Europäischer Wirtschafts- und Sozialausschuss

CCMI/173
Die industrielle Dimension der Sicherheitsunion

STELLUNGNAHME

Europäischer Wirtschafts- und Sozialausschuss

Die industrielle Dimension der Sicherheitsunion
(Initiativstellungnahme)

Berichterstatter: **José Custódio LEIRIÃO**
Ko-Berichterstatter: **Jan PIE**

Beschluss des Plenums	20. Februar 2020
Rechtsgrundlage	Artikel 29 Absatz 2 der Geschäftsordnung Initiativstellungnahme
Zuständiges Arbeitsorgan	Beratende Kommission für den industriellen Wandel (CCMI)
Annahme in der CCMI	26/06/2020
Verabschiedung im Plenum	15/07/2020
Plenartagung Nr.	553
Ergebnis der Abstimmung (Ja-Stimmen/Nein-Stimmen/Enthaltungen)	209/3/4

1. **Schlussfolgerungen und Empfehlungen**

1.1 Wir begrüßen die Entschlossenheit der neuen Europäischen Kommission, die technologische Souveränität der Union zu stärken, und betonen die diesbezügliche Bedeutung des Sicherheitssektors. Ohne Technologie gibt es keine Sicherheit, und deshalb muss Europa die Technologien beherrschen, die für seine Sicherheit unerlässlich sind.

1.2 Um dieses Ziel zu erreichen, fordern wir die Europäische Kommission auf, eine Strategie auf den Weg zu bringen, die die industriellen und technologischen Fähigkeiten Europas im Sicherheitsbereich stärkt. Dies ist dringend erforderlich, insbesondere in sensiblen Bereichen, in denen die Abhängigkeit von außereuropäischen Lieferanten an sich schon zu einem Sicherheitsrisiko werden kann. Die Strategie muss die Ziele der neuen Strategie der inneren Sicherheit unterstützen und sie durch eine industrielle Dimension ergänzen. Sie sollte dazu beitragen, den derzeitigen und künftigen Fähigkeitenbedarf europäischer Endnutzer zu decken und die wesentlichen Probleme zu beheben, vor denen die Branche in Europa steht, nämlich Marktfragmentierung, Mangel an langfristiger Fähigkeiten- und Technologieplanung sowie Inkohärenz der politischen Maßnahmen und Finanzierungsinstrumente der EU.

1.3 Die Strategie für die Sicherheitsindustrie sollte auf folgenden Grundsätzen basieren:

a) Die Existenz einer innovativen Sicherheitsindustrie ist für die technologische Souveränität und strategische Autonomie Europas von entscheidender Bedeutung;
b) Sicherheit ist eine Frage der Souveränität, die nicht ausschließlich den Kräften des Marktes überlassen werden darf. Es bedarf politischen Willens und entsprechender Maßnahmen, um die Kapazität zur Entwicklung komplexer Hi-Tech-Sicherheitslösungen aufrechtzuerhalten.
c) Angesichts der Covid-19-Pandemie muss die Widerstandsfähigkeit gegen größere Katastrophen – seien sie natürlichen Ursprungs oder vom Menschen verursacht – zu einer der wichtigsten politischen Prioritäten der Union werden; diese Resilienz kann nur unter Mitwirkung der europäischen Sicherheitsindustrie erreicht werden.

Die Strategie sollte als Teil der Sicherheitsunion entwickelt werden und die sicherheitspolitischen Maßnahmen der EU wirksamer machen. Sie sollte einem ganzheitlichen Ansatz folgen und folgende Ziele umfassen:

- Bewertung der Anfälligkeit und der Abhängigkeit Europas in kritischen Bereichen der nichtmilitärischen Sicherheit;
- Überprüfung der neuesten Technologien auf mögliche Sicherheitsrisiken;
- Festlegung unerlässlicher Schlüsseltechnologien, für die Europa aus Sicherheitsgründen nicht von Lieferanten aus Drittstaaten abhängig sein sollte;
- Ermittlung strategischer Wertschöpfungsketten im Sicherheitssektor;
- Einsatz von EU-Agenturen als Triebkräfte für Fähigkeitenplanung und die Harmonisierung nationaler Erfordernisse;
- Nutzung sicherheitsrelevanter EU-Instrumente (ISF, IBMF, Digitales Europa, Horizont Europa, RescEU) für gezielte Investitionen in wesentliche Sicherheitstechnologien und -anwendungen;

- Nutzung anderer EU-Instrumente (Strukturfonds, InvestEU usw.) für sicherheitsrelevante Investitionen (Infrastruktur), idealerweise durch die Schaffung einer Fazilität zur Sicherung Europas (analog zur Fazilität „Connecting Europe“);
- Nutzung der europäischen Auftragsvergabe und Koordinierung der nationalen Auftragsvergabe zur Unterstützung der entsprechenden industriellen Basis;
- Nutzung fähigkeitenorientierter Finanzierungsinstrumente (wie ISF und IBMF) zur Förderung der Marktakzeptanz der EU-Sicherheitsforschung über Horizont Europa hinaus;
- Ermittlung möglicher neuer Gesetzgebungsinitiativen, etwa eine Überarbeitung der Richtlinie für den Schutz kritischer Infrastrukturen oder ein Instrument für Sicherheit in der Stadt;
- Koordinierung einschlägiger EU-Programme (Verteidigung, Sicherheit, Raumfahrt, Cybersicherheit).

Einführung

1.4 Europas Sicherheitsumfeld ist hochkomplex: Die derzeitigen Sicherheitsbedrohungen sind vielschichtig, länderübergreifend, in rascher Entwicklung begriffen und schwer vorhersehbar. Sie können ein breites Spektrum von Zielen in der gesamten Union betreffen (z. B. Massenveranstaltungen, Verkehr, kritische Infrastruktur und Institutionen) und gehen von einer ebenso großen Vielzahl von Bedrohungsakteuren aus (z. B. Einzeltäter, kriminelle Vereinigungen, terroristische Gruppierungen, Nationalstaaten), die sehr unterschiedliche Beweggründe (z. B. Geopolitik, religiöser oder politischer Extremismus, wirtschaftliche bzw. finanzielle Interessen oder psychische Störungen) haben und Mittel aller Art einsetzen könnten (z. B. Feuerwaffen, unkonventionelle Spreng- und Brandvorrichtungen, CBRN-Waffen, Cyberangriffe oder Desinformation), um ihre böswillige Absicht in die Tat umzusetzen.

1.5 Zusätzlich zu den vom Menschen verursachten Sicherheitsbedrohungen gibt es Naturkatastrophen wie Überschwemmungen, Dürren, Stürme oder Pandemien, die aufgrund des Klimawandels, der Umweltverschmutzung und der übermäßigen Ausbeutung natürlicher Ressourcen ein wachsendes Risiko darstellen. Naturkatastrophen sind in der Regel noch verheerender als anthropogene Katastrophen und stellen eine unmittelbare oder indirekte Gefahr für die Sicherheit dar.

1.6 Sicherheitsbedrohungen sind unterschiedlich und das gilt natürlich auch für die Sicherheitskräfte und die Fähigkeiten, über die sie verfügen müssen. Gleichzeitig arbeiten Sicherheitskräfte häufig zusammen, etwa als Ersthelfer bei einer Katastrophe, und benötigen daher interoperable Ausrüstungen, die der jeweiligen Bedrohung entsprechen.

1.7 Trotz ihrer Unterschiedlichkeit haben die heutigen Sicherheitsbedrohungen eines gemein: Sie können ohne technologische Unterstützung nicht bewältigt werden. Technik an sich kann keine Sicherheit bieten, aber in unseren komplexen und vernetzten Gesellschaften ist ihre Nutzung eine unverzichtbare Voraussetzung in allen Sicherheitsbereichen und in allen Phasen des Sicherheitszyklus (Prävention, Vorbereitung, Reaktion und Wiederherstellung). Die rasche Entwicklung und Verbreitung neuer digitaler Technologien wie künstliche Intelligenz, Quantencomputer und Blockchain wird die Bedeutung der Technik für die Sicherheit noch

verstärken, da sie nicht nur neue Möglichkeiten bieten, sondern zugleich auch viele Schwachstellen und potenzielle Angriffsflächen schaffen.

1.8 Ohne das Fachwissen einer spezialisierten Sicherheitsindustrie ist es unmöglich, modernste Technologien zu entwickeln, die für die Bewältigung aktueller und künftiger Sicherheitsbedrohungen erforderlich sind. Die Sicherheitsindustrie ist ein überaus wichtiger Partner, insbesondere für komplexe Sicherheitssysteme und den Schutz vor raffinierten Bedrohungsakteuren.

1.9 Die sicherheitsindustrielle und sicherheitstechnische Basis in Europa ist so vielfältig wie die Sicherheitserfordernisse moderner Gesellschaften und Volkswirtschaften. Sie umfasst Unternehmen aller Größen aus der gesamten Union mit unterschiedlichen Angeboten und Spezialisierungen. Viele von ihnen sind auch in den Bereichen Verteidigung, Luft- und Raumfahrt oder kommerzielle IT tätig oder sind Tochtergesellschaften größerer Konzerne aus diesen Sektoren. Sie entwickeln und produzieren Hochtechnologiesysteme und erbringen Dienstleistungen, die erforderlich sind, um unsere Gesellschaften, Unternehmen, Behörden und Bürger vor allen Arten von Sicherheitsbedrohungen und Katastrophen zu schützen. In der jüngsten umfassenden Studie wird der Umsatz der Sicherheitsindustrie in der EU auf fast 200 Mrd. EUR geschätzt; in dieser Branche sind 4,7 Millionen Menschen beschäftigt[1].

2. Allgemeine Bemerkungen

2.1 Die Union hat ein wirtschaftliches, aber auch ein strategisches Interesse an der Förderung einer dynamischen sicherheitsindustriellen Basis in Europa. Je kritischer ein Sicherheitsbereich ist, desto größer kann die Abhängigkeit von Lieferanten aus Drittländern an sich zu einem Sicherheitsrisiko werden. Gerade wenn es um den Schutz kritischer Infrastrukturen und staatlicher Einrichtungen vor Bedrohungen durch staatliche oder staatlich unterstützte Akteure geht, müssen unbedingt Technologien, Dienste und Ausrüstung genutzt werden, die von vertrauenswürdigen Quellen stammen.

2.2 Der Verlauf der Covid-19-Pandemie und ihre direkten und indirekten Folgen haben ebenfalls gezeigt, dass wir eine starke europäische Sicherheitsindustrie brauchen. Der massive Rückgriff auf digitale Instrumente hat beispielsweise zu einer dramatischen Zunahme von Cyberangriffen sowohl von nichtstaatlichen als auch von staatlichen Akteuren auf Unternehmen und Betreiber wesentlicher Dienste geführt. Die Stärkung der Abwehrfähigkeit gegenüber Cyberangriffen und der Cybersicherheit in allen digitalen Prozessen von Unternehmen und Behörden sollte daher eine wichtige Lehre aus der Pandemie sein. Seit dem Ausbruch des Virus haben wir erneut Desinformationskampagnen erlebt, hinter denen häufig ausländische Regierungen stehen und die ohne ausgeklügelte technische Tools nicht wirksam bekämpft werden können. Covid-19 hat auch große Defizite bei den Krisenbewältigungsfähigkeiten der EU aufgezeigt, wie etwa das

[1] Angesichts der Vielfalt des Sektors gibt es derzeit keine klare Definition der Sicherheitsindustrie und nur grobe Schätzungen der Marktgröße. Eine methodische Klassifizierung dieses Wirtschaftszweigs wird durch eine Reihe von Faktoren behindert: 1) die Sicherheitsindustrie wird von den wichtigsten statistischen Systematiken (NACE, Prodcom usw.) nicht erfasst; 2) die sicherheitsrelevanten Posten sind unter einer Vielzahl von Rubriken verborgen, und die Statistiken für diese Rubriken unterscheiden nicht zwischen sicherheitsrelevanten und nicht sicherheitsrelevanten Tätigkeiten; 3) von Seiten der Branche selbst gibt es keine Quelle für europaweite statistische Daten. Siehe die Studie über die Erhebung statistischer Daten über die technologische und industrielle Basis der europäischen Sicherheit – Ecorys-Abschlussbericht für die Europäische Kommission, GD Migration und Inneres, Juni 2015.

Fehlen eines gemeinsamen Vorrats an CBRN-Schutzausrüstung. Kurz gesagt bedarf es einer Vielzahl von Maßnahmen, um Europa widerstandsfähiger gegenüber Katastrophen größeren Ausmaßes zu machen. Angesichts der Sensibilität der meisten dieser Maßnahmen ist es unerlässlich, sich bei deren Umsetzung auf vertrauenswürdige Lieferanten zu stützen, die die Versorgungssicherheit auch in Krisenzeiten gewährleisten.

2.3 Die Union hat daher ein strategisches Interesse daran, die industriellen Fähigkeiten in Europa zu erhalten, die erforderlich sind, um ein angemessenes Maß an Autonomie und technologischer Souveränität in kritischen Sicherheitsbereichen zu gewährleisten. Gleichzeitig ist es unter den derzeitigen Marktbedingungen leider schwer, diesem strategischen Interesse gerecht zu werden. Die Besonderheiten des europäischen Sicherheitsmarktes erschweren es den Unternehmen nämlich häufig, tragfähige Geschäftsszenarien für die betreffenden Technologien zu entwickeln.

2.4 Außerdem ist aus kommerzieller Sicht die Nachfrage nach kostenintensiven, dem neuesten Stand der Technik entsprechenden Sicherheitsprodukten begrenzt. Da private Marktteilnehmer ständig bemüht sind, ihre Kosten zu senken, beschränken sie Investitionen in die Sicherheit in der Regel auf das absolut Notwendige und bevorzugen das billigste Standardprodukt (häufig von Lieferanten aus Drittländern).

2.5 Bei der öffentlichen Nachfrage auf dem Sicherheitsmarkt gibt es eine breite Palette von Käufern und Endnutzern, von denen die meisten über begrenzte Budgets verfügen, kleinere Bestellungen tätigen und rechtlich verpflichtet sind, zum niedrigsten Preis einzukaufen. Darüber hinaus verfügt die überwiegende Mehrheit der öffentlichen Kunden im Bereich der Sicherheit über keinerlei Pläne für die Fähigkeitenentwicklung. Sie kaufen Standardlösungen, um ihren unmittelbaren Bedarf zu decken und ohne langfristige Überlegungen darüber anzustellen, wie sich Bedrohungen und Technologien in der Zukunft entwickeln könnten, geschweige denn welche Investitionen notwendig sind, um entsprechend vorbereitet zu sein.

2.6 Angesichts der Besonderheiten beider Seiten der Nachfrage im Bereich der Sicherheit gibt es nur einen kleinen Markt für kritische Technologien und Anwendungen. Komplexe Sicherheitslösungen werden häufig für einen einzelnen oder sehr wenige Kunden maßgeschneidert, wodurch Produktionsvolumen und Größenvorteile auf ein Minimum beschränkt sind. Bestenfalls können die für solche Systeme verwendeten Technologien für andere, weniger sensible Anwendungen auf einem breiteren Markt für gewerbliche Kunden eingesetzt werden. Aufgrund der derzeitigen Marktbedingungen ist es daher unmöglich, eine technologische und industrielle Basis in der EU zu erhalten, die diejenigen Sicherheitsfähigkeiten zu entwickeln vermag, mit denen Europa seine Außengrenzen, sein Hoheitsgebiet und seine Bürgerinnen und Bürger schützen kann. Dies beschädigt die Glaubwürdigkeit der Sicherheitsunion und verlangt nach stärkeren EU-Maßnahmen.

Aktueller Stand der EU-Sicherheitspolitik

2.7 Seit dem Start der Europäischen Sicherheitsagenda im April 2015 bemüht sich die EU um eine echte Sicherheitsunion, die die Instrumente, die Infrastruktur und das Umfeld bietet, in denen die nationalen und europäischen Behörden wirksam zusammenarbeiten, um gemeinsame Herausforderungen zu bewältigen und gleichzeitig die Rechte und Freiheiten der Bürgerinnen

und Bürger zu schützen[2]. Allein schon die Zahl der Initiativen in diesem Zusammenhang zeigt, dass Sicherheit endgültig zu den vorrangigen Prioritäten der Union gehört:

- Richtlinie zur Terrorismusbekämpfung[3]
- Neue Vorschriften zur Bekämpfung der Geldwäsche[4]
- Einrichtung des Schengener Informationssystems (SIS)[5]
- Interoperabilität zwischen EU-Informationssystemen in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung[6]
- Einrichtung der Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA)[7]
- Rechtsakt zur Cybersicherheit[8]
- Gestärkte Europäische Grenz- und Küstenwache („Frontex“)[9]
- Europäisches Reiseinformations- und -genehmigungssystem (ETIAS)[10].

Mit diesen Initiativen werden bereits bestehende Programme und Finanzierungsinstrumente wie der Fonds für die innere Sicherheit ergänzt.

2.8 Der Kommissionsvorschlag für den nächsten mehrjährigen Finanzrahmen (MFR) enthielt im Vergleich zum vorangegangenen MFR eine erhebliche Aufstockung der einschlägigen Haushaltslinien (z. B. 35,3 Mrd. EUR für Migration und Grenzmanagement, 4 Mrd. EUR für innere Sicherheit, 15,6 Mrd. EUR für Resilienz und Krisenreaktion)[11]. Die Union finanziert über Horizont Europa auch ein weiteres Programm für Sicherheitsforschung, das im Rahmen

2 Mitteilung der Kommission „Umsetzung der Europäischen Sicherheitsagenda im Hinblick auf die Bekämpfung des Terrorismus und die Weichenstellung für eine echte und wirksame Sicherheitsunion“, Brüssel, 20.4.2016, COM(2016) 230 final https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:52016DC0230&from=DE.

3 Richtlinie zur Terrorismusbekämpfung (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32017L0541&from=DE).

4 Richtlinie zur Verhinderung der Nutzung des Finanzsystems zum Zwecke der Geldwäsche und der Terrorismusfinanzierung (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015L0849&from=DE).

5 Verordnung über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen (https://data.consilium.europa.eu/doc/document/PE-35-2018-INIT/de/pdf) & Verordnung über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen (https://data.consilium.europa.eu/doc/document/PE-36-2018-INIT/de/pdf).

6 Verordnung zur Errichtung eines Rahmens für die Interoperabilität (Grenzen und Visa) (https://data.consilium.europa.eu/doc/document/PE-30-2019-INIT/de/pdf) & Verordnung zur Errichtung eines Rahmens für die Interoperabilität (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) (https://data.consilium.europa.eu/doc/document/PE-31-2019-INIT/de/pdf).

7 Verordnung über die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32018R1726&from=de).

8 Verordnung über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R0881&from=DE).

9 Verordnung über die Europäische Grenz- und Küstenwache, http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R1896&from=DE.

10 Verordnung über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystem (ETIAS) http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R1896&from=DE.

11 Zu aktuellen Preisen. Siehe die Mitteilung der Kommission „Der EU-Haushalt als Motor für den Europäischen Aufbauplan“, Brüssel, 27.5.2020, COM(2020) 442 final: https://ec.europa.eu/transparency/regdoc/rep/1/2020/DE/COM-2020-442-F1-DE-MAIN-PART-1.PDF.

von Horizont 2020 bereits erheblich zur Gestaltung und Entwicklung künftiger Sicherheitsfähigkeiten beigetragen hat.

2.9 In Bezug auf digitale Technologien schlägt die Europäische Kommission außerdem vor, die Ausgaben (z. B. für Horizont Europa oder das Programm „Digitales Europa“) erheblich zu erhöhen, um die technologische Souveränität Europas in strategisch wichtigen Bereichen zu verstärken. In diesem Zusammenhang verkündete die Kommission auch ihre Absicht, Synergien zwischen dem Raumfahrt-, dem Verteidigungs- und dem Sicherheitssektor zu fördern.

2.10 Technologische Souveränität ist auch ein Schlüsselbegriff in der „neuen Industriestrategie für Europa“, in der die Kommission betont, dass der „digitale Wandel, die Sicherheit und (die) künftige technologische Souveränität (Europas) von unseren strategischen digitalen Infrastrukturen (abhängen)“ und angekündigt wird, dass sie „die Entwicklung von Schlüsseltechnologien unterstützen (wird), die für die industrielle Zukunft Europas strategisch wichtig sind“[12].

Besondere Bemerkungen

2.11 Die Zuständigkeit der EU im Bereich der Sicherheit ist nach wie vor begrenzt und äußert sich sehr oft nur in einer Koordinierung zwischen den nationalen Behörden. Daher ist die Sicherheitspolitik nach wie vor fragmentiert und oft unwirksam. Gleiches gilt für andere sicherheitsrelevante Bereiche wie die öffentliche Gesundheit.

2.12 Sicherheit in der EU ist eine politische Priorität, der die industrielle Dimension fehlt. Es gibt eine beeindruckende Zahl sicherheitsrelevanter Maßnahmen und Finanzierungsinstrumente mit beträchtlichen Budgets. Allerdings gibt es weder eine Koordinierung des Fähigkeitenbedarfs noch eine kohärente Politik zur Unterstützung der einschlägigen industriellen und technologischen Basis. Begriffe wie industrielle Wettbewerbsfähigkeit, strategische Autonomie, Fähigkeitenplanung und kritische Technologien tauchten in der Debatte über die Sicherheitsunion nicht auf und wurden nirgendwo als Ziele sicherheitsbezogener Finanzierungsprogramme betrachtet.

2.13 Bei dem *Maßnahmenkatalog für eine innovative und wettbewerbsfähige Sicherheitsbranche* aus dem Jahr 2012 mangelte es der Kommission an Ehrgeiz; seine Tragweite war begrenzt und daher hatte er auch keine nennenswerte Wirkung.

2.14 Durch das Sicherheitsforschungsprogramm der EU werden zwar beträchtliche Ressourcen mobilisiert, es weist jedoch gravierende Schwächen auf. Die Aufnahme von Forschungsergebnissen durch den Markt bleibt ein großes Problem, denn es gibt weder ein gemeinsames Verfahren zur Fähigkeitenplanung für Sicherheit, mit dem die Nachfrage öffentlicher Endnutzer konsolidiert würde, noch einen systematischen Einsatz anderer fähigkeitenorientierter EU-Finanzierungsinstrumente, um die Einführung von Sicherheitslösungen zu unterstützen.

12 Mitteilung der Kommission „Eine neue Industriestrategie für Europa“, Brüssel, 10.3.2020, COM(2020) 102 final https://eur-lex.europa.eu/legal-content/dE/TXT/PDF/?uri=CELEX:52020DC0102&from=dE.

2.15 Die neue Strategie der inneren Sicherheit dient als Richtschnur für die Sicherheitspolitik der EU und sollte daher darauf abzielen, diese Defizite zu beseitigen. So muss die rasche technische Entwicklung und ihre Auswirkungen auf die Sicherheit behandelt, auf eine gemeinsame Definition des Bedarfs an Sicherheitsfähigkeiten gedrängt und die europäische Zusammenarbeit zur Befriedigung dieses Bedarfs gefördert werden. Dies würde die Sicherheitsunion stärken und erheblich zur Schaffung eines echten Binnenmarkts für Sicherheit sowie zur Aufrechterhaltung einer wettbewerbsfähigen Sicherheitsindustrie in Europa beitragen.

2.16 Wenn Technologien zu Lösungen werden sollen, ist die Industrie unerlässlich. Eine ehrgeizige Industriepolitik für Kernbereiche der Souveränität sollte daher eine politische Priorität für die Union sein. Die Entwicklung einer solchen Politik ist für den Sicherheitssektor besonders dringend, der derzeit unter gravierendem Marktversagen leidet, was die Aufrechterhaltung kritischer industrieller und technologischer Kapazitäten erschwert.

2.17 Daher rufen wir die Europäische Kommission auf, eine spezifische Strategie für die Sicherheitsindustrie zu entwickeln, um die neue Strategie der inneren Sicherheit zu unterstützen und die Sicherheitsunion wirksamer zu machen. Mit dieser Industriestrategie, die ambitioniert und umfassend sein sollte, muss gewährleistet werden, dass alle einschlägigen Maßnahmen und Instrumente zur technologischen Souveränität der Union in kritischen Sicherheitsbereichen beitragen. Außerdem sollte sichergestellt werden, dass alle sicherheitsbezogenen EU-Instrumente (ISF, IBMF, RescEU) eine industrielle Dimension und alle technologiebezogenen Programme (Digitales Europa, Horizont Europa) eine Sicherheitsdimension beinhalten. Dies würde dazu beitragen, die Sicherheitsbedürfnisse öffentlicher Kunden zu befriedigen, der europäischen Industrie neue Möglichkeiten eröffnen und es leichter machen, rechtzeitig auf die sicherheitsrelevanten Auswirkungen neuer Technologien zu reagieren.

2.18 Zu diesem Zweck muss das Konzept der technologischen Souveränität näher definiert und praktisch umgesetzt werden. Es ist begrüßenswert, dass die Kommission den Schwerpunkt derzeit auf digitale Technologien legt; dies sollte jedoch nicht ausschließlich so sein. Vorrangig sollte es um alle kritischen Technologien in Kernbereichen der Souveränität – Sicherheit, Verteidigung und Raumfahrt – gehen. Das Konzept sollte auch vor dem Hintergrund der Covid-19-Pandemie überarbeitet und Resilienz als strategisches Ziel darin aufgenommen werden.

2.19 Die „Neue Industriestrategie für Europa“ der Kommission enthält Elemente, die für die Förderung der technologischen Souveränität in kritischen Sicherheitsbereichen wichtig sind. Insbesondere das Konzept der strategischen Wertschöpfungsketten sollte als Rahmen für einen umfassenden Ansatz dienen, der den gesamten industriellen Zyklus von der Lieferung kritischer Materialien bis hin zur Industrialisierung und Wartung abdeckt und den Einsatz aller geeigneten politischen Instrumente, einschließlich der Kontrolle ausländischer Direktinvestitionen, koordiniert.

2.20 Der nächste mehrjährige Finanzrahmen muss den Erfordernissen der (Post-) Covid-19-Ära angepasst werden, ebenso wie die politischen Maßnahmen, die durch den MFR unterstützt werden, und die von ihm finanzierten Programme. Zuvor festgelegte Prioritäten und

Instrumente müssen überprüft werden, wobei die Lehren aus den Schwierigkeiten Europas bei der Bewältigung der Pandemie zu berücksichtigen sind. Dies gilt auch für die Sicherheitsunion und die neue Strategie der inneren Sicherheit, in der die Notwendigkeit größerer technologischer Souveränität und Widerstandsfähigkeit hervorgehoben werden sollte.

2.21 Um die durch die Pandemie ausgelöste Rezession zu überwinden, sollte die EU im nächsten Haushaltszyklus Investitionen auf Hochtechnologiebranchen konzentrieren, da diese den größten Mehrwert und Multiplikatoreffekte für die Wirtschaft insgesamt aufweisen[13]. Eine Strategie für die Sicherheitsindustrie der EU, die dazu beiträgt, Europa autonomer und widerstandsfähiger zu machen, würde sich nahtlos in diesen Ansatz einfügen und sollte daher dringend im Rahmen des Covid-19-Wiederaufbauprogramms der Union lanciert werden.

Brüssel, den 15. Juli 2020

Luca Jahier
Präsident des Europäischen Wirtschafts- und Sozialausschusses

_____

13 Siehe z. B. „Il ruolo dell'innovazione et dell'alta technologia in Italia nel confronto con il contesta internazionale“, Centro economia digitale, Rom, Oktober 2019.