Eine digitale Checkliste für die Nationale Sicherheitsstrategie

Schlussfolgerungen des BAKS-Seminars Digitalisierung und Sicherheitspolitik 2022

von Jan Bittner und Daniel Hiller
für das Fachseminar Digitalisierung und Sicherheitspolitik 2022

Im Rahmen des Fachseminars Digitalisierung und Sicherheitspolitik 2022 studierten Führungskräfte aus Industrie, Verwaltung, Sicherheitsbehörden und angewandter Forschung die deutsche Digitalisierungs- und Cybersicherheitsarchitektur und untersuchten in Südkorea und Singapur, wie die Schnittstellen von Sicherheit und Digitalisierung dort organisiert und umgesetzt werden. Ausgehend von den gewonnenen Erkenntnissen setzt dieses Papier Impulse, wie Digitalisierung in der entstehenden Nationalen Sicherheitsstrategie zur Geltung kommen kann.

Die Einsicht, dass Cybersicherheit in unserer hochvernetzten Welt eine zentrale Aufgabe der Sicherheitspolitik ist, setzt sich in Deutschland zu langsam durch und bleibt oft ein Expertenthema. In Südkorea und noch deutlicher in Singapur haben wir gesehen, wie das Thema in einem gesamtstaatlichen Ansatz strategisch bearbeitet und operativ umgesetzt wird. **Digitalisierung sollte sich daher als roter Faden durch alle Themen der Nationalen Sicherheitsstrategie ziehen.**

Zwar gehören Föderalismus und Ressortprinzip zur DNA unseres Staates und seines Regierungssystems. Angesichts der Geschwindigkeit von digitalen Innovationen und der Komplexität von Problemlagen werden aber immer wieder die Grenzen dieser Prinzipien deutlich. Wir haben gesehen, wie bedeutend eine schnelle und strategisch geplante Umsetzung von Digitalisierungsprojekten ist. **Die Sicherheitsstrategie muss daher klare Verantwortlichkeiten für Digitalisierungsvorhaben in der Sicherheitsarchitektur auf Bundesebene benennen und ein Format vorschlagen, in dem unter Beteiligung der Länder einer zu beobachtenden Verantwortungsdiffusion bei Digitalthemen mit Sicherheitsbezug entgegengewirkt wird.**

Unsere Gesprächspartner in Korea und Singapur haben immer wieder betont, wie wichtig der grundlegende Perspektivwechsel für eine erfolgreiche Digitalisierung ist. Es kann nicht gelingen, bestehende Prozesse einfach 1:1 zu digitalisieren. Prozesse müssen mit der Bereitschaft hinterfragt werden, sie von Grund auf neu zu strukturieren. Dazu gehört auch, Lösungen aus Sicht von Sicherheitsbehörden und Katastrophenschützern („Nutzerorientierung“) zu erarbeiten. **Die Sicherheitsstrategie sollte daher Ressourcen und Werkzeuge zur resilienten Bewältigung einer Großschadenslage identifizieren und auf die Einbindung bzw. Einführung digitaler Lösungen drängen. Erst nachdem diese gefunden sind, sollten Abläufe zwischen verschiedenen politischen Akteuren abgestimmt werden.**

Digitale Werkzeuge bieten die Möglichkeit, Risikoanalyse und Foresight, Gefahrenabwehr und Schutz, sowie Krisenmanagement und -vorsorge institutionenübergreifend zu bearbeiten. Allerdings agieren in Deutschland Polizei, Streitkräfte sowie Zivil- und Katastrophenschutz mit ihrem jeweiligen System nur für sich. Die wenigen Schnittstellen, die es gibt, sind mühsam herbeigeführte Einzellösungen. **Die Sicherheitsstrategie sollte daher auf die Schaffung gemeinsamer Datenräume der Sicherheitsinstitutionen hinwirken. In diese müssen auch Akteure der Wirtschaft, und insbesondere Betreiber kritischer Infrastrukturen eingebunden sein.**

Besonders eindrücklich war in Südkorea, wie verschiedene Ressorts und Sicherheitsbehörden themenbezogen im Rahmen von Umsetzungsprojekten zusammenarbeiten: in einem definierten Projekt mit eindeutiger Projektleitung einer Institution, entsprechendem Budget und einer Projektmanagementstruktur, die losgelöst von Ressort- und Behördenzuständigkeiten aufgesetzt wird. Dies sollte in Deutschland Schule machen. **So könnte die Sicherheitsstrategie als Pilotprojekt die Einführung eines einheitlichen sicheren Messengers für die Behörden von Bund und Ländern vorantreiben.**

Jeder Bürger trägt Verantwortung, wenn es um unsere Sicherheit geht, besonders in der Cybersicherheit. In Singapur hieß es: „Die Aufgabe des Staates ist nicht, alle Risiken der Bürger zu minimieren, sondern Risiken und Nutzen in eine sinnvolle Balance zu bringen." Der gezielte Aufbau digitaler Kompetenz trägt daher nicht nur zum Schutz der Gesellschaft bei, sondern stärkt auch ihre Innovationskraft. **Die Sicherheitsstrategie sollte daher sowohl messbare Ziele für staatliche Akteure formulieren, als auch klar die Verantwortung eines jeden Einzelnen thematisieren.**

Auch in Deutschland entstehen in der Start-up-Szene neue Lösungen und Geschäftsmodelle in Höchstgeschwindigkeit. Deren Nutzen für die staatliche Sicherheitsarchitektur braucht experimentelle Räume in der Verwaltung, um in realer Umgebung getestet werden zu können. Die BMWK-Strategie, „Reallabore" als Testräume für Innovation und Regulierung einzurichten, geht in diese Richtung, und auch der *Cyber Innovation Hub* der Bundeswehr bietet hier Möglichkeiten. **Die Sicherheitsstrategie sollte Bereiche benennen, in denen sicherheitsrelevante Reallaborprojekte enger zusammenarbeiten können.**

Trotz deutlicher Defizite in den Bereichen IT und Digitalisierung, die im Ausland nicht unbemerkt bleiben, wurden wir wiederholt auf Deutschlands sehr gute Grundlagenwissenschaft und auch anwendungsnahe Forschungslandschaft angesprochen. Es braucht eine neue Kombination aus staatlicher (Forschungs-) Anschlussfinanzierung und privatem Kapital, um Innnovationen in Deutschland umzusetzen. **Die Sicherheitsstrategie sollte daher deutlich machen, dass es wirtschaftlich und sicherheitspolitisch geboten ist, deutsche Forschungsergebnisse in mehr eigene Produkte und Dienstleistungen umzusetzen.**

Sicherheit für den Staat und seine Bürger hängt im Cyberbereich von der Funktionsfähigkeit zentraler staatlicher Dienste ab: digitale Identität, E-Payment, Gesundheitsdaten usw. Diese erfordern eine übergeordnete digitale Infrastruktur, die mit deutschlandweit einheitlichen Standards abgesichert ist. Das Fundament hierfür muss technisch und organisatorisch erst noch gelegt werden. **Die Sicherheitsstrategie sollte Sicherheitsstandards daher als wichtige Voraussetzung für gesamtstaatliche Sicherheit benennen.**

Hohe Komplexität und hohe Vernetzung führen in der digitalen Welt zu mehr Verwundbarkeiten und zu potentiell katastrophalen Kaskadeneffekten in der Versorgung von Menschen. Um das zu vermeiden, muss das Konzept der Resilienz für Staat und Wirtschaft noch stärker operationalisiert werden. **Die Sicherheitsstrategie sollte dem Konzept der Resilienz daher breiten Raum widmen. Es kommt darauf an, dass relevante Daten zu klima- wie menschinduzierten Katastrophen strukturiert gesammelt und für sämtliche Sicherheitsbehörden verfügbar gemacht werden. Es braucht Maße und Metriken, um die Krisenfestigkeit von Staat, Wirtschaft und Gesellschaft vor, während und nach einem Schock erfassen zu können.**

Aus unseren Gesprächen in Deutschland haben wir den Eindruck gewonnen, dass trotz der hohen Innovationsgeschwindigkeit im Digitalbereich, deutsche Planungs- und Beteiligungsprozesse sehr viel Zeit in Anspruch nehmen. Dafür gibt es oft gute Gründe. In Singapur und Südkorea haben wir eine pragmatische Vor-

gehensweise kennengelernt, die Lösungen für konkret bestehende Probleme in den Vordergrund stellt und sich mit einem „gut genug“ zufriedengibt anstatt ein „perfekt“ anzustreben. **Die Sicherheitsstrategie sollte dafür werben, in bestimmten Bereichen von bestehenden Planungs- und Beschaffungsprozessen abzuweichen, um schnelle Lösungen zu erreichen.**

Obwohl Singapur technologisch und in der Sicherheitsarchitektur weit fortgeschritten ist, besteht bei den dortigen (Cyber-)Sicherheitsbehörden großes Interesse an Kooperation. Die grenzüberschreitende Natur der Gefahren im Cyberraum wird als Antrieb verstanden, sich international zu vernetzen. **Die Sicherheitsstrategie sollte daher die internationale Kooperation unserer Sicherheitsinstitutionen als wichtiges Ziel benennen.**

Durch das Fachseminar Digitalisierung und Sicherheitspolitik hat die Gruppe Einsicht bekommen in zwei Digitalisierungs-Champions in Asien, und auch andere Länder in anderen Erdteilen haben inspirierende Projekte und Lösungen zu bieten. **Abschließend empfehlen wir daher ein globales Best-Practice-Screening der Schnittstelle Sicherheit und Digitalisierung.**

Die Autoren geben ihre persönliche Meinung wieder.

Am Fachseminar Digitalisierung und Sicherheitspolitik 2022 der BAKS haben teilgenommen:

Jan Bittner, Ministerialrat, Leiter des Referats „Internationales“,
Vertretung des Landes Nordrhein-Westfalen beim Bund, Berlin

Fanny Fascar, Korrespondentin, Deutsche Welle, Wien

Dr. Alexandra Forster, *Head of Corporate Global Security,* Bayer AG, Leverkusen

Gerd Friedsam, Präsident der Bundesanstalt Technisches Hilfswerk, Bonn

Daniel Hiller, Geschäftsführer Fraunhofer Zentrum
für die Sicherheit Sozio-Technischer Systeme (SIRIOS), Berlin

Anja Misselbeck, Fachgebietsleiterin „Technologiestrategie“,
Verband der Automobilindustrie e.V., Berlin

Dr. Christoph Reichle, Ministerialdirigent, Unterabteilungsleiter „Grundsatzfragen Klimaschutzabteilung“, Bundesministerium für Wirtschaft und Klimaschutz, Berlin

Hans-Jörg Schäper, Ministerialdirigent, Stellvertretender Abteilungsleiter „Informationstechnik“ und Unterabteilungsleiter VI A, Bundesministerium der Finanzen, Berlin

Carmen Schmudlach, Regierungsdirektorin, Referatsleiterin „Grundsatz Personal“,
ZITiS - Zentrale Stelle für Informationstechnik im Sicherheitsbereich, München

Christoph Scholz, Leitender Polizeidirektor, Referatsleiter „IKT-Strategie“,
Bundespolizeipräsidium, Potsdam

Maurizio Skerlj, Leiter der geschäftsführenden Einheit *Identity Solution*
der Division "Connected Secure Systems", Infineon Technologies AG, München

Thomas Süptitz, Ministerialrat, Referatsleiter „Cybersicherheit und Interoperabilität“,
Bundesministerium für Gesundheit, Berlin

Das Seminar widmet sich Fragen von Digitalisierung und Sicherheitspolitik anhand eines fokussierten Austauschs mit Fachleuten sowie zentralen Akteuren des Digitalbereichs. Eine Auslandsreise ist dabei fester Bestandteil. Die Zielgruppe sind Fach- und Führungskräfte, die sich als Multiplikatoren mit grundsätzlichen Fragen der Digitalisierung befassen. Eine Teilnahme ist nur auf Nominierung möglich. Weitere Informationen finden Sie hier: www.baks.bund.de/de/fachseminar-digitalisierung-und-sicherheitspolitik