BREMISCHE BÜRGERSCHAFT Drucksache 21/
Landtag
21. Wahlperiode

Große Anfrage der Fraktion der CDU

Cyberkriminalität und Wirtschaftsspionage: Wie reagiert der Senat Bovenschulte auf die anhaltende Bedrohungslage im Land Bremen?

Cybersicherheit ist für das Funktionieren unseres staatlichen Gemeinwesens von herausragender Bedeutung. Insbesondere eine Beeinträchtigung oder ein Ausfall Kritischer Infrastrukturen hätte für die öffentliche Sicherheit und Daseinsvorsorge, die Wirtschaft und jeden Einzelnen dramatische Folgen. Laut Bundeslagebild Cybercrime 2023 des BKA ist die Zahl der Cyberstraftaten im engeren Sinn, d.h. Straftaten, die sich gegen das Internet und informationstechnische Systeme richten, erneut gestiegen. (Der Begriff Cyberkriminalität wird hier als Synonym für diese Definition verwendet.) Das zeigt sich insbesondere, wenn man neben der inländischen Polizeilichen Kriminalstatistik (PKS) den Blick auch auf Straftaten richtet, die hierzulande Auswirkungen haben, bei denen sich die Täter jedoch im Ausland oder an einem unbekannten Aufenthaltsort befinden (Auslands-PKS). Schließlich spielen geographische Grenzen für Cyberkriminelle kaum eine Rolle. Die PKS bildet dabei nur das Hellfeld ab, also die polizeilich bekannt gewordene Kriminalität. Gerade im Bereich der Cyberkriminalität ist das Dunkelfeld jedoch sehr groß, da nur ein Teil der Vorfälle bemerkt und von diesen wiederum nur ein Teil zur Anzeige gebracht wird.

Durch das Fortschreiten der Digitalisierung, insbesondere durch die Nutzung entsprechender KI-Tools, nehmen die Sicherheitsrisiken und möglichen Auswirkungen von Cyberkriminalität stetig zu. Der internationale Aspekt der Cyberkriminalität tritt dabei immer weiter in den Vordergrund. Dies gilt insbesondere seit dem Beginn des russischen Angriffskriegs gegen die Ukraine am 24. Februar 2022. Eine klare Zuordnung der Cyberangriffe zu bestimmten Verursachern ist dabei häufig schwierig bis unmöglich. Die Grenze zwischen politisch ideologischer und finanziell motivierter Cyberkriminalität verschwimmt zunehmend. Der durch Cyberkriminalität verursachte Schaden ist immens: Der Branchenverband Bitkom e.V. rechnet für das Jahr 2023 mit Schäden in Höhe von rund 206 Mrd. Euro für deutsche Unternehmen. Fast drei Viertel davon (148,2 Mrd. Euro bzw. 72 Prozent) sind auf Cyberattacken zurückzuführen. Laut dem Bitkom-Bericht „Wirtschaftsschutz 2023“ waren 80 Prozent der befragten Unternehmen betroffen oder vermutlich betroffen. Erstmals fühlt sich die Mehrheit der Unternehmen durch Cyberattacken in ihrer geschäftlichen Existenz bedroht. Dabei spielen Cyberspionage – als eine Methode der Wirtschaftsspionage – und, besonders bei Betreibern kritische Infrastrukturen, Cybersabotage eine exponierte Rolle.

Auch das Phänomen der Wirtschaftsspionage und Konkurrenzausspähung ist durch ein großes Dunkelfeld gekennzeichnet, wobei hier die Schäden noch schwieriger abzuschätzen sind als bei Cyberkriminalität. Im ersten Fall findet die Ausspähung durch fremde Staaten oder deren Nachrichtendienste statt. Es handelt sich dabei um ein Staatsschutzdelikt, für dessen Verfolgung der Generalbundesanwalt und für dessen Prävention die Verfassungsschutzbehörden des Bundes und der Länder zuständig sind. Im zweiten Fall handelt es sich um die Ausforschung eines Unternehmens durch andere Unternehmen, Einzelpersonen oder organisierte Gruppen. Die Verfolgung obliegt der Justiz der Länder und fällt in die Zuständigkeit der Wirtschaftskriminalität. Beide Fälle zielen darauf ab, unbemerkt und unter Verwendung von „unehrlichen“ Mitteln an Know-how und Informationen (z.B. über neue Technologien, Produktionsabläufe, Strategiepapiere, Kunden- und Lieferantenlisten etc.) zu gelangen, die die Wirtschaftskraft des eigenen Unternehmens oder des eigenen Landes verbessern. Wirtschaftsspionage ist eine ernstzunehmende und dennoch oft unterschätzte Gefahr in unserer globalisierten, vernetzten Welt. Der ungewollte Abfluss von Wissen gefährdet unmittelbar den wirtschaftlichen Erfolg von Unternehmen, aber mittelbar auch die Wettbewerbsfähigkeit unseres Wirtschaftsstandorts.

Um schwerwiegende Gefahren durch Cyberkriminalität und Schäden durch Wirtschaftsspionage für Staat, Wirtschaft und Gesellschaft besser und effektiver abwehren zu können, ist eine ganzheitliche Betrachtung dieser Phänomene sowie eine abgestimmte Vorgehensweise der beteiligten Institutionen und föderalen Ebenen erforderlich. Die Ausstattung und Handlungsmöglichkeiten der Strafverfolgungsbehörden und Nachrichtendienste müssen dafür – auch im Land Bremen – gestärkt werden.

Vor diesem Hintergrund fragen wird den Senat:

1. Wie bewertet der Senat die aktuelle Bedrohungslage durch Cyberkriminalität sowie Wirtschaftsspionage im Land Bremen?

    a. Welche Gefahr sieht er auf diesem Feld konkret für bremische Unternehmen, Forschungseinrichtungen und sonstige Institutionen durch staatliche, staatlich gesteuerte oder nicht staatliche Akteure und welche Erkenntnisse liegen ihm dazu vor?

    b. Welche Gefahr sieht er konkret durch Cyberangriffe fremder Nachrichtendienste auf die Liefer- bzw. Wertschöpfungskette (sog. „Supply-Chain-Angriff“) und welche Erkenntnisse liegen ihm dazu vor?

    c. Wie hoch schätzt der Senat die materiellen, immateriellen und finanziellen volkswirtschaftlichen Schäden durch Cyberkriminalität und Wirtschaftsspionage im Land Bremen?

2. Wie viele privatwirtschaftliche Unternehmen, Forschungseinrichtungen und Institutionen etc. im Land Bremen waren nach Kenntnis des Senats in den Jahren 2020 bis 2023 von Cybercrime im engeren Sinne (einschließlich Cyberspionage und -sabotage) sowie von Wirtschaftsspionage oder Konkurrenzausspähung betroffen? Welche Erkenntnisse hat der Senat im Hinblick auf die betroffenen Unternehmenstypen und -branchen, Schadensart und -höhe, Methode bzw. Angriffstyp sowie das Dunkelfeld?

a. Wie schätzt der Senat Risikobewusstsein und Sicherheitsvorkehrungen des privaten Sektors im Land Bremen gegen Cyberkriminalität, Wirtschaftsspionage oder Konkurrenzausspähung ein? Worin liegen signifikante Unterschiede zwischen einzelnen Unternehmen und Branchen seines Erachtens begründet?

3. Welche Behörden (inkl. Eigen- und Beteiligungsbetriebe, Betriebe gewerblicher Art, Stiftungen etc.) im Konzern Bremen waren in den Jahren 2020 bis 2023 von Cybercrime im engeren Sinne (einschließlich Cyberspionage und -sabotage) betroffen? Welche Arten von Cyberattacken wurden dabei verübt und welche Schäden sind dadurch entstanden? (bitte jeweils nach Organisationseinheit, Sachschaden, Angriffstyp und entstandenem wirtschaftlichem Schaden gliedern) Inwieweit spielt(e) bei Beteiligungsbetrieben der FHB auch das Phänomen Wirtschaftsspionage oder Konkurrenzausspähung eine Rolle (bitte erläutern)?

   a. Wie schätzt der Senat Risikobewusstsein und Sicherheitsvorkehrungen gegen Cyberkriminalität und ggf. Wirtschaftsspionage oder Konkurrenzausspähung im Konzern Bremen ein? Worin liegen signifikante Unterschiede zwischen einzelnen Dienststellen und Organisationseinheiten seines Erachtens begründet?

   b. Welche konkreten Schritte hat der Senat unternommen, um dem Aufruf des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Überprüfung der IT-Sicherheitsmaßnahmen und Anpassung an die gegebene Bedrohungslage nachzukommen?

   c. Wie genau gestaltet sich die fachliche Zusammenarbeit und Kooperationen der Freien Hansestadt Bremen, ihrer Behörden, Institutionen und öffentlicher Unternehmen mit dem Bund und anderen Bundesländern zur Abwehr von Cyberkriminalität, Wirtschaftsspionage und Konkurrenzausspähung? (bitte auflisten und rechtliche Grundlagen, Tätigkeitsbereiche, handelnde Personen bzw. Dienststellen sowie Ergebnisse darstellen)

4. Welche Betreiber Kritischer Infrastruktur (KRITIS) im Land Bremen waren in den Jahren 2020 bis 2023 von Cybercrime im engeren Sinne (einschließlich Cyberspionage und -sabotage) betroffen? Welche Arten von Cyberattacken wurden dabei verübt, welche Schäden sind dadurch entstanden und wie lange haben etwaige Ausfälle kritischer Infrastruktur gedauert? (bitte jeweils nach Betreiber, Sachschaden, Angriffstyp und entstandenem wirtschaftlichem Schaden gliedern)

   a. Wie schätzt der Senat Risikobewusstsein und Sicherheitsvorkehrungen gegen Cyberkriminalität bei den KRITIS-Betreibern im Land Bremen ein? Worin liegen signifikante Unterschiede zwischen einzelnen Betreibern seines Erachtens begründet?

   b. Wie viele Sicherheitsüberprüfung für den vorbeugenden personellen Sabotageschutz in lebens- und verteidigungswichtigen Einrichtungen fanden in den Jahren 2020 bis 2023 unter Beteiligung des Landesamts für Verfassungsschutz Bremen mit welchem Ausgang statt? (wenn möglich, nach Art der Einrichtung gliedern)

c. Welchen konkreten Beitrag hat der Senat in welchen Bereichen geleistet bzw. leistet er, um die 2023 in Kraft getretene EU-Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie) im Land Bremen umzusetzen? Inwiefern ist die in der Richtlinie geforderte „Kultur der Sicherheit“ in systemrelevanten Bereichen (z.B. Energie- und Wasserversorgung, Verkehr und Häfen, Bank- und Finanzdienstleistungen, Gesundheitsversorgung und digitale Infrastruktur) im Land Bremen aus Sicht des Senats vollumfänglich gewährleistet bzw. was ist dafür noch zu tun?

d. Wie ist der Stand der Arbeiten an dem ganzheitlichen Cybersicherheitskonzept für die bremischen Häfen und wer ist daran beteiligt? Welche konkreten Ziele sollen damit bis wann erreicht werden? Welche Maßnahmen wurden bzw. werden daraus wann, vom wem, mit welchem Erfolg umgesetzt und wie werden diese finanziert?

5. Wie hat sich die Zahl der Straftaten sowie deren Aufklärungsquote im Bereich Cybercrime im engeren Sinne nach dem PKS-Summenschlüssel 897000 und den dazugehörigen Straftatenschlüsseln bzw. Deliktbereichen (einschließlich der Schlüssel 5430**, 6742**, 6780** und 897100) in den Jahren 2020 bis 2023 im Land Bremen jeweils entwickelt? (bitte tabellarisch darstellen)

6. Wie hat sich der Anteil der Cyberstraftaten an den im Land Bremen registrierten Auslandsstraftaten (in absoluten und relativen Zahlen) sowie deren Aufklärungsquote nach dem PKS-Summenschlüssel 897000 und den dazugehörigen Straftatenschlüsseln bzw. Deliktbereichen (einschließlich der Schlüssel 5430**, 6742**, 6780** und 897100) in den Jahren 2020 bis 2023 im Land Bremen jeweils entwickelt? (bitte tabellarisch darstellen)

7. Unter welchem Straftatenschlüssel/Deliktsbereich wird Wirtschaftsspionage oder Konkurrenzausspähung (näherungsweise) in der PKS abgebildet (z.B. Summenschlüssel 719200 und Straftatenschlüssel 6780**)? Wie hat sich die Anzahl dieser Straftaten sowie deren Aufklärungsquote in den Jahren 2020 bis 2023 im Land Bremen jeweils entwickelt? (bitte tabellarisch darstellen)

8. Wie viele Ermittlungsverfahren seitens der Polizei und der Staatsanwaltschaft gab es in den Jahren 2020 bis 2023 im Land Bremen in den Bereichen Cybercrime im engeren Sinne (einschließlich Cyberspionage und -sabotage) sowie Konkurrenzausspähung und wie gingen diese aus (Einstellung, Strafbefehl, Verurteilung, Freispruch etc.)?

9. Wie sind die Polizei Bremen, die Staatsanwaltschaft Bremen und das Landesamt für Verfassungsschutz im Kampf gegen Cyberkriminalität, Wirtschaftsspionage und Konkurrenzausspähung personell, materiell und finanziell ausgestattet und aufgestellt? Inwiefern hält der Senat die Ausstattung für die gezielte Bearbeitung dieses Deliktfeldes für ausreichend bzw. wo sieht er Nachsteuerungsbedarf?

a. Inwieweit erschweren in diesem Feld fehlende Gesetzesgrundlagen wie die der Quellentelekommunikationsüberwachung, der Standortermittlung oder der Telekommunikationsüberwachung die Arbeit der Polizei Bremen und des Landesamts

für Verfassungsschutz? Wie geht der Senat mit dem Problem um, dass im Netz vielfach anonym und verschlüsselt kommuniziert wird?

b. Welchen Änderungsbedarf bestehender Gesetze sieht der Senat, um Cyberkriminalität besser bekämpfen zu können? Welche gesetzlichen Änderungen gab es seit dem Jahr 2020 auf Bundesebene in diesem Bereich und wie bewertet der Senat diese? Inwieweit können (neuere) gesetzliche Möglichkeiten der Fahndung und Strafverfolgung durch die Sicherheits- und Ermittlungsbehörden im Land Bremen tatsächlich genutzt werden und welche gegebenenfalls nicht oder nicht in ausreichendem Maße?

10. Wie erfolgt die Zusammenarbeit der Bremer Sicherheitsbehörden mit den Sicherheitsbehörden der anderen Bundesländer, des Bundes und auf europäischer Ebene im Bereich Cyberkriminalität, Wirtschaftsspionage und Konkurrenzausspähung? Welche gemeinsamen Strukturen gibt es bzw. sollen etabliert werden?

11. Welche Beratungsleistungen und Hilfsangebote erhalten bremische Unternehmen und Institutionen von der Zentralen Ansprechstellen Cybercrime (ZAC) der Polizei Bremen? Wann, wie und wo wird hierüber informiert? In wie vielen Fällen bzw. von wie vielen Unternehmen wurden diese Beratungsleistungen und Hilfsangebote in den Jahren 2020 bis 2023 in Anspruch genommen? Um welche Arten von Fällen handelt es sich dabei typischerweise? An wen können sich Betriebe und Institutionen wenden, deren Sitz in Bremerhaven liegt?

    a. Wie ist die ZAC personell, materiell und finanziell ausgestattet und aufgestellt?

    b. Inwiefern kooperiert die ZAC mit Unternehmen der Privatwirtschaft (einschließlich der freien Berufe) bzw. deren Interessenvertretungen (z.B. Kammern, Verbände und Zusammenschlüsse, wie die Allianz für Sicherheit in der Wirtschaft Norddeutschland e.V. – ASW Nord)? Wie genau gestaltet sich diese Kooperation und wie wird diese ggf. finanziert?

    c. Wie bewertet der Senat, insbesondere hinsichtlich der oben abgefragten Aspekte, die Arbeit der ZAC? Wo sieht er ggf. noch Nachsteuerungsbedarf?

12. Durch welche Maßnahmen unterstützt das Landesamt für Verfassungsschutz Bremen bremische Unternehmen, Forschungseinrichtungen und sonstige Institutionen, die von Wirtschaftsspionage (einschließlich Cyberspionage oder Cybersabotage) fremder Staaten oder Nachrichtendienste betroffen oder bedroht sind? Um wie viele Fälle bzw. Unternehmen handelte es sich dabei in den Jahren 2020 bis 2023? Um welche Arten von Fällen handelt es sich dabei typischerweise?

13. Welche weiteren Angebote macht der Senat bremischen Unternehmen, Forschungseinrichtungen und sonstige Institutionen, um sich vor Cyberkriminalität und Wirtschaftsspionage bestmöglich schützen zu können? (bitte ausführlich erläutern)

Theresa Gröninger, Marco Lübke, Frank Imhoff und Fraktion der CDU