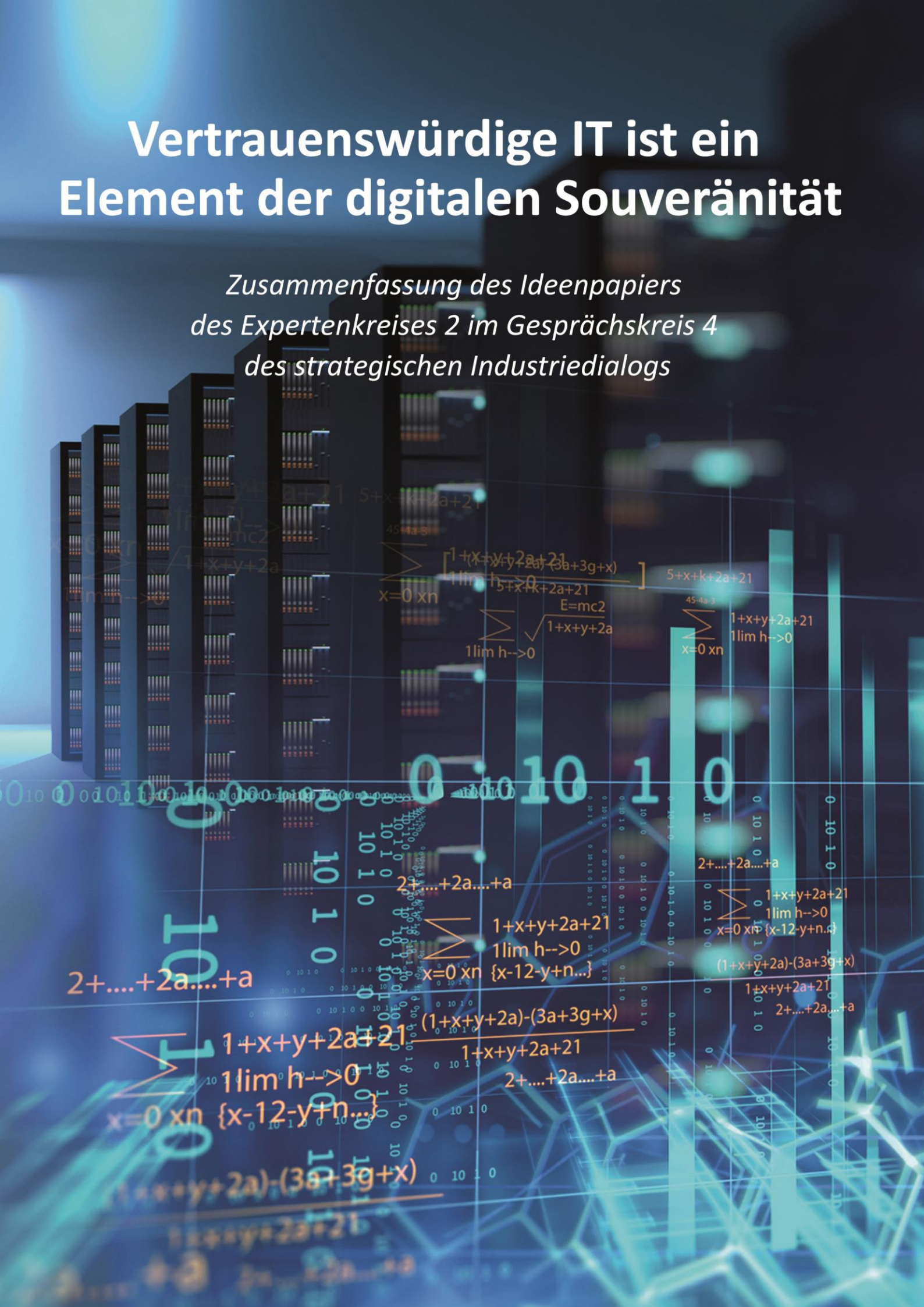
Vertrauenswürdige IT ist ein Element der digitalen Souveränität

Zusammenfassung des Ideenpapiers
des Expertenkreises 2 im Gesprächskreis 4
des strategischen Industriedialogs



Im Rahmen des strategischen Industriedialogs hat das BMVg gemeinsam mit dem BDSV und dem Bitkom im Expertenkreis 2 *„Nationale Schlüsseltechnologien und -fähigkeiten für Entwicklung, Realisierung und Lebenszyklusunterstützung vertrauenswürdiger IT der Bundeswehr“ (Kurzform: „Vertrauenswürdige IT“)* einen offenen und unverbindlichen Dialog ermöglicht, der sich außerhalb konkreter Beschaffungsabsichten befindet und keine als Verschlusssache oder kommerziell-vertraulich eingestuften Informationen behandelt.

Kernaussage:
Die Anteile von Cyber/IT, die wesentliche nationale Sicherheitsinteressen betreffen, sollten im Rahmen der nationalen Schlüsseltechnologien[1] angemessen Berücksichtigung finden.

<u>Weitere Ideen und Empfehlungen</u>

- *Der Begriff der Schlüsselfähigkeiten[2] sollte für den Bereich Cyber/IT zusätzlich eingeführt, übergreifend abgestimmt und definiert sowie detailliert werden.*
- *Die Anwendungsfälle vertrauenswürdiger IT, die derzeit noch nicht hinreichend verlässlich regulatorisch abgebildet sind, sollten präzisiert werden, um Handlungssicherheit zu gewährleisten.*
- *Spezifische Handlungsfelder (insbesondere das Thema „sichere Lieferketten“) sollten weiter betrachtet werden.*
- *Die Fähigkeit zur quantitativen und qualitativen Bemessung des Bedarfes an Sicherheit inklusive der Berücksichtigung des Aufwandes sollte sowohl im Hinblick auf das benötigte Maß an Vertrauenswürdigkeit als auch an Verfahrensstärke und Wirksamkeit verbessert werden.*
- *Allgemein sollten bei weiteren Überlegungen geplante sowie bereits laufende Forschungs- und Entwicklungsvorhaben im nationalen und internationalen Bereich mit einbezogen werden.*

Es kommt auch zukünftig darauf an, die Herausforderungen bzgl. der Verfügbarkeit ausreichend vertrauenswürdiger IT zur Sicherstellung der „digitalen Souveränität“ für alle Beteiligten nachhaltig mit der notwendigen Qualität und Agilität, aber auch wirtschaftlich und synergetisch zu lösen. Hierbei sind die jeweiligen Kompetenzen und Rahmenbedingungen sowie Sachzwänge/Interessen aller Beteiligten stets angemessen transparent zu machen und zu berücksichtigen.

Die Ergebnisse des fachlichen Ideenaustauschs und der Diskussionen im EK 2 spiegeln die teils komplementären Fähigkeiten und Schwerpunkte wider, die sich durch die Rolle als potenzieller Auftraggeber/Forderer (BMVg/GB BMVg) bzw. potenzieller Auftragnehmer/Bereitsteller (Industrie) im Bereich Cyber/IT herausbilden.

Weitere Details und begleitende Informationen können dem durch die Leitung BMVg und den Industrieverbänden gebilligten Ideenpapier entnommen werden. Das vollständige Dokument ist abrufbar unter:

- https://www.bmvg.de/de/aktuelles/vertrauenswuerdige-it-bundeswehr-140710
- https://www.bdsv.eu/aktuelles/aktuelle-meldungen.html
- https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Verteidigung/index.jsp

[1] Definition Schlüsseltechnologien: Schlüsseltechnologien sind Technologien, die aus den außen-, sicherheits- und europapolitischen Interessen Deutschlands, dem militärischen Bedarf der Bundeswehr, den Bündnisverpflichtungen sowie der Verantwortung Deutschlands abgeleitet und regelmäßig überprüft werden.

[2] Definition Schlüsselfähigkeiten: Unter Schlüsselfähigkeiten im Kontext Cyber/IT werden die Fähigkeiten verstanden, welche unter Nutzung von Technologieelementen (sowohl Schlüsseltechnologien als auch Nicht-Schlüsseltechnologien) elementar für die Konzeption, Realisierung und Nutzung sowie Lebenszyklusunterstützung von vertrauenswürdigen Informationssystemen, einzelnen Systemkomponenten oder Systemfunktionalitäten sind. (Arbeitshypothese bis zur Bereitstellung einer umfänglichen und formal abgestimmten Definition)

Über den Gesprächskreis Innovation Cyber/IT im Strategischen Industriedialog

Auf Initiative der Leitung BMVg vom Juni 2017 ist der strukturierte Dialog zwischen dem BMVg und dem Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie (BDSV) zum Strategischen Industriedialog (SID) weiterentwickelt worden. Dessen Kern besteht aus sechs Gesprächskreisen (GK). Der GK 4 „Innovation Cyber/IT“, wird von Seiten der Industrie gleichberechtigt durch den Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) und BDSV betreut, wobei die industrielle Leitung vom Bitkom gestellt wird. Der GK 4 „Innovation Cyber/IT“ hat auf Fachebene in einem Expertenkreis 2 (EK 2) einen Ideenaustausch zum Thema „Vertrauenswürdige IT“ mandatiert. Die thematische Schwerpunktsetzung des EK 2 greift die zunehmende Abhängigkeit sämtlicher Lebensbereiche von Informationstechnologie (IT) und die Notwendigkeit der Stärkung der „digitalen Souveränität“ auf.

Kompetenzen und Rahmenbedingungen

BMVg/GB BMVg verfügt im Bereich Cyber/IT über umfangreiche methodische Kompetenzen zur Nachweisführung und formalen sowie technischen Verifikation von Leistungen der Industrie. Im BMVg/GB BMVg erforderliche Strukturen, Prozesse, Vorhaben und materielle sowie personelle Ressourcen sind entweder bereits aufgebaut oder auf der Zeitschiene ausgeplant und für die zukünftige Realisierung vorgesehen. Kompetenzen, praktische Fähigkeiten und Lösungsangebote der Industrie im Bereich Cyber/IT folgen wesentlich der Beschaffenheit des Marktes. Insbesondere optimiert die Industrie ihr Angebotsprofil entsprechend der z.Zt. adressierbaren Volumina bezogen auf die verschiedenen Marktsegmente. In der Folge stehen der kommerzielle globalisierte Massenmarkt (a) und der nationale Bedarf im sicherheitssensitiven Umfeld (b) hinsichtlich der Rahmenbedingungen und Anforderungen grundsätzlich in einem Spannungsverhältnis. Dies betrifft sowohl die formalen und technischen Anforderungen als auch die Marktmechanismen. Beispielsweise richten sich IT-Sicherheitsvorgaben einerseits nach best-practice-Lösungen (a) bzw. andererseits nach Vorgaben gemäß der Common Criteria bzw. der Verschlusssachenanweisung (b) aus. Umweltbedingungen und Einsatzumgebung sind einerseits gemäßigte Standardumgebungen mit ggf. erweiterter Alltagstauglichkeit (a) oder hochmobile schwimmende/fliegende/fahrende Plattformen mit extremen physikalischen Randbedingungen (b). Dieses mit dem Schutzbedarf der Informationen und der Kritikalität und Besonderheit des Einsatzzweckes steigende Spannungsfeld erfordert gerade auch vor dem Hintergrund knapper Ressourcen, deren bzgl. Leistung, Zeit und Kosten optimierte Verwendung zur Schaffung und Aufrechterhaltung hinreichend verlässlicher Kommunikations- und Informationssysteme bzw. -technologien.