

Beschluss Nr. 603/2022
Schwyz, 23. August 2022 / ju

Interpellation I 3/22: Ist unsere Polizei in Sachen Cyberkriminalität genügend mit Ressourcen ausgestattet?

Beantwortung

1. Wortlaut der Interpellation

Am 10. Februar 2022 haben Kantonsrat Roland Lutz und vier Mitunterzeichnende folgende Interpellation eingereicht:

«Ausgangslage: Die Cyberkriminalität schädigt mit hohen Zuwachsraten Schwyzer Bürger und Unternehmen. In den Medien liest man täglich von Vorfällen in der Schweiz und im Ausland. Ein Auszug aus der Polizeiliche Kriminalstatistik 2020: Die Anzahl Cybercrime-Straftaten ist um 100 auf 520 Delikte gestiegen (2019: 420). Davon entfielen 232 Delikte auf den Cyberbetrug. Die Deliktssumme betrug total CHF 5 135 778.¹

2021 dürfte sich die Schadenssumme – notabene ohne Berücksichtigung der hohen Dunkelziffer an nichtgemeldeten Fällen – wieder stark erhöht haben. Dasselbe ist für 2022 und die kommenden Jahre zu erwarten.

Die Delikte sind vielfältiger Natur, vorwiegend handelt es sich um:

- Online-Anlagebetrug*
- Ransomware (Erpressung und Betriebsunterbrüche)*
- Sextortion*
- Diebstahl Cryptowährungen*
- Kleinanzeigebetrug*

Die Gefahr, Opfer von kriminellen Hackern und Betrügern zu werden, ist mittlerweile höher als die von Naturkatastrophen. Sextortion kann bei betroffenen Jugendlichen ein gravierendes Sui-

¹ Quelle sz.ch / Statistik 2021 ist per 03 / 2022 zu erwarten

zidrisiko darstellen. Online-Anlagebetrug ist nicht nur wegen hohen Deliktsummen von Bedeutung, die Aufklärung erfordert auch einen hohen Mitteleinsatz. Bei all diesen Risiken wäre eine angemessene Prävention enorm wichtig und effektiv.

Im Schwyzer Polizeicorps kümmern sich per 2022 fünf Personen um die Cyberdelikte. Zum Vergleich: Zürich ist mit rund 85 Stellen dotiert; was auf die Bevölkerungszahlen der beiden Kantone umgelegt ca. 8.5 Stellen entspricht. Anzumerken ist, dass es sich im Kanton Schwyz fast ausschliesslich nicht um Informatiker handelt, sondern um informatikaffine Polizeikräfte mit diversen zielgerichteten Ausbildungen. Das zusätzlich benötigte IT-Know-how wird jeweils gezielt eingekauft.

Angesichts der aktuellen personellen Ausstattung bleibt nach unserer Einschätzung und Beobachtung zu wenig Raum für effektive Vorbeugemassnahmen wie Aufklärung. Es können zudem mutmasslich nur die allerwichtigsten Fälle seriös aufgearbeitet werden.

Die Polizeiarbeit der "Cybertruppe" kann grob wie folgt eingeteilt werden:

- Unterstützung Sicherheitspolizei bei (neuen) Cyberfällen
- Ermittlungen
- Präventionsarbeit
- Aufklärung
- Fahndung

Es stellt sich nun die Frage, ob die eingesetzten Ressourcen (Personal / sonstige Mittel) mit der stark steigenden Deliktzahl Schritt halten können. Bereits heute dürften nach einer Triage nur noch die wichtigsten, resp. aussichtsreichsten Fälle mit dem nötigen Ressourceneinsatz verfolgt werden können. Angesichts der Gefahrenlage und der Schäden ist es u.E. unabdingbar, unsere Sicherheitsbehörden entsprechend aufzustellen.

Fragen an den Regierungsrat

1. Wie beurteilt der Regierungsrat die Entwicklung der nächsten Jahre im Cyberbereich?
 - a. Wachstum der Kriminalitätsraten
 - b. Qualität der Delikte hinsichtlich Schäden
2. Erachtet der Regierungsrat die eingesetzten Ressourcen als adäquat im Hinblick auf die Bedrohung / Bewältigung?
 - a. Personal
 - b. Budgets für andere Mittel
3. Sind Anpassungen der Ressourcen in nächster Zeit geplant?
 - a. Kurzfristig
 - b. Mittel- / Langfristig

Für die Beantwortung danken wir im Voraus.»

2. Antwort des Regierungsrates

2.1 Allgemeine Bemerkungen

Der Regierungsrat hat im Zusammenhang mit der Thematik Cyberkriminalität bereits mit Beschlüssen Nr. 685 vom 18. September 2018 und Nr. 439 vom 29. Juni 2021 entsprechend Stellung genommen. Im Jahre 2018 war die Kantonspolizei in Bezug auf die Bekämpfung der Cyberkriminalität hinsichtlich Ressourcen und Fachwissen noch semiprofessionell aufgestellt. In der Folge schaffte sie innerhalb der Abteilung Kriminalpolizei einen Fachbereich «Cybercrime» und besetzte die Stellen mit einem Cyber-Techniker und zwei Cyber-Ermittlern. Vorerst ging es

darum, innerhalb der Kantonspolizei das Fachwissen zu bündeln, die verschiedenen Aufgaben rund um die Cyber-Kriminalität zu koordinieren und die Schnittstellen auf kantonaler und nationaler Ebene sicherzustellen. Der Regierungsrat bewilligte per 1. Januar 2022 eine Aufstockung um zwei weitere Stellen in diesem Bereich. Per 1. April 2022 konnte nun die Letzte der insgesamt fünf Stellen besetzt werden. Ursprünglich war vorgesehen, nebst Cyber-Ermittlern auch mindestens einen Cyber-Techniker zu beschäftigen. Dieses Vorhaben scheiterte, da solche Spezialisten nur schwer zu finden sind. Nun wird das benötigte technische Knowhow bei Bedarf extern eingekauft. Zudem wurde der Fachbereich Cybercrime in einen eigenen Dienst Cybercrime überführt und angesiedelt bei der Abteilung Kriminalpolizei. Die Arbeiten des Dienstes Cybercrime können im Wesentlichen in folgende Teilbereiche aufgeteilt werden:

- Unterstützung der beiden Frontabteilungen: Bereits bei der Entgegennahme von Cybercrime-Anzeigen ist die Polizei ressourcenmässig und fachlich gefragt. Der Dienst Cybercrime unterstützt die Frontkräfte bereits ab der Anzeigeerstattung und stellt so den fachlichen Support zugunsten der beiden Frontabteilungen Sicherheitspolizei und Kriminalpolizei sicher. Bei komplexen Sachverhalten wird die Anzeige direkt durch den Dienst Cybercrime entgegengenommen und weiterbearbeitet.
- Ermittlungen bei Cyber-Delikten im engeren Sinne: Der Dienst Cybercrime stellt bei Cyber-Delikten im engeren Sinne (z. B. bei einem Hackerangriff) die polizeilichen Ermittlungen umfassend sicher.
- Ermittlungsunterstützung: Sie ist ein wesentlicher Bestandteil des Dienstes Cybercrime. Dazu zwei Beispiele: In Fällen polizeilicher Gefahrenabwehr, wie z. B. bei einem Vermisstenfall, unterstützt der Dienst Cybercrime die Ermittlungen mit umfassenden Internet-Recherchen und dem Einholen entsprechender Verbindungsdaten. Die Erfahrungen zeigen, dass es mit Cyber-Ermittlungen möglich ist, innert kürzester Zeit entscheidende Erkenntnisse zu erarbeiten. Cyber-Ermittlungen kommen weiter u. a. auch bei Betrugsdelikten zum Zuge. Stehen Krypto-Währungen im Fokus, so wird mittels aufwändiger Transaktionsanalyse versucht, dem Geldfluss zu folgen, verbunden mit dem Ziel, inkriminiertes Geld sicherzustellen und die Täterschaft zu eruieren.
- Prävention: Dem Präventionsansatz kommt bei der Bekämpfung der Cyber-Kriminalität eine ganz besondere Bedeutung zu. Daher will die Kantonspolizei ihre Bestrebungen diesbezüglich deutlich ausbauen. Gemäss erarbeitetem Konzept ist es sinnvoll, mittelfristig pro Jahr mindestens 1800 Arbeitsstunden in verschiedenste Präventionstätigkeiten zu investieren. In diesem Kontext ist zu erwähnen, dass der Dienst Cybercrime in der Konzeptions- wie auch in der Umsetzungsphase amtsintern stark vom Dienst «Prävention» unterstützt wird.
- Aus und Weiterbildung: Der Dienst Cybercrime muss trotz komplexer technischer, kriminalistischer und juristischer Fragestellungen fähig sein, die vorerst unbekannte Täterschaft zu eruieren und schliesslich der Justiz zuzuführen. Erfahrungen der letzten beiden Jahre zeigen zudem, dass in diesem dynamischen Umfeld grosser Bedarf besteht, dass Mitarbeitende auf allen Ebenen jederzeit und zentral auf entsprechendes Fachwissen und beratende Dienstleistungen zurückgreifen können. Ebenso gilt es, die Frontmitarbeitenden punkto Basiswissen auszubilden. Das bedingt, dass die Cyberermittler eine solide Grundausbildung erhalten und sich laufend weiterbilden.

2.2 Beantwortung der Fragen

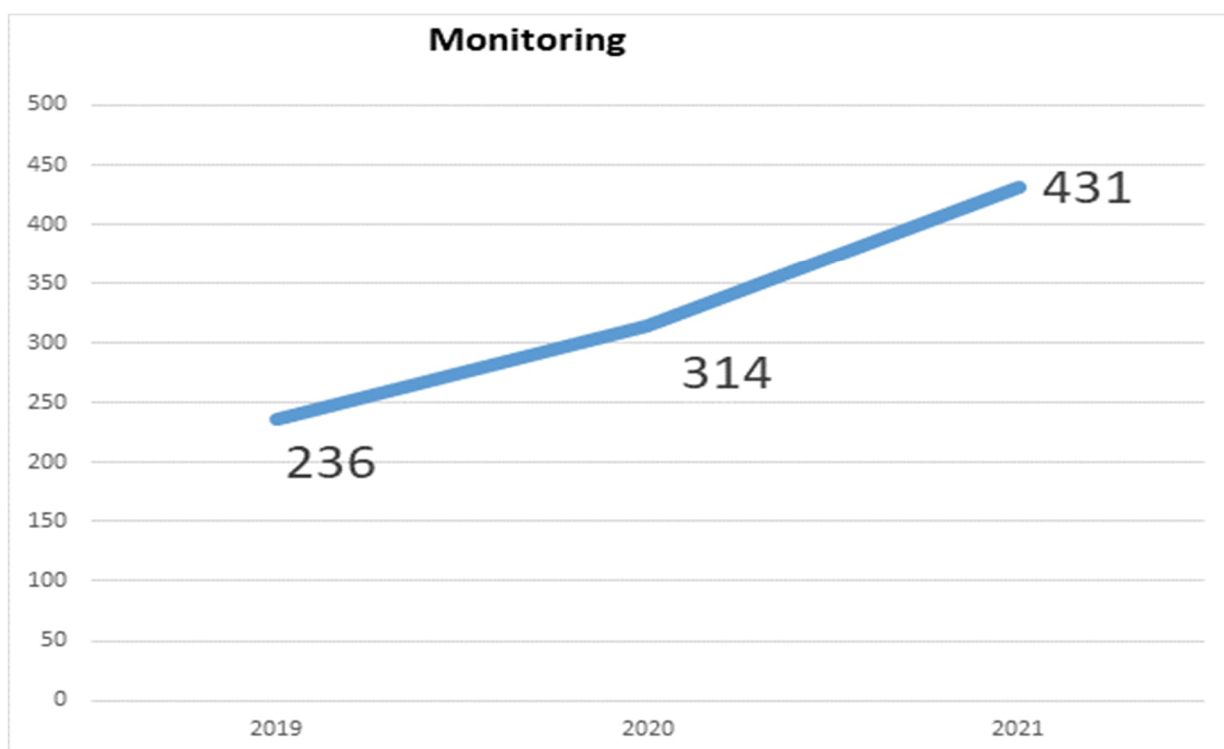
1. Wie beurteilt der Regierungsrat die Entwicklung der nächsten Jahre im Cyberbereich?

a) Wachstum der Kriminalitätsraten

Durch die zunehmende Verlagerung ihrer Aktivitäten in das Internet ist die Bevölkerung des Kantons Schwyz neuen Gefahrenformen wie Online-Anlagebetrug, Cybermobbing, Identitätsdiebstahl durch Social-Engineering oder dem Verlust der Privatsphäre ausgesetzt, oder sie kann gar unfreiwillig zu Beteiligten der Cyberkriminalität werden. Die Sicherstellung der sozialen Integrität und die Befriedigung eines grundlegenden Schutzbedürfnisses sowie die effektive und effiziente Verfolgung und Aufklärung oben beispielhaft genannter Cyber-Delikte sind enorm aufwändig.

Die nachfolgenden statistischen Daten des Dienstes Cybercrime zeigen die rasante Entwicklung und die damit verbundene deutliche Steigerung des Aufwandes insbesondere in den letzten beiden Jahren auf (die Zahlen werden erst seit 2019 erhoben). Es ist davon auszugehen, dass die Zunahme in den nächsten Jahren weitergehen wird.

- Fallzahlen Monitoring:



Der Dienst Cybercrime geht sämtlichen der Polizei gemeldeten Ereignissen mit Bezug zur Cyber-Kriminalität nach, klassifiziert diese und führt eine Fallpriorisierung durch. Diese dient dem gezielten Einsatz der vorhandenen Ressourcen gemäss dem Konzept der Staatsanwaltschaft bzw. durch ein national vorgegebenes Raster. Je nach Klassifizierung ergeben sich keine Weiterungen, aber in den allermeisten Fällen folgen weitere Massnahmen (Unterstützung bei der Entgegennahme der Anzeige, Vorbereiten fachspezifischer Fragekataloge, eigenständige Ermittlungen und Abklärungen, NEDIK-Verbreitungen, usw.).

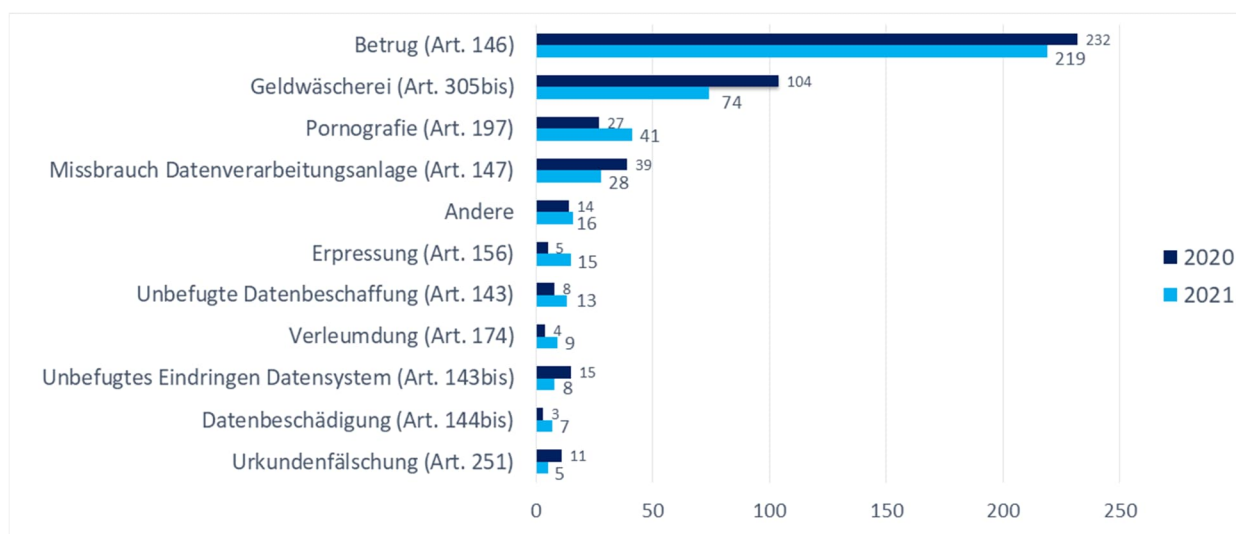
- Fallzahlen Aufträge:

Im Jahr 2020 wurden im Rahmen der erstmaligen Erfassung 130 Aufträge verzeichnet, diese Zahl stieg im Jahr 2021 bereits auf 240 Aufträge an.

Jeder einzelne Auftrag (bzw. Ermittlungsauftrag der Staatsanwaltschaft) löst beim Dienst Cybercrime verschiedenste Aktivitäten aus. Dies geschieht einerseits im Rahmen der Ermittlungsunterstützung in Form von Internetrecherchen, Datenerhebungen, Transaktionsanalysen usw., und andererseits können es auch komplett eigenständige Ermittlungen und Fallführungen von A-Z sein.

Festzuhalten ist, dass die Beantwortung von Bürgeranfragen (z. B. Auskunft an Privatpersonen per E-Mail oder telefonisch) und die weiteren Präventionstätigkeiten hier nicht speziell ausgewiesen werden. Diese Dienstleistungen werden durch den Dienst Cybercrime (noch) nicht erfasst. Das Gleiche gilt auch für die spezifischen Beratungen im Bereich Cyber-Security.

- Kennzahlen Polizeiliche Kriminalstatistik 2021:



Dieser Auszug aus der Polizeilichen Kriminalstatistik des Kantons Schwyz zeigt die Deliktentwicklung für das Jahr 2021 im Vergleich zu 2020 für bestimmte Straftatbestände auf, die im Zusammenhang mit Cyberkriminalität stehen. Es handelt sich dabei um Cyberdelikte im engeren Sinne (z. B. Hackerangriffe) oder Cyberdelikte im weiteren Sinne, bei denen das Internet als Tatmittel eingesetzt wird.

Die digitale Kriminalität wird anhand der Kombination «Straftat – Tatvorgehen» ermittelt. Sie umfasst 33 verschiedene Tatvorgehen und 28 Straftaten des Strafgesetzbuches, die in fünf grosse Bereiche gegliedert werden. Ein Grossteil der 2021 polizeilich registrierten Straftaten mit einer digitalen Komponente betrifft die «Cyber-Wirtschaftskriminalität» (87.4 %), gefolgt von «Cyber-Sexualdelikten» (9.9 %) sowie «Cyber-Rufschädigung und unlauteres Verhalten» (2.5 %).

Zusammengefasst wurden 2021 gegenüber 2020 im Kanton Schwyz 6 % weniger Delikte zur Anzeige gebracht. Konkret bedeutet dies ein Rückgang um 27 Anzeigen. Gesamtschweizerisch wird hingegen eine Zunahme um 24 % verzeichnet. Auch wenn die Zahlen im Kanton Schwyz im letzten Jahr etwas rückläufig waren, bestätigen die nationalen Daten nach wie einen rasanten Anstieg. Zu erwähnen ist in diesem Zusammenhang, dass die Zahlen in dieser Form erst seit 2020 so erfasst werden. Aus diesem Grund lassen sich noch keine genügend fundierten Aussagen über die weitere Entwicklung machen.

b) Qualität der Delikte hinsichtlich Schäden

Gemäss den im Rahmen der Polizeilichen Kriminalstatistik 2021 für den Kanton Schwyz ausgewiesenen Zahlen hat sich die Schadenssumme gegenüber 2020 von rund fünf Mio. Franken auf mehr als 15 Mio. Franken verdreifacht.

2. *Erachtet der Regierungsrat die eingesetzten Ressourcen als adäquat im Hinblick auf die Bedrohung / Bewältigung?*

a) *Personal*

Mit den derzeit zur Verfügung stehenden personellen Mittel ist es möglich, die Fallbearbeitungen zeitnah und in einer vertretbaren Tiefe zu tätigen. Dies gelingt mittels geschickter Priorisierung die verschiedensten Aufgaben. Inskünftig werden zur optimalen Aufklärung der Bevölkerung und der Unternehmen mittels umfassender Präventionsarbeit diesem Bereich ergänzende Ressourcen zugeteilt werden.

b) *Budget für andere Mittel*

Gemäss den bisherigen Erfahrungswerten fallen für die Aus- und Weiterbildung jährlich wiederkehrende Kosten von rund Fr. 60 000.-- und für die Ausrüstung (Büro-Infrastruktur, IT-Hardware, Software-Lizenzen) einmalige Kosten von mindestens Fr. 50 000.-- an. Um zum Beispiel die zukünftigen Anforderungen im Bereich der Transaktionsanalysen sicherzustellen, wird die Beschaffung weiterer IT-Werkzeuge geprüft. Auf dem Markt sind diesbezüglich Software-Lösungen vorhanden, die pro Jahr wiederkehrende Kosten von gegen Fr. 50 000.-- hervorrufen, im Gegenzug werden entsprechend Mannsstunden an Arbeit eingespart.

3. *Sind Anpassungen der Ressourcen in nächster Zeit geplant?*

a) *Kurzfristig*

Kurzfristig geht es operativ darum, dass sich der neu geschaffene Dienst Cybercrime konsolidiert, die Cyber-Ermittler fundiert ausgebildet werden, das Fachwissen innerhalb der Kantonspolizei gebündelt wird und entsprechend allen zeitnah und kundengerecht zur Verfügung steht. Ebenso sind die verschiedensten Schnittstellen auf kantonaler und nationaler Ebene sicherzustellen.

b) *Mittel- / Langfristig*

Der Personalbestand der Kantonspolizei wird jährlich durch den Regierungsrat festgelegt. Für das Jahr 2022 wurden fünf zusätzliche Stellen bewilligt. Für das Jahr 2023 werden bei der Kantonspolizei weitere 5.2 Stellen geschaffen.

Beschluss des Regierungsrates

1. Der Vorsteher des Sicherheitsdepartements wird beauftragt, die Antwort im Kantonsrat zu vertreten.

2. Zustellung: Mitglieder des Kantonsrates.

3. Zustellung elektronisch: Mitglieder des Regierungsrates; Staatsschreiber; Sekretariat des Kantonsrates; Staatskanzlei; Sicherheitsdepartement; Kantonspolizei.

Im Namen des Regierungsrates:

Dr. Mathias E. Brun
Staatsschreiber

