BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
22. Wahlperiode

Drucksache 22/7467
01.03.22

Schriftliche Kleine Anfrage

der Abgeordneten Dennis Gladiator und Richard Seelmaecker (CDU)
vom 22.02.22

und Antwort des Senats

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

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 2020 zeigt Art und Ausmaß der Gefahren, die von Kriminellen in der digitalen Welt ausgehen, erneut auf erschütternde Weise auf: Unter anderem steigt die Anzahl erfasster Cyberstraftaten weiter an, die Täter sind global vernetzt und agieren zunehmend professioneller und die Underground Economy wächst – sie stellt eine kriminelle, globale Parallelwirtschaft dar, die maßgeblich auf finanziellen Profit aus ist. Einer der Gründe für diese Entwicklung ist die stark voranschreitende Digitalisierung aller Lebensbereiche, die coronabedingt einen zusätzlichen Antrieb erhielt; so entstehen mehr Tatgelegenheiten für Cyberkriminelle.

Insbesondere die Wirtschaft erleidet hohe Schäden durch Cybercrime-Delikte: „Durch Diebstahl, Spionage und Sabotage entsteht der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro. Damit haben kriminelle Attacken erneut für Rekordschäden gesorgt: Die Schadenssumme ist mehr als doppelt so hoch wie in den Jahren 2018/2019, als sie noch 103 Milliarden Euro p.a. betrug. Neun von zehn Unternehmen (88 Prozent) waren 2020/2021 von Angriffen betroffen. In den Jahren 2018/2019 wurden drei Viertel (75 Prozent) Opfer.“, stellte eine repräsentative Studie des Digitalverbands Bitkom fest (https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr).

Aber nicht nur der Bereich der Bekämpfung und Strafverfolgung von Cybercrime im engeren Sinne, also der Angriffe, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten, sondern auch die Verfolgung von steigenden Straftaten, bei denen das Internet „lediglich“ als Tatmittel eingesetzt wird, erfordern 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 drei 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).

Im Zuge der aufwendigen und zahlreichen EncroChat-Ermittlungsverfahren wurde mit der Drs. 22/4733 auch eine befristete Aufstockung von IT-Fachkräften beschlossen; dies reicht in Anbetracht der Bedrohungslage durch Cybercime-Delikte aber nicht aus.

Vor diesem Hintergrund fragen wir den Senat:

Frage 1: *Wie haben sich im Jahr 2021 jeweils im Vergleich zum Vorjahr 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/Anfangens von Daten gemäß §§ 202a, 202b, 202c StGB 715100 Softwarepiraterie (private Anwendung zum Beispiel Computerspiele) 715200 Softwarepiraterie in Form gewerbsmäßigen Handelns)?*

Frage 2: *Wie haben sich im Jahr 2021 jeweils im Vergleich zum Vorjahr 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 im Jahr 2020 und 2021 die unter den PKS-Summenschlüsseln 897000 sowie 897100 erfassten Vermögensschäden jeweils entwickelt?*

Frage 4: *Wie haben sich im Jahr 2021 im Vergleich zum Vorjahr 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 im Jahr 2021 im Vergleich zum Vorjahr entwickelt?*

Antwort zu Fragen 1 bis 5:

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

Die statistische Erfassung eines Falles erfolgt nach den Richtlinien für die Führung der PKS mit Abschluss aller polizeilichen Ermittlungen durch die für die Endbearbeitung zuständige Dienststelle bei endgültiger Abgabe der entstandenen Ermittlungsvorgänge beziehungsweise des Schlussberichts an die Staatsanwaltschaft oder das Gericht.

Der PKS-Summenschlüssel 897000 Computerkriminalität wurde zum 1. Januar 2021 umbenannt in „Cybercrime“ und umfasst folgende Straftatenschlüssel/Deliktsbereiche:

511120 Betrügerisches Erlangen von Kfz § 263a StGB

511212 Weitere Arten des Warenkreditbetruges § 263a StGB

516300 Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN

516520 Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB

516920 Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB

517220 Leistungskreditbetrug § 263a StGB

517500 Computerbetrug (sonstiger) § 263a StGB

517900 Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB

518112 Abrechnungsbetrug im Gesundheitswesen § 263a StGB

518302 Überweisungsbetrug § 263a StGB

543000 Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB

674200 Datenveränderung, Computersabotage §§ 303a, 303b StGB

678000 Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB

Die Straftatenschlüssel

715100 Softwarepiraterie (private Anwendung, zum Beispiel Computerspiele),

715200 Softwarepiraterie in Form gewerbsmäßigen Handelns

werden seit dem 1. Januar 2021 nicht mehr berücksichtigt.

In den Jahren vor 2021 umfasste der Summenschlüssel 897000 Computerbetrug die folgenden Straftatenschlüssel/Deliktsbereiche:

5430** Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung § 269, 270 StGB

6742** Datenveränderung, Computersabotage §§ 303a, 303b StGB

6780** Ausspähen, Abfangen von Daten einschließlich Vorbereitungshandlungen und Datenhehlerei gemäß §§ 202a, 202b, 202c, 202d StGB

715100 Softwarepiraterie (private Anwendung, zum Beispiel Computerspiele)

715200 Softwarepiraterie in Form gewerbsmäßigen Handelns

897100 Computerbetrug

Eine Vergleichbarkeit der Werte des Summenschlüssels 897000 ab dem Jahr 2021 mit den Vorjahren ist daher nur noch eingeschränkt möglich.

Straftaten, die im oder mittels des Internets begangen wurden, werden in unterschiedlichen Abteilungen der Staatsanwaltschaft bearbeitet. Im Vorgangsverwaltungs- und Vorgangsbearbeitungssystem MESTA der Staatsanwaltschaft wird nicht erfasst, ob eine Straftat im oder mittels des Internets begangen wurde. Zur Beantwortung der Frage müssten daher sämtliche Verfahren händisch ausgewertet werden, die ein Delikt zum Gegenstand haben, welches im Internet oder mittels des Internets begangen werden kann. Darunter fallen beispielsweise auch Beleidigungsdelikte, die allein für das Jahr

2021 Verfahren im vierstelligen Bereich ausmachen. Eine solche Auswertung ist in der für die Beantwortung einer Parlamentarischen Anfrage zur Verfügung stehenden Zeit nicht möglich.

Im Übrigen siehe Anlage.

Frage 6: *Wie hat sich die Gesamtzahl der Ermittlungsverfahren wegen „Computersachen pp.“, für die die Abteilung 74 zuständig ist, in den Jahren 2020 und 2021 entwickelt?*

Antwort zu Frage 6:

Ausweislich des internen Controllingberichtes der Staatsanwaltschaft vom 3. Januar 2022 waren in der Abteilung 74 für das Jahr 2020 1.555 Js-Neueingänge und für das Jahr 2021 2.297 Js-Neueingänge zu verzeichnen.

Frage 7: *Wie hat sich die Gesamtzahl der Ermittlungsverfahren wegen Computerbetrugs bei der Staatsanwaltschaft Hamburg in den Jahren 2020 und 2021 entwickelt?*

Frage 8: *Wie hat sich die Gesamtzahl der von der Staatsanwaltschaft Hamburg erhobenen Anklagen wegen Computerbetrugs in den Jahren 2020 und 2021 entwickelt?*

Frage 9: *Wie hat sich die Anzahl der Verurteilten wegen Computerbetrugs in Hamburg in den Jahren 2020 und 2021 entwickelt?*

Antwort zu Fragen 7, 8 und 9:

Für die Aktenzeichenjahrgänge 2020 und 2021 wurden im Vorgangsverwaltungs- und Vorgangsbearbeitungssystem MESTA jeweils 1.007 Verfahren wegen Computerbetruges nach § 263a StGB erfasst, für den Aktenzeichenjahrgang 2020 gegen 1.201 Beschuldigte und für den Aktenzeichenjahrgang 2021 gegen 1.256 Beschuldigte. Hinsichtlich der Verfahren des Aktenzeichenjahrgangs 2020 wurde bisher in 111 Verfahren gegen 118 Beschuldigte Anklage erhoben oder der Erlass eines Strafbefehls beantragt, wobei es bisher in 49 Verfahren gegen 50 Beschuldigte zu rechtskräftigen Verurteilungen kam. Hinsichtlich der Verfahren des Aktenzeichenjahrgangs 2021 wurde bisher in 52 Verfahren gegen 55 Beschuldigte Anklage erhoben oder der Erlass eines Strafbefehls beantragt, wobei es bisher in 18 Verfahren gegen 18 Beschuldigte zu rechtskräftigen Verurteilungen kam.

Die Erfassung des Tatbestandes § 263a StGB für ein Verfahren in MESTA bedeutet jedoch nicht, dass auch die Anklageerhebung beziehungsweise der Antrag auf Erlass eines Strafbefehls und/oder der Schuldspruch wegen § 263a StGB erfolgten. Die Feststellung, aufgrund welcher Delikte die Anklage, der Antrag auf Erlass eines Strafbefehls und der Schuldspruch tatsächlich erfolgten, wäre nur durch eine händische Einzelauswertung der genannten Verfahren möglich. Eine solche Auswertung ist in der für die Beantwortung einer Parlamentarischen Anfrage zur Verfügung stehenden Zeit nicht möglich.

Frage 10: *Wie stellt sich die Entwicklung der Personalsituation im Fachkommissariat Cybercrime (LKA 54) dar? Bitte Stellen-Soll und VPK zum Stichtag 1. Januar 2022 darstellen.*

Antwort zu Frage 10:

Mit Stichtag 1. Januar 2022 sind dem Fachkommissariat Cybercrime (LKA 54) 71 Dienstposten zugeordnet, der Besetzungsumfang beträgt 65,8846 in Vollzeitäquivalenten (VZÄ).

Vorbemerkung: *In der Drs. 22/3086 gab der Senat auf die Frage nach der Fortbildung von Mitarbeitern des LKA 54 zu „Cyber-Experten“ hin an: „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.“

Frage 11: *Wie stellt sich die aktuelle Situation dar? Wie viele fertig fortgebildete Mitarbeiter/innen sind aktuell beim LKA 54 beschäftigt, wie viele befinden sich aktuell in einer entsprechenden Weiterbildung?*

Antwort zu Frage 11:

Beim LKA 54 sind aktuell sieben Mitarbeitende beschäftigt, die bereits eine Fortbildung im Sinne der Fragestellung abgeschlossen haben. Die Fortbildungen erfolgten in einem Fall als einjähriges Studium an der TH Brandenburg im Rahmen einer Kooperation der Länder des Nordverbundes, in drei Fällen als einjähriges Studium zum „Nordic Computer Forensic Investigator“ (NCFI) an der Polizeihochschule Oslo, in einem Fall als dreieinhalbjähriges Masterstudium „Information Security” an der Technisch-Naturwissenschaftlichen Universität Norwegens und in zwei Fällen als einjähriges Studium an der FH Kiel im Rahmen einer Kooperation der Länder des Nordverbundes.

Zudem befindet sich aktuell ein weiterer Mitarbeiter in einem einjährigen Studium an der FH Kiel im Rahmen einer Kooperation der Länder des Nordverbundes.

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 ist, die Überlegungen jedoch noch nicht abgeschlossen seien. Mittlerweile sind zwei weitere Jahre vergangen. Weiterhin bestätigte der Senat in der Drs. 21/16127, dass es konkrete Überlegungen für speziell auf solche Spezialisten-Laufbahnen zugeschnittene Besoldungs- und Beförderungsperspektiven, die für geeignete Bewerber im angespannten Arbeitsmarkt Attraktivität versprechen, geben soll, aber auch hier die Überlegungen noch nicht abgeschlossen seien. Auf die Fragen nach dem Sachstand teilte der Senat in der Drs. 22/3086 hin mit: „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 12: *Wird weiterhin an der Schaffung spezieller Laufbahnen für IT-Kriminalisten nach dem Vorbild der Länder Baden-Württemberg, Rheinland-Pfalz und Bayern sowie dem BKA 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 13: *Wird weiterhin an den konkreten Überlegungen für speziell auf solche Spezialisten-Laufbahnen zugeschnittene Besoldungs- und Beförderungsperspektiven, die für geeignete Bewerber im angespannten Arbeitsmarkt Attraktivität versprechen, 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 12 und 13:

Siehe Drs. 22/3086.

Frage 14: *Wie stellt sich die personelle Situation in der Abteilung 74 der Staatsanwaltschaft, die für die Bearbeitung von „Computersachen pp." zuständig ist, aktuell dar? Bitte zum Stichtag 1. Januar 2022 in Stellen-Soll und Besetzungsumfang (VZÄ) darstellen.*

Antwort zu Frage 14:

Ausweislich des Jahresgeschäftsverteilungsplans für das Jahr 2022 waren folgende Stellen (Angaben in VZÄ) zum 1. Januar 2022 für die Abteilung 74 vorgesehen:

Abteilungsleitung: 1

Dezernentenstellen: 5,6

Besetzt waren (inklusive Abteilungsleitung): 5,6

Erfasste Fälle und Aufklärungsquoten für ausgewählte Delikte

Hamburg gesamt

Schlüssel-zahl	Delikte	2020		2021		Zu/-Abnahmen	
		erfasste Fälle	AQ in %	erfasste Fälle	AQ in %	Fälle absolut	Fälle in %
897000	**Computerkriminalität ***	4.727	19,4	4.624	13,3	-103	-2,2
davon							
5430**	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung §§ 269, 270 StGB	150	50,7	123	28,5	-27	-18,0
6742**	Datenveränderung, Computersabotage §§ 303a, 303b StGB	122	8,2	126	7,1	4	3,3
6780**	Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen und Datenhehlerei §§ 202a, 202b, 202c, 202d StGB	641	9,4	898	6,6	257	40,1
715100	Softwarepiraterie (private Anwendung, z. B. Computerspiele) **	10	40,0	8 **	62,5	-2	-20,0
715200	Softwarepiraterie in Form gewerbsmäßigen Handelns **	1	100,0	2 **	50,0	1	100,0
897100	**Computerbetrug**	3.803	20,2	3.477	14,8	-326	-8,6
davon							
511120	Betrügerisches Erlangen von Kfz § 263a StGB	1	0,0	1	100,0	0	0,0
511212	Weitere Arten des Warenkreditbetruges § 263a StGB	580	18,4	710	19,6	130	22,4
516300	Computerbetrug mittels rechtswidrig erlangter Zahlungskarten mit PIN gemäß § 263a StGB	1.879	16,4	1.572	12,7	-307	-16,3
516520	Computerbetrug mittels rechtswidrig erlangter Daten von Zahlungskarten § 263a StGB	609	10,7	602	8,6	-7	-1,1
516920	Computerbetrug mittels rechtswidrig erlangter sonstiger unbarer Zahlungsmittel § 263a StGB	409	52,8	145	20,0	-264	-64,5
517220	Leistungskreditbetrug § 263a StGB	96	21,9	129	15,5	33	34,4
5175**	Computerbetrug (sonstiger) § 263a StGB (soweit nicht unter den Schlüsseln 511120, 511212, 516300, 516520, 516920, 517220, 517900, 518112 bzw. 518302 zu erfassen)	206	23,3	263	23,6	57	27,7
517900	Missbräuchliche Nutzung von Telekommunikationsdiensten § 263a StGB	2	0,0	2	0,0	0	0,0
518112	Abrechnungsbetrug im Gesundheitswesen § 263a StGB	3	100,0	2	100,0	-1	-33,3
518302	Überweisungsbetrug § 263a StGB	18	5,6	51	15,7	33	183,3
1432**	Verbreitung, Erwerb, Besitz und Herstellung kinderpornographischer Schriften § 184b StGB	312	78,2	952	71,6	640	205,1
———	**Tatmittel "Internet" alle Delikte**	9.452	27,8	10.489	29,8	1.037	11,0

Schlüssel-zahl	Vermögensschaden in EUR	2020	2021	Zu/-Abnahmen absolut	Zu/-Abnahmen in %
897000	**Computerkriminalität ***	2.921.917	2.526.245	395.672	-8,6%
897100	**Computerbetrug**	2.921.351	2.526.245	395.106	-8,6%

* Bezeichnung ab 2021 lautet: Cybercrime (geänderte Zusammensetzung ab 01.01.2021 in Bezug auf die Delikte)

** seit dem 01.01.2021 nicht mehr Bestandteil des Summenschlüssels 897000 Cybercrime