BREMISCHE BÜRGERSCHAFT **Drucksache 20/479**
Landtag **(zu Drs. 20/311)**
20. Wahlperiode **23.06.20**

Mitteilung des Senats vom 23. Juni 2020

Wie ist Bremen im Kampf gegen Cyber- und Internetkriminalität aufgestellt?

Die Fraktion der CDU hat unter Drucksache 20/311 eine Große Anfrage zu obigem Thema an den Senat gerichtet.

Der Senat beantwortet die vorgenannte Große Anfrage wie folgt:

I. Angriffe auf Bremer Behörden und Organisationen

1. Welche Formen und wie viele Angriffe auf Netzwerke, Server, Computer, Internetseiten und -angebote von Behörden im Land Bremen und Unternehmen mit Aufgaben der öffentlichen Daseinsvorsorge hat es von 2019 bis heute (Stichtag: 1. März 2020) gegeben, welcher Schaden ist dabei entstanden, und wie wird seitens der Behörden jeweils darauf reagiert? Welche Entwicklung sieht der Senat hinsichtlich der Quantität und Qualität der Angriffe auf die Einrichtungen der bremischen Verwaltung in den letzten Jahren?

   Die Zahl der Angriffe kann nicht valide beziffert werden. Die bremische Verwaltung und Unternehmen mit Aufgaben der öffentlichen Daseinsvorsorge sind täglich mehreren tausend, wenn nicht gar hunderttausend Angriffsversuchen, insbesondere Anfragen und Scans aus automatisierten Systemen, ausgesetzt.

   Bisher konnten alle erkannten Angriffe in der Verwaltung letztendlich abgewehrt werden. Vereinzelte Rechner wurden kurzfristig befallen, was zu geringfügigen Störungen im Betriebsablauf durch notwendige Neuinstallationen führte. Finanzielle Schadensauswirkungen, für die etwaige Wiederherstellung von Systemen, werden nicht nachgehalten.

   In der Ortspolizeibehörde Bremerhaven (OPB) gab es aber einen herausragenden Vorfall, bei dem durch einen Cyberangriff die Erreichbarkeit der externen Webpräsenz (www.polizei.bremerhaven.de) außer Kraft gesetzt wurde. Ein finanzieller oder datentechnischer Schaden ist nicht entstanden. Die Homepage der OPB war jedoch für zwei Tage nicht erreichbar.

   Die Verwaltung reagiert auf die Angriffe mit technischen und organisatorischen Maßnahmen. Technisch und organisatorisch ist die Abwehr seit der Einführung des bremischen Informationssicherheitsmanagements (2013) an den zentralen Eingangspunkten des Internets stark verbessert worden. Potenzielle Schadsoftware wird frühzeitig erkannt. Organisatorisch wurde mit sogenannten Awareness-Maßnahmen reagiert:

   a) Dauerhafte Durchführung von Veranstaltungen, wie „Die Hacker kommen“,

   b) Sensibilisierungskampagnen (zum Beispiel Kameraschutzschilder für Laptops),

   c) Hinweise im Intranet (Mitarbeiterportal),

d) Aus- und Fortbildungsangebote für die Beschäftigten, das IT-Personal und für Informationssicherheitsmanagementbeauftragte,

e) Veröffentlichung/Verbreitung von Informationen aus dem Computer Emergency Response Team (CERT-Nord) für die Verwaltungen der Länder Schleswig-Holstein, Hamburg, Bremen und Sachsen-Anhalt CERT-Nord, dem VerwaltungsCERT Verbund von Bund und Länder.

Insbesondere die E-Mailbasierten Angriffe (zum Beispiel EMOTET) haben in Qualität und Quantität zugenommen. Nutzer können zum Teil nicht mehr erkennen, ob eine E-Mail „echt" ist oder Schadsoftware enthält, da die Schadsoftware sehr oft abgefangene E-Mail-Wechsel mit bekannten Adressen nutzt, sodass sie vertrauenswürdig wirkt. Gleichwohl wird durch die eben aufgezählten Maßnahmen versucht, auch dieser Bedrohung entgegenzuwirken. Durch die Einführung der elektronischen Akte und elektronischen Geschäftsgänge versucht der Senat, die Abhängigkeit des Verwaltungshandelns von der E-Mail-Infrastruktur zu reduzieren.

2. Welche Motive haben die Täter möglicher Attacken auf das Netz Bremer Behörden und Organisationen?

Die Motivlagen von Angreifern sind vielfältig. Beispielhaft sind folgende:

a) Verhinderung von Diensten aufgrund individueller oder wirtschaftlicher Interessen an der Verwundbarkeit von IT-Systemen.

b) Organisierte und individuelle Kriminalität, um Erpressung mit Gewinnerzielungsabsicht durchzuführen.

c) Allgemeine Motive des Ausspähens von Daten zur Ermöglichung von Datendiebstahl, Datenmissbrauch und Datenmanipulation.

Der Datendiebstahl dient wiederum häufig als Vorbereitungshandlung für weitere Folgeangriffe (siehe oben „vertrauenswürdige E-Mail"). Ebenso können gehackte/gehijackte PCs als Werkzeuge für weitere, gut getarnte Angriffe dienen (Bot-Netze).

3. Welche konkreten Gefahren sieht der Bremer Senat im Zusammenhang mit möglichen Attacken auf die Bremer Verwaltung, und wie hoch schätzt er das Risiko künftig zum Opfer von Attacken zu werden? Welche vorbeugenden Maßnahmen werden ergriffen, um bestmöglich geschützt zu sein?

Konkrete Gefahren bestehen für die Bremer Verwaltung aufgrund der dynamischen und qualitativ verbesserten Angriffe. Durch sogenannte DDos-Angriffe (Distributed-Denialof-Service, deutsch wörtlich: verteilter Dienstverweigerungs-Angriff, ist die Nichtverfügbarkeit eines Datendienstes, einer Internetpräsenz, durch Überlastung mittels einer Vielzahl von Anfragen aus verschiedenen Quellen) und insbesondere die allgemeine Gefährdung durch infizierte E-Mail (EMOTET) ist das Risiko, dass ganze Netze stillgelegt werden, erheblich gestiegen. Gezielte und ungezielte Angriffe zusammen mit weiteren Ereignissen, wie die derzeit andauernde ressourcenschwächende Pandemielage, erhöhen das Risiko eines erfolgreichen Angriffs auf die Verwaltung Bremens (Kumulationseffekt).

Die Freie Hansestadt Bremen (FHB) hat ein Informationssicherheitsmanagement im Land etabliert. Besondere Aufmerksamkeit wird dabei auf die Sensibilisierungsmaßnahmen der Beschäftigten gelegt. Daneben werden technische und organisatorische Maßnahmen getroffen, die die Widerstandsfähigkeit der IT-Systeme erhöhen. Weiterhin hat die FHB zusammen mit weiteren Ländern ein Computer Emergency Response Team (CERT Nord) eingerichtet, um den erforderlichen Informationsaustausch zu gewährleisten. Begleitend werden rechtliche Voraussetzungen geschaffen, um sich rechtskonform mit modernen Mitteln den Angreifern zu erwehren.

4. Wie sind die Behörden mit Sicherheitsaufgaben in Bremen im Kampf gegen Angriffe aus dem Internet personell, materiell und finanziell aufgestellt, strukturiert und ausgestattet? Inwiefern hält der Senat das

vorgehaltene Personal und die finanziellen vorgehaltenen Mittel für ausreichend? Welche Veränderungen der Ausstattung sind beabsichtigt? Wie ist der Stand der quantitativen und qualitativen Ausstattung Bremens im Vergleich mit der des Bundes und der anderen Bundesländer (unter Berücksichtigung von Größenordnungen und Aufgabenteilungen) zu beurteilen?

Das zentrale Informationssicherheitsmanagement beim Senator für Finanzen, insbesondere der IT-Sicherheitsbeauftragte der FHB, arbeitet in enger Abstimmung mit dem Senator für Inneres zusammen.

Bezugsgrößen im Bund-Länder-Vergleich liegen zur Bewertung nicht vor, da auch organisatorische Aufgabenzuschnitte, der Einsatz von IT-Dienstleistern und Beratungsunternehmen einen Vergleich nicht zulassen.

Zum 1. August 2018 wurde die Referentenstelle des strategischen Informationssicherheitsbeauftragten beim Senator für Inneres und der zugeordneten Behörden/Ämter erstmalig besetzt. Dadurch wurden die Grundvorrausetzungen für die Etablierung eines wirksamen Informationssicherheitsmanagements nach den geforderten Grundschutzstandards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geschaffen. Das operative Informationssicherheitsmanagement der zugeordneten Behörden und Ämter befindet sich im Aufbau.

Vor dem Hintergrund der besonderen datenschutzrechtlichen Schutzbedarfe der hier verarbeiteten personenbezogenen Daten und aufgrund der eigenen Geheimschutzinteressen sind die Anforderungen der Polizei an technische und organisatorische Schutzmechanismen sehr hoch. Die Polizeibehörden des Bundes und der Länder haben sich im „Corporate Network Polizei"-Verbund (CNP) zusammengeschlossen und stimmen die erforderlichen Schutzmaßnahmen auf Basis der BSI-Standards „200-1" bis „200-4" untereinander ab. Diese werden dann in den Polizeibehördenumgesetzt. Im Kernbereich der IT sind bei der Polizei Bremen 38 Vollzeitstellen eingerichtet, drei Funktionsstellen sind unmittelbar mit der Informationssicherheit befasst, operativ arbeiten alle Mitarbeitenden an Fragestellungen der IT-Sicherheit mit.

Der Betrieb für Informationstechnologie Bremerhaven (BIT) ist personell und materiell ausreichend aufgestellt Die technische Ausstattung entspricht dem Stand der Technik unter Berücksichtigung von Wirtschaftlichkeitsaspekten. Eine personelle und finanzielle Stärkung des Themenbereiches ist grundsätzlich erstrebenswert, da ergänzende Schutzmaßnahmen immer möglich sind, ein zwingender Handlungsbedarf besteht diesbezüglich aktuell nicht. Aufgrund der sich ständig ändernden Anforderungen durch neue Technologien wird das Erfordernis der technologischen und personellen Verstärkung ständig neu bewertet.

Die Feuerwehr Bremen hat Maßnahmen zur Erhaltung der Informationssicherheit ergriffen. Anders als bei der Polizei gibt es jedoch keine bundesweiten Absprachen/Vorgaben, sondern es gelten die Regelungen der FHB. Die Feuerwehr Bremen ist bemüht, die Informationssicherheit auf den geforderten Stand zu bringen. Die Betriebssysteme sollen angepasst und auf den aktuellen Stand gehoben werden. Zurzeit finden Gespräche zur Finanzierung der Maßnahme statt.

5. Inwieweit arbeitet der Bremer Senat mit den zuständigen Behörden der anderen Bundesländer und dem Bundesamt für Sicherheit in der Informationstechnik zusammen, welche regelmäßigen Treffen gibt es auf diesen Ebenen, und wo besteht nach Ansicht des Senats noch Verbesserungsbedarf in der Zusammenarbeit?

   Bund und Länder arbeiten beim Thema Informationstechnik der öffentlichen Verwaltungen auf Ebene des IT-Planungsrates (IT-PLR) zusammen. Eine ständige Arbeitsgruppe des IT-PLR ist die AG Informationssicherheit, mit Mitgliedern aus dem Bund (Bundesministerium des Innern, für Bau

und Heimat [BMI] und Bundesamt für Sicherheit in der Informationstechnik [BSI]), den Ländern und den kommunalen Spitzenverbänden, die sich regelmäßig austauscht. Die in der AG entwickelte Informationssicherheitsleitlinie von Bund und Ländern enthält gemeinsame Vorgehensweisen zur Erhöhung der Resilienz der IT von öffentlichen Verwaltungen. Die vereinheitlichte und übergreifende Sensibilisierung, Aus- und Fortbildung von Beschäftigten stehen im Fokus der Bundesakademie für öffentliche Verwaltung (BAköV).

Das BSI hat für den Bund in Aussicht gestellt, mit jedem Land eine Absichtserklärung zu schließen, die eine kooperative Zusammenarbeit des Bundes mit dem jeweiligen Land sichert und vertieft. Aufbauend auf dieser Absichtserklärung soll ein Verwaltungsabkommen zwischen dem BMI und dem Land geschlossen werden. Bremen befindet sich in der Abstimmung.

Bund und Länder haben den erwähnten Verbund der CERTs etabliert. Die CERTs der Länder und des Bundes tauschen sich über aktuelle Bedrohungslagen aus und teilen sich erkannte Angriffsmuster untereinander mit.

Übergreifende Cybersicherheitsthemen werden in einer regelmäßig stattfindenden Bund-Länder-AG Cybersicherheit der Innenministerkonferenz erarbeitet. Auch hier sind die Behörden im Geschäftsbereich des BMI vertreten (ebenfalls das BSI), gegebenenfalls die Bundesanstalt für den Digitalfunk (BDBOS) oder auch das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK). Auch Aus- und Fortbildungsmaßnahmen werden von dort gesteuert. Die Umsetzung entsprechender Maßnahmen können aufgrund fehlender finanzieller und personeller Ressourcen oftmals nur mit Verzögerung umgesetzt werden.

Auf ministerieller und polizeilicher Ebene findet ein intensiver Informations- und Erfahrungsaustausch zwischen den Landes- und Bundesbehörden statt. Die Polizeien des Landes Bremen kooperieren mit dem BSI über länderübergreifende Gremien. Das Statistische Landesamt (StaLA) Bremen ist Mitglied der AG Sicherheit im statistischen Verbund, an der auch das Statistische Bundesamt beteiligt ist.

II. Radikalisierung und Hass im Internet

1. Welche Internetplattformen werden nach Kenntnis des Senats häufig von radikalen Gruppen zum Anwerben von neuen Mitgliedern genutzt?

   Generell kann Radikalisierung und Anwerbung über zahlreiche Wege erfolgen, beispielsweise über verschiedene Social-Media-Plattformen, Messenger-Gruppen, aber auch selbst angelegte Blogs und Internetseiten.

   Die Bandbreite genutzter Rekrutierungsplattformen im Internet variiert und bedingt sich aus vielen verschiedenen Faktoren: In allen Phänomenbereichen werden nach wie vor besonders mitgliederreiche Netzwerke wie zum Beispiel Facebook, Twitter, YouTube, Telegram oder vk.com genutzt, um darin möglichst weite Teile der Gesellschaft mit populistisch aufbereiteten Feindbildszenarien, Schuldzuweisungen und Opfer-Narrativen zu erreichen. Auch auf Instagram oder im Netzwerk Gab finden sich entsprechende Inhalte. Auf diese Weise sollen Ängste geschürt, Vorbehalte geweckt und Zustimmung für extremistische Ideologeme generiert werden. Daneben bieten spezielle virtuelle Communities, wie zum Beispiel Gaming-Plattformen oder andere themenbezogene Foren, Extremisten erleichterte Zugangsmöglichkeiten zu Menschen, die sich auf der Basis eines gemeinsamen Interesses begründen. Es gibt keine staatlichen Standards oder Lizenzierungen, die Anbieter von Online-Spielen zu Schutzmechanismen verpflichten. Das Spektrum der virtuellen Umgebungen ist breit gefächert und eröffnet nur in konkreten Einzelfällen ausreichende Anhaltspunkte für den Verdacht extremistischer Bestrebungen, wie zum Beispiel die Gruppe „Reconquista Germanica“ (aufgelöst im November 2019) auf der Plattform „Discord“.

Instagram ist für die jüngere Zielgruppe eine beliebte Plattform. Videos und Fotos können gestaltet und anschließend gepostet beziehungsweise weitergeleitet werden. Extremisten nutzen den sogenannten Explore-Feed geschickt aus, um Jugendliche kontinuierlich zu beeinflussen. Jugendschutz.net kommt zu folgender Einschätzung: „Sucht jemand nach bestimmten Schlagworten, werden […] im ExploreFeed der Userin beziehungsweise des Users automatisiert Inhalte angezeigt, darunter auch klar extremistische Inhalte."

Der Kernaspekt der extremistischen Arbeit besteht darin, eine „Wir" und „Die"-Dichotomie zu etablieren und junge Menschen durch ihre Ansprache ideologisch zu gewinnen. Ein „Anwerben" im Sinne einer Ansprache junger Menschen, mit dem Ziel sich mit ihnen zu treffen, steht nicht im Vordergrund.

2. Welche Maßnahmen können ergriffen werden, um derartigen Radikalisierungen im Internet vorzubeugen beziehungsweise diese zu verhindern?

Demokratie- und menschenfeindliche Akteurinnen/Akteure nutzen Social-Media-Plattformen sehr intensiv. Dies stellt ein Risiko dar, das gesellschaftlich kaum beachtet wird. Ein effektives Monitoring der Inhalte und die konsequente Sichtbarmachung von Meinungen, die Vielfalt und Demokratie befürworten, setzt dieser Gefahr etwas entgegen und wirkt präventiv. Dazu gehört die nachhaltige Aufklärung über die Bedeutung und Funktion von „Counter-Speech" zum Beispiel in Kommentarspalten und die konsequente Ahndung strafbarer Inhalte.

Die medienpädagogischen Ansätze, die im Rahmen des Modellprojekts #denk_net (Servicebureau/LidiceHaus) entwickelt wurden, sind gut geeignet, um Medienkompetenz und einen adäquaten Umgang mit demokratie- und menschenfeindlichen Einstellungen im Netz zu vermitteln.

Das Landesamt für Verfassungsschutz (LfV) ist eng eingebunden in die in Bremen bestehenden Präventionsnetzwerke, insbesondere beim Kompetenzzentrum Deradikalisierung und Extremismusprävention (KODEX). In diesem Rahmen ist das LfV an der konzeptionellen Arbeit zur Verhinderung von Radikalisierungsprozessen, nicht zuletzt im Internet, kontinuierlich beteiligt. Das LfV setzt zudem seit Januar 2018 datenwissenschaftliche Analyseverfahren aus dem Forschungsfeld der „Computational Social Sciences" zur Erfüllung seines gesetzlichen Auftrags in den Communities extremistischer Bestrebungen ein. Mit Hilfe solcher empirischen Methoden lassen sich zum Beispiel latente strukturelle Zusammenhänge, personelle Verbindungen oder inhaltliche Schwerpunkte in virtuellen Communities analysieren sowie relevante Hauptakteure darin identifizieren. Insbesondere im Phänomenbereich Rechtsextremismus und innerhalb des „Reichsbürger"-Spektrums konnten derartige Verfahren in Bremen bereits erfolgreich eingesetzt und quantitative Belege generiert werden, die in die Bewertungen von Beobachtungsobjekten und die Öffentlichkeitsarbeit des Landesamtes für Verfassungsschutz eingeflossen sind.

Auch die Polizei schöpft alle zur Verfügung stehenden gefahrenabwehrenden und strafrechtlichen Möglichkeiten aus, um unter anderem verfassungsfeindliche, volksverhetzende und extremistische Inhalte im Internet zu bekämpfen. Die Polizei verstärkt personell den Bereich der Auswertung aller Formen politisch motivierter Kriminalität und beteiligt sich an Forschungsprojekten, um ihre Fähigkeiten weiterzuentwickeln.

Für die Präventionsarbeit werden pädagogische Konzepte herangezogen (zum Beispiel des Bundesministeriums für Familie, Frauen, Senioren und Jugend), um einer Radikalisierung im Internet vorzubeugen.

Das Bremische Schulgesetz setzt mit den in § 5 formulierten Bildungs- und Erziehungszielen einen verbindlichen Rahmen für die primär präventiv ausgerichtete Arbeit an Schulen gegen Radikalisierung, Kriminalität, Hass und gruppenbezogene Menschenfeindlichkeit sowie für die Vermittlung

demokratischer Werte und Toleranz. Unabhängig vom Weg, über den Hate Speech beziehungsweise radikales Gedankengut jeder Ausrichtung verbreitet wird, betrachtet der Senat fortlaufende Aufklärung, Erinnern und Gedenken sowie menschliche Begegnung als wirksamstes Mittel, um einer Radikalisierung präventiv entgegenzutreten. Zahlreiche entsprechend konzipierte Maßnahmen sind im „Sechsten Bericht über Rechtsextremismus und Fremdenfeindlichkeit im Land Bremen“ (Drucksache 19/1438) aufgeführt worden.

Zu den weiteren präventiv gegen Radikalisierung im Internet wirkenden Maßnahmen gehört die Medienbildung in der Schule, die als kontinuierlicher, pädagogisch strukturierter und begleiteter Prozess angelegt ist und Schülerinnen/Schüler befähigen soll, sich konstruktiv und kritisch mit der Medienwelt auseinanderzusetzen und Medien selbstbestimmt und kompetent zu nutzen. Im Unterricht werden die Voraussetzungen geschaffen, Schülerinnen und Schüler an den kommunikativen Möglichkeiten der globalisierten Gesellschaft teilhaben zu lassen, sie zugleich aber zu befähigen, neben den Chancen auch die Risiken und Manipulationsmöglichkeiten der Mediennutzung, insbesondere der sozialen Medien, zu erkennen und den Herausforderungen mit Werteklarheit zu begegnen.

Im Programm „Respekt Coaches“ der Jugendmigrationsdienste (JMD) arbeiten pädagogische Fachkräfte in der primären Prävention im Lebensraum Schule, um junge Menschen Phänomen übergreifend, insbesondere vor religiös begründetem Extremismus, zu schützen. Die „Respekt Coaches“ unterstützen Schülerinnen und Schüler dabei, in einer pluralen, demokratischen Gesellschaft ihren eigenen Standpunkt zu finden, sich selbst im Diskurs mit anderen zu positionieren und mit unterschiedlichen Auffassungen umzugehen. Mitarbeitenden des Programms „Respekt Coaches“ arbeiten mit den Trägern der politischen Jugendbildung und der Radikalisierungsprävention zusammen.

Im Bereich der politischen Weiterbildung sind die Themen Fremdenfeindlichkeit, Hass und Ausgrenzung seit jeher zentrale Bestandteile und gehören zum Kernbereich der ebenfalls präventiv ausgerichteten Bildungsaktivitäten der nach dem Bremischen Weiterbildungsgesetz anerkannten Weiterbildungseinrichtungen.

3. Wie werden Lehrpersonal, Professoren- und Professorinnen, Mitarbeiterinnen und Mitarbeiter öffentlicher Stellen et cetera auf den Umgang mit möglicherweise Radikalisierten vorbereitet und geschult? Inwieweit gibt es Stellen, an die sie sich bei Verdacht auf Radikalisierung wenden können?

Im Zusammenhang mit religiös begründetem Extremismus steht die Fach- und Beratungsstelle kitab (Träger Vaja e. V.) zur Verfügung. Im Umgang mit Rechtsextremismus sind das Mobile Beratungsteam Bremen (Träger LidiceHaus) und die Distanzierungsberatung reset (Träger Vaja e. V.) ansprechbar. Das Demokratiezentrum Land Bremen bietet eine Verweisberatung an und vermittelt Anfragen an die zuständigen Stellen. Die Beratungs- und Fortbildungsangebote sowie Sensibilisierungsmaßnahmen des Demokratiezentrums wenden sich an alle Fachkräfte (insbesondere der Kinder- und Jugendhilfe) und Personen, die sich zu dem Thema Rechtsextremismus und Gruppenbezogene Menschenfeindlichkeit beziehungsweise religiös begründeten Extremismus weiterbilden möchten.

Beim Senator für Inneres wurde 2018 das Kompetenzzentrum für Deradikalisierung und Extremismusprävention (KODEX) eingerichtet. Im Bereich der Arbeit an gewaltbereiten und stark radikalisierten Personen soll durch Kodex die notwendige Kooperation des Präventionsnetzwerks mit den Sicherheitsbehörden geregelt werden.

KODEX ist verantwortlich für Maßnahmen der Deradikalisierungsarbeit und Ausstiegsberatung im Bereich der tertiären Prävention. Mit der Umsetzung dieser Arbeit wurde der Verein Ambulante Maßnahmen Altona e. V. im Rahmen des Projekts „Legato-Disengagement" beauftragt.

An der Universität Bremen können sich Lehrpersonen, Professorinnen/Professoren et cetera an die Arbeitsstelle gegen Diskriminierung und Gewalt (ADE) wenden, um konkrete schwierige Situationen im Sinne von diskriminierenden, übergriffigen oder konfliktträchtigen Haltungen und Verhaltensweisen von Studierenden, Mitarbeiterinnen/Mitarbeiter und Dritten zu reflektieren und Handlungsmöglichkeiten zu entwickeln. Bei weiterführenden Fragen zum Thema „Radikalisierung" wird an Kooperationspartnerinnen/Kooperationspartner verwiesen.

Zu den Kooperationspartnerinnen/Kooperationspartnern in Bremen gehören beispielsweise Soliport und kitab, die Beratungsstelle „Radikalisierung" im Bundesamt für Migration, die Mobile Beratung gegen Rechtsextremismus, Rassismus und Antisemitismus im Land Bremen (früher „pro aktiv gegen rechts") oder die Fachstelle Rechtsextremismus und Familie.

Auch an der Hochschule Bremen, der Hochschule Bremerhaven und an der Hochschule für Künste werden Weiterbildungsangebote genutzt, die dieses Thema aufgreifen.

Im Rahmen seiner Öffentlichkeitsarbeit bietet das LfV Bremen Vorträge über extremistische Bestrebungen an. In den Vorträgen kann es um aktuelle Entwicklungen und extremistische Erscheinungsformen im Lande Bremen gehen, jedoch können nach Bedarf auch andere Schwerpunkte gesetzt werden. Die Vorträge richten sich insbesondere an Behörden, Einrichtungen, Vereine und Schulen. Das Thema Radikalisierung durch Inhalte im Internet spielt dabei eine hervorgehobene Rolle. Zudem hat das LfV Bremen ein vertrauliches Telefon unter der Telefonnummer 0421-5377-250 eingerichtet, über das jederzeit anonym Hinweise übermittelt werden und über das Betroffene Kontakt aufnehmen können.

An der Hochschule für Öffentliche Verwaltung (HfÖV) wird das Thema „Radikalisierung" inhaltlich im Bachelorstudiengang Polizeivollzugsdienst geschult und in der Fortbildung angeboten. Im Rahmen der Schulungen für Kontaktbereichsbeamte wird das Thema bearbeitet. Zielrichtung ist hier das Erkennen von Radikalisierungen und das Wissen um die verschiedenen Hilfsangebote.

Das Landesinstitut für Schule (LIS) bietet im Bereich der Ausbildung zur Prävention von Radikalisierung auf der Basis von demokratischem Handeln eine breite Angebotsebene:

Das Thema Demokratieerziehung ist, neben Empathie, Verantwortungsübernahme und Mündigkeit als Bildungsziel Bestandteil des Curriculums der Bildungswissenschaften.

Die Empfehlungen der Kultusministerkonferenz (KMK) zu Demokratiebildung und Menschenrechtsbildung aus Oktober 2018 sind im Besonderen fakultativer Bestandteil in den bildungswissenschaftlichen Seminaren. Das Thema „Demokratie in Schule" steht dabei im Vordergrund. Dieser Inhalt wird in der Ausbildung am LIS verstetigt und weiter ausgebaut, damit eine demokratische Schule von Anfang an gestaltet sowie erlebbar gemacht werden kann. Die Referendarinnen und Referendare haben die Möglichkeit, bereits während ihrer Ausbildung am Wahlpflichtkurs „Die Bremische Bürgerschaft als außerschulischen Lernort" teilzunehmen. Dieses Angebot wird zurzeit inhaltlich ausgebaut und steht allen Referendarinnen und Referendare offen. Hier lernen sie nicht nur die Institution Bremische Bürgerschaft kennen, sondern auch, wie man Schülerinnen und Schülern Demokratie in handlungs- und produktorientierter Form näherbringen kann. Sie lernen selbst, wie man Demokratie erlebbar vermitteln kann.

Die Referendarinnen und Referendare können (seit Jahren) auch an den Veranstaltungen von „Demokratisch Handeln“ teilnehmen, die an verschiedenen Orten im Land Bremen stattfinden. Sie lernen verschiedene Demokratieprojekte aus dem Land Bremen kennen, die in den Schulen initiiert wurden und werden. Sie haben dadurch die Möglichkeit, sich Anregungen zu holen, sich zu vernetzen, neue Ideen gemeinsam zu entwickeln, um das Thema Demokratie kreativ mit den Schülerinnen und Schülern in den Schulen (alle Schulstufen/-formen) umzusetzen. Ziel ist es, dass alle Referendarinnen und Referendare diese Angebote mit ihren jeweiligen Fächern und den Bildungsplänen während ihrer Ausbildung am LIS verknüpfen.

Spezielle Angebote, Schulungen, Trainings et cetera im direkten Umgang mit Radikalisierung (im Internet) gibt es in der Ausbildung nicht. In vielen Angeboten zu digitaler Bildung wird das Thema aber berührt und/oder konkret thematisiert (Ausbildungsseminare, Wahlpflichtangebote, Medientag in der Einführungsphase).

Das LIS bietet zudem Fortbildungen und Fachtage zu den Themen Islam, Islamfeindlichkeit, Salafismus, Rechtsextremismus, Antisemitismus, Hate Speech, Fake News, Völkischer Nationalismus, Populismus und Sprache und Politik an. In diesen regelmäßig stattfindenden Fortbildungen wird insbesondere mit Internetquellen gearbeitet, da bekannt ist, dass Radikalisierungen in Foren, über YouTube-Videos und andere stattfinden und die Verbreitung von Verschwörungstheorien, manipulierten Bildern und falschen Mitteilungen hoch ist. Entsprechend werden in Fortbildungen aktualisierte Quellen zur Aufklärung genutzt und einschlägige Portale, Verlage, Personen, Musikgruppen und Symbole benannt, um so die Kenntnis und Sensibilität beim pädagogischen Personal an Schulen zu erhöhen. Außerdem wird regelmäßig auf Initiativen und Träger verwiesen, die kostenlos ihre neusten Erkenntnisse, auch mit Lehrmaterial zum Einsatz im Unterricht, online veröffentlichen. Hierzu zählen beispielsweise www.Ufuq.de für den Bereich Islam, Salafismus und Islamfeindlichkeit, die Kreuzberger Initiative gegen Antisemitismus, die Amadeu-Antonio-Stiftung gegen gruppenbezogene Menschenfeindlichkeit sowie die Bundeszentrale für politische Bildung unter anderem zu „Fake News“, „Hate Speech“ und vielem mehr.

Das LIS hat an der Broschüre „Vielfalt“ mitgewirkt und vermittelt Kontaktdaten zu Einrichtungen in Bremen und Bremerhaven, an die sich Betroffene wenden können, wie zum Beispiel reset bei VAJA e. V., LidiceHaus.

Das Zentrum für Medien (ZfM) am LIS bietet in Kooperation mit den Referaten Gesundheit und Suchtprävention, Schulkultur und Politische Bildung seit 2015 die „MediaCoach Zertifikatsfortbildung“ an.

MediaCoaches spezialisieren sich im Rahmen dieser Fortbildung im Bereich der Medienbildung und unterstützen damit Kolleginnen und Kollegen in vielfältigen Themenbereichen. Dabei geht es nicht um technischen Support, sondern um Unterstützung bei den Herausforderungen im Leben mit unterschiedlichsten Medienwelten und Ressourcen in der Institution Schule. Im Rahmen der einjährigen Fortbildung wird unter anderem ein verpflichtend zu belegender Workshop zum Thema Hate Speech und Fake News angeboten, darüber hinaus werden die MediaCoaches in einem weiteren Workshop über Beratungs- und Unterstützungsangebote bei fehlgeleiteter und/oder exzessiver Mediennutzung informiert.

4. Welche Anlaufstellen für Angehörige von Radikalisierten (links, rechts, islamistisch et cetera) gibt es im Land Bremen? Wie wird den Betroffenen dort geholfen? Welche Einrichtung gibt es direkt für radikalisierte Menschen, die aus ihrem Spektrum aussteigen möchten? Wie sind diese Stellen finanziell ausgestattet, und inwieweit sieht der Senat einen künftig höheren Finanzierungsbedarf?

Die Beratungsstelle „reset – Beratung und Begleitung bei der Loslösung vom Rechtsextremismus im Land Bremen“ ist für junge Menschen, die mit der rechtsextremen Szene sympathisieren, erste Kontakte geknüpft haben oder sich bereits in der Szene verorten. Zielgruppe sind vorrangig Heranwachsende, die bereit sind, sich in eine langfristige Auseinandersetzung mit ihren rechtsextremen Einstellungen und Verhaltensweisen zu begeben, um sich von diesen zu distanzieren. Angehörige werden ebenfalls als Signalgeberinnen/Signalgeber beraten und begleitet. Für ausstiegswillige Kader und Führungskräfte der rechten Szene besteht ein Beratungsangebot in Kooperation mit der niedersächsischen Arbeitsstelle Rechtsextremismus und Gewalt (ARUG) mit Sitz in Braunschweig.

Die bundesweit tätige Fachstelle Rechtsextremismus und Familie (Träger LidiceHaus) berät sowohl Angehörige rechtsextremer Jugendlicher als auch pädagogische Fachkräfte und Institutionen, die in ihrer Arbeit mit rechtsextremen Einstellungen konfrontiert sind. Die Fachstelle bietet Informationsmaterialien und Qualifizierungsmaßnahmen für Fachkräfte an.

Menschen, die sich in einem Hinwendungsprozess zu religiös begründeten Extremismus befinden, sowie deren Eltern und Angehörige, können sich an die Beratungsstelle kitab (Träger VAJA e. V.) wenden. Im Beratungsprozess werden individuelle Lösungs- und Distanzierungsansätze gemeinsam entwickelt. Die Arbeit von kitab ist auch darauf ausgerichtet, Ängste und Vorurteile abzubauen, Missverständnisse aufzuklären und akute Situationen besser einschätzen zu können.

Das Projekt Legato Bremen KulturBildungBeratung (KuBiBe) versucht der Problematik mit der Gewährleistung präventiver Maßnahmen, systematischer Ausstiegsberatung, Demokratieförderung sowie der Schaffung von Alternativen für Personen in und außerhalb der Haft entgegenzutreten. Legato Bremen KuBiBe strebt darüber hinaus eine Sensibilisierung radikalisierungsrelevanter Thematiken durch die Entwicklung innovativer Trainingsinhalte für Justizmitarbeiterinnen/Justizmitarbeiter an.

Zudem steht den Angehörigen jederzeit die Möglichkeit einer Kontaktaufnahme mit dem Landeskriminalamt, dem Landesamt für Verfassungsschutz oder KODEX offen. KODEX ist verantwortlich für Maßnahmen der Deradikalisierungsarbeit und Ausstiegsberatung im Bereich der sogenannten tertiären Prävention. Mit der Umsetzung dieser Arbeit wurde der Verein Ambulante Maßnahmen Altona e. V. im Rahmen des Projekts „Legato-Disengagement“ beauftragt.

5. Welche Erkenntnisse hat der Senat über den Zusammenhang von psychischen Erkrankungen und Radikalisierungen, und welche handlungsleitenden Rückschlüsse leitet er hieraus ab?

   Es gibt keine monokausale Wirkungsbeziehung zwischen psychischen Störungen und Radikalisierung beziehungsweise extremistischen Karrieren. Verschiedene Untersuchungen legen aber nahe, dass schwerwiegende psychische Belastungssituationen die Anfälligkeit für Radikalisierungen begünstigen.

   Beispielsweise weisen oftmals Lebensgeschichten von jungen Menschen, die sich salafistisch radikalisieren, auf ungünstige frühe Beziehungserfahrungen zu primären Bezugspersonen in der Familie hin.

   Erfahrungen aus der Kinder- und Jugendpsychiatrie zeigen, dass es bei einem Teil der gefährdeten beziehungsweise radikalisierten Jugendlichen erhebliche traumatische Vorbelastungen gibt, zum Beispiel bei den Müttern oder bei den Kindern selbst. In der Folge kann es in der Entwicklung von der späten Kindheit bis zum jungen Erwachsenen, zum Beispiel hervorgerufen durch den Kontakt mit ideologisch-gewaltverherrlichenden Angeboten im Internet, zu einer Reaktivierung früher Traumatisierungen kommen.

Aus empirischer Sicht sind die Zusammenhänge zwischen Extremismus und psychischer Gesundheit nicht belegt. Kritische Aspekte der Forschung sind neben der Datenlage, die unterschiedlichen Definitionen, sowohl der psychologischen Diagnosen, als auch der Konzepte von Extremismus.

Psychische Instabilität kann die Empfänglichkeit für extremistische Ideologien erhöhen. Sie liefern scheinbar leichte Antworten und können dem Leben scheinbar einen Sinn verleihen. Ähnlich wie bei Suchtkranken kann die Ideologie genutzt werden, um der Realität zu entfliehen.

Psychologische und ärztliche Psychotherapeuten, die sich mit jungen Menschen beschäftigen, können als Partner in der Prävention und im direkten Kontakt mit diesen jungen Menschen, aber auch als Berater von Facheinrichtungen, hilfreich sein und sollten verstärkt in die lokalen und regionalen Netzwerke einbezogen werden.

Seit Mitte 2019 findet ein fachlicher Austausch zwischen dem Referat für Psychiatrie und Sucht bei der Senatorin für Gesundheit, Frauen und Verbraucherschutz und KODEX beim Senator für Inneres statt. Dabei stehen vor allem eine Vernetzung mit Akteuren aus der psychotherapeutischen und psychiatrischen Versorgung sowie folgende Handlungsfelder zu dem Themengebiet im Fokus:

— Fortbildungen für Beratende aus dem Bereich der Extremismusprävention zu psychologischen Aspekten,

— Fortbildungen für Psychologinnen/Psychologen zu den Themen (De)Radikalisierung und Extremismusprävention und zu aktuellen Entwicklungen extremistischer Phänomenbereiche,

— Aufbau eines regionalen, psychologisch-therapeutischen Expertinnen-Pools/Experten-Pools für:

  — die schnelle/direkte Vermittlung von Klientinnen/Klienten mit psychologischen Bedarfen an entsprechend geschulte Therapeutinnen/Therapeuten,

  — Ansprechpartner für psychologische Fragestellungen,

    • Fortbildung/Supervision.

Fachleute aus der kinder- und jugendpsychiatrischen Versorgung haben im Dezember 2019 an einem von KODEX organisierten Fachtag zum Thema „Ganzheitlicher Umgang mit Rückkehrer-Familien aus Kampfgebieten – Fragen der praktischen Umsetzung für Behörden“ teilgenommen.

Für das Frühjahr 2020 ist ein Fachaustausch zwischen KODEX, ambulant arbeitenden Trägern im Bereich von Deradikalisierungs- und Ausstiegsberatung und leitenden Vertreterinnen/Vertretern aus der ambulanten und stationären Kinder- und Jugendpsychiatrie geplant. Im Juni 2020 wird dann ein fachlicher Austausch zu dem Thema im Fachausschuss Allgemeinpsychiatrie stattfinden. Hier sind aufgrund der Corona-Lage Verschiebungen wahrscheinlich. Im Fokus steht dabei eine Sensibilisierung der Akteure in Psychotherapie und Psychiatrie für das komplexe Themenfeld der Radikalisierung und eine Vernetzung der verschiedenen Hilfen.

6. Inwieweit tragen die Internetanbieter der sozialen Medien nach Ansicht des Senats durch Algorithmen dazu bei, dass sich potenziell zur Radikalisierung tendierende Menschen nur noch mit ihrem Agitationsspektrum befassen? Wie kann und sollte diesem Phänomen entgegengewirkt werden?

Algorithmen dienen dazu, den Nutzenden sozialer Medien aus der Vielzahl zur Verfügung stehender Informationen möglichst relevante Inhalte anzubieten. Welche gesellschaftlichen Auswirkungen im Kontext politischer oder religiöser Radikalisierung damit verbunden sind, ist noch weitgehend unerforscht: Die Heterogenität der sich bildenden Netzwerke, die

überregionale Ausstrahlkraft von Communities sowie die konkreten gesetzlichen Rahmenbedingungen sicherheitsbehördlicher Aufträge zeigen, vor welchen interdisziplinären Herausforderungen die wissenschaftliche Betrachtung der hieraus resultierenden Radikalisierungspotenziale steht.

Eine Trennung von Algorithmen in einem komplexen System wie den sozialen Netzwerken in „Gut und Böse“ erscheint aus technischer Sicht nahezu unmöglich. Solange radikale und extreme Botschaften auf den Plattformen vorhanden und die Algorithmen entsprechend konfiguriert sind, werden sich keine Veränderungen ergeben. Die Verwendung von Algorithmen im Internet führt insbesondere bei der Vorschlagssuche unweigerlich zu einer Fokussierung im stetig enger werdenden Rahmen der abgefragten Themenbereiche. Die Abfragen beziehen sich immer mehr auf sich selbst und die zuvor angezeigten Ergebnisse.

Wobei nicht die Suche nach Vorschlägen zu dem kontrovers diskutierten „Echokammer-Effekt“ führt, sondern die algorithmisch ausgewertete Reflektion gleichgelagerter Eigenschaften nach dem Muster „Deinen Freunden … gefällt der Beitrag … – er könnte Dich auch interessieren…“ oder „Du bist Mitglied in der Gruppe…, den meisten Gruppenmitgliedern gefällt auch die Gruppe…“. So wird der Nutzer immer weiter in die gleiche Richtung geführt. Der Blick über den „Tellerrand“ wird verstellt. Dieses Phänomen ist ein allgemeines Nutzungsproblem im Internet.

Das symbiotische Zusammenwirken von maschinellen Lernprozessen und menschlichen, auf kognitiver Wahrnehmung und Emotionen beruhenden Interaktionen, wirkt sich in vielerlei Hinsicht begünstigend auf Radikalisierungsprozesse aus. Eine herausragende Rolle spielen in diesem Kontext vor allem emotionalisierende Beiträge, die die Ängste und Sorgen oder das Ungerechtigkeitsempfinden weiter Teile der Gesellschaft ansprechen, hohe Öffentlichkeitswirkung entfalten und dabei Gefühle von Wut oder Zorn auslösen. Derartige Beiträge berühren besonders viele Menschen, gehen viral, lösen Solidarisierungs- oder Segregationseffekte aus und führen zu einer zunehmenden Polarisierung der Gesellschaft. Betroffene, die sich häufig in derartigen virtuellen Atmosphären bewegen, laufen Gefahr, sich selbsterfüllenden Prophezeiungen und einer verzerrten Wahrnehmung von Realität zu unterliegen. Radikalisierungsprozesse können hierdurch in erheblichem Maße begünstigt werden.

Um diesem komplexen Phänomen und den Gefahren, die hieraus erwachsen, wirksam begegnen zu können, bedarf es umfassender datenwissenschaftlicher Untersuchungen, auf deren Grundlage es adäquate Ansätze und Maßnahmen zu erschließen gilt.

Das LfV Bremen hat vor diesem Hintergrund im August 2019 ein Projekt zur Früherkennung von Radikalisierungsprozessen in sozialen Netzwerken gestartet und analysiert darin – mit Hilfe spezieller empirischer Verfahren aus dem Forschungsfeld „Computational Social Sciences“ – virtuelle Interaktionen im Phänomenbereich Rechtsextremismus.

7. Welche Erkenntnisse hat der Senat über Internetforen- und Plattformen, die zur Radikalisierung in jegliche extremistischen Richtungen genutzt werden? Inwieweit erachtet der Senat Verbote derartiger Foren als zielführend und möglich?

Extremisten aller Phänomenbereiche nutzen das Internet als Medium zur Kontaktpflege, Verbreitung von Propaganda und Rekrutierung neuer Anhänger. Interaktionsmessungen im Phänomenbereich Rechtsextremismus anlässlich des „Sechsten Berichts über Rechtsextremismus und Fremdenfeindlichkeit im Land Bremen“ zeigen, dass es insbesondere Rechtsextremisten zunehmend gelingt, in sozialen Netzwerken Zustimmung zu generieren und Einfluss auf Communities zu nehmen. Vor allem übersteigerte Bedrohungsszenarien zu Themenkomplexen, wie dem islamistischen Terrorismus oder den Straftaten von Ausländern zum Nachteil

deutscher Opfer, weisen eine besonders hohe Anziehungskraft und damit verbundene Öffentlichkeitswirkung auf.

Rechtsextremisten nutzen solche Inhalte als vermeintliche Belege für ihre Thesen. Aus einer Vielzahl gleichgelagerter Einzelfälle werden gesellschaftspolitische Defizite heraufbeschworen. Besucher unterliegen dem Phänomen der kognitiven Dissonanz: Das ist zum Beispiel dann der Fall, wenn durch eine „Flut“ von emotional ergreifenden Beiträgen über gewaltsame Übergriffe vermeintlicher Flüchtlinge Realitätsabbilder verzerrt und dadurch Radikalisierungsprozesse begünstigt werden. Hierdurch werden zum Beispiel Staatsverdrossenheit, Anti-Establishment-Vorbehalte, fremdenfeindliche – insbesondere muslimfeindliche und antisemitische Vorurteile sowie verschwörungstheoretische Argumentationsmuster bedient. „Flüchtlinge“, „Muslime“ oder „Juden“ und ein vermeintlich korrumpiertes politisches System werden verstärkt als Bedrohung wahrgenommen und sowohl verbal als auch aktiv angegangen. Nutzer, die den aufgezeigten manipulativen Einflüssen virtueller Communities unterliegen, scheinen aufgrund der Zustimmungswerte zunehmend bereit, ein vermeintliches Gemeinwohl über das des Individuums zu stellen.

Im Phänomenbereich Islamismus entfalten vor allem „Narrative“, wie der Verlust des Kalifats, außenpolitische Ungerechtigkeiten oder eine wahrgenommene Unterdrückung des Islams Bindungswirkung. Islamisten nutzen dies vor allem, um junge Menschen anzusprechen, ihnen „Erlösung“ zu bieten und sie zu ermutigen oder dazu anzuhalten, die Kontrolle über ihr Leben wiederzuerlangen, gegebenenfalls im Kampf für den Islam.

Die Radikalisierung von jungen Menschen kann insbesondere über im Internet abrufbare islamistische Propaganda erfolgen. Das Internet dient Islamisten als wichtiges Medium zur Kontaktpflege, Verbreitung von Propaganda und Rekrutierung von neuen Anhängern. Die Präsenz dieser Propaganda sowie der dahinterstehenden Organisationen im Internet hat sich in den vergangenen Jahren, insbesondere durch die Nutzung sozialer Netzwerke im Internet beziehungsweise entsprechender Programme wie Twitter, WhatsApp, Facebook, YouTube oder Telegramm, deutlich erhöht.

Themenfelder, wie „Anti-Faschismus“, „Anti-Rassismus“, „Anti-Repression“ oder „Anti-Kapitalismus“ werden von Linksextremisten instrumentalisiert, um sich auf dieser Grundlage breit zu vernetzen und in sozialen Medien gesellschaftlichen Rückhalt zu erfahren.

Polizisten und Rechtsextremisten gelten als Feindbilder der linksextremistischen Szene. Übergriffe auf sie und Brandanschläge verdeutlichen, dass Personen auch in diesem Phänomenbereich Radikalisierungsprozesse durchlaufen, aus denen eine gesteigerte Gewaltakzeptanz erwächst.

Der Senat sieht zunächst die Betreiber und Verantwortlichen der jeweiligen Foren in der Pflicht, den Missbrauch dieser modernen Form der Kommunikation zu unterbinden. Sofern dies nicht hinreichend erfolgt und ein entsprechendes Einwirken ergebnislos bleibt, kommt als letztes Mittel auch ein Verbot derartiger Foren in Betracht. Allerdings darf nicht übersehen werden, dass dies vielfach zu Ausweichbewegungen führt, beispielsweise indem inländische Angebote danach fast unverändert von ausländischen Servern zur Verfügung gestellt werden und sich in der Praxis damit häufig dem Zugriff der deutschen Justiz entziehen. Bremen unterstützt eine entsprechende Bundesratsinitiative mit der in Deutschland ansässige Anbieter von Telemediendiensten verpflichtet werden sollen, im Gesetz genannte Straftatbestände den zuständigen Behörden zu melden und die Inhalte zu löschen beziehungsweise zu sperren.

8. Inwieweit nutzen welche radikalen Kräfte das Internet in und aus Bremen heraus zur Verbreitung ihrer Ideologie (bitte getrennt darstellen nach rechts, links und islamistisch)? Inwieweit werden politische Mandatsträger

oder Mitarbeiter von Behörden in Bremen durch Hasszuschriften oder andere Formen der Verbreitung im Internet (zum Beispiel in Foren oder Netzwerken) bedroht, genötigt, betrogen oder beleidigt? Wie will der Senat diesen mutmaßlich zunehmenden Aktivitäten begegnen?

Personen aus dem rechtsextremen Spektrum im Land Bremen nutzen das Internet, um Konzertveranstaltungen zu bewerben und die oft konspirativ organisierten Anreisen zu koordinieren. Die Verbreitung und Zugänglichmachung von rechtsextremistischen Inhalten findet insbesondere über die Verwendung der Messenger-Dienste Telegram und WhatsApp statt.

In öffentlich zugänglichen Chatgruppen organisieren rechtsextremistische Akteurinnen/Akteure aus dem Land Bremen regionale Vernetzungsplattformen. In ihrer Außendarstellung verzichten die Betreiberinnen/Betreiber zumeist auf die Propagierung eines explizit rechten, gefestigten Weltbildes. Dennoch finden sich in den, in ihrer Selbstbezeichnung „patriotischen“ Chatgruppen eindeutig rassistische und extrem rechte Argumentationsmuster wieder.

Die Bremer Landesverbände der Parteien „Die Rechte“ (DR) und „Nationaldemokratische Partei Deutschland“ (NPD) nutzen, neben der Präsenz auf ihren Websites, verstärkt soziale Medien wie beispielsweise Twitter, YouTube oder Facebook. Gleiches gilt für die Partei Alternative für Deutschland (AfD).

Auch Kleingruppen und Einzelakteurinnen/Einzelakteure, wie Reichsbürgerinnen/Reichsbürger, greifen auf diese Kommunikationsmöglichkeiten zurück. Auf Sperrungen von Accounts auf diesen Plattformen reagieren Akteurinnen/Akteure des rechtsextremen Spektrums mit Ausweichbewegungen auf andere Social-Media-Formate, wie das in Russland ansässige soziale Netzwerk VK, ehemals „Vkontakte“, oder das Portal „BitChute“.

Rechtsextreme Versandhändler und Musikgruppen aus dem Bundesland Bremen sind im Internet vertreten. Darüber hinaus bestehen neonazistische Publikationen wie das Magazin „Ein Fähnlein“, das in Bremen ansässig ist und von dort aus bundesweit vertrieben wird.

Das zuvor dargestellte Verhalten gilt grundsätzlich auch für Akteure der linken sowie der islamistischen Szene. Die linksextremen Gruppen in Bremen nutzen häufig Twitter, Instagram und Facebook sowie diverse Internetseiten und Blogs. Die islamistische Szene ist vorwiegend auf Facebook und Instagram vertreten und nutzt diese neben anderen Medien, um ihre Ideologie zu verbreiten.

Dem Senat liegen folgende Zahlen zur Bedrohung von Mandatsträgern und Mitarbeitern der Verwaltung über das Internet vor:

2014: ein Delikt – einmal rechtsmotiviert

2015: ein Delikt – einmal rechtsmotiviert

2016: fünf Delikte – zweimal rechtsmotiviert, zweimal nicht zuzuordnen, einmal ausländisch motiviert

2017: sechs Delikte – zweimal rechtsmotiviert, zweimal linksmotiviert, einmal ausländisch motiviert, einmal nicht zuzuordnen

2018: zwei Delikte – einmal linksmotiviert, einmal nicht zuzuordnen

2019: zwei Delikte – einmal ausländisch motiviert, einmal nicht zuzuordnen

2020: ein Delikt – einmal rechts motiviert (Stand: 26. März 2020)

Bereits im Oktober 2019 hat der Senator für Inneres die Mitglieder der Bremischen Bürgerschaft, der Stadtverordnetenversammlung, der Beiräte, des Senats, des Magistrats der Seestadt Bremerhaven sowie die Landesverbände der in der Bremischen Bürgerschaft vertretenen Parteien in einem

Schreiben über Empfehlungen zum Umgang mit Hasspostings in Kenntnis gesetzt.

Gemeinsam mit der Bremer Medienanstalt war das LKA Bremen zudem an der Gründung der Initiative „RIKO – Resignieren ist keine Option!“ beteiligt, um Hasskriminalität im Internet noch entschlossener zu begegnen. Hierbei wurden zur Vereinfachung der direkten Meldewege das Postfach hassanzeigen@polizei.bremen.de eingerichtet, um zielgenau eine Mitteilung an die Abteilung Staatsschutz richten zu können. Dieses Mailpostfach wurde auch den Bremer Parteien als Meldepostfach für anzeigewürdige Sachverhalte genannt. Die Fallzahlen in dem Phänomen der Hasskriminalität, das verschiedene Ausprägungen/Unterkategorien umfasst, sind aktuell als gering zu bezeichnen. Die mediale Berichterstattung zu der Initiative wird als positive Sensibilisierung der Gesellschaft für das Thema Hasskriminalität im Internet gewertet.

Um dem Phänomen der Hasspostings zu begegnen hat die OPB Bremerhaven ebenso wie die Polizei Bremen ihre Online-Wache um einen Link zur Meldung solcher Postings erweitert, um effektiv gegen Hass im Internet vorzugehen. Dazu werden die Hinweise bundesweit von der Meldestelle „respect!" entgegengenommen und geprüft. Beiträge die den Tatbestand der Volksverhetzung, Beleidigung, üblen Nachrede oder Verleumdung erfüllen, leitet die Meldestelle dann Plattformbetreibern mit der Aufforderung zur Löschung weiter. Fälle der Volksverhetzung nach § 130 Strafgesetzbuch (StGB) werden von der Meldestelle zur strafrechtlichen Verfolgung angezeigt.

Die Meldestelle „respect!" der Jugendstiftung Baden-Württemberg im Demokratiezentrum setzt sich für eine respektvollere Kommunikation im Internet und die Achtung deutschen Rechts durch internationale Unternehmen ein. Gefördert durch das Bundesprogramm „Demokratie leben!“ unterstützen in allen Bundesländern Landesdemokratiezentren die Weiterentwicklung von Konzepten und Strategien zur Förderung von Demokratie und Vielfalt. Der Senat bewertet dieses Verfahren derzeit als ein wirkungsvolles Mittel, gegen Hasskommentare vorzugehen.

Der Bundestag hat am 18. Juni 2020 den Entwurf eines Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität beschlossen. Der Gesetzentwurf sieht umfassende Verschärfungen des Strafrechts vor. Zudem werden Plattformbetreiber wie etwa YouTube, Spotify und Facebook künftig nicht mehr nur löschen, sondern strafbare Posts dem Bundeskriminalamt (hierfür werden dort mehr als 300 Stellen geschaffen) melden müssen. Das BKA prüft Hasspostings und leitet sie an die zuständigen Staatsanwaltschaften weiter.

Am 1. Januar 2018 trat das Netzwerkdurchsetzungsgesetz (NetzDG) als zentrale Grundlage zur Eindämmung von Hasskriminalität und „Fake News“ im Internet in Kraft. Es verpflichtet Online-Plattformen dazu auf, Hassbotschaften zeitnah von ihren Websites zu löschen. Verstöße werden mit hohen Geldbußen sanktioniert.

Der Senat hält es vor dem Hintergrund, dass das Internet nicht als rechtsfreier Raum wahrgenommen werden darf und zum Schutz der Gesellschaft für erforderlich, die Identifizierbarkeit von Personen, die Hasskriminalität in sozialen Netzwerken und Spieleplattformen verbreiten, zu verbessern. Der Senat unterstützt daher eine entsprechende Gesetzesinitiative.

9. Welche Möglichkeiten haben die Bremer Polizei oder der Verfassungsschutz in einschlägigen Internetforen zu ermitteln?

Zentrale Voraussetzung für eine Wahrnehmung der Aufgabe des Landesamtes für Verfassungsschutz Bremen gemäß § 3 Absatz 1 Nummer 1 des Bremer Verfassungsschutzgesetzes (BremVerSchG) ist das Vorliegen von tatsächlichen Anhaltspunkten für Bestrebungen die sich etwa gegen die

freiheitliche demokratische Grundordnung richten. Im Rahmen der Aufgabenerfüllung können Informationen aus offenen Quellen erhoben werden, also aus Informationsträgern, die für jedermann zugänglich sind. Abhängig von den näheren Umständen des Einzelfalls kommt auch eine Informationsgewinnung in abgeschotteten Bereichen des Internets in Betracht, die den Einsatz nachrichtendienstlicher Mittel nach Maßgabe von § 9 Absatz 1 BremVerSchG erfordert.

Auch die Polizei verfügt über die rechtlich ausgestalteten Befugnisse zur Ermittlung in Internetforen.

10. Wie werden Informationen hinsichtlich von „Hasspostings“ im Internet erlangt? Wie hoch schätzt der Senat die Dunkelziffer der erfolgten „Hasspostings“ im Land Bremen ein? Wie will der Senat sicherstellen, dass die Such-, Informations- und Anzeigehäufigkeit von „Hasspostings“ künftig erhöht wird?

    Das Dunkelfeld kann vom Senat nicht valide bewertet werden. Studien geben allerdings Anlass zur Vermutung, dass das Dunkelfeld hoch einzuschätzen ist. Beispielsweise waren 8 Prozent der Teilnehmenden an der Studie ‚#Hass im Netz: Der schleichende Angriff auf unsere Demokratie: (https://www.idzjena.de/fileadmin/user_upload/_Hass_im_Netz_-_Der_schleichende_Angriff.pdf). Eine bundesweite repräsentative Untersuchung 2019‘ des Instituts für Demokratie und Zivilgesellschaft persönlich von Hate Speech im Netz betroffen. Dieser Anteil steige unter 18- bis 24-Jährigen auf 17 Prozent und bei Menschen aus Einwandererfamilien auf 14 Prozent.

    „Hasspostings“ werden in aller Regel durch Bürgerinnen/Bürger oder Institutionen bei der Polizei in Bremen oder in anderen Bundesländern zur Anzeige gebracht. Zum Teil gelangen Anzeigen nach Bremen, wenn es im konkreten Fall Anlass für die Vermutung gibt, dass die Täterin oder der Täter in Bremen wohnt. Anzeigen erfolgen in der Regel, weil eine Person selbst betroffen ist oder weil sie solche Postings wahrgenommen hat. Bürgerinnen und Bürger haben außerdem die Möglichkeit bei Bedarf eine Online-Anzeige zum Themenfeld der Internethasskriminalität auf der Homepage der Polizei Bremen und der OPB Bremerhaven über ein zentrales Anzeigeportal der Meldestelle „respect!" der Jugendstiftung Baden-Württemberg im Demokratiezentrum zu erstatten, die dann im Falle eines strafrechtlich relevanten Vorfalls mit Bremen-Bezug das LKA Bremen kontaktieren. Eine anlasslose Internetauswertung wird aufgrund der Größe des Bundeslandes und der transnationalen Dimension des Internets als nicht zielführend bewertet. Der Senat unterstützt die Initiative des Bundeskriminalamts, entsprechende Kapazitäten auf Bundesebene aufzubauen.

    Die Polizei Bremen verfolgt ferner die Entwicklung eines Programmes, das derzeit in Nordrhein-Westfalen erprobt wird. Es soll noch leichter ermöglichen, Hasspostings an die Polizei zu melden, da der Hinweisgeber lediglich den Link in dieses Programm kopieren muss. Alle weiteren Angaben zieht das Programm selbstständig aus dem Internet. Sobald Anwendungsreife vorliegt, wird eine Übernahme geprüft.

11. Wie wird die vom Bremer Landesamt für Verfassungsschutz eingerichtete „Meldestelle für Hetze im Internet“ von der Bevölkerung angenommen? Wie will der Senat dafür sorgen, dass diese Meldestelle häufiger genutzt wird?

    Über die eingerichtete Meldestelle konnten in Einzelfällen bereits wertige Hinweise erlangt werden, die zur weiteren Bearbeitung an die zuständigen Analysereferate übermittelt wurden. Ein Teil des bisher eingegangenen Meldeaufkommens befasst sich mit der Einrichtung der Meldestelle an sich oder es werden Fragen zu den Phänomenbereichen und den Auf-

gaben des Verfassungsschutzes gestellt. Das Landesamt für Verfassungsschutz in Bremen hat innerhalb der letzten Jahre mehrfach darauf hingewiesen, welche gesellschaftlichen Gefahren aus extremistischen Bestrebungen, vor allem in virtuellen Communities, erwachsen und dabei die Dringlichkeit einer gemeinschaftlichen, interdisziplinären Bekämpfung unterstrichen. Im Rahmen seiner Öffentlichkeitsarbeit wird das LfV auch künftig konsequent dazu anhalten, etwaige Hinweise über die eingerichteten Meldewege an die Behörde weiterzugeben.

12. Welche rechtlichen Veränderungen (Bundes- und Landesrecht) hält der Senat für notwendig, um die Effektivität der Möglichkeiten seiner Behörden zu erhalten oder zu verbessern, beziehungsweise um eine angemessene Strafverfolgung zu gewährleisten?

    Im Hinblick auf das materielle Strafrecht bestehen nach Auffassung des Senats mit den derzeitigen Regelungen bereits gesetzliche Vorschriften, um Handlungen und Verhaltensweisen, die dem Bereich „Hass im Netz“ zuzuordnen sind, weitgehend zu sanktionieren.

    Die weitergehenden materiell-rechtlichen Änderungen, durch den am 18. Juni 2020 vom Bundestag beschlossenen Gesetzesentwurf der Bundesregierung zur „Bekämpfung des Rechtsextremismus und der Hasskriminalität“, stellen eine gravierende Erweiterung der geltenden Vorschriften dar, um einzelne für strafwürdig erachtete Verhaltensweisen verfolgen zu können. Im Strafgesetzbuch werden die Tatbestände der „Störung des öffentlichen Friedens durch Androhung von Straftaten“ (§ 126 StGB), der „Belohnung und Billigung von Straftaten“ (§ 140 StGB) und der „Bedrohung“ (§ 241 StGB) erweitert. Öffentlich oder durch Verbreiten von Schriften getätigte Beleidigungen (§ 185 StGB) unterliegen künftig einer höheren Strafandrohung. Ferner wird klargestellt, dass der besondere Schutz von im politischen Leben des Volkes stehenden Personen vor übler Nachrede und Verleumdung (§ 188 StGB) bis hin zur kommunalen Ebene reicht.

    Auch dürfte die im Zuge des gleichen Artikelgesetzes beabsichtigte Änderung des Netzwerkdurchsetzungsgesetzes (NetzDG) mit der vorgesehenen Meldepflicht für die dem NetzDG unterliegenden Anbieter in Bezug auf bestimmte strafbare Inhalte gegenüber dem Bundeskriminalamt dazu führen, dass die Strafverfolgungsbehörden vermehrt Kenntnis von zum Beispiel strafbaren „Hasspostings“, erhalten und damit überhaupt erst Anlass haben, die entsprechenden Ermittlungen aufzunehmen.

    Eine Problematik bei der strafrechtlichen Verfolgung von „Hasspostings“ liegt im Bereich der Ermittlung der Identitäten von unbekannten Tätern, welche regelmäßig unter „Alias“-Personalien oder unter nur schwer nachzuverfolgenden Internetadressen agieren. Hier hat der Senat mit einer Bundesratsinitiative das sogenannte Marktortprinzip eingefordert, was bedeutet, dass nationales Recht – zum Beispiel was den Auskunftsanspruch anbetrifft – auch gegenüber Firmen mit Sitz im Ausland Anwendung findet, wenn sie hier tätig sind.

    Auch die beabsichtigten strafprozessualen Änderungen durch das Gesetz zur „Bekämpfung des Rechtsextremismus und der Hasskriminalität“, insbesondere die Ausweitung der Norm des § 100g Strafprozessordnung (StPO) (Erhebung von Verkehrsdaten) auf Telemediendienstleister, können zu Verbesserungen der Effektivität der Strafverfolgung in diesem Deliktsbereich führen, sofern eine verfassungskonforme Ausgestaltung erzielt werden kann.

III. Internetkriminalität

1. Welche sind die häufigsten Kriminalitätsfelder im Internet im Land Bremen? Inwieweit wird Internetkriminalität in der jährlichen Polizeilichen Kriminalstatistik Bremens gesondert geführt, und wie hat sich diese in den

letzten fünf Jahren entwickelt? Welche Gruppen der Bevölkerung sind durch welche „modi operandi“ besonders betroffen?

In der Polizeilichen Kriminalstatistik werden Delikte aus dem Internet beziehungsweise mit Tatmittel Internet erfasst.

Straftaten, bei denen eine Tatausführung im Internet naheliegt, wie etwa bei bestimmten Betrugsdelikten, Computersabotage und Softwarepiraterie, erhalten den Merker Internet/Cybercrime automatisch. Bei vielen anderen Delikten besteht die Möglichkeit, dass der Merker „Internet“ bei der Datenerfassung gesetzt wird. Bei anderen Delikten ist eine Begehung unter Nutzung des Internets nicht möglich und der Merker kann nicht gesetzt werden. Die Daten der letzten fünf Jahre sind der nachfolgenden Tabelle zu entnehmen.

Land Bremen

Schl.-Zahl der Tat	Straftat	erfasste Fälle 2015	erfasste Fälle 2016	erfasste Fälle 2017	erfasste Fälle 2018	erfasste Fälle 2019
1	2	3	4	5	6	7
------	Straftaten insgesamt	5.408	4.988	2.430	1.207	962
100000	ST gg. die sex. Selbstbestimmung insg.	96	76	44	12	46
200000	Rohheitsdelikte und ST gg. die persönliche Freiheit	265	254	101	11	13
500000	Vermögens- und Fälschungsdelikte	4.286	3.820	1.890	1.093	757
600000	Sonstige Straftatbestände (StGB)	628	713	342	79	130
700000	Strafrechtliche Nebengesetze	133	125	53	12	16
894000	Cybercrime			2.430	1.207	962
897000	Computerkriminalität	915	980	412	197	220
897100	Computerbetrug		676	253	155	162

Im Jahr 2016 wurde festgestellt, dass zuvor eine Vielzahl von Betrugsfällen fälschlicherweise als Internetkriminalität erfasst worden ist. Aufgrund der dadurch erforderlichen Änderung der Erfassungsregeln und verbesserter Qualitätssicherungsmaßnahmen für diesen Bereich kam es in den Jahren ab 2017 zu einem deutlichen Rückgang der Fallzahlen.

Internetkriminalität betrifft viele Deliktsbereiche. Dabei sind viele verschiedene modi operandi zu beobachten. Nachfolgend eine Übersicht der zurzeit häufig genutzten Tatbegehungsweisen:

— Ransomware (Verschlüsselungstrojaner), eingesetzt gegen Unternehmen, Firmen, Behörden et cetera (jegliche Art von Institution, welche angreifbar erscheint, von Krankenhäusern bis Energieversorgern).

— Identitätsdiebstahl (mittels Phishingmails), Abfrage verifizierter Informationen, wie Personalien, Passwörter, Zugangsdaten unter Vorspiegelung vermeintlich korrekter Anfragen, zum Beispiel Amazon, ebay, Paypal, eingesetzt gegen Internetnutzer.

— Datendiebstahl (mittels Schadcode), Eindringen in Systeme mittels Schadcode, zum Beispiel Exploit, fehlerhafte konfigurierte Systeme, fehlende Updates, fehlerhafte Bedienung, eingesetzt gegen Unternehmen, Firmen, Behörden et cetera.

— Betrugsverfahren mit Internet als Tatmittel, zum Beispiel sogenannten Microsoft-Betrug (vermeintlicher Anruf vom MS-Support), ebay-Betrug, eingesetzt gegen Internetnutzer.

2. Wie viele Ermittlungsverfahren gab es in den Jahren 2019 und 2020 im Bereich Internetkriminalität und wie gingen diese aus (Einstellung, Strafbefehl, Verurteilung, Freispruch et cetera)?

Für Zahlen der Polizei wird auf die Tabelle in Frage III/1 verwiesen.

Bei der Staatsanwaltschaft Bremen erfolgt keine gesonderte Erfassung aller Ermittlungsverfahren im Bereich Internetkriminalität, also eines jeden Verfahrens, bei dem eine Tatbegehung über das Internet in Frage kommt. In den beiden bei der Staatsanwaltschaft Bremen bestehenden Sonderdezernaten für Internetkriminalität sind in den Jahren 2019 und 2020 bislang 109 Ermittlungsverfahren gegen namentlich bekannte Beschuldigte anhängig geworden, von denen elf nicht abgeschlossen sind. Ein Verfahren ist vorläufig gemäß § 154f StPO, ein weiteres gemäß § 154e Absatz 1 StPO eingestellt. Drei Verfahren wurden an auswärtige Staatsanwaltschaften abgegeben. In 86 der Verfahren erfolgte eine Verbindung zu einem anderen Verfahren. Von den verbleibenden sieben Verfahren wurden fünf gemäß § 170 Absatz 2 StPO, eines gemäß § 154 Absatz 1 StPO und eines gemäß § 45 Jugendgerichtsgesetz (JGG) eingestellt. Zu einer Anklageerhebung beziehungsweise der Beantragung eines Strafbefehls ist es in den seit Beginn 2019 eingegangenen Verfahren nicht gekommen.

3. Wie sind die Polizei Bremen und das Bremer Landesamt für Verfassungsschutz im Kampf gegen Internetkriminalität in diesem Bereich personell, materiell und finanziell aufgestellt? Inwiefern hält der Senat das vorgehaltene Personal bei der Bremer Polizei und des Bremer Landesamts für Verfassungsschutz für die gezielte Bearbeitung dieses Deliktfeldes noch für ausreichend? Inwiefern gibt es Probleme bei der Nachwuchsgewinnung insbesondere bei den Organisationseinheiten, die für Internetkriminalität zuständig sind? Welche Veränderungen, zum Beispiel in den Bezahlungsstrukturen oder Arbeitsgestaltung, hält der Senat gegebenenfalls für erforderlich?

   Die Zuständigkeit für die Bekämpfung von Cybercrime liegt für die Polizei Bremen und die Ortspolizeibehörde Bremerhaven (OPB) beim LKA. Die OPB verfügt über keine Fachdienststelle für den Bereich Cybercrime. Die Bündelung der Fachbereiche IT-Forensik, Video, Telekommunikationsüberwachung (TKÜ) und Cybercrime beim LKA im Rahmen der Polizeireform hat zu einer Vielzahl von Synergien geführt. Hier werden im Rahmen des zur Verfügung stehenden Personalrahmens Stellenbesetzungen vorgenommen.

   Die Bündelung der Fachbereiche IT-Forensik, Video, Telekommunikationsüberwachung (TKÜ) und Cybercrime im Rahmen der Polizeireform zu einer Fachdienststelle Cybercrime hat zu einer Vielzahl von Synergien geführt; separate Informatiker im Bereich Cybercrime sind daher nicht vonnöten.

   Eine Nachwuchsgewinnung aus der freien Wirtschaft gestaltet sich zurzeit problematisch. Zum einen werden IT-Fachleute in vielen Bereichen der privaten Wirtschaft stark nachgefragt und stehen damit in direkter Konkurrenz mit den öffentlichen Arbeitgebern. Zum anderen werden in der privaten Wirtschaft zumeist bessere Konditionen geboten.

   Die Anstellung von Nicht-Vollzugs-Kräften für den Bereich Open Source Intelligence (OSINT, quelloffene Recherche im Internet) zur Unterstützung aller sachbearbeitenden Dienststellen der Polizei Bremen befindet sich in der Planung. Vor dem Hintergrund der zumeist besseren Konditionen in der privaten Wirtschaft wird die Einführung einer IT-Zulage geprüft.

   Das Landesamt für Verfassungsschutz in Bremen hat die dargelegten Entwicklungen innerhalb der letzten Jahre – insbesondere im Phänomenbereich Rechtsextremismus – zum Anlass genommen, spezielle personelle Expertise und die notwendigen technischen Ressourcen für eine wirksame Extremismusbekämpfung in virtuellen Communities aufzubauen. In diesem Kontext leistet das LfV Bremen wichtige Pionierarbeit für den Verbund der Verfassungsschutzbehörden. Dies gilt es weiter auszubauen, um

auch künftig den Herausforderungen, die aus Radikalisierungsprozessen im Internet erwachsen, gerecht zu werden.

4. Wie ist die Staatsanwaltschaft Bremen in Bezug auf Ermittlungsverfahren, die Kriminalität im Internet betreffen, aufgestellt? Inwieweit gibt es die Überlegung ein Sonder- oder Schwerpunktdezernat zu bilden? Inwiefern ist das derzeitig vorgehaltene Personal bei der Staatsanwaltschaft ausreichend für dieses Deliktfeld?

   Bei der Staatsanwaltschaft Bremen bearbeiten zwei Dezernenten zu je einem Viertel ihres Arbeitsvolumens Straftaten aus dem Bereich der Internetkriminalität. Darunter fallen insbesondere die Straftatbestände des Ausspähens von Daten, des Computerbetruges, der Fälschung beweiserheblicher Daten, der Datenveränderung sowie der Computersabotage, soweit für die Bearbeitung der Verfahren besondere Kenntnisse im Bereich des Internets oder der Datenverarbeitung erforderlich sind. Hassreden oder Hasspostings im Internet werden von dieser Sonderzuständigkeit grundsätzlich nicht erfasst. Die beiden Dezernenten sind auch beratend tätig und zudem als Ansprechpartner für andere Staatsanwaltschaften in diesem Kriminalitätsbereich benannt worden.

   Ermittlungsverfahren wegen Hasskriminalität im Internet, die einen politischen Bezug aufweisen, sind bei der Staatsanwaltschaft Bremen den politischen Dezernaten zugewiesen. Hier bearbeiten zwei Staatsanwälte mit jeweils 0,425 Anteilen politische Straftaten aus den Phänomenbereichen rechts/links sowie – aufgrund der häufig politischen Ausrichtung der bremischen Ultra-Szene – zudem Verfahren wegen szenetypischer Straftaten im Zusammenhang mit Fußballspielen. Ein weiterer Dezernent bearbeitet mit einem Anteil von 0,45 Straftaten Verfahren mit Bezug zum islamistischen Terrorismus. Hasskriminalität aus dem islamistischen Bereich wird in diesem Dezernat bearbeitet. Für Hasskriminalität ohne politischen Bezug gibt es derzeit keine Sonderzuständigkeit, diese werden in den allgemeinen Dezernaten bearbeitet.

   Die Bearbeitung von Ermittlungsverfahren wegen Hasskriminalität mit politischem Bezug wird auch zukünftig in den Politikdezernaten und nicht in denen für Internetkriminalität erfolgen. Bei dem, insbesondere aufgrund der geplanten Gesetzesänderungen durch das Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität, zu erwartenden Anstieg der Ermittlungsverfahren, wird eine Aufstockung der Anteile der politischen Dezernate erforderlich werden. In dem Koalitionsvertrag für die 20. Wahlperiode der Bremischen Bürgerschaft 2019 bis 2023 ist vorgesehen ein „Schwerpunktdezernat zur Verfolgung von Online – Hasskriminalität“ einzurichten.

5. Wie erfolgt die Zusammenarbeit der Bremer Sicherheitsbehörden mit den anderen Bundesländern und dem Bund im Bereich Internetkriminalität, vor dem Hintergrund der fließenden und nicht trennbaren Landesgrenzen im Internet? Inwieweit können und werden gegebenenfalls gemeinsame Strukturen mit anderen Bundesländern in Betracht gezogen?

   Der Cybercrime-Fachbereich der Polizei Bremen ist eng vernetzt mit den Bundesländern des erweiterten Nordverbundes (Niedersachsen, Hamburg, Schleswig-Holstein, Mecklenburg-Vorpommern, Berlin, Brandenburg und Bremen), dem Bundeskriminalamt, dem Zollkriminalamt, der Bundespolizei sowie den Staaten Österreich und Schweiz und Europol (über das Bundeskriminalamt als Zentralstelle).

   Zurzeit wird auf Ebene der Landeskriminalämter und des BKA geprüft, unter welchen Voraussetzungen bundesländerübergreifende zentrale Ermittlungsstellen lageangepasst eingerichtet werden können.

   Seitens der Staatsanwaltschaft Bremen, als Ermittlungs- und nicht als Sicherheitsbehörde, findet eine Zusammenarbeit mit anderen Staatsanwaltschaften in Form des gemeinsamen Führens von Ermittlungsverfahren

bislang nicht statt und ist auch derzeit nicht geplant. Sofern notwendig, erfolgt in Einzelfällen eine koordinierte Übermittlung von Ermittlungsverfahren unter vorheriger Erörterung der erforderlichen Ermittlungsmaßnahmen zwischen den jeweiligen Dezernenten der beteiligten Staatsanwaltschaften.

Durch den sogenannten Zuständigkeitsatlas IuK der Generalstaatsanwaltschaft Celle (4. Auflage, Februar 2020) wird eine Vernetzung zwischen den einzelnen im Bereich der Internet- und Kommunikationskriminalität zuständigen Stellen bei den bundesdeutschen Generalstaatsanwaltschaften und Staatsanwaltschaften (IuK-Dienststellen) gewährleistet. In diesem wird die jeweilige Organisationsform in den einzelnen Bezirken dargestellt und so eine erste Kontaktaufnahme zu einer möglichst zentralen Stelle, die in der Lage ist, im konkreten Bedarfsfall die passende Verbindung herzustellen, ermöglicht.

Überdies veranstaltet die „Zentrale Stelle Organisierte Kriminalität und Korruption (ZOK)“ der Generalstaatsanwaltschaft Celle einmal jährlich eine zweitägige „Arbeitstagung zu Fragen der Internet- und Computerkriminalität“ mit Teilnehmern von Generalstaatsanwaltschaften, Staatsanwaltschaften und verschiedenen Polizeidienststellen aus mehreren Bundesländern. Ferner findet einmal jährlich ein bundesweites Arbeitstreffen der IuK-Zentralstellen und IuK-Koordinatoren mit Teilnehmern aus dem gesamten Bundesgebiet statt. Die Tagungen dienen dem bundesländerübergreifenden Informationsaustausch über Ermittlungsmöglichkeiten und aktuelle Entwicklungen im Bereich der Internet- und Computerkriminalität. An den Tagungen nimmt jeweils ein Cybercrime-Dezernent der Staatsanwaltschaft Bremen teil.

Das Landesamt für Verfassungsschutz in Bremen steht in engem Austausch mit dem Bundesamt für Verfassungsschutz sowie weiteren Landesämtern, beteiligt sich an Arbeitskreisen für Extremismusforschung und speziellen Analyseforen, fertigt Forschungsberichte für den Verbund und bietet Vortragsveranstaltungen zu computergestützten Analyseverfahren für eine wirksame Extremismusbekämpfung unter digitalen Rahmenbedingungen an.

6. Inwieweit erschweren in diesem Feld fehlende Gesetzesgrundlagen wie die der Quellentelekommunikationsüberwachung, der Standortermittlung oder der Telekommunikationsüberwachung die Arbeit der Bremer Polizei und des Landesamts für Verfassungsschutz? Wie geht der Senat mit dem Problem um, dass im Netz vielfach anonym und verschlüsselt kommuniziert wird?

   Die technische Entwicklung und die Verbreitung neuer Formen der Kommunikation stellen die Sicherheitsbehörden vor eine zunehmend größer werdende Herausforderung. Dem Ausweichen von Extremisten und Straftätern in diese vielfach nur schwer aufzuklärenden virtuellen Räume muss neben der personellen und materiellen Ausstattung der Behörden auch mit den Mitteln des Rechts und gegebenenfalls mit Rechtsänderungen begegnet werden. Es ist gleichwohl nicht überzeugend, dies zu aller erst an den Begriffen Quellen-Telekommunikationsüberwachung oder Online-Durchsuchung festzumachen. Derartige Maßnahmen kommen aufgrund ihrer technischen Komplexität und den einzuhaltenden verfassungsrechtlichen Vorgaben nur für eine extrem geringe Zahl von Fällen in Betracht. Wichtiger erscheint eine Anpassung des allgemeinen Telekommunikationsrechts an die fortschreitende technische Entwicklung. Dies betrifft etwa die konsequente Einführung des Marktortprinzips nicht nur für klassische Telekommunikationsunternehmen, sondern für sämtliche sogenannte Over-the-Top-Anbieter, etwa die regelmäßig im Ausland befindlichen Anbieter von Messenger-Diensten. Auch die Möglichkeit, eine wirksame justizielle Kontrolle zu verhindern, muss gesetzlich unterbunden werden.

Für den gesamten Bereich der Internetkriminalität stellt das Fehlen einer verfassungs- und europarechtskonformen Vorratsdatenspeicherung zumindest eine Erschwernis dar. Hier erfolgen Anzeigen häufig erst mit einem Zeitverzug, sodass die bei den Providern nur kurze Zeit vorliegenden Daten häufig nicht mehr zur Verfügung stehen.

Zu berücksichtigen ist jedoch auch, dass den Sicherheitsbehörden durch die zunehmende Nutzung von elektronischen Kommunikationsmittel in der Gesellschaft oftmals Informationen und Ermittlungsansätze in einem ungleich größeren Umfang als in früheren Zeiten zur Verfügung stehen, insbesondere nach Sicherstellung und Auswertung der entsprechenden Geräte.

7. Welchen Änderungsbedarf bestehender Gesetze sieht der Senat, um gegen Internetkriminalität besser gewappnet zu sein? Welche Änderungen gab es in den vergangenen fünf Jahren bereits auf Bundesebene in diesem Bereich, und wie bewertet der Senat diese Entwicklungen? Inwieweit können (neuere) gesetzliche Möglichkeiten der Fahndung und Strafverfolgung durch die Sicherheits- und Ermittlungsbehörden in Bremen technisch genutzt werden und welche gegebenenfalls nicht oder nicht ausreichend?

   Bezüglich der Gesetzesänderungen der vergangenen fünf Jahre sind insbesondere die Wiedereinführung der Vorratsdatenspeicherung, welche gegenwärtig ausgesetzt ist, sowie die Einführung des § 202d StGB (Datenhehlerei) durch das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10. Dezember 2015 als Schritte zu einer Verbesserung der Effektivität der Strafverfolgung zu nennen.

   Des Weiteren wurden durch das Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens vom 17. August 2017 mit der Online-Durchsuchung (§ 100b StPO) und der Quellen-Telekommunikationsüberwachung (§ 100a Absatz 1 Satz 2, 3 StPO) neue digitale Ermittlungsmöglichkeiten in die Strafprozessordnung aufgenommen und damit den Ermittlungsbehörden weitere Möglichkeiten zur Aufklärung von Straftaten an die Hand gegeben.

   Seitens der Polizeibehörden wird die Wiedereinsetzung der Vorratsdatenspeicherung nach Klärung der Verfassungskonformität gefordert. Zudem wird darauf hingewiesen, dass die gemäß § 100g StPO (Erhebung von Verkehrsdaten) erhobenen Daten in der heutigen Kommunikation via Internet in allen Deliktsbereichen einen wichtigen Ermittlungsansatz darstellen, diese jedoch nur für Straftaten von auch im Einzelfall erheblicher Bedeutung und insbesondere die im §100a StPO genannten Katalog erhoben werden dürfen. Cybercrime-Delikte sind hier bislang nicht aufgeführt und erreichen auch sonst oft nicht die erforderliche Erheblichkeitsschwelle im Sinne des § 100g StPO.

   Im § 100j StPO (Bestandsdatenauskunft) in Verbindung mit § 113 Telekommunikationsgesetz (TKG), wären verpflichtende Zeitvorgaben sinnvoll, nach denen die Telekommunikationsdiensteanbieter innerhalb eines eng gesetzten Zeitraums die Daten zur Verfügung stellen müssen. Häufig vergehen Wochen, bis Monate, bis eine Antwort eintrifft.

8. Welche Präventions- und Informationsmaßnahmen gibt es aktuell im Land Bremen, um über Kriminalität im Internet zielgruppenspezifisch (zum Beispiel Heranwachsende, ältere Menschen, Menschen mit Migrationshintergrund et cetera) aufzuklären? Wer richtet derartige Angebote aus und wie werden diese angenommen? Welche zusätzlichen Maßnahmen plant der Senat, um Internetkriminalität noch effektiver vorzubeugen?

   Das Präventionszentrum der Polizei Bremen und die Präventionsstelle der Ortspolizeibehörde Bremerhaven bieten zum Thema Cybercrime Vorträge für Erwachsene an (unter anderem in Bremen „Leben online – wirklich sicher? - Polizeiliche Empfehlungen für einen bewussten Umgang mit dem

Internet“). Neben Tipps zum generellen Verhalten beziehungsweise zu Vorgehensweisen werden zusätzlich Präventionsmedien angeboten (Broschüren, Informationsblätter, Flyer, eine SafeCard-Hülle). Generell gelten die Empfehlungen für alle Nutzer des Internets und sind für alle Altersgruppen zielführend.

Die Vorträge werden in verschiedenen Stadtteilen abgehalten (zum Beispiel in Ortsämtern, Stadtteilfilialen der Sparkasse Bremen, im Justizzentrum Am Wall, Verbraucherzentrale). Die Veranstaltungen werden gut angenommen und sind in der Regel ausgebucht. Teilnehmerinnen/Teilnehmer sind meist lebenserfahrenere Personen. Die Gruppe der Heranwachsenden ist selten vertreten.

Es wurden und werden Vorträge nach Anfragen in anderen Institutionen durchgeführt, zum Beispiel der Verbraucherzentrale, der Handwerkskammer sowie Kundencentern. Auf Anfrage gibt es für Jugendliche/Heranwachsende abgestimmte Vorträge in Bildungseinrichtungen, außerhalb der gesetzlichen Schulen und Jugendfreizeiteinrichtungen.

Grundsätzlich können sich Bürgerinnen und Bürger während der Öffnungszeiten (jüngere wie ältere) telefonisch und persönlich bei verschiedenen Problemen und Unsicherheiten hinsichtlich Cybercrime beraten lassen. Vielfach werden Beratungsfragen per E-Mail an das Postfach des Präventionszentrums gestellt und von dort schnellstmöglich beantwortet.

Auf der Homepage der Polizei Bremen sind Tipps zum Thema Cybercrime eingestellt. Verlinkungen führen zu bundesweiten Informationsangeboten anderer Einrichtungen/Institutionen, zum Beispiel Bundesamt für Sicherheit in der Informationstechnik (BSI), Verbraucherzentrale, Programm für polizeiliche Kriminalprävention (ProPK). Dort werden auch aktuelle Warnhinweise veröffentlicht.

Anfragen von Medieneinrichtungen zu Veröffentlichungen werden genutzt, um die Zielgruppe der Internetnutzer zu erreichen. In der aktuellen Jahresplanung (2020) des Präventionszentrums der Polizei Bremen war Cybercrime das Schwerpunktthema im Monat Februar. Anlässlich dieser Planung wurde der polizeiliche Newsletter „Augen unserer Stadt“ mit Inhalten dieses Themenfeldes versehen und an circa 1 500 Empfänger per E-Mail versandt. In dem Newsletter wurden fünf Vorträge, die in verschiedenen Stadtteilen geplant waren, beworben und Anmeldungen über die Antwortfunktion entgegengenommen. Im Monat Februar haben fünf geplante Veranstaltungen stattgefunden, die zu verschiedenen Presseveröffentlichungen/Beiträgen geführt haben. Durch die Teilnahme an einer Livesendung in der Hörfunksendung „Zebra 4“ von Radio Bremen, konnten Botschaften in vier Gesprächsrunden platziert werden.

Darüber hinaus existiert speziell für den präventiven Bereich der sogenannte ZAC-Verbund (Zentrale Ansprechstellen der Länder und des Bundes) zum Zwecke des Wirtschaftsschutzes. Die Polizei Bremen ist Teil dieses Verbundes, der durch das LKA abgebildet wird.

Zudem werden in Bremerhaven durch das Dienstleistungszentrum Schulungen im Bereich der Medienkompetenz an Bremerhavener Schulen angeboten und durchgeführt.

9. Wie ist die Relation der erfolgten Straftaten im Internet in Bezug auf tatsächlich zur Anzeige gebrachter Straftaten nach Einschätzung des Senats? Wie will der Senat darauf hinwirken, dass mehr Menschen, die von Internetkriminalität betroffen sind, auch Strafanzeige stellen?

   Hinsichtlich der Relation zwischen den erfolgten Straftaten und der tatsächlich zur Anzeige gebrachten Straftaten können keine validen Aussagen getroffen werden.

   Zur positiven Beeinflussung des Anzeigeverhaltens wird auf die Beantwortung der Frage III Nummer 8 verwiesen.

Neben den bereits beschriebenen Maßnahmen der Präventionsstellen wird die Öffentlichkeit durch die polizeiliche Öffentlichkeitsarbeit proaktiv und anlassbezogen über die Printmedien und die sozialen Medien informiert. Dies dient einerseits einer Sensibilisierung und andererseits der Schaffung von Sensibilität für die modi operandi.

10. Inwieweit gibt es die Planung eines jährlichen Lagebildes „Cybercrime“ wie auf Bundesebene auch in Bremen zu erstellen? Welche Gründe sieht der Senat dafür oder dagegen?

    Aufgrund der zunehmenden Bedeutsamkeit von Cybercrime-Delikten werden diese im zukünftig regelmäßig erscheinenden bremischen Periodischen Sicherheitsbericht berücksichtigt. Grundlage des Berichts ist das Gesetz zur fortlaufenden Untersuchung der Kriminalitätslage und ergänzenden Auswertung der polizeilichen Kriminalitätsstatistik im Land Bremen (Bremisches Kriminalitätsstatistikgesetz - BremKStatG).

    Da Cybercrime-Delikte grundsätzlich kein regionales Phänomen darstellen, sieht der Senat ein bundes-/europaweites) Lagebild grundsätzlich als ausreichend an.