfalls selbst ihre Cyberkapazitäten aus, um eine Art Gleichgewicht der Kräfte wiederherzustellen.

Nach Meinung der Expertin vergrößere dies die Unsicherheit im internationalen System und führe zur Entstehung nationaler Arsenale von Exploits. Die Expertin beschrieb außerdem die Gefahr, dass staatliche Cyberwaffen politisch-strategisch motiviert gegen öffentliche Infrastrukturen wie Städte eingesetzt werden könnten, wo sie besonders weitreichende Auswirkungen auf die Bevölkerung, deren Versorgung und für die politische Stabilität haben können: *„Wir gehen davon aus, dass eben besonders wenn man die gegen Smart Cities benutzen würde […] es dann besonders gravierende, kaskadierende Effekte haben könnte"*. Eine weitere Herausforderung bestehe zudem darin, dass *„es dann nicht ist wie in der Genfer Konvention, […] dass man dort unterscheidet zwischen militärisch und zivil, sondern ehm ja, dass es da eben keine Regulierung für gibt"*.

Lösungsansätze. Gesellschaftliche Ansätze beinhalten eine öffentliche Debatte über Nutzen, Kosten und Gefahren von Cyberkapazitäten, über die Vermischung militärischer und ge-

heimdienstlicher Aufgaben und über Investitionen in defensive Strategien wie „Ethical Hacking“ zur Identifikation von Schwachstellen in den eigenen Systemen. Nach Meinung der Expertin wäre es ideal, wenn Staaten die *„Exploits, die sie finden, gar nicht für sich behalten, sondern veröffentlichen, am besten alle, damit alle, also besonders auch die Zivilbevölkerung, ihre eigenen Geräte dagegen sichern kann“*.

Zudem könnte auch durch internationale Vereinbarungen eine Norm etabliert werden, dass Cyberangriffe auf kritische Infrastrukturen, wegen des besonderen zivilen Schadens, inakzeptabel würden. Aber auch technische Lösungen, ähnlich zu Ansätzen zur Kontrolle anderer Waffensysteme, sind möglich. Diese müssten staatliche Interessen nach Geheimhaltung der spezifischen technischen Gestaltung respektieren, bei gleichzeitiger Reduktion strategisch weniger relevanter Waffen. Denkbar wäre zudem der intransparente Vergleich der Exploits mehrerer Staaten, um jene Exploits zu identifizieren, die mehrere Staaten haben und die dadurch für einen gegenseitigen Angriff nutzlos werden. Dies könnte mithilfe einer vertrauenswürdigen neutralen Instanz oder einer abstrakten technischen Beschreibung der Exploits erreicht werden *„[…] dann können diese [Exploits] nicht mehr auf dem Schwarzmarkt gehandelt werden, weil die komplett ihren Wert verlieren“*.

Fazit und Ausblick

Die beschriebenen Befragungsergebnisse und Szenarien zeigen auf, dass Cybersicherheit im Kontext von Smart Cities ein hochrelevantes und aktuelles Thema ist, das aber von verschiedenen Stakeholdergruppen unterschiedlich betrachtet wird, z. B. mit unterschiedlichen Erwartungen bezüglich Ursachen und Angreifer:innen. Auch die Interviews zeigen, dass die Herausforderungen je nach Kontext äußerst vielschichtig sind und technische Anforderungen an Systeme ebenso wie gesellschaftliche Aspekte wie Sensibilisierung der Bürger:innen und Diskurse über ethische Aspekte der Datenerfassung beinhalten.

Es zeigt sich, dass z. B. Bürger:innen andere Anforderungen an den Privatsphärenschutz und entsprechenden Unterstützungsbedarf haben als der Staat oder Organisationen, die Daten zur Gewährleistung der Sicherheit oder bestimmter Funktionalitäten benötigen. Im Falle der Smart Grids zeigte sich, dass individuelle Stromnutzungsbedürfnisse im Krisenfall im Widerspruch zu notwendigen Einschnitten zur Stabilisierung des Stromnetzes stehen können.

Die skizzierten Szenarien legen nahe, dass technische Lösungen die Einbindung verschiedener Stakeholder wie Infrastrukturbetreibende, staatliche Akteure sowie besonders von Bürger:innen unterstützen können. Eine weitere zentrale Herausforderung im Bereich smarter städtischer Infrastrukturen stellen die komplexen Wechselwirkungen zwischen Betriebs- und Angriffssicherheit dar. Diese zeigten sich unter anderem in der Bedrohung des Betriebs städtischer Infrastrukturen durch Ausfälle oder Angriffe auf einzelne Bereiche wie die Stromversorgung als auch in der möglichen politisch motivierten Ausnutzung von Sicherheitslücken mithilfe von Exploits.

Handlungsempfehlungen

- Berücksichtigung verschiedener Stakeholdergruppen und Wechselwirkungen zwischen Infrastrukturen für nachhaltige und sichere Lösungen notwendig
- Zielgruppenspezifische Entwicklung von Sicherheitslösungen wie z. B. digitale Assistenten
- Entwicklung von (inter-)nationalen Standards und Gesetzen für Smart Cities

Aus diesen Erkenntnissen können Handlungsempfehlungen für eine gelingende Implementierung von smarten Infrastrukturen in den urbanen Alltag abgeleitet werden. Zunächst sollten die unterschiedlichen Stakeholder und ihre spezifischen und zum Teil widersprüchlichen Anforderungen und Erwartungen an Sicherheit und Privatsphäre für smarte Lösungen analysiert werden. Zielgruppenspezifische Angebote für Sicherheitslösungen wie beispielsweise digitale Assistenten, könnten Hürden bei der Nutzung smarter Infrastrukturen senken und Bürger:innen aktiv einbinden.

Danksagung. Diese Forschungsarbeit wurde vom Bundesministerium für Bildung und Forschung (BMBF) und vom Hessischen Ministerium für Wissenschaft und Kunst (HMWK) im Rahmen ihrer gemeinsamen Förderung für das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE unterstützt.

Funding. Open Access funding enabled and organized by Projekt DEAL.

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), & Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Kritische Infrstrukturen – Definition und Übersicht. https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html. Zugegriffen: 25. Jan. 2021.

[2] Defense Use Case. "Analysis of the cyber attack on the Ukrainian power grid". In: *Electricity Information Sharing and Analysis Center (E-ISAC)* 388 (2016).

[3] Die Anstalt für kommunale Datenverarbeitung in Bayern (AKDB) Bürgerservice-Portal. https://www.akdb.de/loesungen/okegov/buergerservice-portal/uebersicht/. Zugegriffen: 25. Jan. 2021.

[4] Digitalstadt Darmstadt Smart Parking – Ein intelligentes Parkplatzkonzept für Darmstadt. https://www.digitalstadt-darmstadt.de/projekte/smart-parking/. Zugegriffen: 25. Jan. 2021.

[5] e.on Smart Grid: Aufbau, Definition und Funktionen. https://www.eon.de/de/eonerleben/smartgrid-so-funktioniert-das-intelligente-stromnetz.html. Zugegriffen: 2. Jan. 2021.

[6] Etezadzadeh, C. (2020). *Smart City – Made in Germany: Die Smart-City-Bewegung als Treiber einer gesellschaftlichen Transformation*. Springer.

[7] Reuter, C. (2020). Towards secure urban infrastructures: Cyber security challenges for information and communication technology in smart cities. In C. Hansen, A. Nürnberger & B. Preim (Hrsg.), *Mensch und Computer 2020 – Workshopband*. Bonn: Gesellschaft für Informatik e. V. https://doi.org/10.18420/muc2020-ws117-408.