Interpellation Simmler-St.Gallen (54 Mitunterzeichnende) vom 20. September 2017

Cybercrime: Herausforderungen für die St.Galler Sicherheitspolitik

Schriftliche Antwort der Regierung vom 25. September 2018

Monika Simmler-St.Gallen erkundigt sich in ihrer Interpellation vom 20. September 2017 nach der Bekämpfung von Cyber-Kriminalität und stellt verschiedene Fragen dazu. Angesichts zahlreicher Aktivitäten auf Bundesebene und umfangreicher kantonsinterner Abklärungen kann die Beantwortung der Interpellation erst heute erfolgen.

Die Regierung antwortet wie folgt:

Die Schweiz befindet sich im Prozess der Digitalisierung. Dieser Prozess eröffnet grosse Chancen, birgt aber auch Risiken. Die damit einhergehende zunehmende Abhängigkeit von Informations- und Kommunikationstechnologien (IKT) macht unser Land verwundbarer gegenüber Ausfällen, Störungen und Missbräuchen dieser Technologien. Die Bedrohungen durch Cyber-Angriffe sind in den letzten Jahren stark gestiegen.

Die Cyber-Kriminalität ist eine der fünf Bedrohungsformen, die in der Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022[1] (nachfolgend NCS 2018–2022) unterschieden werden. Unter Cyber-Kriminalität im engeren Sinn werden dabei Straftaten verstanden, bei denen Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind (z.B. unbefugtes Eindringen in ein Datenverarbeitungssystem, Art. 143bis des Schweizerischen Strafgesetzbuches [SR 311.0; abgekürzt StGB]). Unter Cyber-Kriminalität im weiteren Sinn werden alle Straftaten verstanden, bei denen Informations- und Kommunikationstechnik zur Planung, Vorbereitung oder Ausführung eingesetzt wird.

Die über das Internet verfügbare digitale Infrastruktur eröffnet potenziellen Straftäterinnen und Straftätern laufend neue Möglichkeiten mit enormem Schadenspotenzial für Gesellschaft und Wirtschaft. Zeitliche und räumliche Einschränkungen für Taten gibt es kaum mehr. Cyber-Kriminalität überschreitet territoriale Grenzen, und dies in einem hochdynamischen Prozess mit kurzen Innovationszyklen. Dieser permanent wachsenden Professionalisierung der Täterschaft in der Fortentwicklung krimineller Geschäftsideen und -modelle und der Herstellung und Nutzung neuer Schadsoftware stehen auf der Opferseite fehlende Sensibilität und digitale Kompetenz im geschäftlichen, im privaten und im politischen Umfeld gegenüber. Je stärker die digitale Vernetzung ist, desto grösser wird die Gefahr, dass Cyber-Vorfälle zwar in der virtuellen Welt beginnen, aber ihre schädigende Wirkung in der realen Welt entfalten. Vor dem Hintergrund dieser Entwicklung ist es dringend angezeigt, auch in der Strafverfolgung nach neuen Lösungsansätzen zu suchen. Es gilt gesamtschweizerisch und in Zusammenarbeit mit internationalen Partnern, die Interoperabilität und Reaktionsfähigkeit zu verbessern sowie die fachlichen, technischen und personellen Kompetenzen wirksam aufeinander abzustimmen, ohne dabei die Befugnisse zwischen den verschiedenen Behörden und Staatsebenen zu verschieben. Dass dabei den äusserst rasanten globalen Aktionsmöglichkeiten der digitalen Kriminalität die oft kleinräumig anzuwendenden Instrumente der internationalen Rechtshilfe in Strafsachen mit ihren schwerfälligen und langfristigen Arbeitsgängen gegenüberstehen, ist offensichtlich.

1 Die NCS 2018–2022 wurde vom Bundesrat am 18. April 2018 verabschiedet und ist abrufbar unter https://www.newsd.admin.ch/newsd/message/attachments/52071.pdf.

Zu den einzelnen Fragen:

1. Für Private, Wirtschaft und Behörden hat in den letzten Jahren kein Risiko derart an Bedeutung gewonnen wie die Cyber-Kriminalität. Für die Schweizer Wirtschaft gehören Cyberattacken und deren Auswirkungen längst zur Realität. Beinahe die Hälfte (42 Prozent) der Unternehmen, die Opfer einer Cyberattacke wurden, erlitt dadurch finanzielle Schäden und Störungen der Geschäftstätigkeiten. Bei 33 Prozent der Firmen gelangten vertrauliche Informationen an die Öffentlichkeit, und bei einem Viertel verursachten die Angriffe Reputationsschäden.[2]

   Bis anhin werden Straftaten, die unter Cyber-Kriminalität fallen, in der Polizeilichen Kriminalstatistik nicht separat und gesamthaft ausgewiesen. Aus diesem Grund kann gestützt auf die Polizeiliche Kriminalstatistik keine Aussage zu Ausmass und Entwicklung der Cyber-Kriminalität an sich gemacht werden. Eine solche lässt sich auch nicht aus der Entwicklung der Straftaten der Cyber-Kriminalität i.e.S.[3] ableiten, auch nicht aus den vom fedpol in den «Statistiken zum Jahresbericht fedpol» jährlich veröffentlichten «eingegangenen Meldungen bezüglich Cyber-Kriminalität»[4]. Die Regierung begrüsst deshalb Massnahme 4 des NCS 2018–2022, mit der die Fähigkeiten zur Beurteilung und Darstellung der Cyber-Bedrohungslage ausgebaut werden sollen.

   Die Sensoren der kantonalen Sicherheitsinfrastruktur registrieren täglich Tausende von Angriffsversuchen aus dem Cyberraum, die erkannt und abgewehrt werden. Trotz den vorhandenen Massnahmen kommt es hin und wieder vor, dass noch unbekannte Malware über den E-Mail-Verkehr auf die Client-Infrastruktur gelangt, Benutzer auf Phishing-E-Mails reagieren oder Webserverdienste ausser Gefecht gesetzt werden.

   In der kantonalen Verwaltung werden Sicherheitsvorfälle dem Leiter Informationssicherheit rapportiert und von ihm dokumentiert. Über die Anzahl der Vorfälle gibt der jeweilige Jahresbericht zu den Informatikvorhaben Auskunft. In den Jahren 2017 und 2016 wurden 16 bzw. 21 solcher Sicherheitsvorfälle aufgezeichnet. Es handelte sich dabei meistens um installierte Malware (Schadsoftware) und in wenigen Fällen um kompromittierte Webseiten. In zwei Fällen, beides E-Mails mit erpresserischem Inhalt, wurde eine Strafanzeige eingereicht.

2./7. Die polizeiliche und strafrechtliche Verfolgung der Cyber-Kriminalität gestaltet sich im Kanton St.Gallen heute grundsätzlich so wie bei der übrigen Kriminalität. Ein in Kooperation zwischen der Staatsanwaltschaft und der Kantonspolizei St.Gallen betriebenes «Kompetenzzentrum Cybercrime» ist im Entstehen begriffen und die entsprechenden Fachkompetenzen mit spezialisierten Fachgruppen werden derzeit aufgebaut. In diesem Zusammenhang hat am 1. August 2018 ein erster Cyber-Staatsanwalt seine Arbeit aufgenommen. Der damit bei der Kantonspolizei einhergehende Personalaufbau musste initial mit einer internen Stellenverschiebung zulasten anderer Abteilungen realisiert werden. Ohne zusätzliche Ressourcen ist die Realisierung des «Kompetenzzentrums Cybercrime» indessen nicht möglich. Die hierfür erforderlichen finanziellen Mittel sind im Budget 2019 und im Aufgaben- und Finanzplan 2020–2022 eingestellt (Projekt «CU» Cybercrime Unit, vgl. Ziff. 3).

---

2 Studie der KMPG zu «Clarity on Cyber Security», abrufbar unter https://home.kpmg.com/ch/de/home/medien/medienmitteilungen/2018/05/gefaehrliche-alleingaenge-bei-der-bekaempfung-von-cyberkriminalitaet.html.

3 Die Straftaten der Cyber-Kriminalität i.e.S. sind in der Polizeilichen Kriminalitätsstatistik erfasst. Die Polizeiliche Kriminalstatistik Kanton St.Gallen 2017 ist abrufbar unter https://www.kapo.sg.ch/home/informationen/statistiken/_jcr_content/Par/downloadlist/DownloadListPar/download_1963624855.ocFile/2017%20PKS_Jahresbericht.pdf, S. 77. Die Entwicklung ist nicht linear und «nur» zunehmend.

4 Abrufbar unter https://www.fedpol.admin.ch/dam/data/fedpol/publiservice/publikationen/berichte/jabe/jabe-2017-stat-d.pdf. Im Jahr 2017 waren es 9'831 Meldungen gegenüber 14'033 im Jahr 2016, 11'575 im Jahr 2015 und 10'214 im Jahr 2014.

Die Bildung des «Kompetenzzentrums Cybercrime» ändert nichts daran, dass entsprechende Grundkompetenzen auch bei allen Mitarbeiterinnen und Mitarbeitern der Strafverfolgungsbehörden des Kantons St.Gallen geschaffen werden müssen. Denn auch bei der Cyber-Kriminalität muss die Erstermittlung vor Ort jederzeit sichergestellt werden und schnell erfolgen.

3. Seit einiger Zeit werden die Kantonspolizei und die Staatsanwaltschaft zunehmend mit dem Thema Cyber-Kriminalität konfrontiert und sehen sich damit hohem Ermittlungsaufwand, technisch versierter und gut dotierter Täterschaft, grenzüberschreitenden Tatbeständen, mangelnden eigenen Fachkenntnissen, beschränkter eigener technischer Infrastruktur sowie fehlenden personellen Ressourcen gegenüber. Daraus resultierte die Erkenntnis, dass im Kanton St.Gallen die technischen, organisatorischen, personellen, finanziellen und infrastrukturellen Voraussetzungen für eine nachhaltige Bekämpfung der Internetkriminalität fehlen. Aus diesem Grund wurde im Juli 2017 das Projekt «CU» (Cybercrime Unit) initiiert, das den Aufbau eines nachhaltigen Kooperationsmodells der Staatsanwaltschaft und der Kantonspolizei zur Ermittlung der Täterschaft im Netz auch über die Landesgrenzen hinaus betreffend Aufbau, Infrastruktur und Know-how sowie die Befähigung der Strafverfolgungsbehörden in den Bereichen Tatbestandserfassung, Rapportierung, Ermittlung, Fahndung und Untersuchungsführung zum Inhalt hat. In der Umsetzung dieses Projekts wurde der Handlungsbedarf konkretisiert. Zur Erfüllung des Grundauftrags werden die notwendigen organisatorischen, personellen, infrastrukturellen und technischen Massnahmen ab September 2018 im Rahmen der bestehenden Ressourcen schrittweise realisiert.

   Problemstellungen resultieren auch daraus, dass die Cyber-Kriminalität im Unterschied zu den Strafverfolgungsbehörden keine territorialen Grenzen kennt und dass es für die Strafverfolgung keine einheitliche sachliche Zuständigkeit gibt. Je nach Straftat können die Strafverfolgungsbehörden der Kantone oder die Strafverfolgungsbehörde des Bundes (Bundespolizei, Bundesanwaltschaft) zuständig sein. Um unter anderem auch Gerichtsstandskonflikte zu vermeiden, wurde das «Konzept Cyberboard» ins Leben gerufen (vgl. Ziff. 4).

4. Die Bekämpfung der Cyber-Kriminalität ist eine Aufgabe aller in der Strafverfolgung tätigen Behörden von Bund und Kantonen. Sie müssen sicherstellen, dass es in der Schweiz keine rechtsfreien Räume gibt. Sie müssen ebenso sicherstellen, dass die Strafverfolgung auch über die Landesgrenze hinaus effizient und effektiv erfolgt. All dies erfordert eine gemeinsame Steuerung und die Kooperation aller involvierten Behörden. Aus diesen Gründen haben die Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS), die Schweizerische Staatsanwälte-Konferenz (SSK), die Bundesanwaltschaft (BA) und das Bundesamt für Polizei (fedpol) im Januar 2018 eine gemeinsame Strategie – die «Strategie zur effizienten Bekämpfung von Cybercrime» – festgelegt. In dieser wird festgehalten, dass die Bekämpfung der Cyber-Kriminalität eine Verbundaufgabe darstellt und dass eine gewisse Spezialisierung und Regionalisierung unumgänglich ist. Angestrebt werden:
   – ein gemeinsames Lagebild und eine nationale Fallübersicht;
   – das Vermeiden von Gerichtsstandkonflikten bei Cyber-Kriminalität;
   – die gemeinsame Analyse und Triage von eingehenden Meldungen;
   – die Konzeption spezifischer Ausbildungen.

   Mit welcher Organisation und mit welchen Massnahmen diese Ziele erreicht werden sollen, ist im «Konzept Cyberboard» dargelegt. Der Kanton St.Gallen beteiligt sich aktiv daran. Als nächster Schritt soll die Schaffung von Kompetenzzentren zur Bekämpfung der Cyber-Kriminalität vorangetrieben werden.

Dieses Konzept zur effizienten Bekämpfung von Cybercrime wurde in der Frühjahrsversammlung der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD)vom 12. April 2018 zur Kenntnis genommen.

5. Die heutigen Massnahmen, Verfolgungsaktivitäten und vorhandenen Ressourcen für eine wirkungsvolle Bekämpfung der Cyber-Kriminalität sind im Kanton St.Gallen nicht ausreichend und müssen ausgebaut werden. Dieser Ausbau soll mit der Umsetzung des Projekts «CU» (Cybercrime Unit) erfolgen. Ohne zusätzliche Ressourcen ist dies nicht machbar. Es sind zusätzliche Ressourcen (Personal- und Sachaufwand) sowohl bei der Kantonspolizei als auch bei der Staatsanwaltschaft erforderlich. Die für die Realisierung des Projekts «CU» (Cybercrime Unit) erforderlichen finanziellen Mittel sind im Budget 2019 und im Aufgaben- und Finanzplan 2020–2022 eingestellt.

6. Wie in der «Strategie zur effizienten Bekämpfung von Cybercrime» (siehe oben Ziff. 4) festgehalten ist, ist eine gewisse Spezialisierung und Regionalisierung unumgänglich. Noch kein anderer Mitgliedskanton des Ostschweizerischen Polizeikonkordats (ostpol) verfügt über eine Organisationseinheit «Cybercrime». Aus diesen Gründen kann sich die Regierung grundsätzlich vorstellen, dass die neu zu etablierende Cybercrime-Organisationseinheit mittel- und langfristig zu einem «Kompetenzzentrum Cybercrime ostpol» entwickelt und innerhalb von ostpol fest verankert wird; selbstverständlich nur bei Kostenneutralität für den Kanton, was namentlich durch die Nutzung von Synergieeffekten erzielt werden könnte.

8. Auch die Aus- und Weiterbildung ist bei Cyber-Kriminalität eine Verbundaufgabe. Eine ausschliesslich auf den Kanton fokussierte kantonsinterne Aus- und Weiterbildung wird daher nicht angestrebt und auch nicht aktiv gefördert.

   Die Ausbildung der Strafverfolgungsbehörden ist Gegenstand des NCS 2018–2022; sie ist eine der vier Massnahmen im Handlungsfeld «Strafverfolgung» (Massnahme 20). In Zusammenarbeit zwischen der Konferenz der kantonalen Polizeikommandanten der Schweiz (KKPKS) und der Schweizerischen Staatsanwälte-Konferenz (SSK) werden spezifische Ausbildungskonzepte für einen nachhaltigen Aufbau der erforderlichen Kompetenzen in der Strafverfolgung geschaffen. Losgelöst von der Strafverfolgung ist der Bereich «Kompetenzen- und Wissensaufbau» eines der zehn Handlungsfelder des NCS 2018–2022. Dies macht deutlich, wie wichtig dieser Bereich ist.

   Für die Aus- und Weiterbildung der Strafverfolgungsbehörden des Kantons St.Gallen sind namentlich die Polizeischule Ostschweiz und das Schweizerische Polizei-Institut für Polizistinnen und Polizisten sowie die Staatsanwaltsakademie der Universität Luzern für Staatsanwältinnen und Staatsanwälte von zentraler Bedeutung. Das Schweizerische Polizei-Institut ist schweizweit daran, Ausbildungsmodule für verschiedene Wissensstufen zu erarbeiten (E-Learnings). Für die Kantonspolizei St.Gallen bietet sich zudem auch die Gelegenheit, an Kursen anderer Polizeikorps oder ausländischen Polizeiakademien teilzunehmen. Auch gibt es an der Staatsanwaltsakademie der Universität Luzern bereits eine Konzeptgruppe (in der auch der Kanton St.Gallen vertreten ist), die ein Ausbildungskonzept für Staatsanwältinnen und Staatsanwälte im Bereich Bekämpfung Cyber-Kriminalität erarbeitet. Zur technischen Kompetenzbildung werden Angebote sowohl von in- und ausländischen Hochschulen und Universitäten als auch von anderen Anbietern genutzt.