Gemeinsame Stellungnahme

vom Bitkom und BDSV zum Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie

30. März 2020

Einleitung

Der Bitkom und der BDSV begrüßen, dass sich die Bundesregierung in ihrem Strategiepapier zur Stärkung der Sicherheits- und Verteidigungsindustrie zu dem Erfordernis einer innovativen, leistungs- und wettbewerbsorientierten Sicherheits- und Verteidigungsindustrie bekennt. In Anbetracht wachsender sicherheitspolitischer Herausforderungen ist eine Stärkung heimischer sicherheitsrelevanter Technologien von größter strategischer Bedeutung. Das Strategiepapier erkennt richtig die Bedeutung der Digitalisierung als technologische Herausforderung für unsere Sicherheit und Verteidigung sowie die Gewährleistung der Cybersicherheit als Grundvoraussetzung für die fortschreitende Digitalisierung von Staat, Wirtschaft und Gesellschaft und als Element der Souveränität Deutschlands und Europas. Vor diesem Hintergrund ist auch der angekündigte strukturierte Dialog mit der zivilen Sicherheitsindustrie zur Stärkung der digitalen Souveränität im Hinblick auf den Bedarf der Kritischen Infrastrukturen unter Leitung des BMI begrüßenswert.
Ein Strategiepapier kann jedoch nur so gut wie seine Umsetzung sein. Aus Sicht des Bitkom und des BDSV werden die folgenden Maßnahmen für eine Operationalisierung empfohlen:

1. Partnerschaft zwischen Staat und Wirtschaft

In Bezug auf das jeweilige sicherheitspolitische Umfeld gehen wir als Wirtschaft davon aus, von Seiten der Bundesregierung bei der Analyse der aktuellen digitalen Bedrohungen angemessen über anstehende Herausforderungen informiert zu werden. Nur wenn für die Wirtschaft Planbarkeit und Transparenz bestehen, kann von ihr erwartet werden, dass sie auch langfristig als Partner der Sicherheitsorgane in Deutschland erhalten bleibt. Eben dies gilt auch für alle Maßnahmen, die im Bereich der Förderung von digitalen Schlüsseltechnologien geplant und umgesetzt werden. Wir unterstützen nachdrücklich alle Maßnahmen, die auf eine digitale Souveränität in den im Strategiepapier umrissenen Bereichen abzielen und arbeiten hieran gerne auch aktiv mit. Dies betrifft nicht zuletzt auch den sog. »Ausverkauf« von Assets, die für die nationale Sicherheit von Bedeutung sind. Allerdings erwarten wir, dass in gleichem Maße auch solche industriellen Assets identifiziert werden, die diese Sicherheitsrelevanz nicht haben. Solche Assets müssen gem. AWG/AVO entsprechend fungibel ausgestaltet werden, um eine wirtschaftliche Werthaltigkeit zu gewährleisten.

2. Optimierung der Beschaffungsorganisation

Wie im Strategiepapier identifiziert besteht der dringende Bedarf einer Optimierung der Beschaffungsvorgänge innerhalb der Einkaufsorganisationen. Die Berücksichtigung der strategischen Vorgaben muss formal in die Beschaffungsrichtlinien Eingang finden und sich spürbar auf allen Ebenen des Beschaffungswesens auswirken. Darüber hinaus müssen als Grundlage für die Beschaffungsabwicklung Veränderungen der Budget- und Beschaffungsplanung sowie die zeitnahe Adaption von Innovationen durch Verwender erfolgen. Speziell in dem Bereich Cyber/IT unterliegen Innovationen sehr kurzen Zyklen und können bereits bei einem vergleichsweise niedrigen Mittelaufwand einen erheblichen Nutzen bringen. Neben der Reform der Vorgänge in den Verwender- und Beschaffungsorganisationen wird eine Einbindung des Finanzministeriums bezüglich der Mittelbereitstellung, sowie des Justizministeriums zur möglichen Anpassung von Beschaffungsrichtlinien als potenziell notwendig erachtet.

3. Präzisierung der Schlüsseltechnologien

Die im Strategiepapier vorgenommene Darstellung der Technologiefelder ist weder ebenengerecht noch vollständig. Zudem sind sie aus systemischer Sicht auf unterschiedlichen Systemebenen verankert. Unsere Unternehmen gehen davon aus, auch hinsichtlich der Präzisierung der der digitalen Schlüsseltechnologien und -fähigkeiten an der Diskussion beteiligt und jeweils zeitnah in die Erarbeitung entsprechender Ergebnisse einbezogen zu werden. Aufgrund der bestehenden Unklarheiten sollten Unternehmen eine Ansprechstelle haben, die ihnen dabei hilft festzustellen, ob sie »nationale Schlüsseltechnologie« führen und ggf. entsprechende Vor- und Nachteile berücksichtigen müssten.

4. Klarheit zur Exportkontrolle schaffen

Insbesondere in innovativen Nischen im Dual-Use-Güterbereich entstehen innerhalb der Digitalwirtschaft Schlüsseltechnologien. Die derzeitigen Vorschriften der Exportkontrolle und der im Vergleich zum (europäischen) Ausland für den Bereich der sicherheitskritischen Technologien sehr langwierige Genehmigungsprozess mit unklarer Auskunftslage gegenüber Kunden ist insbesondere für KMUs problematisch. Es besteht eine signifikante Gefahr, dass innovative KMUs und auch größere Konzerne ihren Entwicklungs- und Produktionsstandort ins Ausland verlagern müssen, um nicht Insolvenz zu riskieren, wenn internationale Kunden wegen einer fehlenden zeitnahen Zu-/Absage Bestellungen stornieren.

5. Ressortübergreifenden Ansatz ausbauen

Der Erfolg des Strategiepapieres hängt mit Blick auf Start-ups und den Mittelstand davon ab, dass die Maßnahmen von allen Ressorts getragen und umgesetzt werden. Es wäre sinnvoll, auch das Bundesministerium für Bildung und Forschung eng in den Austausch mit Verwendern von Sicherheitstechnologie und den entwickelnden Unternehmen einzubinden. Damit das Strategiepapier auch einen praktischen positiven Effekt hat, ist die Umsetzung in allen betroffenen Bereichen und auf allen Hierarchiestufen eng zu begleiten. Periodisch sollte der Fortschritt der getroffenen Maßnahmen erfasst und evaluiert werden. Dies wäre als Zielvorgabe für eine hiermit speziell betraute Stelle oder einen Ausschuss wünschenswert.

6. Industrie- und Forschungsförderung gleichberechtigt ausgestalten

Im Strategiepapier wird dargelegt, dass die Sicherheits- und Verteidigungsindustrie durch Investitionen in Forschungsmaßnahmen gefördert werden soll. Als mögliche Maßnahmen sehen wir die gleichberechtigte Förderung von Forschungseinrichtungen und Wirtschaft.
Zwei Aspekte stehen hier im Vordergrund: Zum einen die Offenlegung von Forschungsergebnissen im Sinne einer »Open-Source« Politik und die Sicherung der Nutzung von Forschungsergebnissen durch die hier im Fokus stehenden Unternehmen. Zum anderen die konsequente Weiterführung von »Open Data«, indem die Daten maschinenlesbar per API bereitgestellt werden. Über die Veröffentlichung als Studien hinaus sind die Rohdaten und maschinenlesbaren Ergebnisse ebenfalls zur Verfügung zu stellen.

7. Abhängigkeiten vermeiden – Souveränität sicherstellen

Die Nutzung von Kernfähigkeiten der SVI durch öffentliche Auftraggeber kann unter Umständen mit signifikanten Abhängigkeiten verbunden sein. Zur Sicherung der Handlungsfähigkeit des öffentlichen Auftraggebers sollte sichergestellt werden, dass Kernfähigkeiten nicht nur durch einzelne Anbieter, sondern im europäischen und transatlantischen Wettbewerb erbracht werden können. Dieser Wettbewerb sichert zusätzlich die Weiterentwicklung und Innovation in den Kernfähigkeitsclustern und schafft damit Wettbewerbsfähigkeit im internationalen Wettbewerb.

Ihr Ansprechpartner BDSV

Kim-Laura Wöhlk
Referentin Cyber/ IT
T 030 2061899-15
k.woehlk@bdsv.eu

Friedrichstraße 60 | 10117 Berlin | www.bdsv.eu

Ihr Ansprechpartner Bitkom

Dr. Christian Weber
Bereichsleiter
Öffentliche Sicherheit & Verteidigung
T 030 27576-136
c.weber@bitkom.org

Albrechtstraße 10 | 10117 Berlin | www.bitkom.org