Positionspapier „Sicherheit, Superwahljahr, strategische Partnerschaften – der digitale Faktor"

Die Krisen der der aktuellen Zeit stellen Deutschland und Europa vor neue Herausforderungen. Von 600 befragten CEOs weltweit erwarten 70 Prozent in den nächsten fünf Jahren eine Zunahme der Auswirkungen von Krisen durch Kriege, den Klimawandel oder Störungen der Lieferketten (Future Shocks Studie, IBM Institute for Business Value, Nov. 2023). Zudem werden die Auswirkungen des demografischen Wandels spürbar. Diese Herausforderungen zu meistern, erfordert eine gemeinsame Kraftanstrengung von Politik, Wirtschaft, Wissenschaft und Gesellschaft sowie den gezielten Einsatz digitaler Technologien.

Künstliche Intelligenz ist die transformative Technologie unserer Zeit. 32 Prozent der deutschen Unternehmen setzen sie bereits aktiv ein, weitere 44 Prozent experimentieren aktiv mit ihr, laut IBM Global AI Adoption Index. Die generative KI wird diesen Prozess weiter beschleunigen. KI-basierte Assistenten sowie der Einsatz von KI in Datenanalysen und in der Entscheidungsfindung werden viel stärker Einzug in unseren Alltag halten und können insbesondere in einem veränderten Sicherheitsumfeld einen Mehrwert für Entscheidungsträger in Politik, Unternehmen und Gesellschaft schaffen.

Während unseres Parlamentarischen Abends am 12. September 2024 zu „Sicherheit, Superwahljahr, strategische Partnerschaften – der digitale Faktor" haben wir die zentralen Herausforderungen unserer Zeit in den Fokus gerückt. Dabei wollten wir insbesondere beleuchten, welche Rolle digitale Technologien für unsere Sicherheit spielen, wie sie die Umsetzung der Zeitenwende beschleunigen und welche Auswirkungen die Zusammenarbeit mit transatlantischen und europäischen Partnern auf die IKT-Technologien haben. Dieses Positionspapier fasst unsere Perspektive auf diese Themen zusammen – wir freuen uns sehr auf den weiterführenden Dialog.

Sicherheit → Verteidigungsfähigkeit durch digitale Technologien steigern

Technologische Entwicklungszyklen werden immer schneller und komplexer. Anstelle langwieriger Neuentwicklungen für den Verteidigungsbereich, sehen wir eine große Chance darin, bestehende Lösungen aus anderen Sektoren zu übertragen:

- **Steigerung der Agilität durch den Einsatz von Prototypen und Demonstratoren** → erstes vollautonomes, KI-gesteuertes Schiff, die Mayflower, wurde 2022 erfolgreich über den Atlantik geschickt. Die Erfahrungen können u.a. für die Weiterentwicklung von Drohnen genutzt werden.
- **Erleichterung von Routinetätigkeiten durch digitale Assistenzsysteme** → IBM hat mit CIMON den ersten KI-Assistenten auf die internationalen Raumstation ISS gebracht.
- **Erfahrungen der Software Defined Vehicles nutzen für Verteidigungssektor** → Erfahrungswerte aus digitalen Innovationen auf dem gleichen Modelltyp in der Automobilindustrie nutzen für den Sicherheits- und Verteidigungsbereich.

IBM ist strategische Partnerin der deutschen Verteidigungsindustrie, um IT-Workloads mit Hilfe von KI-Technologie zu verwalten und zu optimieren. Vor dem Hintergrund angespannter Haushalte und multipler Krisenlagen, sollte der Fokus einer Steigerung der Verteidigungsfähigkeit nicht auf abgekapselten Entwicklungen in einzelnen Bereichen, sondern auf der Integration von Fähigkeiten

und Systemen durch digitale Lösungen liegen. Ein breites Ökosystem, kombiniert mit offenen Standards, ist der beste Weg zur kurzfristigen Integration technologischer Innovationen.

- **Software Defined Defence (SDD)** als Enablement von Hardware (Metall und Fahrzeuge) durch Software (Digitalisierung) durch die Verbindung vorhandener und künftiger Einsatzsysteme über offene Schnittstellen → ermöglicht eine bessere Zusammenarbeit der Bundeswehr mit der Industrie und den Bündnispartnern → IBM als Technologiepartnerin mit offenen Schnittstellen (Open Source) und Integratorin für den Einsatz von Edge-Technologie.
- **Unterstützung bei Entscheidungsfindung durch KI-gestützte Echtzeit-Datenanalysen** → Kombination ausgeklügelter Dateninformationssysteme, die über mehrere Domänen hinweg betrieben werden.

74 Prozent der Cyberangriffe in der EU galten 2023 kritischen Infrastrukturen, laut des IBM X-Force Threat Intelligence Index 2024. IBM begrüßt das Ziel der ersten Nationalen Sicherheitsstrategie, ein ganzheitliches Cyberlagebild zu schaffen. Zur Steigerung von Sicherheit in einer multiplen Krisenlage ist die Vernetzung von Informationen und Systemen unabdingbar.

Superwahljahr → vertrauenswürdige digitale Technologien fördern

Der Einfluss sogenannter Deep Fakes im B-2-C Bereich und die Gefahren eines Missbrauchs digitaler Plattformen, die Wahlentscheidungen beeinflussen können, nimmt zu. Dies erfordert eine Cybersicherheitsarchitektur auf der Höhe der Zeit, Stärkung der digitalen Bildung und einen Schulterschluss zwischen Politik, Wirtschaft und Gesellschaft.

- **Gegen Verbreitung von Desinformation durch gemeinsame und sichere KI-Lösungen** → IBM ist Mitunterzeichnerin des „Tech Accord to Combat Deceptive Use of AI in 2024 elections“ der Münchner Sicherheitskonferenz sowie der Bayern-Allianz gegen Desinformation.
- **Wertegeleitete KI Governance ist entscheidend** → IBM hat seit 2019 ein AI ethics board und Grundsätze zur verantwortungsvollen Umgang mit Technologien → IBM begrüßt den risikobasierten Ansatz des EU AI Acts und setzt sich für eine faire Verteilung der Haftung und eine innovationsfreundliche Umsetzung ein.

Strategische Partnerschaften → High-Tech gemeinsam und werteorientiert voranbringen

Angesichts der eingangs skizzierten Herausforderungen wird eine wertegeleitete Außen- und Sicherheitspolitik zunehmend wichtiger - in Deutschland, Europa, der Welt. Entscheidend dabei sind konkrete Umsetzungsschritte in der Kooperation mit Wertepartnern und ein chancenorientierter Blick auf internationale Kooperation, anstelle einer reinen Fixierung auf den Firmensitz.

- **Strategische Zusammenarbeit mit Wertepartnern stärkt Sicherheit** → in Zeiten des geopolitischen Wandels sollte mehr Fokus auf technologische Souveränität gelegt werden – im engen Schulterschluss mit einer aktiven, transatlantischen Wirtschafts- und Handelspolitik. Einseitige, protektionistische Tendenzen, wie Immunitätsschutzklauseln im Entwurf der EU-Agentur für Cybersicherheit (ENISA) zum Zertifizierungssystem für Cloud-Dienste (EUCS), lehnen wir ab.
- **Transatlantische Kooperation bei KI und Quantum ausbauen** → IBM unterstützte den EU-US Trade and Technology Council und hätte sich Ausweitung und Vertiefung gewünscht →

notwendig bleibt der Aufbau transatlantischer Governance-Agenda für KI, Quantum und Halbleiter in der nächsten EU-Kommission. Das kürzlich unterzeichnete, bilaterale Joint Statement in Quantum Information Science and Technology ist ein gutes Zeichen, muss nun aber mit konkreten Umsetzungsschritten ausgestaltet werden.

- **Vorbereiten auf Post-Quanten-Kryptografie** → IBM ist globaler Vorreiter bei Standards für quantensichere Kryptografie (NIST) → öffentliche Sektor sollte Migration zur quantensicheren-Kryptografie vorantreiben, quantenresistente kryptografische Systeme fördern.
- **Harmonisierung gesetzlicher Regelungen notwendig** → KRITIS-Dachgesetz, NIS-2, Cyber Resilience Act, DORA, Nationale Sicherheitsstrategie etc. dürfen nicht zu unklaren Strukturen, Meldebehörden und -fristen und mehr Bürokratie führen.

IBM als verlässliche Partnerin auf beiden Seiten des Atlantiks

Die IBM ist mit ihrer mehr als 110-jährigen Geschichte fest in Deutschland und Europa verwurzelt. Mehr als 4.000 Regierungsorganisationen und Unternehmen in kritischen Infrastrukturbereichen wie Finanzdienstleistungen, Telekommunikation und Gesundheitswesen verlassen sich weltweit bei ihrer digitalen Transformation auf die bahnbrechenden Innovationen von IBM in den Bereichen KI, Cloud und Quantum Computing.

Kontakt

Government & Regulatory Affairs IBM DACH

Martin Wegele, Director

Svenja Frerichs, Senior Manager