**BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG** **Drucksache 22/3086**

22. Wahlperiode **09.02.21**

Schriftliche Kleine Anfrage

**der Abgeordneten Dennis Gladiator und Richard Seelmaecker (CDU)
vom 02.02.21**

und Antwort des Senats

Betr.: Die dunkle Seite der Digitalisierung – wie wappnen sich Hamburgs Strafverfolgungsbehörden für die rasant steigende Zahl an Cybercrime-delikten?

Einleitung für die Fragen:

Leider bietet die Digitalisierung nicht nur Chancen, sondern bringt auch erhebliche Risiken mit sich: Straftaten, die im Internet (Cybercrime im engeren Sinne) oder mittels des Internets (Cybercrime im weiteren Sinne) begangen werden, nehmen seit Jahren rasant zu. Das Cybercrime Bundeslagebild 2019 zeigt Art und Ausmaß der Gefahren, die von Kriminellen in der digitalen Welt ausgehen, auf erschütternde Weise auf. Auch wenn in diesem Bereich sogar von einem weit überdurchschnittlichen Dunkelfeld ausgegangen wird, ist die deutsche Wirtschaft laut Bitkom-Studie vom Februar 2020 (Bundeslagebild 2019, Seite 32) ein beliebtes Ziel für Cyberkriminelle: Drei von vier Unternehmen wurden 2019 Opfer von Cyberangriffen, 2017 war es „nur" jedes zweite. Im Jahre 2019 entstand ein Schaden von 102,9 Milliarden Euro durch Cyberangriffe auf Wirtschaftsunternehmen. Bundesweit wurden in der PKS des Bundes 2019 100.514 Fälle von Cybercrime im engeren Sinne erfasst, was eine Steigerung von 15,4 Prozent gegenüber dem Vorjahr bedeutet. Die Anzahl der erfassten Delikte, bei denen Internet als Tatmittel genutzt wurde, stieg um 8,4 Prozent auf 294.665 Fälle. Gerade bei diesen Delikten werden auch häufig Bürger zum Opfer von Kriminellen.

Nicht nur der Bereich der Bekämpfung und Strafverfolgung von Cybercrime im engeren Sinne, also den Angriffen, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten, sondern auch die Verfolgung von Straftaten, bei denen das Internet „lediglich" als Tatmittel eingesetzt wird, erfordert von den Mitarbeitern der Strafverfolgungsbehörden besondere Kenntnisse und Strategien. Hinzu kommt, dass die Taten meist grenzüberschreitende Bezüge aufweisen, Täter arbeitsteilig vorgehen und über verschlüsselte Kanäle, häufig sogar im Darknet, kommunizieren.

Mehrere Bundesländer haben darauf bereits vor einigen Jahren konkret reagiert und ihre Strafverfolgungsbehörden entsprechend fachlich und personell ausgestattet, so zum Beispiel Hessen mit der Errichtung der Zentralstelle zur Bekämpfung der Internet- und Computerkriminalität (ZIT) bei der Generalstaatsanwaltschaft Frankfurt oder Bayern, wo in der bei der Generalstaatsanwaltschaft Bamberg eingerichteten Zentralstelle Cybercrime Bayern IT-Fachkräfte die Arbeit der Staatsanwälte mit ihrem technischen Wissen unterstützen.

Vor zwei Jahren teilte der damalige Leiter des Landeskriminalamtes in einem Interview gegenüber dem „Hamburger Abendblatt" mit, dass das LKA damit begonnen habe, Mitarbeiter zusätzlich in Cyberthemen zu qualifizieren und es

einen ersten „Cyber-Kommissar“ gebe. Die effektive Bekämpfung von Cyberkriminalität sei eine zentrale Aufgabe der heutigen Zeit, für die eine adäquate Personalsituation unerlässlich sei (https://www.abendblatt.de/hamburg/article216325695/Der-LKA-Chef-und-der-erste-Cyber-Kommissar.html).

Es stellt sich die Frage, was sich seitdem in Hamburgs Strafverfolgungsbehörden getan hat. Dies ist umso dringender, da davon auszugehen ist, dass infolge der Corona-Pandemie-bedingten Einschränkungen der Schwerpunkt der Kriminalität noch rasanter von der Straße ins Internet gewechselt ist.

Vor diesem Hintergrund fragen wir den Senat:

Frage 1: *Wie haben sich seit dem Jahr 2018 jährlich nach der Polizeilichen Kriminalstatistik (PKS) folgende Deliktszahlen sowie die entsprechenden Aufklärungsquoten in Hamburg entwickelt: 897000 Computerkriminalität (5430** Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB, 6742** Datenveränderung, Computersabotage §§ 303a, 303b StGB, 6780** Ausspähen/Abfangen von Daten, Vorbereiten des Ausspähens/Abfangens von Daten gemäß §§ 202a, 202b, 202c StGB, 715100 Softwarepiraterie (private Anwendung zum Beispiel Computerspiele), 715200 Softwarepiraterie in Form gewerbsmäßigen Handelns 897100 Computerbetrug)?*

Frage 2: *Wie haben sich seit dem Jahr 2018 jährlich nach der PKS folgende Deliktszahlen sowie die entsprechenden Aufklärungsquoten in Hamburg entwickelt: 897100 Computerbetrug (511120 Betrügerisches Erlangen von Kfz § 263a StGB, 511212 Weitere Arten des Warenkreditbetruges § 263a StGB, 516300 Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN § 263a StGB 516520 Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB, 516920 Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB, 517220 Leistungskreditbetrug § 263a StGB, 5175** Computerbetrug (sonstiger) § 263a Absatz 1 und 2 StGB, Vorbereitung § 263a Absatz 3 StGB, 517900 Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB, 518112 Abrechnungsbetrug im Gesundheitswesen § 263a StGB, 518302 Überweisungsbetrug § 263a StGB)?*

Frage 3: *Wie haben sich seit dem Jahr 2018 jährlich die unter dem PKS-Summenschlüssel 897000 erfassten Vermögensschäden entwickelt?*

Frage 4: *Wie haben sich seit dem Jahre 2018 jährlich nach der PKS folgende Deliktszahlen sowie die entsprechenden Aufklärungsquoten in Hamburg entwickelt: 1432** (Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Schriften § 184b StGB)*

Frage 5: *Wie hat sich die Gesamtzahl der mit dem Internet als Tatmittel begangenen Delikte seit dem Jahre 2018 jährlich entwickelt?*

Antwort zu Fragen 1 bis 5:

Die Polizei erfasst Straftaten gemäß dem Straftatenkatalog der bundesweit einheitlichen Richtlinien für die Erfassung und Verarbeitung der Daten in der Polizeilichen Kriminalstatistik (PKS).

Im Übrigen siehe Anlage 1.

Frage 6: *Gab es in Hamburg seit dem Jahre 2018 Angriffe auf Kritische Infrastrukturen?*

Falls ja, wann und wie stellte sich der Sachverhalt gegebenenfalls jeweils dar?

Antwort zu Frage 6:

Dem Informationssicherheitsmanagement der Freien und Hansestadt Hamburg liegen keine Informationen über Angriffe auf Unternehmen der kritischen Infrastruktur in Hamburg vor. Im Übrigen kommunizieren Unternehmen solche Vorfälle grundsätzlich direkt an das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Frage 7: *Wie stellt sich die Entwicklung der Personalsituation im Fachkommissariat Cybercrime (LKA 54) dar? Bitte Stellen-Soll und VPK, differenziert nach Polizeibeamten und Informatikern seit 2018 jeweils zum Stichtag 1. Januar darstellen.*

Antwort zu Frage 7:

Siehe Anlage 2.

Frage 8: *Wie viele Mitarbeiter des LKA 54 wurden bereits zu „Cyber-Experten" fortgebildet (beispielsweise an der Technischen Hochschule Brandenburg oder mit Fernstudiengängen „Master in Internet Security" beziehungsweise „Master in Digital Forensic"), wie viele befinden sich aktuell in der entsprechenden Weiterbildung?*

Antwort zu Frage 8:

Sechs Mitarbeiterinnen beziehungsweise Mitarbeiter des LKA 54 haben eine Fortbildung im Sinne der Fragestellung bereits abgeschlossen. Zwei Mitarbeiterinnen beziehungsweise Mitarbeiter haben ein einjähriges Studium an der TH Brandenburg im Rahmen einer Kooperation der Länder des Nordverbundes, drei Mitarbeiterinnen beziehungsweise Mitarbeiter ein einjähriges Studium zum „Nordic Computer Forensics Investigator" (NCFI) an der Polizeihochschule Oslo, sowie ein Mitarbeiter beziehungsweise eine Mitarbeiterin ein dreieinhalbjähriges Masterstudium „Information Security" an der Technisch-Naturwissenschaftlichen Universität Norwegens absolviert. Zudem befinden sich aktuell zwei Mitarbeiterinnen beziehungsweise Mitarbeiter in einem einjährigen Studium an der TH Kiel im Rahmen einer Kooperation der Länder des Nordverbundes und ein Mitarbeiter beziehungsweise Mitarbeiterin beginnt im Laufe des Jahres ein einjähriges Studium zum „Nordic Computer Forensics Investigator" (NCFI) an der Polizeihochschule Oslo.

Vorbemerkung: *In der Drs. 21/16127 gab der Senat an, dass die Schaffung spezieller Laufbahnen für IT-Kriminalisten nach dem Vorbild der Länder Baden-Württemberg, Rheinland-Pfalz und Bayern sowie dem BKA geplant, die Überlegungen jedoch noch nicht abgeschlossen seien. Mittlerweile sind zwei weitere Jahre vergangen.*

Frage 9: *Wird weiterhin daran festgehalten?*

Falls ja, wie ist der aktuelle Sachstand der Planungen und wann soll das umgesetzt werden?

Falls nein, wer hat das wann aus welchen Gründen entschieden?

Frage 10: *Weiterhin bestätigte der Senat in der Drs. 21/16127, dass es konkrete Überlegungen für speziell auf solche Spezialistenlaufbahnen zugeschnittene Besoldungs- und Beförderungsperspektiven, die für geeignete Bewerber im angespannten Arbeitsmarkt Attraktivität versprechen, geben soll, aber auch hier die Überlegungen noch nicht abgeschlossen seien. Wird weiterhin daran festgehalten?*

Falls ja, wie ist der aktuelle Sachstand der Planungen und wann soll das umgesetzt werden?

Falls nein, wer hat das wann aus welchen Gründen entschieden?

Antwort zu Fragen 9 und 10:

Bei der Polizei wurden, um den Bedarf an entsprechend qualifizierten Spezialistinnen und Spezialisten zu gewährleisten, im LKA 54 höherwertige Dienstposten beschrieben,

für deren Besetzung ein mindestens einjähriges Cybercrimestudium erforderlich ist. Hierdurch besteht für die Absolventen eines solchen Studiums eine Karrieremöglichkeit innerhalb der Dienststelle. Darüber hinaus sind die Überlegungen noch nicht abgeschlossen.

Frage 11: *Wie hat sich die personelle Situation in der Abteilung 74 der Staatsanwaltschaft, die für die Bearbeitung von Cybercrimedelikten zuständig ist, seit dem Jahr 2018 jährlich entwickelt? Bitte jeweils zum Stichtag 1. Januar in Stellen-Soll und Besetzungsumfang (VZÄ) darstellen.*

Frage 12: *Wie beurteilt die zuständige Behörde die personelle Ausstattung der Mitarbeiter der Staatsanwaltschaft im Hinblick auf die erheblich steigende Zahl an Cybercrimedelikten im weiteren und engeren Sinne? Inwiefern hält sie den Einsatz von IT-Fachkräften zur Unterstützung der Dezernenten für sinnvoll beziehungsweise erforderlich? Bitte detailliert begründen.*

Antwort zu Fragen 11 und 12:

Aufgrund des Anstiegs der Cybercrimedelikte wurde die Abteilung 74 durch interne Stellenverschiebungen verstärkt. Ob eine weitere Personalaufstockung erforderlich sein wird, wird derzeit in enger Abstimmung zwischen den zuständigen Behörden geprüft. Ergänzend ist darauf hinzuweisen, dass nicht alle Straftaten, die im oder mittels des Internets begangen werden, in der Abteilung 74 bearbeitet werden, der Zuständigkeitsbereich der Abteilung 74 sich in Teilbereichen im oben genannten Zeitraum verändert hat und in der Abteilung 74 derzeit auch Strafverfahren wegen §§ 201, 201a, 184 fortfolgende Strafgesetzbuch (StGB) bearbeitet werden, soweit sie nicht mittels des Internets begangen wurden.

Ausweislich der Jahresgeschäftsverteilungspläne 2018 bis 2021 waren folgende Stellen (Angaben in VZÄ) zum 1. Januar des jeweiligen Jahres für die Abteilung 74 vorgesehen und aufgrund der internen Stellenverschiebungen wie folgt besetzt:

2018:

Abteilungsleitung	1
Dezernentenstellen	3,65
Besetzt waren	3,75

2019:

Abteilungsleitung	1
Dezernentenstellen	3,65
Besetzt waren	3,75

2020:

Abteilungsleitung	1
Dezernentenstellen	3,65
Besetzt waren	4,35

2021:

Abteilungsleitung	1
Dezernentenstellen	3,95
Besetzt waren:	4,95

Der Einsatz von IT-Fachkräften bei der Staatsanwaltschaft ist für den Ermittlungsbereich grundsätzlich nicht erforderlich. Die Staatsanwaltschaft arbeitet regelmäßig eng mit dem LKA zusammen, das die IT-Fachkräfte aus dem dortigen Bereich einbindet.

Frage 13: *Wurden seitens der Gerichte Bedarfe an Spezialisierungen, personellen Aufstockungen oder Fortbildungen in der Strafjustiz vor dem Hintergrund der steigenden Cybercrimedelikte gemeldet?*

Falls ja, wie bewertet die zuständige Behörde die Bedarfe im Einzelnen?

Antwort zu Frage 13:

Nein.

Frage 14: *Wie beurteilen die zuständigen Behörden die Entwicklung der im beziehungsweise mittels des Internets begangenen Straftaten seit der Corona-Pandemie? Inwiefern erhöht sich das Risiko durch verstärkte Inanspruchnahme von Homeoffice?*

Antwort zu Frage 14:

Die mit dem Tatmittel Internet begangenen Fälle sind 2020 im Vergleich zu 2019 um 12,6 Prozent angestiegen. Den mit 84,3 Prozent größten Anteil machen hierbei die Betrugstaten aus. Von der Gesamtkriminalität wurden 4,6 Prozent der Fälle mit dem Tatmittel Internet begangen. Im Zuge der Pandemie wird das Internet zum einen für die Bevölkerung verstärkt zur Informationsquelle und Freizeitbeschäftigung, zum anderen haben Homeoffice-Maßnahmen zu einer verstärkten Nutzung geführt, auch zur Meidung von Geschäften und Banken werden Transaktionen eher online vorgenommen. Somit entstehen mehr Tatgelegenheiten für Straftäter im Internet.

Statistische Daten zur Risikoerhöhung von Straftaten durch Homeoffice-Nutzung liegen den Strafverfolgungsbehörden nicht vor. Zur Beantwortung dieser Frage wäre eine Auswertung aller Akten im Zusammenhang mit Straftaten im Internet oder mittels des Internets im Hinblick auf einen Zusammenhang mit der Corona-Pandemie erforderlich. Dies ist im Rahmen der für eine Parlamentarische Anfrage zur Verfügung stehenden Zeit nicht möglich. Allein die in der Abteilung 74 ausweislich der internen Controllingberichte für die Monate März bis Dezember 2020 geführten Verfahren liegen im vierstelligen Bereich.

Erfasste Fälle und Aufklärungsquoten für ausgewählte Delikte

Hamburg gesamt

Frage	Schlüssel-zahl	Delikte	2018		2019		2020	
			erfasste Fälle	AQ in %	erfasste Fälle	AQ in %	erfasste Fälle	AQ in %
1.	897000	**Computerkriminalität**	3.889	24,3	3.795	19,6	4.727	19,5
	davon							
	5430**	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	44	27,3	64	20,3	150	50,7
	6742**	Datenveränderung, Computersabotage §§ 303a, 303b StGB	58	22,4	132	11,4	122	8,2
	6780**	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	285	14,4	448	11,2	641	9,4
	715100	Softwarepiraterie (private Anwendung, z. B. Computerspiele)	7	85,7	6	50,0	10	40,0
	715200	Softwarepiraterie in Form gewerbsmäßigen Handelns	0	-	2	100,0	1	100,0
	897100	**Computerbetrug**	3.495	24,9	3.143	21,0	3.803	20,2
	davon							
2.	511120	Betrügerisches Erlangen von Kfz § 263a StGB	0	-	2	0,0	1	0,0
	511212	Weitere Arten des Warenkreditbetruges § 263a StGB	769	30,2	690	18,0	580	18,4
	516300	Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN gemäß § 263a StGB	2.140	21,4	1.810	21,2	1.879	16,4
	516520	Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	123	31,7	201	26,9	609	10,7
	516920	Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	72	37,5	62	22,6	409	52,8
	517220	Leistungskreditbetrug § 263a StGB	135	34,8	58	27,6	96	21,9
	5175**	Computerbetrug (sonstiger) § 263a StGB (soweit nicht unter den Schlüsseln 511120, 511212, 516300, 516520, 516920, 517220, 517900, 518112 bzw. 518302 zu erfassen)	238	28,2	299	21,1	206	23,3
	517900	Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	8	0,0	8	12,5	2	0,0
	518112	Abrechnungsbetrug im Gesundheitswesen § 263a StGB	1	100,0	3	66,7	3	100,0
	518302	Überweisungsbetrug § 263a StGB	9	22,2	10	20,0	18	5,6
4.	1432**	Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Schriften § 184b StGB	107	77,6	200	81,5	312	78,2
5.		Tatmittel "Internet" alle Delikte	7.789	32,5	8.392	24,0	9.452	27,8

Frage	Schlüssel-zahl		2018	2019	2020
3.	897000	Vermögensschaden	2.673.960	2.417.448	2.921.917

Mitarbeitende LKA 54 (Cybercrime)

	Stellen /Dienst-posten	davon Planstel-len	davon Stellen für Arbeitneh-merinnen und Arbeitnehmer	von den Stellen für Arbeitnehmerinnen und Arbeitnehmer „Beschäftigte in der Informationstechnik“	VPK	davon Beamtin-nen und Beamte	davon Angestellte gesamt	Von den Angestellten „Beschäftigte in der Informationstechnik“	DP-Besetzungsumfang (ab KoPers)
01.01.2018	49	35	14	9	41,6038	22,9	18,7038	13,3654	-
01.01.2019	50	35	15	9	44,4999	25,7	18,7999	12,5128	-
01.01.2020*	56								50,1654
01.01.2021*	58								52,8442

* Eine Differenzierung der Dienstposten für Polizeivollzug und Verwaltung erfolgt im aktuell benutzten Programm KoPers nicht, daher sind „Informatiker“ bezogen auf das LKA 5 seit dem 1. Januar 2020 nicht auswertbar.