BREMISCHE BÜRGERSCHAFT
Landtag
21. Wahlperiode

Drucksache 21/852
(zu Drs. 21/735)
12. November 2024

Mitteilung des Senats

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

Große Anfrage
der Fraktion der CDU vom 3. September.2024
und Mitteilung des Senats vom 12. November 2024

Vorbemerkung des Fragenstellers:

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.

Der Senat beantwortet die Große Anfrage wie folgt:

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

   Insbesondere seit dem russischen Angriffskrieg gegen die Ukraine hat sich das Spektrum der Bedrohungslage erweitert. Neben politisch motivierten Cyberbedrohungen durch staatliche und staatlich beeinflusste Akteure, wie z. B. Hack-and-Leak-Operationen (das gezielte Eindringen in Systeme der Informationstechnik (IT), um beispielsweise diskreditierendes oder belastendes Material über das Opfer zu erlangen, welches anschließend im Original oder in verfälschter Form beispielsweise über Kanäle der sozialen Medien veröffentlicht wird) und Desinformationskampagnen, stellt Cyberkriminalität eine wachsende Gefahr für Wirtschaftsunternehmen in Deutschland dar. Die aktuelle Bedrohungslage im Cyberraum wird daher bundesweit als hoch eingeschätzt.

   Die Bedrohungslage durch Cyberkriminalität im Land Bremen unterscheidet sich nicht von der Bedrohungslage im gesamten Bundesgebiet oder anderen europäischen Staaten. Die aktuelle Lage im Bundesgebiet wird im Lagebild des Bundeskriminalamts (BKA) 2023 dargestellt und zeigt, dass insbesondere so genannte Ransomware, also das Eindringen in IT-Systeme mit der anschließenden Verschlüsselung der dort vorhandenen Daten sowie so genannte Data Extortion (die Erpressung mit der etwaigen Veröffentlichung zuvor illegal erlangter sensibler oder personenbezogener Daten), und Ausspähen von Daten weiterhin eine ernstzunehmende Gefahr der Cyberkriminalität darstellen.

   In Bezug auf Cyberspionage wie auch Cybersabotage wird die Bedrohungslage in Deutschland und im Land Bremen als hoch eingeschätzt. Kritische Infrastrukturen, Logistik- und Rüstungsunternehmen sowie Hochtechnologieunternehmen sind hierbei besonders gefährdet. Das Eskalationspotenzial im Cyberraum durch russische Akteure befindet sich darüber hinaus vor dem Hintergrund des Angriffskriegs gegen die Ukraine auf einem hohen Niveau. Neben staatlichen und staatlich beeinflussten russischen Akteuren entfalten jedoch auch weitere fremde staatliche Akteure Cyberaktivitäten gegen Unternehmen aus den genannten Sektoren.

   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?

      Der Senat vertritt die Einschätzung, dass Unternehmen, Forschungseinrichtungen und sonstige Institutionen in Bremen potenzielle Ziele für Cyberkriminelle darstellen. Dies gilt in Bremen ebenso wie für vergleichbare Einrichtungen im Bund und in Europa.

Einzelne andere Staaten haben ein großes Interesse daran, ihre eigene Wirtschaft zu stärken und ökonomische Abhängigkeiten zu reduzieren. Gleichzeitig bestehen häufig noch qualitative und technologische Defizite gegenüber den in Deutschland und seinen Partnerstaaten entwickelten Produkten, Maschinen und Technologien. Um diesen Widerspruch aufzulösen, versuchen ausländische Nachrichtendienste, teilweise auf illegalem Weg und durch den Einsatz nachrichtendienstlicher Mittel, bestehende Lücken zu schließen. Für dahinterstehende ausländische Regierungen stellt die Wirtschaftsspionage ungeachtet der Strafbarkeit nach deutschem Recht in diesen Fällen ein legitimes Mittel zur Förderung der eigenen Volkswirtschaft und technologischen Entwicklung dar.

Als weltweit anerkannter Forschungs- und Industriestandort verfügt das Land Bremen mit den hier ansässigen Unternehmen und Institutionen – teils als Weltmarktführer – über umfassendes und spezifisches Know-how in unterschiedlichsten Wirtschafts- und Forschungsbereichen, welches vor illegalem Abfluss ins Ausland zu schützen ist.

Die Größe der Forschungseinrichtung oder des Unternehmens ist dabei zweitrangig. Um das Interesse eines fremden Nachrichtendienstes zu wecken, sind allein die vorhandenen Fähigkeiten, Technologien und das Know-how ausschlaggebend, sodass auch kleine und mittelständische Unternehmen in den Fokus geraten können.

Im Phänomenbereich Cybercrime können Grenzen zwischen ausschließlich finanziell orientierten, staatlich unterstützten bzw. gelenkten oder rein nachrichtendienstlich agierenden Gruppen fließend oder gar nicht vorhanden sein. Es ist nicht auszuschließen, dass kriminelle Gruppen in bestimmten Staaten ihre erbeuteten Daten aus nachrichtendienstlich lukrativen Zielen mit staatlichen Akteuren teilen. Entsprechend sind alle Einrichtungen mit verwertbaren Informationen für Dritte grundsätzlich ein Ziel. Konkrete Erkenntnisse liegen hierzu aktuell nicht vor.

Die Gefahr durch Wirtschaftsspionage für bremische Unternehmen und Forschungseinrichtungen ist vor diesem Hintergrund insgesamt als hoch zu bewerten.

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?

Fremde Nachrichtendienste verfügen zum Teil über eine große Expertise und Erfahrung bei Cyberangriffen. Zugleich besitzen sie erfahrungsgemäß umfassende finanzielle und personelle Ressourcen sowie eine Gesetzeslage, die ihnen den Zugang zu bislang nicht bekannten Sicherheitslücken („Zero-Day-Exploits“) erleichtert. Aufgrund dieser Ausgangslage sind fremde Dienste oftmals zu verschiedenen Formen von Cyberangriffen fähig, von denen so genannte „Supply-Chain-Angriffe“ eine besondere Untergruppe darstellen. Bei dieser Methode werden oftmals gezielt Zuliefernde oder Geschäftspartner des eigentlichen Ziels, das womöglich über einen besonders hohen oder zumindest höheren Schutzstandard verfügt, infiltriert, um Schadsoftware dann entlang der Liefer- bzw. Wertschöpfungskette weiter zu verbreiten. Da in der etablierten Kommunikation mit verlässlichen Zuliefernden oder Geschäftspartnern normalerweise nicht mit Angriffsversuchen zu rechnen ist, ist die Methode des „Supply-Chain-Angriffs“ aus Sicht der Angreifenden besonders vielversprechend. Hierbei besteht die Gefahr, dass Daten über einen langen Zeitraum unbemerkt kopiert und ausgeleitet werden können. Ebenso wird die Gefahr gesehen, dass die betroffenen Produkte des kompromittierten Zuliefernden durch einen gezielten Angriff flächendeckend ausfallen können, was, je nach Kritikalität der entsprechenden Komponente, weitere Auswirkungen auf die Erbringung der Dienstleistung der betroffenen Nutzenden haben kann und somit zum Ausfall weiterer Dienste führen kann (Kaskadeneffekt).

Nach Einschätzung des Landesamtes für Verfassungsschutz (LfV) Bremen ist anzunehmen, dass diese Methode künftig weiter an Bedeutung gewinnen wird.

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

Eine dedizierte Schätzung der durch Cyberkriminalität und Wirtschaftsspionage im Land Bremen verursachten Schäden liegt dem Senat nicht vor.

Anzumerken ist, dass sich Schäden aus Cybercrime, insbesondere bei der Verschlüsselung der IT-Infrastrukturen, häufig in allen Staaten und in der Bundesrepublik in allen Ländern auswirken, in denen das betroffene Unternehmen tätig ist. Auch kann ein Cyberangriff in einem anderen Land ebenfalls (indirekte) Auswirkungen auf ein Unternehmen im Land Bremen haben. Somit kann regelmäßig nur eine gesamtwirtschaftliche Schätzung der Schäden erfolgen.

Generell sind bei der Ermittlung der durch Cyberkriminalität und Wirtschaftsspionage verursachten volkswirtschaftlichen Schäden mehrere Faktoren zu berücksichtigen. So kann es etwa vereinzelt zu langwierigen Produktions- oder Nutzungsunterbrechungen durch Verschlüsselung der IT-Infrastrukturen oder die eigene Abschaltung von externen Zugängen (wie der Internetverbindung) zum Schutz und zur Bereinigung der IT-Infrastruktur kommen. Auch können bei einem Abfluss von personenbezogenen Daten Folgekosten, wie z. B. Geldbußen, Kosten für Rechtsverfahren sowie etwaige Schadensersatzforderungen, entstehen.

Finanzielle Schäden, die etwa durch cyberspezifische Erpressungsdelikte oder durch damit einhergehenden Produktionsausfällen bei Unternehmen entstehen, werden polizeilich nicht erfasst und fließen statistisch nicht in erfasste Cybercrime-Schadenssummen ein. Eine konkrete Einschätzung zu finanziellen, volkswirtschaftlichen Schäden für das Land Bremen kann somit nicht getroffen werden.

Gemäß dem Lagebild Cybercrime des BKA werden 205,9 Milliarden Euro als bundesweiter Gesamtschaden für 2023 angegeben.

Im Rahmen der bitkom e. V.-Studie „Wirtschaftsschutz 2024“ wurde bei einer Umfrage, an der mehr als 1.000 Unternehmen teilnahmen, ein Schaden von 266,6 Milliarden Euro für das Jahr 2024 als Gesamtschaden in Folge von Cybercrime in Deutschland angegeben (2023: 205,9 Milliarden Euro / 2022: 202,7 Milliarden Euro).

Laut dieser Studie entstanden hierbei die folgenden Schäden:

Schaden durch	Schadenssumme in Mrd. Euro (2024)	Schadenssumme in Mrd. Euro (2023)	Schadenssumme in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4	18,3
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3	23,6
Patentrechtsverletzungen, auch vor Anmeldung	14,8	10,4	18,8

Erpressung mit gestohlenen Daten	13,4	16,1	10,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5	41,5
Geldabfluss durch Betrugsversuche	0,8	3,9	-
Sonstige Schäden	0	1,1	0,9
Gesamtschaden	266,6	205,9	202,7

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?

   Es existieren unterschiedlich eng gefasste Definitionen von Cybercrime im engeren Sinne (CCieS), sodass die jeweilige Verwendung auf den Fragezweck abgestimmt sein sollte. Für die vorliegende Frage wird ein rechtsdogmatisches Verständnis des Begriffs zugrunde gelegt, das ausschließlich Straftaten umfasst, die unmittelbar den Schutz von Informationstechnik bzw. seiner Verfügbarkeit, Integrität und Vertraulichkeit zum Gegenstand haben. Straftaten mit anderen Schutzzwecken (wie §§ 263a, 269, 270 StGB) fallen dann nicht hierunter.

   Dem Senat liegen keine validen Zahlen zur Anzahl der durch Cybercrime, Wirtschaftsspionage oder Konkurrenzausspähung betroffenen Unternehmen vor.

   Eine Unterscheidung zwischen privatwirtschaftlichen Unternehmen, Forschungseinrichtungen und Institutionen ist auf Basis der Polizeilichen Kriminalstatistik (PKS) nicht möglich. Die in der PKS registrierten Fallzahlen für den Summenschlüssel Cybercrime (897000) und die einzelnen Deliktbereiche werden in der Antwort auf Frage 5 tabellarisch dargestellt.

   Anzumerken ist, dass Unternehmen oder Institutionen durchaus von Fällen der Verschlüsselung bzw. Erpressung (Ransomware) betroffen sind, welche als Grunddeliktsform nicht unter den Begriff „Cybercrime“ im Sinne des PKS-Summenschlüssels subsumiert werden. Konkrete Daten für die zurückliegenden Jahre können ferner nicht genannt werden, da die Erfassung des Phänomens Ransomware in der PKS erst seit dem 01.01.2024 verpflichtend ist.

   Die Beeinträchtigungen müssen abhängig vom betroffenen Unternehmen betrachtet werden, da es vereinzelt zu langwierigen Produktions- und Nutzungsunterbrechungen durch

   - Verschlüsselung der IT-Infrastrukturen (kein Zugriff möglich) oder
   - eigene Abschaltung von externen Zugängen (wie Internetverbindung) zum Schutz und zur Bereinigung der IT-Infrastruktur

   kommen kann. Weiterhin kann es zwischenzeitlich als Standard angesehen werden, dass häufig zunächst ein Datenabfluss von internen Informationen an Cyberkriminelle stattfindet, bevor diese dann eine Verschlüsselung der Unternehmensdaten vornehmen.

   In Bezug auf Cyberspionage und Cybersabotage wird auf die Gefährdungseinschätzung zur Frage 1a) verwiesen. Dem Senat werden vielfach Sachverhalte durch das LfV bekannt, die in den gesetzlichen Zuständigkeitsbereich gem. § 3 Bremisches Verfassungsschutzgesetz (BremVerfSchG) fallen und über die der Parlamentarischen Kontrollkommission berichtet wird. Weitere Erkenntnisse sind als Verschlusssache eingestuft. Darüber hinaus

birgt eine öffentliche Bekanntgabe die Gefahr, dass Informationen über interne Geschäftsprozesse offenbart würden, die Angreifenden Hinweise auf mögliche Gefährdungswege geben könnten sowie die Fähigkeiten zur Aufdeckung und Analyse derartiger Angriffe beeinträchtigen könnten.

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?

   Das Risikobewusstsein für und die Sicherheitsvorkehrungen des privaten Sektors im Land Bremen gegen Cyberkriminalität, Wirtschaftsspionage oder Konkurrenzausspähung hängen von vielfältigen Faktoren ab. Sie unterscheiden sich innerhalb des privaten Sektors und selbst innerhalb einzelner Branchen zum Teil erheblich, weshalb allgemeingültige Aussagen nicht möglich sind. Die Gründe dafür sind dabei vielfältig. So ergeben sich für einige Unternehmen aufgrund gesetzlicher Verpflichtungen bereits umfassender Sicherheitsvorkehrungen – zum Beispiel für kritische Infrastrukturen oder die geheimschutzbetreute Industrie – die ein entsprechendes Risikobewusstsein sowie Sicherheitsvorkehrungen bereits gesetzlich vorschreiben, während das in anderen Wirtschaftssektoren nicht der Fall ist.

   Generell lässt sich feststellen, dass die branchenübergreifende Abhängigkeit der Digitalisierung für alle unternehmerischen Aktivitäten und die damit verbundene notwendige Beschäftigung auch in der Unternehmensleitung zu einer sich verändernden Gesamtbetrachtung der Unternehmenssicherheit führt. Neben den bisherigen Standards, z. B. im Brand-, Einbruch- oder Unfallschutz, werden IT- und Cybersicherheit in immer mehr Bereichen ein Schwerpunkt der jeweiligen Geschäftsführung.

   Unternehmen mit Standorten im (außereuropäischen) Ausland sind besonders davon betroffen, da bestimmte geschützte Kommunikationsmittel in einigen Staaten nicht genutzt werden dürfen. Eine Abwägung zwischen unternehmerischem Risiko und notwendigen Maßnahmen zum Schutz der Unternehmenssicherheit bleibt grundsätzlich bestehen.

   Unterschiede zwischen Unternehmen und Branchen können sich u. a. aus der Abhängigkeit zur IT (Produktion vs. Dienstleistung) und überregionalen Aktivität ergeben. Darüber hinaus hängt die individuelle Bewertung der Notwendigkeit von Schutzmaßnahmen oftmals mit verschiedenen Faktoren, wie etwa der geschäftlichen Ausrichtung des Unternehmens, dem Grad und Umfang schützenswerter Informationen, sowie den vorhandenen Ressourcen für IT-Sicherheit, zusammen.

   Weiterhin hängt eine individuelle Risikoabwägung maßgeblich auch vom Geschäftszweck des jeweiligen Unternehmens ab. So existieren diverse Branchen, die zwar auch durch Cyberkriminalität betroffen sein können, faktisch aber nicht im Aufklärungsinteresse fremder Nachrichtendienste stehen und bei denen sich niedrigere Sicherheitsvorkehrungen auf eine rationale, betriebswirtschaftliche Entscheidung zurückführen lassen. Auch fehlt es gerade kleineren und mittelgroßen Unternehmen oftmals an finanziellen Ressourcen, um bestimmte Sicherheitsvorkehrungen umzusetzen. Andere Unternehmen verfügen hingegen über schützenswertes Know-how oder sie erforschen und produzieren einzigartige, neuartige oder hochqualitative Produkte, bei denen ein ungewollter (Wissens-)Abfluss für das Unternehmen, aber auch die Bundesrepublik Deutschland, erheblichen Schaden verursachen könnte. Die Entscheidung für bestimmte Schutzstandards innerhalb des Unternehmens ist somit häufig ein Abwägungsprozess, in welchen die Bewertung der Ausrichtung des Unternehmens, die Einstufung der Sensibilität der Produkte und Dienstleistungen, sowie die Bewertung der eigenen wirtschaftlichen Ressourcen fällt.

Das unternehmensinterne Agieren im Rahmen einer transparenten Unternehmenssicherheit sowie die damit verbundene Awareness ist immanent wichtig, um Mitarbeiter:innen in die Prozesse der IT-Sicherheit zu integrieren und für diese zu sensibilisieren. Die Kernverantwortung für die Unternehmenssicherheit unterliegt grundsätzlich der jeweiligen Geschäftsführung. Damit geht auch die Notwendigkeit einher, sich mit aktuellen Bedrohungen und Risiken für das eigene Unternehmen proaktiv auseinanderzusetzen und eigenständig Maßnahmen zu treffen.

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)?

   Für die Beantwortung der Frage muss zunächst definiert werden, welche Einrichtungen dem „Konzern Bremen“ zugerechnet werden. Während „Behörden“ üblicherweise durch organisatorische Anbindung oder anhand ihrer Aufgabenwahrnehmung im Bereich der öffentlichen Verwaltung identifiziert werden können, sollen von der Fragestellung offenbar auch weitere Einrichtungen, etwa solche, die wirtschaftlich bzw. gewerblich tätig sind, oder Stiftungen erfasst sein, ohne dass dieser Kreis aber näher definiert wird. Unklar bleibt insbesondere, ob nur öffentlich-rechtlich oder auch privatrechtlich organisierte Einrichtungen gemeint sind und ob Letztere dann ganz, teilweise oder mehrheitlich im Eigentum des Landes oder der Stadtgemeinden stehen müssen, ob die aufzuführenden Einrichtungen wirtschaftlich tätig sein müssen und ob auch öffentlich-organisierte Einrichtungen mit Selbstverwaltungsrechten, die grundsätzlich nur einer Rechtsaufsicht unterliegen, angesprochen werden. Die meisten Ressorts haben bei der Beantwortung der Frage dem jeweiligen Geschäftsbereich unmittelbar zugeordneten Einrichtungen (Dienststellen, Eigenbetriebe, juristische Personen des öffentlichen Rechts, Gesellschaften) zugrunde gelegt.

   Grundlage für die Aussagen zur Betroffenheit von Cyberangriffen sind daher die Rückmeldungen der in der **Anlage 1** aufgeführten Stellen und Einrichtungen, die für den Zweck der Beantwortung dieser Frage mit dem Begriff „Konzern Bremen“ beschrieben werden.

   Grundsätzlich unterliegen die durch den „Konzern Bremen“ betriebenen IT-Systeme, welche eine Schnittstelle zu öffentlichen Netzen haben, permanent der Gefahr von Cyberangriffen. Durch entsprechende Schutzmaßnahmen, wie z. B. Mailfilter, Systeme zur Angriffserkennung sowie Antivirussoftware, wird eine Vielzahl dieser Cyberangriffe automatisiert abgewehrt.

   Nach Kenntnis des Senats kam es im Zeitraum von 2020 bis 2023 lediglich zu zwei erfolgreichen Cyberangriffen auf den „Konzern Bremen“, durch die ein bezifferbarer Schaden entstanden ist (weitere Ausführungen hierzu s. u.). Konkret wurden die folgenden versuchten bzw. erfolgreichen Cyberangriffe festgestellt, welche der Übersicht halber im Folgenden nach Ressorts gegliedert dargestellt werden:

   Der Senator für Finanzen

   In den Zuständigkeitsbereich des Senators für Finanzen fällt der Betrieb der zentral genutzten IT-Infrastruktur. Hierunter fallen auch der Betrieb der Software VIS und das zur Erstellung der Websites genutzte Contentmanagementsystem (CMS) KOGIS. Beim Betrieb der Software VIS sind keine Cyberangriffe bekannt geworden.

Im Serviceportal und dem Transparenzportal wurden vereinzelt so bezeichnete Distributed Denial of Service-Angriffe (DDoS-Angriffe, d. h. Überlastungsangriffe auf das Rechnernetz oder den Netzwerkdienst) festgestellt, die den Betrieb der Portale jedoch nicht stören konnten.

Beim Betrieb des CMS KOGIS sind im genannten Zeitraum ebenfalls DDoS-Angriffe festgestellt worden, die zu minimalen Verzögerungen im Aufruf der Webseite führten.

Betroffen waren die Websites der folgenden Behörden und Institutionen:

- Landesinstitut für Schule (2020)
- Der Senator für Finanzen (2020, 2022)
- Hansestadt Bremisches Hafenamt (2023)
- Polizei Bremen (2023)
- Senatskanzlei (2023)
- Ortsamt Hemelingen (2023).

Durch diese DDoS-Angriffe ist kein Sachschaden entstanden. Zudem wurde versucht, KOGIS für den Versand von Spam-Mails zu missbrauchen.

Darüber hinaus sind im Ressortbereich des Senators für Finanzen im Zeitraum von 2020 bis 2023 keine Cyberangriffe bekannt geworden.

Die Senatorin für Bau, Mobilität und Stadtentwicklung

Im Ressortbereich der Senatorin für Bau, Mobilität und Stadtentwicklung ist im Zeitraum von 2020 bis 2023 der folgende Fall bekannt geworden:

Im Jahr 2021 wurde auf unbekanntem Weg Zugriff auf eine E-Mail-Inbox der Bremer Straßenbahn Aktiengesellschaft (BSAG) genommen und diese zum begrenzten Versand unerwünschter E-Mails genutzt. Der dadurch entstandene Schaden basiert auf finanziellen und personellen Aufwänden für Eindämmung, Analyse und Forensik, den Neuaufbau sowie die Härtung der IT-Landschaft (< 10 TEUR).

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz

Im Ressortbereich der Senatorin für Gesundheit, Frauen und Verbraucherschutz sind im Zeitraum von 2020 bis 2023 die folgenden Fälle bekannt geworden:

Im Jahr 2023 wurde die Gesundheit Nord (GeNo) Opfer eines Cyberangriffs (Kompromittierung der IT-Infrastruktur) in Kombination mit einem Datendiebstahl. Hierbei wurden Daten im Umfang von ca. 250 GB kopiert. Es entstand ein wirtschaftlicher Schaden von ca. 240 TEUR.

Zudem war der Lebensmittelüberwachungs-, Tierschutz- und Veterinärdienst des Landes Bremen (LMTVet) in den Jahren von 2020 bis 2023 mehrfach von groß angelegten Spam- und Phishing-Kampagnen per E-Mail getroffen. In den meisten Fällen handelte es sich um Betrugsversuche („Scam“) aus finanziellen Beweggründen. Ziel der Angriffe waren die Mitarbeitenden, deren dienstliche E-Mail-Adressen auf der Website des LMTVet veröffentlicht wurden, sowie dort publizierte Funktionspostfach-Adressen. Sachschäden und sonstige wirtschaftliche Schäden sind nicht entstanden.

Die Senatorin für Wirtschaft, Häfen und Transformation

Im Ressortbereich der Senatorin für Wirtschaft, Häfen und Transformation sind im Zeitraum von 2020 bis 2023 die folgenden Fälle bekannt geworden:

DDoS-Angriffe auf die Website des Hansestadt Bremischen Hafenamtes (2023) (siehe auch Auflistung beim Senator für Finanzen), die Website der Wirtschaftsförderung Bremen (2023), sowie die Website des Flughafen Bremen (2022).

Der erfolglose Versuch der Ausnutzung einer Word-Press-Lücke auf einer Subdomain der Wirtschaftsförderung Bremen (2022) und die Ausnutzung eines 0-Day-Exploits bei bremenports. Sachschäden und sonstige wirtschaftliche Schäden sind nicht entstanden.

Der Magistrat der Stadt Bremerhaven

Dem Magistrat der Stadt Bremerhaven sind im Zeitraum von 2020 bis 2023 keine Cyberattacken oder Fälle von Wirtschaftsspionage bekannt geworden. Im August 2024 wurde die Installation eines Trojaners auf einem Arbeitsplatzrechner eines städtischen Amtes festgestellt. Durch Sofortmaßnahmen des Betriebs für Informationstechnologie (BIT) konnte ein Schadenseintritt verhindert werden.
Weitere Erkenntnisse zur Betroffenheit in Bezug auf Wirtschaftsspionage oder Konkurrenzausspähung liegen dem Senat nicht vor.

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?

   Bei der Aufrechterhaltung der Cybersicherheit handelt es sich um eine permanente Anstrengung, deren Erfolg maßgeblich von dem Risikobewusstsein sowie den getroffenen Sicherheitsvorkehrungen abhängt.

   Der Senat hat mit der Informationssicherheitsleitlinie 2018 (IS-LL FHB) ein Fundament für eine einheitliche Herangehensweise an die Informationssicherheit innerhalb der Ressorts geschaffen. Die Sicherheitsanforderungen korrespondieren hier regelmäßig und wenn nicht anders festgelegt mit einem normalen Schutzbedarf gemäß dem Grundschutzstandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI-Grundschutz). Weitergehende Anforderungen existieren für Dienststellen, in denen ein höherer Schutzbedarf deklariert worden ist. Dort sind regelhaft auch höhere Sicherheitsvorkehrungen durch technische und organisatorische Maßnahmen zu treffen.

   Als allgemeine Sensibilisierungsmaßnahme steht allen Mitarbeiter:innen, die Zugriff auf das Intranet der Freien Hansestadt Bremen haben, das Behörden-IT-Sicherheitstraining (BITS) zur Verfügung. In diesem Training werden allgemein anerkannte Sicherheitsrichtlinien erläutert und konkrete Verhaltenshinweise vermittelt, womit auch das individuelle Risikobewusstsein gestärkt wird.

   Darüber hinaus werden bei Bedarf unterschiedliche, weiterführende Maßnahmen zur Steigerung des Risikobewusstseins der Mitarbeiter:innen innerhalb der Ressorts initiiert und durchgeführt, die auf einer individuellen Risikoeinschätzung der Ressorts basieren. Hierbei handelt es sich u. a. um weitergehende Schulungen zu Angriffsszenarien im Bereich der Cyberkriminalität, die Ausbildung von Mitarbeiter:innen zu BSI-Grundschutzpraktiken oder die Schulung zur Vermittlung weiterer Fachkunde, z. B. im Umgang mit personenbezogenen oder weiteren sensiblen Daten.

   Dataport ist der zentrale IT-Dienstleister für einen Großteil der in den Ressorts genutzten Informationstechnik. In ihrer IT-Sicherheitsleitlinie hat Dataport sich dazu verpflichtet, grundsätzlich BSI-Grundschutz mit einem normalen Sicherheitsniveau anzuwenden. Dataport weist dies für einige Infrastrukturen durch Zertifizierungen und umfassende Sicherheitstests nach.

   Wesentliche Eckpfeiler der Informationssicherheit bei Dataport sind:

   - nach BSI-Grundschutz zertifiziertes Rechenzentrum;
   - 10-Schichtenmodell für IT-Sicherheit;
   - nach BSI-Anforderungen ausgelegte Zugangsnetze;

- Warn- und Informationsdienst (CERT-Nord) und ein
- Security Operations Center (SOC)

Konkret ergreift Dataport u.a. folgende Maßnahmen:

Prävention: Maßnahmen zur Verhinderung von Sicherheitsverletzungen und Bedrohungen.
z. B. Implementierung von Sicherheitsrichtlinien, Firewalls, Verschlüsselung, gemanagte Endgeräte.

Detektion: Identifizierung von Sicherheitsvorfällen und Angriffen, sobald sie auftreten. Überwachung von Systemen und Netzwerken, um verdächtige Aktivitäten und Anomalien zu erkennen.

Reaktion: Maßnahmen, die bei Sicherheitsvorfällen ergriffen werden. Ziele sind Schadensbegrenzung, Isolation der Angreifer und Wiederherstellung der Systeme.

Große Teile sicherheitskritischer Fachverfahren der Justiz Bremen werden zusätzlich in besonders gesicherten Bereichen des „DataCenterJustiz“ betrieben. Gleiches gilt für den IT-Betrieb der Polizei Bremen. Durch die Polizei Bremen wird der BSI IT-Grundschutz auf Basis des sogenannten Grundschutzprofils „Polizei“ umgesetzt und in regelmäßigen Abständen auditiert. Zudem wird jedes Fachverfahren vor der Inbetriebnahme durch das Informationssicherheitsmanagement (ISM) der Polizei Bremen geprüft und freigegeben.

Durch die vorgenannte Herangehensweise werden die Voraussetzungen für ein gleichermaßen hohes Risikobewusstsein im „Konzern Bremen“ geschaffen. Dem Senat ist allerdings bewusst, dass es sich bei dem Phänomen der Cyberkriminalität um eine komplexe und dynamische Erscheinung handelt. Insbesondere im Zusammenhang mit aktuellen Entwicklungen, etwa der sich verbreitenden Verfügbarkeit von künstlicher Intelligenz, ist abzusehen, dass sich die Angriffstaktiken und -techniken weiterentwickeln und immer zielgerichteter möglich werden. Sensibilisierungsmaßnahmen müssen daher stets an die sich verändernde Bedrohungslage angepasst werden.

Anhand der eingegangenen Rückmeldungen der Ressorts besteht nach Ansicht des Senats ebenfalls ein angemessenes Risikobewusstsein bzgl. Cyberkriminalität und Wirtschaftsspionage.

Auch hier findet eine Schärfung des Risikobewusstseins, z. B. durch wiederkehrende oder anlassbezogene Awareness-Schulungen oder Phishing-Simulationen, statt. Die implementierten Sicherheitsvorkehrungen orientieren sich hierbei ebenfalls am Stand der Technik.

So wurden beispielsweise im Nachgang zum Cyberangriff auf die GeNo weitere Maßnahmen, wie die Einführung einer so bezeichneten Endpoint Detection and Response (EDR) / Managed Defense-Lösung umgesetzt, um das bestehende Sicherheitsniveau zu steigern.

Aufgrund der Heterogenität der Tätigkeitsbereiche des „Konzern Bremens“ können in der Umsetzung technischer Sicherheitsvorkehrungen Unterschiede bestehen, die sich auf die unterschiedlichen Bedrohungsszenarien zurückführen lassen.

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?

Die aktuelle Bedrohungslage wird generell als hoch eingeschätzt (es wird auf die Beantwortung von Frage 1 verwiesen). Es handelt sich somit um eine permanente Aufgabe, die bestehenden IT-Sicherheitsmaßnahmen zu überprüfen und bei Bedarf anzupassen.

Aufgrund der weiten Auslegungsmöglichkeiten des Begriffs der IT-Sicherheitsmaßnahmen ist eine qualitative Beantwortung der Frage nicht ohne weiteres möglich. Generell unterhält der Senat regelmäßige Arbeitsbeziehungen mit dem BSI sowohl direkt als auch über den Verwaltungs-CERT-Verbund (VCV; beim CERT handelt es sich um ein Computer Emergency Response Team, d. h. ein Computersicherheits-Ereignis- und Reaktionsteam). Dort wird die aktuelle IT-Sicherheitslage kontinuierlich beobachtet und Informationen zum Lagebild werden ausgetauscht; hierzu gehören etwa auch Lageberichte des Nationalen Cyberabwehrzentrums (NCAZ).

Zudem werden in den einzelnen Ressorts sowie den zugeordneten Dienststellen und Gesellschaften in eigener Zuständigkeit unterschiedliche, auf die jeweilige Risikoexposition angepasste, Maßnahmen technischer, organisatorischer und personeller Art umgesetzt (es wird auf die Beantwortung von Frage 3 verwiesen). Diese Maßnahmen finden hierbei unabhängig vom Aufruf des BSI statt.

Durch den Senat wurde im April 2023 die Bremische Cybersicherheitsstrategie verabschiedet. In dieser werden anhand von neun Handlungsfeldern strategische Ziele definiert, deren Erfüllung zur Steigerung der Cybersicherheit in der Freien Hansestadt Bremen beiträgt. Ebenso wurde im Mai 2023 die „Zentralstelle Cybersicherheit“ beim Senator für Inneres und Sport errichtet. Aufgabe der Zentralstelle Cybersicherheit ist die Koordinierung der strategischen Ausrichtung der Cybersicherheit in der Freien Hansestadt Bremen. Zudem fällt der Zentralstelle Cybersicherheit die Aufgabe zu, die auf dem Gebiet der Cybersicherheit tätigen Akteure in der Freien Hansestadt Bremen zu vernetzen und so zu einer Steigerung der gesamtstaatlichen Resilienz gegenüber Cyberbedrohungen beizutragen.

Die Zentralstelle Cybersicherheit hat in enger Abstimmung mit dem Senator für Finanzen den Abschluss einer Kooperationsvereinbarung zwischen der Freien Hansestadt Bremen und dem BSI vorangetrieben, welche am 15.08.2024 unterzeichnet wurde (es wird auf die Beantwortung von Frage 3c) verwiesen), und somit eines der gesteckten Ziele der Bremischen Cybersicherheitsstrategie bereits erreicht.

Ebenso hat der Senat zur Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) in der unmittelbaren Landesverwaltung das von der AG Informationssicherheit vorgelegte Identifizierungskonzept der Länder zur Umsetzung der NIS-2-Richtlinie auf regionaler Ebene angewandt und anhand dieses Konzepts kritische Bereiche der unmittelbaren Landesverwaltung identifiziert. Rechtsakte zur Umsetzung der NIS-2-Richtlinie auf Ebene der unmittelbaren Landesverwaltung befinden sich zum aktuellen Zeitpunkt in der Abstimmung.

Im Rahmen der weiteren Umsetzung der NIS-2-Richtlinie wird durch den Senat geprüft werden, welche zusätzlichen Maßnahmen erforderlichenfalls zu ergreifen und umzusetzen sind, um angemessen auf die bestehende Bedrohungslage reagieren zu können.

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)

Der Senator für Inneres und Sport nimmt sowohl auf der Arbeitsebene, vertreten durch die Zentralstelle Cybersicherheit, als auch auf Leitungsebene, vertreten durch den Staatsrat, an der Länderarbeitsgruppe Cybersicherheit (LAG Cybersicherheit) teil. In dieser werden neben allgemeinen Themenkomplexen, die den Bereich Cybersicherheit betreffen, die Zusammenarbeit zwischen den Ländern sowie die Zusammenarbeit mit dem Bund zu Themen der Cybersicherheit und zukünftigen Cybersicherheitsstrukturen bearbeitet. An den Sitzungen der LAG Cybersicherheit nehmen alle Länder, das BSI sowie das Bundesministerium des Innern und für Heimat (BMI) teil. Die LAG Cybersicherheit ist regelmäßig an Beschlüssen der IMK beteiligt bzw. erstellt im Auftrag dieser Konzepte und Stellungnahmen zu aktuellen Themen mit Bezug zur Cybersicherheit. Zudem dient sie dem allgemeinen Erfahrungsaustausch der Länder und des Bundes über Aspekte der Cybersicherheit sowie der Koordination von Initiativen und Maßnahmen zur Erhöhung der Cybersicherheit.

Zwischen der Freien Hansestadt Bremen und dem BSI wurde am 15.08.2024 eine Kooperationsvereinbarung zur vertieften Kooperation im Bereich der Cyber- und Informationssicherheit unterzeichnet (es wird auf die Antwort zu Frage 3b) verwiesen). Das Ziel der Vereinbarung besteht darin, die Zusammenarbeit zwischen dem BSI und der Freien Hansestadt rechtlich abzusichern und auszubauen und so, sowohl in der öffentlichen Verwaltung als auch in der Wirtschaft, das Cybersicherheitsniveau zu stärken. Hierfür sollen im 4. Quartal 2024 erste Gespräche zwischen dem BSI sowie der Zentralstelle Cybersicherheit bezüglich der Konkretisierung der in der Kooperationsvereinbarung benannten Handlungsfelder stattfinden.

Weiterhin wurde aufgrund der strategischen Bedeutung des Phänomenbereichs Cybercrime im Hinblick auf dessen zunehmende sicherheits- und kriminalpolitische Relevanz innerhalb des Gremienstranges der Arbeitsgemeinschaft der Leiterinnen und Leiter des Bundeskriminalamtes und der Landeskriminalämter (AG Kripo) die Leiter:innentagung Cybercrime (LTCC) als kommissionsähnliches Gremium institutionalisiert. Bei der AG Kripo handelt es sich um einen Unterausschuss des Arbeitskreises II „Innere Sicherheit“ (AK II) der IMK. Dieser befasst sich mit Themen der Inneren Sicherheit, die eine bundesweite Relevanz entfalten und die zwischen den Polizeien des Bundes und der Länder abgestimmt und harmonisiert werden sollen. Die von der LTCC behandelten Themen sind von strategischer Bedeutung für den Phänomenbereich Cybercrime und werden dort auf Managementebene zielgerichtet und adressatengerecht behandelt. Hierdurch wird ein wichtiger Beitrag zur erfolgreichen Bekämpfung der Cyberkriminalität im nationalen Kontext geleistet. Die Polizei Bremen ist durch eine Abteilungsleitung des Landeskriminalamtes in der LTCC vertreten und ständiges Mitglied. Unterhalb der LTCC bestehen weitere bundesweite Arbeitsgruppen und Formate zur nationalen Vernetzung im Kontext der Bekämpfung der Cyberkriminalität.

Das Landesamt für Verfassungsschutz unterhält umfassende Kontakte zu den Sicherheitsbehörden und Nachrichtendiensten von Bund und Ländern. Neben dem grundsätzlichen und fachlichen Austausch oder z. B. der gemeinsamen Erstellung von Präventionsmaterialien ist die weitere Zusammenarbeit und Kooperation vom Einzelfall abhängig. Insbesondere nachrichtendienstlich orchestrierte Cyberangriffe erfolgen meist bundes- bzw. europaweit – entsprechende Informationen über derzeit laufende Kampagnen und Schwachstellen werden regelmäßig auf Grundlage der Verfassungsschutzgesetze im Verfassungsschutzverbund ausgetauscht, für die zielgerichtete Sensibilisierung von Zielgruppen aufbereitet und beispielsweise durch die Übermittlung von so genannten Indicators of Compromise (IoC, d. h. Kompromittierungs-Indikatoren) mit entsprechenden Unternehmen und Einrichtungen geteilt.

Der Landesbeauftragte für Informationssicherheit (auch Chief Information Security Officer, CISO) ist in der Bund-Länder Arbeitsgruppe Informationssicherheit des IT-Planungsrates sowie rollierend in der AG Verbindungsnetz tätig. Die Rechtsgrundlagen ergeben sich aus dem Grundgesetz (Art. 91c), dem IT-Netzgesetz und dem IT-Staatsvertrag zur Gründung des IT-Planungsrates.

Zudem betreibt die Freie Hansestadt Bremen zusammen mit den weiteren Dataport-Trägerländern (Schleswig-Holstein, Sachsen-Anhalt und der Freien und Hansestadt Hamburg) das CERT Nord. Dieses ist Bestandteil des VCV und erhält über diesen z. B. Hinweise zu bestehenden Sicherheitslücken oder sonstige relevante Informationen. Teilnehmer des VCV sind die CERT der Länder sowie das CERT Bund des BSI. Ebenso erhält das CERT Nord unterstützende Hinweise aus weiteren Quellen sowie aktuelle vertraulichen Informationen zur Cybersicherheitslage.

Die Dataport-Trägerländer stehen über regelmäßige Treffen ihrer CISO in engem Kontakt und stimmen hier Sicherheitsmaßnahmen ab.

Die Senatorin für Justiz und Verfassung, primär in Funktion der oder des Informationssicherheitskoordinator:in der IT-Stelle Justiz, beteiligt sich zudem an einer Vielzahl von Gremien, deren Aufgabe es ist, die IT-Sicherheit für die eigene Infrastruktur zu erhöhen. Hervorzuheben sind hierbei die

- Arbeitsgemeinschaft Informationssicherheitsmanagement DataCenterJustiz (AG ISM DCJ), in der sich die Dataport-Trägerländer des „DataCenterJustiz“ gemeinsam mit Dataport zu betrieblichen Informationssicherheitsthemen austauschen,
- die Bund-Länder-Kommission IT-Sicherheit, bei der es sich um eine länderübergreifende Austauschrunde zu ISM-Themen in der Justiz handelt, sowie
- den e²-Verbund mit seinem e²-ITSB (Sicherheitsboard des e²-Verbundes), der u. a. für die Entwicklung der e-Aktensoftware zuständig ist.

Ein Treffen der Informationssicherheitsbeauftragten (ISB) der Senatskanzleien fand zuletzt im Jahr 2022 statt. Bei diesem wurden Themen wie z. B. die IT-Sicherheit bei Auslandsreisen erörtert.

Das Amt für Straßen und Verkehr (ASV) der Freien Hansestadt Bremen ist Mitglied im UP KRITIS. Zudem ist das ASV Mitglied im Open Traffic Systems City Association e.V., der als Arbeitskreis KRITIS fungiert und den bundesweiten Austausch zwischen Betreibern kritischer Infrastrukturen fördert.

Zusätzlich zu den zuvor genannten Strukturen sind die folgenden Zusammenarbeiten und Kooperationen mit dem Bund und anderen Ländern bekannt. Die Auflistung basiert hierbei ebenfalls auf den Rückmeldungen der in **Anlage 1** aufgeführten Stellen und Einrichtungen:

Die Flughafen Bremen GmbH bezieht sowohl Informationen des BSI (automatisierter täglicher Bedrohungs- bzw. Tagesbericht) und tauscht sich zudem über die Arbeitsgemeinschaft Deutscher Verkehrsflughäfen (ADV) fachlich aus.

Die Flughafen Bremen GmbH ist gemäß der „Grundsätze zur Umsetzung der DVO (EU) 2019/1583 im Zuständigkeitsbereich des Bundesministeriums des Innern und für Heimat (§§ 5 und 8 Luft-SiG)“ verpflichtet, sich für das „Melde- und Informationswesen des BSI“ zu registrieren. Diese Registrierung ist erfolgt.

Die bremenports GmbH & Co. KG betreibt einen anlass- und projektbezogenen fachlichen Austausch mit dem BSI sowie einen regelmäßigen Austausch mit der Bundespolizei. Darüber hinaus ist die bremenports GmbH & Co. KG Mitglied im UP KRITIS. Der UP KRITIS ist eine öffentlich-private Kooperation zwischen Betreibern Kritischer Infrastrukturen (KRITIS), deren Verbänden und den zuständigen staatlichen Stellen. Zudem ist die bremenports GmbH & Co. KG Mitglied in der Allianz für Cybersicherheit (ACS). Ebenso findet ein monatlicher Austausch der oder des Informationssicherheitsbeauftragten mit den Hafenbeteiligten anderer Bundesländer statt.

Die Wirtschaftsförderung Bremen (WFB) ist Mitglied in der ACS, über die ebenfalls ein Austausch stattfindet.

Aufgrund mit dem Land Niedersachsen gemeinsam genutzter Fachverfahren finden anlassbezogen Gespräche zwischen den betroffenen Akteur:innen des LMTVet und des Landes Niedersachsen statt, um organisatorische und technische Maßnahmen zur Sicherstellung und Erhöhung der Informationssicherheit abzustimmen.

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)

   Für den angefragten Zeitraum zwischen 2020 bis 2023 ist dem Senat ein Fall bekannt, bei dem es zu einem Cyberangriff auf ein nach der BSI-KritisVerordnung (BSI-KritisV) eingestuftes Unternehmen kam. Hierbei wurden personenbezogene Daten kopiert und im Internet veröffentlicht. Im Rahmen der Überprüfung der Systeme kam es zu einer Einschränkung der externen Kommunikation. Die Erbringung der Kerndienstleistung des Unternehmens war nicht beeinträchtigt. Es entstanden finanzielle Schäden. Weitere Angaben können nicht öffentlich mitgeteilt werden, da die Einstufung der Betreiber Kritischer Infrastruktur dem BSI obliegt und die entsprechenden Informationen als „Verschlusssache – Nur für den Dienstgebrauch“ (VS-NfD) eingestuft sind.

   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?

      Grundlage für die Regulierung Kritischer Infrastrukturen ist das BSI-Gesetz, welches zuletzt 2015 und 2021 überarbeitet und signifikant erweitert wurde (IT-Sicherheitsgesetz 1.0 (2015) und 2.0 (2021)). Weitere erhebliche Anpassungen werden voraussichtlich durch das Inkrafttreten des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG), das sich gegenwärtig im parlamentarischen Gesetzgebungsprozess befindet, erfolgen. Das BSI-Gesetz verpflichtet die Betreiber Kritischer Infrastrukturen, bestimmte Anforderungen an ihre IT-Sicherheit zu erfüllen. So verpflichtet § 8a BSIG in der aktuellen Fassung die Betreiber Kritischer Infrastrukturen angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind.

      Zudem existieren „Branchenspezifische Sicherheitsstandards“ (B3S), die konkretisieren, wie die Anforderungen zum Stand der Technik erfüllt werden können. Hinzu treten spezialgesetzliche Regelungen der Bundesnetzagentur für Bereiche der öffentlichen Telekommunikation, der Energienetze sowie bestimmter Energieanlagen.

Das BSI bewertet monatlich die Resilienz der KRITIS-Sektoren anhand von Reifegraden der bei Prüfungen vorgefundenen Informationssicherheitsmanagementsysteme (ISMS) und Business Continuity Managementsysteme (BCMS).

Bei einem ISMS handelt es sich um ein Managementsystem, welches durch die Aufstellung von Verfahren und Regeln innerhalb einer Organisation das Ziel verfolgt, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern. Ziel eines BCMS ist es, etwaige Unterbrechungen des Geschäftsbetriebs, unabhängig von der Ursache, zu verhindern oder abzumildern. Die Bewertungsskala der Reifegrade von ISMS und BCMS reicht hierbei von 1 bis 5, wobei folgende Abstufungen gelten:

- Reifegrad 1 – ISMS bzw. BCMS ist geplant, aber nicht etabliert.
- Reifegrad 2 – ISMS bzw. BCMS ist zum Teil etabliert.
- Reifegrad 3 – ISMS bzw. BCMS ist etabliert und dokumentiert.
- Reifegrad 4 – wie 3 + ISMS bzw. BCMS wird regelmäßig auf Effektivität geprüft.
- Reifegrad 5 – wie 4 + ISMS bzw. BCMS wird regelmäßig verbessert.

Basierend auf dem Durchschnitt der letzten 24 Monate gibt das BSI die Reifegrade in den einzelnen Sektoren wie folgt an (IT-Sicherheitslage des BSI - Ausgabe September 2024 - Berichtszeitraum August 2024):

Sektor	**Reifegrad ISMS**	**Reifegrad BCMS**
Energie	3,35	3,17
Wasser	3,93	3,57
Ernährung	3,36	2,96
Informationstechnik und Telekommunikation	4,05	3,59
Gesundheit	3,04	2,63
Finanz- und Versicherungswesen	3,97	3,53
Transport und Verkehr	2,91	2,71

Die vom BSI erhobenen Daten weisen somit darauf hin, dass die Mehrzahl der KRITIS-Betreiber ein ISMS sowie ein BCMS mindestens etabliert und dokumentiert hat. Unterschiede zwischen den Sektoren sind möglicherweise auf unterschiedliche, weiterführende Anforderungen und Industriestandards, die in diesen Sektoren einzuhalten sind, zurückführbar.

Insbesondere auch aufgrund der sich geänderten geopolitischen Lage sowie der sich aus der NIS-2-Richtlinie ergebenden zusätzlichen Anforderungen im Bereich der Cybersicherheit ist eine erhöhte Sensibilität und Schärfung des Risikobewusstseins branchenübergreifend erkennbar.

Eine Sensibilisierung der KRITIS-Betreiber findet im Rahmen der Zuständigkeit des BSI statt. Zudem findet eine lageangepasste Sensibilisierung durch Landesbehörden,

je nach gesetzlicher Zuständigkeit insbesondere durch die Zentralstelle Cybersicherheit, das Landesamt für Verfassungsschutz sowie die Zentrale Ansprechstelle Cybercrime der Polizei Bremen statt.

Erkenntnisse zu signifikanten Unterschieden bzgl. dem Risikobewusstsein und den Sicherheitsvorkehrungen zwischen den einzelnen Sektoren in der Freien Hansestadt Bremen liegen dem Senat nicht vor.

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)

Das Bremische Sicherheitsüberprüfungsgesetz (BremSÜG) weist in seiner derzeitigen Fassung keine Rechtsgrundlage für die Durchführung von Sicherheitsüberprüfungen zum personellen Sabotageschutz auf. Ein entsprechender Änderungsentwurf, der solche Regelungen auch für das BremSÜG vorsieht, befindet sich derzeit in der Ressortabstimmung.

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?

Der Begriff der „Kultur der Sicherheit“ wird nach Kenntnis des Senats nicht in der NIS-2-Richtlinie genutzt. Die Frage kann daher nicht abschließend beantwortet werden.

Aufgrund der föderalen Struktur der Bundesrepublik Deutschland muss bei der Umsetzung der NIS-2-Richtlinie in nationales Recht zwischen der Umsetzung des Bundes und der Länder unterschieden werden. Neben der Regelungskompetenz für die von der NIS-2-Richtlinie betroffenen Teile der Bundesverwaltung besitzt der Bund über Art. 74 Abs. 1 Nr. 11 i. V. m. Art. 72 Abs. 2 GG auch die Befugnis zur Umsetzung der wirtschaftsbezogenen Regelungen der Richtlinie. Von dieser Kompetenz macht der Bund im NIS2UmsuCG weitgehend abschließend Gebrauch und bezieht insoweit auch die öffentlichen Unternehmen der Länder und Kommunen mit ein. Eine Landesumsetzung kann daher grundsätzlich lediglich hinsichtlich der von der NIS-2-Richtlinie zu erfassenden Teile der Landesverwaltung erfolgen (vgl. Art. 2 Abs. 2 Buchst. f Ziff. ii der NIS-2-Richtlinie: „Einrichtung der öffentlichen Verwaltung auf regionaler Ebene, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte“).

Der Regierungsentwurf des NIS2UmsuCG befindet sich zur Beratung im Bundesrat sowie im Bundestag. Nach Auskunft des BMI soll das NIS2UmsuCG im 1. Quartal 2025 verabschiedet werden.

Zur Umsetzung der NIS-2-Richtlinie in der Landesverwaltung ist federführend durch den Senator für Inneres und Sport und in enger Abstimmung mit den weiteren Ressorts eine Verwaltungsvorschrift erarbeitet worden, die sich derzeit in der Abstimmung befindet. Die sich aus Art. 7 der NIS-2-Richtlinie ergebenden Anforderung zur Erstellung einer Cybersicherheitsstrategie wurde bereits mit der Bremischen Cybersicherheitsstrategie 2023 erfüllt. Weiterhin befindet sich ein Cybersicherheitsbasisgesetz in Abstimmung, mit welchem zur Arbeit im Bereich der Informations- und Cybersicherheit

kurzfristig erforderliche grundlegende Regelungen geschaffen werden sollen. Perspektivisch wird die Zusammenführung der vorgenannten Rechtsakte zu einem ganzheitlichen Bremischen Cybersicherheitsgesetz angestrebt, um einen umfassenden Rechtsrahmen zu schaffen.

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?

   Die Ergebnisse des Lagebildes zur Cybersicherheit in den bremischen Häfen 2020/2021 wurden im Rahmen der Smartport-Initiative aufgegriffen und unter Berücksichtigung aller interessierten Stakeholder in den bremischen Häfen weiterentwickelt. Cybersicherheit ist als eines von sieben Themenfeldern zentral in der im März 2024 vom Senat verabschiedeten und vom Bundesministerium für Bildung und Forschung geförderten Smartport-Strategie verankert. Neben abgestimmten lang-, mittel- und kurzfristigen Zielen wurden auf der digitalen Roadmap konkrete Cybersicherheitsprojekte identifiziert, die allen beteiligten Hafenunternehmen entsprechende Mehrwerte bieten sollen.

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)

   Unabhängig von der im Übrigen verwendeten Definition von „Cybercrime im engeren Sinne“ (vgl. dazu schon zu Frage 2) erfolgt die Beantwortung vorliegend anhand der konkret dargelegten PKS-Schlüssel.

   Bei der PKS handelt es sich um eine Ausgangsstatistik, d. h. eine Fallzählung erfolgt erst nach Abschluss der polizeilichen Ermittlungen. Bei der Interpretation der Daten ist daher zu berücksichtigen, dass Tatzeit und Zählung des Falls in der PKS in unterschiedlichen Jahren liegen können, da Fälle nicht immer in dem Jahr angezeigt werden, in dem sie sich ereignet haben und mitunter auch nicht immer im selben Jahr polizeilich abschließend bearbeitet werden.

   Für die vorliegende Auswertung wurde auf Daten der PKS zu Straftaten im Land Bremen zurückgegriffen. Es wurden folgende Straftatenschlüssel berücksichtigt:

   543000 Fälsch. beweiserhebl. Daten, Täusch. im Rechtsverkehr b. Datenverarb.
   543010 Fälschung beweiserheblicher Daten
   543020 Täuschung im Rechtsverkehr bei Datenverarbeitung
   674200 Datenveränderung, Computersabotage
   674210 Datenveränderung
   674220 Computersabotage
   678000 Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei
   678010 Ausspähen von Daten gemäß § 202a StGB
   678020 Abfangen von Daten gemäß § 202b StGB
   678030 Vorbereiten des Ausspähens und Abfangens von Daten
   678040 Datenhehlerei
   897000 Cybercrime
   897100 Computerbetrug § 263a StGB

   Als Auswertungszeitraum wurde der 01. Januar 2020 bis 31. Dezember 2023 gewählt.
   Der Summenschlüssel Cybercrime (897000) wurde zum 01.01.2021 in die PKS eingeführt.
   Bis zum (einschließlich) 31.12.2020 wurden Cybercrime-Delikte über den Summenschlüs-

sel Computerkriminalität (897000) erfasst. Dieser ist mit Cybercrime (897000) nicht vergleichbar, da seither inhaltliche Anpassungen vorgenommen worden sind. Die Fallzahlen für das Jahr 2020 sind in der folgenden Tabelle daher über die einzelnen Cybercrime-spezifischen Straftatenschlüssel abgebildet.

PKS-Straftaten-schlüssel	Delikt	2020		2021		2022		2023	
		Fälle	AQ in %	Fälle	AQ in %	Fälle	AQ in %	Fälle	AQ in %
897000	**Cybercrime**			**4.307**	**10,7**	**3.473**	**11,3**	**2.972**	**13,4**
543000	Fälsch. beweiserhebl. Daten, Täusch. im Rechtsverkehr b. Datenverarb.	96	25,0	133	27,8	94	19,1	169	42,0
543010	Fälschung beweiserheblicher Daten	90	22,2	131	28,2	90	18,9	169	42,0
543020	Täuschung im Rechtsverkehr bei Datenverarbeitung	6	66,7	2	0,0	4	25,0	-	-
674200	Datenveränderung, Computersabotage	27	11,1	128	6,3	47	6,4	14	7,1
674210	Datenveränderung	9	33,3	111	6,3	40	5,0	10	10,0
674220	Computersabotage	18	0,0	17	5,9	7	14,3	4	0,0
678000	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei	333	10,5	349	11,7	241	8,3	115	14,8
678010	Ausspähen von Daten gemäß § 202a StGB	312	6,4	335	11,6	232	8,2	113	15,0
678020	Abfangen von Daten gemäß § 202b StGB	-	-	4	0,0	2	0,0	1	0,0
678030	Vorbereiten des Ausspähens und Abfangens von Daten	5	0,0	5	0,0	5	0,0	1	0,0
678040	Datenhehlerei	16	93,8	5	40,0	2	50,0	-	-
897100	Computerbetrug § 263a StGB	1.770	18,5	3.697	10,1	3.091	11,4	2.674	11,6

Im Jahr 2020 wurden im Land Bremen insgesamt 2.226 Fälle erfasst, welche unter die der Beantwortung der Frage zugrundeliegende Definition fallen. Die Aufklärungsquote lag insgesamt bei 17,49 %. Im Jahr 2021 wurde ein Anstieg auf einen bisherigen Höchstwert von 4.307 Fällen registriert, die Aufklärungsquote sank auf den bisherigen Tiefstwert von 10,7 %. Im Jahr 2022 sanken die Fallzahlen auf 3.473 Fälle mit einer Aufklärungsquote von 11,3 %. Im Jahr 2023 wurde ein erneuter Rückgang der Fallzahlen auf 2.972 Fälle festgestellt, die Aufklärungsquote stieg auf 13,4 %. Detaillierte Fallzahlen und Aufklärungsquoten sind der obigen Tabelle zu entnehmen.

Beim überwiegenden Teil der jährlich erfassten Delikte in der durchgeführten Auswertung handelt es sich um Fälle von Computerbetrug nach § 263a StGB (897100). Der prozentuale Anteil von Computerbetrugsdelikten nach § 263a StGB an allen Cybercrime-Delikten lag zwischen 79,5 % (2020) und 90 % (2023) und nahm im Betrachtungszeitraum kontinuierlich zu. Die für das Land Bremen erfassten Fallzahlen haben sich in den letzten beiden Jahren parallel zu den bundesweiten Fallzahlen entwickelt. Sowohl der ab 2022 leichte Rückgang der cyberspezifischen Straftaten als auch der hohe Anteil an Computerbetrugsdelikten an allen Cybercrime-Delikten zeigte sich auch auf Bundesebene.

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)

Unter Auslandstaten sind in der sogenannten „PKS-Ausland“ zu erfassende Straftaten zu verstehen, bei denen der Ort der Handlung (Tatort) im Ausland liegt oder nicht auf Deutschland konkretisierbar ist, ein Erfolg der Handlung (Erfolgseintritt) aber zumindest teilweise in Deutschland eingetreten ist. Der Erfolgsort ist somit der Ort, an dem ein zum gesetzlichen Tatbestand gehörender Handlungserfolg (Rechtsgutverletzung bzw. versuchte

Rechtsgutverletzung) eingetreten ist oder nach der Vorstellung des Agierenden eintreten sollte. Die Erfassung von Auslandstaten wurde zum 01.01.2020 eingeführt und erfolgt separat in der „PKS-Ausland“. Im Jahr 2021 wurde vom BKA bundesweit eine Evaluation der Erfassung von Auslandstaten durchgeführt. Es wurden Mängel in der Datenqualität festgestellt. Daraufhin wurden in einer Bund-Länder-Projektgruppe Lösungsmöglichkeiten erarbeitet und die Erfassung von Auslandstaten wurde optimiert und präzisiert. Die Umsetzung der Anpassungen erfolgte zum 01.01.2024, so dass für das PKS-Berichtsjahr 2024 eine Verbesserung der Datenqualität und Aussagekraft anzunehmen ist. Für den angefragten Zeitraum liegen jedoch keine validen Daten vor, sodass hierzu keine Aussage getroffen werden kann.

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)

   Anhand der PKS ist keine Auswertung zur Betroffenheit von Unternehmen von Wirtschaftsspionage oder Konkurrenzausspähung möglich. In der PKS werden Deliktsformen erfasst, die zumindest teilweise, jedoch nicht ausschließlich, für Wirtschaftsspionage und/oder Konkurrenzausspähung stehen können.

   Hierzu zählen das

   - Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB (678000),
   - die Verletzung von Geschäftsgeheimnissen § 23 Abs. 1 Nr. 3 und Abs. 4 GeschGehG (715300),
   - die Verletzung von Geschäftsgeheimnissen § 23 Abs. 1 Nr. 1, 1, Abs. 2 und 4 GeschGehG (715400) und
   - die Verletzung von Geschäftsgeheimnissen § 23 Abs 3 GeschGehG; strafbare Werbung gemäß § 16 UWG (719200).

   Für das Land Bremen wurden im Jahr 2020 insgesamt 334 Fälle polizeilich registriert, die den zuvor genannten Straftatschlüsseln zugeordnet werden können. Im Jahr 2021 stieg die Anzahl der erfassten Fälle auf 350 Straftaten. Seit dem Jahr 2022 ist ein Rückgang der Zahlen auf 242 (2022) bzw. 115 (2023) Fälle zu verzeichnen. Die Aufklärungsquote schwankt im Betrachtungszeitraum zwischen 8,7 % (2022) und 14,8 % (2023). Die mit Abstand meisten Fälle wurden unter „Ausspähen von Daten gemäß § 202a StGB“ (678010) erfasst.

   Der folgenden Tabelle ist die detaillierte Fallzahlentwicklung zu entnehmen:

PKS-Straftatenschlüssel	Delikt	2020		2021		2022		2023	
		Fälle	AQ in %	Fälle	AQ in %	Fälle	AQ in %	Fälle	AQ in %
678000 [1]	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei	333	10,5	349	11,7	241	8,3	115	14,8
678010	Ausspähen von Daten gemäß § 202a StGB	312	6,4	335	11,6	232	8,2	113	15,0
678020	Abfangen von Daten gemäß § 202b StGB	-	-	4	0,0	2	0,0	1	0,0
678030	Vorbereiten des Ausspähens und Abfangens von Daten	5	0,0	5	0,0	5	0,0	1	0,0
678040	Datenhehlerei	16	93,8	5	40,0	2	50,0	-	-
715300	Verletzung von Geschäftsgeheimnissen gem. § 23 Abs. 1 Nr. 3 und Abs. 4 GeschGehG	1	100,0	-	-	-	-	-	-
719200	Verletzung von Geschäftsgeheimnissen gem. § 23 Abs. 3 GeschGehG; strafbare Werbung gem. § 16 UWG	-	-	1	100,0	1	100,0	-	-

Gesamt	**334**	**10,8**	**350**	**12,0**	**242**	**8,7**	**115**	**14,8**

[1] *[Der Straftatenschlüssel Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei (678000) wird unter dem Summenschlüssel Cybercrime (897000) erfasst und ist daher auch in der Tabelle zur Beantwortung der Frage 5 dargestellt.].*

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.)?

   In allen Fällen, die in der Beantwortung der Fragen 5 und 7 tabellarisch dargestellt wurden, wurde durch die Polizeien im Land Bremen ein Ermittlungsverfahren eingeleitet.

   Der Beantwortung der Frage durch die Staatsanwaltschaft Bremen wurde die in Bezug auf Frage 2 verwendete Definition von „Cybercrime im engeren Sinne“ zugrunde gelegt. Im Einzelnen wurden folgende Straftatbestände näher ausgewertet:

   - Ausspähen von Daten gemäß § 202a StGB,
   - Abfangen von Daten gemäß § 202b StGB,
   - Vorbereiten des Ausspähens und Abfangens von Daten gemäß § 202c StGB,
   - Datenveränderung gemäß § 303a StGB,
   - Computersabotage gemäß § 303b StGB.

   Gegenstand der durch die Staatsanwaltschaft Bremen durchgeführten Abfrage sind alle Ermittlungsverfahren gegen unbekannte und bekannte Tatverdächtige, die zwischen dem 01.01.2020 und dem 31.12.2023 eingeleitet wurden. Die Abfrage erfolgte dabei, der Systematik des Fachverfahrens entsprechend, personenbezogen *[Richten sich die Ermittlungen in einem konkreten Verfahren gegen vier Beschuldigte, so wird das Verfahren demnach viermal gezählt. Es werden dementsprechend auch vier Ergebnisse zum Stand des Verfahrens mitgeteilt.]* und fand zum Stichtag 12.09.2024 statt. Sie bezieht sich auf die o. g. Straftatbestände.

   Die weitere Darstellung erfolgt getrennt nach Js- und UJs-Verfahren (bei Js handelt es sich um Ermittlungsverfahren, bei UJs um Ermittlungsverfahren gegen Unbekannt).

   Sämtliche nachfolgend und nach Einleitungsjahren getrennte aufgeführten Verfahren gegen unbekannte Täter (UJs) wurden bereits einer Erledigung (durch Einstellung) zugeführt:

Delikt	**2020**	**2021**	**2022**	**2023**
§ 202a StGB	190	144	118	58
§ 202b StGB	0	0	0	1
§ 202c StGB	3	3	1	2
§ 303a StGB	3	65	23	10
§ 303b StGB	10	12	2	2

Bei den Verfahren gegen beschuldigte Personen (Js) ergibt sich, ebenfalls nach Kalenderjahren getrennt, folgendes Bild:

2020:

Delikt	**Anzahl**	**Noch anhängig**	**Abgabe**	**Eingestellt**	**Anklage**	**Strafbefehlsantrag**

§ 202a StGB	81	2	18	59	2	0
§ 202b StGB	3	0	0	3	0	0
§ 202c StGB	1	0	0	1	0	0
§ 303a StGB	7	0	1	6	0	0
§ 303b StGB	0	0	0	0	0	0

Beide angeklagten Verfahren wegen des Tatvorwurfs des Ausspähens von Daten (§ 202a StGB) wurden im gerichtlichen Verfahren durch den Jugendrichter gemäß § 47 JGG nach Ermahnung eingestellt.

2021:

Delikt	Anzahl	Noch anhängig	Abgabe	Eingestellt	Anklage	Strafbefehlsantrag
§ 202a StGB	119	0	36	81	1	1
§ 202b StGB	1	0	0	1	0	0
§ 202c StGB	0	0	0	0	0	0
§ 303a StGB	11	0	1	9	0	1
§ 303b StGB	3	0	0	3	0	0

Das wegen des Tatvorwurfs des Ausspähens von Daten angeklagte Verfahren wurde durch den Jugendrichter gemäß § 47 JGG nach Ermahnung eingestellt. Der wegen des Tatvorwurfs der Datenveränderung beantragte Strafbefehl über 30 Tagessätze zu jeweils zehn Euro ist rechtskräftig.

2022:

Delikt	Anzahl	Noch anhängig	Abgabe	Eingestellt	Anklage	Strafbefehlsantrag
§ 202a StGB	72	3	15	53	0	1
§ 202b StGB	1	0	1	0	0	0
§ 202c StGB	0	0	0	0	0	0
§ 303a StGB	8	0	0	8	0	0
§ 303b StGB	0	0	0	0	0	0

Der wegen des Tatvorwurfs des Ausspähens von Daten beantragte Strafbefehl über eine Geldstrafe von 80 Tagessätzen zu jeweils zehn Euro ist rechtskräftig.

2023:

Delikt	Anzahl	Noch anhängig	Abgabe	Eingestellt	Anklage	Strafbefehlsantrag

§ 202a StGB	69	16	10	43	0	0
§ 202b StGB	1	1	0	0	0	0
§ 202c StGB	2	1	0	1	0	0
§ 303a StGB	6	0	0	6	0	0
§ 303b StGB	1	0	0	1	0	0

Hinsichtlich der im Jahr 2023 neu eingeleiteten Verfahren konnte bislang noch keine Anklageerhebung bzw. keine Strafbefehlsantragstellung verzeichnet werden.

Ursächlich für die Unterschiede zwischen der Anzahl der durch die Polizei erfassten Fälle der o. g. Straftatbestände sowie der Anzahl der durch die Staatsanwaltschaft weiter verfolgten Fälle sind die Abläufe des Ermittlungsverfahrens. Die Fertigung einer Strafanzeige und die hiermit zugrundeliegende Erfassung eines Straftatbestands durch die Polizei (Anzahl der bei der Polizei eingeleiteten Ermittlungsverfahren) hat beispielsweise nicht zwangsläufig zur Folge, dass die Staatsanwaltschaft dieses Ermittlungsverfahren anhand des durch die Polizei erfassten Straftatbestands fortführt. Ebenso kann es bei Tatserien, bei denen durch die Polizei für jede Tat ein eigener Fall erfasst wird, dazu kommen, dass die Staatsanwaltschaft diese Einzelverfahren im Zuge der abschließenden Bearbeitung unter einem staatsanwaltschaftlichen Aktenzeichen zum Zwecke der gleichzeitigen Verhandlung und Entscheidung zusammenfasst (Verfahrensverbindung).

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?

   Der Abschnitt K134 Cybercrime/OSINT, der im Landeskriminalamt für die Bekämpfung CCieS zuständig ist, sowie die für den Bereich Spionage zuständige Staatsschutzabteilung des Landeskriminalamtes (Referat K63) verfügen zur Erfüllung der Aufgaben der Alltagsorganisation über einen angemessenen Personalkörper. Auf Grundlage der stetig zunehmenden Vielfalt in diesem Phänomen wird zukünftig eine personelle Verstärkung angestrebt. Besondere Softwareprodukte und technische Ausstattung sind auf einem adäquaten Stand der Technik. Im Zuge neuer technischer Lösungen werden weitere Haushaltsmittel perspektivisch erforderlich werden, um die gezielte Bearbeitung des Deliktfeldes zu gewährleisten.

   Bei der Staatsanwaltschaft Bremen werden Ermittlungsverfahren – auch gegen Jugendliche und Heranwachsende – wegen Internet-Kriminalität, dabei insbesondere solche gemäß §§ 202a, 202b, 202c, 303a, 303b StGB, soweit besondere Kenntnisse im Bereich des Internets oder der Datenverarbeitung erforderlich sind, durch zwei Sonderdezernent:innen mit einem Gesamtpensum von 0,3 Arbeitskraftanteilen (AKA) bearbeitet. Diese verfügen jedoch im Vergleich zu den übrigen Dezernent:innen der Staatsanwaltschaft nicht über eine besondere materielle oder finanzielle Ausstattung. Die in die Sonderdezernate übernommenen Verfahren konnten in der jüngeren Vergangenheit mit der bestehenden personellen Ausstattung adäquat bearbeitet werden.

   Die Zuständigkeit in der Spionage- und Cyberabwehr obliegt sowohl dem Bundesamt für Verfassungsschutz (BfV) als auch dem Landesamt für Verfassungsschutz (LfV). Die gemeinsame Fallbearbeitung erfolgt in einem sehr engen, regelmäßigen Austausch und erfordert ein hohes Maß an Abstimmung und Kooperation. Das BfV übernimmt dabei

länderübergreifende Sachverhalte als auch grundsätzliche Aufgaben im Verbund, das LfV sowohl die Bearbeitung von Sachverhalten als auch die praktische Arbeit vor Ort. Grundsätzlich ist für die Cyberabwehr die Zusammenarbeit mit nationalen und internationalen Partnerbehörden erfolgskritisch, weil die für Cyberangriffe genutzte Serverinfrastruktur länder- und staatenunabhängig ist. Insbesondere im Zeitverlauf der letzten Jahre ist zu konstatieren, dass die Bedrohung sowohl durch Cyberangriffe als auch durch Cyberspionage und Cybersabotage exponentiell zunimmt und eine immer stärkere Professionalisierung aufgrund des technischen Fortschritts festzustellen ist.

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?

Die strafprozessualen Befugnisnormen §§ 100a und 100b StPO (Quellen-Telekommunikationsüberwachung (TKÜ), Online-Durchsuchung) sehen im Unterschied zu § 100c StPO (Wohnraumüberwachung) ein verdecktes Betretungsrecht der Wohnung nicht vor. Die Regelung des § 100c StPO (Wohnraumüberwachung) umfasst neben dem Einsatz technischer Mittel in der Wohnung auch das verdeckte Betreten zum Einbau der Überwachungstechnik als ggf. erforderliche Begleitmaßnahme, ohne, dass dies in der Befugnisnorm explizit ausgewiesen sein muss. §§ 100a und 100b StPO ermöglichen dagegen zunächst nur den Eingriff in das Fernmeldegeheimnis (Art. 10 GG bei Quellen-TKÜ) und das sog. Computergrundrecht (bei Online-Durchsuchung), nicht jedoch den zusätzlichen Eingriff in die Unverletzlichkeit der Wohnung (Art. 13 GG). Aufgrund dessen scheidet das verdeckte Betreten einer Wohnung für eine Installation der Software bislang als Begleitmaßnahme zur Quellen-TKÜ und Online-Durchsuchung nach überwiegender Auffassung aus. Die Einführung einer strafprozessualen Regelung zum verdeckten Betreten bedürfte zudem einer Änderung des Art. 13 GG. Gleichwohl besteht aus Sicht der polizeilichen Praxis im Kampf gegen Cyberkriminalität, Wirtschaftsspionage und Konkurrenzausspähung der Bedarf, eine Wohnung zur Installation der entsprechenden Software verdeckt betreten zu dürfen.

Das BremVerfSchG räumt dem Landesamt für Verfassungsschutz wesentliche Kompetenzen zum Einsatz nachrichtendienstlicher Mittel ein. Gleichwohl ist festzustellen, dass die sich verstärkende Bedrohungslage gerade im Bereich der Spionage über das Internet und die darauf gestützten (verschlüsselten) Kommunikationsstrukturen einer entsprechenden Antwort des Rechtsstaats bedürfen. Der Senator für Inneres und Sport hat daher in Aussicht genommen, im Zuge der erforderlichen Novellierung des Gesetzes erforderliche Anpassungen vorzuschlagen. Dabei darf nicht übersehen werden, dass gerade der Bereich der TKÜ wesentlich der Kompetenz des Bundes unterfällt, der davon für die Nachrichtendienste des Bundes und der Länder durch das Artikel 10-Gesetz Gebrauch gemacht hat, einschließlich der Quellen-TKÜ. Hierbei gilt es, den Grundrechtsschutz in der Landesverfassung bei der begehrten Kompetenzerweiterung zu achten.

Der Senat vertritt die Ansicht, dass die anonyme und verschlüsselte Kommunikation im Internet nicht zuvörderst als Problem anzusehen ist. Technische Möglichkeiten der Verschlüsselung helfen Privatpersonen sowie Unternehmen, sich vor der unzulässigen Weitergabe vertraulicher Informationen oder Spionage zu schützen. Ebenso ermöglicht die anonyme sowie verschlüsselte Kommunikation auch Menschen in autoritären Staaten den unzensierten Zugang zum Internet und somit den Zugang zu freien Informationen sowie die Möglichkeit, Informationen aus diesen Staaten auch einer breiten Öffentlichkeit zugänglich zu machen. Dem Senat ist ebenfalls bewusst, dass die Möglichkeiten zur anonymen und verschlüsselten Kommunikation für illegale Aktivitäten missbraucht werden und den Strafverfolgungsbehörden adäquate Möglichkeiten zur

Verfolgung und Aufklärung insbesondere schwerer Straftaten zur Verfügung stehen müssen.

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?

Aus Sicht der Senatorin für Justiz und Verfassung ist hinsichtlich bestehender Gesetze für den Bereich CCieS ein Änderungsbedarf aktuell nicht ersichtlich. Die Möglichkeit, im Internet anonym und verschlüsselt zu kommunizieren, stellt die Ermittlungsbehörden generell vor erhebliche und stetig zunehmende Herausforderungen, die sich nicht auf die genannten Deliktsbereiche beschränken.

Als einzige für den Bereich Cybercrime relevante Gesetzesänderung seit dem Jahr 2020 sind die Einführung des § 127 StGB (Betreiben krimineller Handelsplattformen im Internet) mit Wirkung vom 01.10.2021 und damit einhergehende Änderungen der StPO zu nennen. Entsprechende Ermittlungsverfahren sind in den beiden Sonderdezernaten der Staatsanwaltschaft Bremen jedoch bislang nicht geführt worden.

Aus Sicht der Polizeien im Land Bremen bedarf es für Fälle, in denen sich Cybergefahrenlagen länderübergreifend auswirken oder nicht lokalisierbar sind, in der Gefahrenabwehr eines abgestimmten Vorgehens zwischen Bund und Ländern. Vor dem Hintergrund der ausschließlich bei den Ländern liegenden gefahrenabwehrrechtlichen Kompetenzen entstehen Regelungslücken. Der Senator für Inneres und Sport unterstützt daher das Bestreben des BKA zur Schaffung von dortigen gefahrabwehrrechtlichen Kompetenzen für bestimmte Fallkonstellationen.

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?

Am 15.08.2024 wurde eine Kooperationsvereinbarung zwischen der Freien Hansestadt Bremen und dem BSI unterzeichnet. Ziel ist eine verbesserte Zusammenarbeit zwischen dem BSI und der Freien Hansestadt Bremen (es wird auf die Antwort zu Frage 3b) verwiesen).

Im Rahmen der Strafverfolgung ist das Landeskriminalamt über das Referat K13 Cybercrime & Digitale Spuren, Abschnitt K134 Cybercrime/OSINT, mit allen weiteren Landes- und beteiligten Bundesbehörden eng vernetzt. Neben dem bundesweit aktiv agierenden ZAC-Verbund findet ein intensiver Informations- und Unterstützungsaustausch zwischen allen Cybercrime-Dienststellen der Länder und des Bundes statt. Über das BKA und Europol werden notwendige Verbindungen zu allen ausländischen Dienststellen effektiv umgesetzt. Ebenso steht das Referat K63 (Staatsschutz) in regelmäßigem Austausch mit den umliegenden Staatsschutzstellen in Niedersachsen.

Die Arbeit der Spionage- und Cyberabwehr des Landesamtes für Verfassungsschutz erfolgt in enger Abstimmung und Kooperation mit den Partnerbehörden des Verfassungsschutzverbundes, bestehend aus 16 Landesämtern, dem BfV und dem Bundesamt für den Militärischen Abschirmdienst (BAMAD) - Im Übrigen wird auf die Beantwortung der Frage 3c) verwiesen.

Aufgrund der bestehenden verfassungsrechtlichen Grenzen und praktischen Hürden für eine intensivere Zusammenarbeit des Bundes mit den Ländern im Bereich der Cyber- und

Informationssicherheit ist die Bundesregierung bestrebt, das BSI zu einer Zentralstelle, ähnlich dem BKA und dem BfV, auszubauen. Die diesbezüglichen Gespräche zwischen der Bundesregierung und den Ländern sowie im Bundestag bedürfen, insbesondere auch aufgrund bestehender Vorbehalte hinsichtlich einer Verfassungsänderung, weiterer Abstimmungen.

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?

    Die ZAC des Landeskriminalamtes ist die direkte Kontaktstelle für Unternehmen und Institutionen für den spezialisierten Informationsaustausch, Anzeigenerstattung in Cybervorfällen und Wahrnehmung von Beratungsleistungen als Präventivmaßnahme.

    Die ZAC ist Teil des Abschnitts K134; die Aufgaben werden von allen Ermittler:innen als Nebenaufgabe in der Bekämpfung der Cybercrime wahrgenommen. Die Vortragstätigkeit im Rahmen der Prävention erfolgt schwerpunktmäßig durch die Referatsleitung K13 bzw. Abschnittsleitung K134. Die statistische Erhebung von Beratungsleistungen sowie Vorträgen wird seit dem 01.01.2024 durchgeführt. In diesem Jahr wurden bislang 33 größere Veranstaltungen durch die ZAC begleitet. Die Vorträge werden generell als Vor-Ort-Schulungen durchgeführt, wodurch bereits eine Vielzahl verschiedener Unternehmen erreicht werden konnte.

    Die Vortragstätigkeit verfolgt neben der Darstellung aktueller Cyber-Bedrohungslagen und möglicher Schutzmaßnahmen das Ziel, die direkte Kontaktmöglichkeit zur Polizei Bremen bekannt zu machen, um so die polizeilichen Fähigkeiten sowie Unterstützungs- und Ermittlungsmöglichkeiten darstellen zu können. Die ZAC agiert auf Basis direkter Einladungen zu Veranstaltungen von Kammern, Institutionen, Vereinen oder Unternehmen zur Erreichung eines möglichst großen Adressatenkreises. Diese Praxis hat sich aus polizeilicher Sicht bewährt und wird weiterhin durch den betroffenen Adressatenkreis nachgefragt.

    Die ZAC des Landeskriminalamtes ist in Bremerhaven auf Präventionsveranstaltungen nicht aufsuchend aktiv, sondern agiert im Einzelfall auf besondere Anforderung einzelner Verbände. Unternehmen mit Sitz in Bremerhaven können sich grundsätzlich sowohl an die ZAC als auch an die örtlich zuständige Ortspolizeibehörde Bremerhaven wenden. Im Fachkommissariat Betrug der Ortspolizeibehörde Bremerhaven ist die Informations- und Kommunikations (IuK)-Kriminalität integriert und bearbeitet zuständigkeitshalber entsprechende Ermittlungsverfahren. Meldungen, welche bei der ZAC Bremen auflaufen, werden analog zu Flächenländern an die örtlich zuständigen Stellen zur weiteren Bearbeitung gesteuert. Ein aktives Agieren der Cybercrime-Fachdienststelle der Polizei Bremen in Bremerhaven erfolgt ausschließlich auf Grundlage von Amtshilfeersuchen.

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

        Die ZAC verfügt über kein freigestelltes Personal oder eigene Finanzmittel. Die ZAC ist organisatorisch bei der Polizei Bremen innerhalb des Ermittlungsabschnitts Cybercrime eingegliedert. Die Vortragstätigkeit, in der Regel außerhalb der Regelarbeitszeit, erfolgt aktuell durch die Referatsleitung K13 sowie die Abschnittsleitung K134. Hinsichtlich seiner Aufgabenwahrnehmung als Teil des Landeskriminalamtes erfolgt dies integriert in die Organisationsstruktur der Polizei Bremen.

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?

Die ZAC steht in kontinuierlichem Kontakt mit den interessierten bremischen Berufsverbänden (z. B. Handwerks- und Handelskammer) und tauscht sich regelmäßig mit unternehmerischen Zusammenschlüssen wie dem IFIT e.V. intensiv aus. Weiterhin bestehen Verbindungen zu Interessengruppen aus den IT-Bereichen des Gesundheitswesens und großen bremischen Unternehmen.

Die Kommunikation untereinander beruht auf gegenseitigem Vertrauen und Kenntnis der Sensibilität von Informationen. Nur auf diesem Weg kann eine Strafverfolgungsbehörde als vertrauensvoller Partner im Gesamtkomplex Cybercrime wahrgenommen und akzeptiert werden. Der gegenseitige Austausch möglicher erkannter Angriffsstrukturen beziehungsweise allgemeiner Informationen findet aktuell noch über die Polizei Bremen statt. Die Geschwindigkeit eines geschützten gegenseitigen Informationstransfers ausschließlich bezüglich laufender oder abgewehrter Cyberattacken und auf Basis der Erkenntnisse der unternehmerischen IT-Abteilungen und Polizei entscheidet über Erfolg oder Misserfolg einer Informationssteuerung.

Großverbände, wie die aufgeführte Allianz für Sicherheit in der Wirtschaft Norddeutschland e.V. – ASW Nord, sind über die Bundesbehörden intensiv angebunden. Die ZAC arbeitet nach den föderalen Vorgaben und beschränkt sich auf die Betreuung der regionalen Unternehmen.

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

Die ZAC ist ein wichtiger Baustein in der Kommunikation und Unterstützung der Strafverfolgungsorgane mit den bremischen Unternehmen, Institutionen und allen Behörden im Zusammenhang mit der Cyberkriminalität und der Vorbeugung dieser. Der Senator für Inneres und Sport wird die Prüfung der Erfordernisse eines Ausbaus der personellen und materiellen Ausstattung eng begleiten, um den gesellschaftlichen Entwicklungen und anstehenden Aufgaben in der hochkomplexen Cyberkriminalität polizeilich begegnen zu können.

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?

Das Landesamt für Verfassungsschutz betreibt im Rahmen des Wirtschaftsschutzes Präventionsarbeit in Wirtschaft, Wissenschaft, Politik und Verwaltung und sensibilisiert diese für etwaige Gefährdungen. Hierzu zählen neben den Gefahren des Extremismus vor allem auch die der Spionage, Sabotage und Proliferation sowie staatlich gesteuerte Bedrohungen aus dem Cyberraum. Im Fokus steht dabei eine adressaten- und zielgruppengerechte Aufarbeitung der hier vorliegenden Erkenntnisse, um der Rolle des Landesamtes für Verfassungsschutz als Frühwarnsystem gerecht zu werden. Dies wird etwa durch Sensibilisierungsvorträge und -veranstaltungen, die Übermittlung von Sensibilisierungs- und Sicherheitshinweisen sowie die Bereitstellung von technischen Indikatoren und Unterstützung zur Abwehr staatlich gesteuerter Cyberangriffe verwirklicht. Beim Vorliegen konkreter Erkenntnisse zu (Wirtschafts-) Spionage erfolgt eine Einzelfallbearbeitung unter Einsatz verschiedener nachrichtendienstlicher Mittel.

Im Weiteren wird auf die Antwort zu Frage 2 verwiesen.

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)

    Der Senator für Finanzen fördert mit Mitteln des IT-Planungsrates sowie eigenen Mitteln Informationsveranstaltungen, die sich nicht nur an Behörden richten, sondern auch optional andere Einrichtungen (z. B. die Volkshochschule). Zu nennen ist besonders die Veranstaltung „Die Hacker kommen“. Diese Veranstaltung wurde auch im Rahmen der CodeWeek für Schüler:innen angeboten und wurde mit guter Resonanz besucht.

    Im Zuständigkeitsbereich des Magistrats der Stadt Bremerhaven wird am 23.10.2024 eine Veranstaltung „Einblicke in die aktuelle Bedrohungslage und die Psychologie von Cyberkriminellen“ durch die Bremerhavener Gesellschaft für Investitionsförderung und Stadtentwicklung mbH (BIS) angeboten.

    Weitere Angebote sind dem Senat zum aktuellen Zeitpunkt nicht bekannt.

Beschlussempfehlung:

Die Bremische Bürgerschaft (Landtag) nimmt von der Antwort des Senats auf die Große Anfrage Kenntnis.

Anlage(n):
1. ANLAGE_Cyberkriminalität

Anlage 1 zur Großen Anfrage der Fraktion der CDU (Drucksache 21-735) vom 03. September 2024 und Mitteilung des Senats vom 29.10.2024

Übersicht der durch die Ressorts zurückgemeldeten Stellen und Einrichtungen zur Beantwortung der Frage 3:

Der Senator für Finanzen
Senatorische Dienststelle
Finanzamt Bremen
Finanzamt Bremerhaven
Finanzamt für Außenprüfung
Landeshauptkasse
Aus- und Fortbildungszentrum
Verwaltungsschule
Performa Nord
Immobilien Bremen

Der Senator für Inneres und Sport
Senatorische Dienststelle
Polizei Bremen / LKA
Statistisches Landesamt
Bürgeramt
Migrationsamt
Ordnungsamt
Feuerwehr Bremen
Bremer Bäder GmbH
Hochschule für Öffentliche Verwaltung

Die Senatorin für Kinder und Bildung
Senatorische Dienststelle
Schulen der Stadtgemeinde Bremen
Landesinstitut für Schule
Regionale Beratungs- und Unterstützungszentren Quartiersbildungszentren
Institut für Qualitätsentwicklung im Land Bremen (IQHB)
KiTa Bremen

Die Senatorin für Justiz und Verfassung
Senatorische Dienststelle
Gerichte
Staatsanwaltschaft
IT-Stelle der Justiz

Der Senator für Kultur
Senatorische Dienststelle
Landesarchäologie
Landesamt für Denkmalpflege
Landeszentrale für politische Bildung
Staatsarchiv
Musikschule Bremen
VHS-Bremen
Focke-Museum
Stadtbibliothek
Übersee-Museum
Bremer Philharmoniker
Theater Bremen

Die Senatorin für Arbeit, Soziales, Jugend und Integration
Senatorische Dienststelle
Amt für Soziale Dienste
Amt für Versorgung und Integration
Werkstatt Bremen
Ausbildungsgesellschaft Bremen mbH (ABiG)

Die Senatorin für Umwelt, Klima und Wissenschaft
Senatorische Dienststelle
Der Umweltbetrieb Bremen
Die Bremer Stadtreinigung AöR
Botanika GmbH
Studierendenwerk Bremen AöR
Hanseatische Naturentwicklung GmbH

Die Senatorin für Wirtschaft, Häfen und Transformation
Senatorische Dienststelle
Hansestadt Bremisches Hafenamt
Universum Managementges. mbH
Glocke GmbH
M3B GmbH
Bremer Aufbaubank (BAB)
Beteiligungs- und Managementgesellschaft Bremen (BBM)
Wirtschaftsförderung Bremen (WFB)
Fähren Bremen-Stedingen (FBS)
Flughafen Bremen GmbH
bremenports GmbH & Co. KG
BLG
Fischereihafen Betriebsgesellschaft mbH

Die Senatorin für Gesundheit, Frauen und Verbraucherschutz
Senatorische Dienststelle
Eichamt
Gesundheitsamt
Gewerbeaufsicht
LMTVet
LUA
GeNo
InphA GmbH

Die Senatorin für Bau, Mobilität und Stadtentwicklung
Senatorische Dienststelle
Landesamt GeoInformation Bremen
Amt für Straßen- und Verkehr
Bremer Straßenbahn Aktiengesellschaft
BREPARK GmbH
DEGES Deutsche Einheit Fernstraßenplanungs- und –bau GmbH
Grundstücksentwicklung Klinikum Bremen-Mitte GmbH & Co. KG
Grundstücksentwicklungsgesellschaft Klinikum Bremen-Mitte Beteiligungen mbH
LEA GmbH (Gesellschaft für Landeseisenbahnaufsicht
BREBAU GmbH

Senatskanzlei
Senatskanzlei sowie die dazu gehörenden Geschäftsbereiche

Der Magistrat der Stadt Bremerhaven
Der Magistrat
Beteiligungsgesellschaften der Stadtgemeinde Bremerhaven