Regierungsrat des Kantons Schwyz

Beschluss Nr. 685/2018
Schwyz, 18. September 2018 / ju

Brauchen wir mehr Ressourcen gegen Cyber-Attacken?
Beantwortung der Interpellation I 12/18

1. Wortlaut der Interpellation

Am 7. Mai 2018 hat Kantonsrätin Dr. Karin Schwiter folgende Interpellation eingereicht:

*«Im Rahmen der diesjährigen Schwyzer Jugendsession diskutierte eine engagierte Gruppe Jugendparlamentarier*innen am 4. April im Kantonsratssaal über ihre Forderungen an die Politik. Nach einem Tag intensiver Recherchen, Debatten und Abstimmungen standen die Anliegen fest, die sie weiterverfolgen wollen.*
Unter anderem sind die Jugendlichen überzeugt, dass sich die Achillesferse der Schweiz in die digitale Welt verschoben hat: Die Gefahr steigt, dass die Schweiz Zielscheibe von Cyberangriffen wird. Diese veränderte Bedrohungslage stellt nicht nur das Militär vor neue Herausforderungen, sondern auch die Schwyzer Polizei. So zeigt die kürzlich erschienene polizeiliche Kriminalstatistik 2017, dass im Kanton Schwyz zwar insgesamt weniger Straftaten verübt wurden als im Vorjahr, die Anzahl Betrugsdelikte sich aber mehr als verdoppelt hat. Gemäss Polizeikommandant Damian Meier sind die meisten davon der Cyberkriminalität zuzuordnen.
*In ihrer Resolution fordern die Jugendparlamentarier*innen, dass die Ressourcen zur Abwehr und Bekämpfung von Cyberangriffen ausgebaut werden.*

In Anlehnung an die Überlegungen der Jugendlichen möchte ich den Regierungsrat deshalb gerne einladen, die folgenden Fragen zu beantworten:

1. *Welche Ressourcen stehen dem Kanton Schwyz gegenwärtig zur Abwehr und Bekämpfung von Cyberangriffen zur Verfügung?*
2. *Mit welchen Massnahmen wird die Schwyzer Polizei auf die markante Zunahme an Betrugsfällen im Bereich der Cyberkriminalität reagieren?*
3. *Welchen Bedarf sieht der Regierungsrat, die heute in diesen Bereichen eingesetzten Ressourcen zu verstärken, um für die neuen Herausforderungen der zunehmend digitalisierten Welt (Cyberangriffe und Cyberkriminalität) gewappnet zu sein?»*

2. Antwort des Regierungsrates

2.1 Allgemeines

Die zahlreichen Themenfelder rund um die "Cyberkriminalität" bedürfen vorab einer begrifflichen Unterscheidung bzw. Definition:

Als Cyberwar wird die kriegerische Auseinandersetzung im und um den virtuellen Raum, den Cyberraum, mit Mitteln vorwiegend aus dem Bereich der Informations- und Kommunikationstechnologie verstanden. Cyberwar wird von Staaten und ihren Institutionen geführt.

Eine Cyberattacke oder ein Cyberangriff ist der gezielte Angriff auf grössere, für eine spezifische Infrastruktur wichtige Rechnernetze von aussen. Die Angriffe erfolgen computerbasiert über Informations- und Kommunikationstechnologie. Betroffen sind Staaten, die Wirtschaft und/oder die Gesellschaft. Die Angriffe können individuell, politisch oder gesellschaftlich motiviert sein.

Von Cyberkriminalität wird gesprochen, wenn Straftaten unter Ausnutzung der Informations- und Kommunikationstechnologien (IT) begangen werden. Dabei sind verschiedenste Erscheinungsformen auszumachen. Cyberkriminalität wird nochmals unterschieden in Cyberkriminalität im engeren Sinn und digitale Kriminalität. Bei Ersterer sind die Schwachstellen der Informations- und Kommunikationstechnologien selbst das Angriffsziel und damit das Tatobjekt, während bei der digitalen Kriminalität diese nur als Tatmittel der Zielerreichung dient.

Die Cybersicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnologie und in diesem Sinn mit der Abwehr von Cyberangriffen aller Art.

Die Bekämpfung von Cyberkriminalität stützt sich in der Schweiz im Bereich der Strafverfolgung auf drei Säulen, nämlich:
- das Cyberboard;
- das Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK);
- das Vier-Stufe-Ausbildungsmodell (Pyramidenmodell).

Das Cyberboard ist eine Plattform von Kantonen und Bund. Die Bekämpfung von Cyberkriminalität muss von den Strafverfolgungsorganen der Kantone und des Bundes gemeinsam angegangen werden und ist damit faktische eine Verbundaufgabe. Das Cyberboard basiert auf den bisherigen Strukturen und Kompetenzen und setzt sich aus verschiedenen Vertretern der Strafverfolgungsbehörden der Kantone und des Bundes zusammen. Jeder Kanton ist im sogenannten Teilbereich Cyber-CASE durch einen Staatsanwalt (StA-SPoC [Staatsanwaltschafts–Single Point of Contact]) vertreten. Dieses Gremium bezweckt vor allem die Erstellung und Führung einer nationalen Fallübersicht, die Sicherstellung einer koordinierten Beratung sowie die Pflege eines Erfahrungsaustausches zu aktuellen Fällen bzw. Phänomenen.

NEDIK bezeichnet das "Netzwerk Ermittlungsunterstützung digitale Kriminalität". Es besteht aus den regionalen Cybercrime-Kompetenzzentren und dem durch das Bundesamt für Polizei (fedpol) geführten nationalen Cyber Competence Center. Ziel dieses Netzwerkes ist es, im Rahmen der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken die Strafbehörden zu befähigen, die Erkennung, Verhinderung, Bewältigung und Verfolgung von Straftaten effizient zu gestalten, die dazu erforderlichen Fach- und Methodenkompetenzen zu fördern, Spezialkräfte und Instrumente gegenseitig zu ergänzen und diese gemeinsam und aufeinander abgestimmt weiterzuentwickeln. NEDIK hat somit den Auftrag, fachliche und operative Unterstützung zu leisten.

Eine allfällige vierte Säule bilden die spezialisierten Ermittlungsdienste im Bereich Cyberkriminalität bei den kantonalen Polizeikorps oder der Bundeskriminalpolizei.

Das Pyramidenmodell besteht wiederum aus folgenden Stufen:

Stufe 1: Ausbildung der Mitarbeitenden der Polizeikorps mittels eines E-Learning Programms;
Stufe 2: Weiterbildung der Ermittler der Polizeikorps mittels eines Ausbildungskurses am Schweizerischen Polizeiinstitut (SPI);
Stufe 3: Weiterbildung von ausgewählten und spezialisierten Ermittlern der Polizeikorps mittels einer externen Weiterbildung an Fachhochschulen usw.;
Stufe 4: Anstellung von externen ausgebildeten Spezialisten (Fachhochschulen, Universitäten) in den regionalen und im nationalen Kompetenzzentren.

2.2 Beantwortung der Fragen

2.2.1 Welche Ressourcen stehen dem Kanton Schwyz gegenwärtig zur Abwehr und Bekämpfung von Cyberangriffen zur Verfügung?

Seit dem Jahr 2011 spielt der Kanton Schwyz für die schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) des Bundesamtes für Polizei (FEDPOL) eine grosse Rolle, indem das Schwyzer Polizeirecht Grundlage für die verdeckten Vorermittler des Bundes darstellt. Aufgrund derer Tätigkeit erhält der Kanton Schwyz regelmässig Anzeigen, die im Kanton Schwyz wohnende Personen betreffen bzw. bei denen die Tatausführung im Kanton Schwyz erfolgte. Meist betrifft dies Kinderpornographie. Im Weiteren meldet die Kantonspolizei Schwyz der KOBIK mittels einer vordefinierten Liste national bestimmte Cyber-Delikte. Die gemeldeten Delikte werden fallvergleichend analysiert, mit dem Ziel, Ermittlungsansätze, Schwerpunkte, neue Vorgehensweisen usw. zu erkennen. Im Zuge der Reorganisation der Bundeskriminalpolizei (BKP) des Bundesamtes für Polizei wurde die KOBIK sowohl personell wie auch das Tätigkeitsgebiet betreffend stark ausgebaut. Dies verbunden mit dem Ziel, ein nationales Cybercime-Zentrum zu errichten.

Die Kantonspolizei Schwyz verfügt jedoch noch über keine speziell ausgewiesenen personellen Ressourcen, die sich ausschliesslich der Bekämpfung der Cyberkriminalität widmen. Zurzeit wird diese Ermittlungsleistung von Mitarbeitern der Sicherheits- und Kriminalpolizei erbracht. Bei der Sicherheitspolizei sind dies insbesondere die Mitarbeitenden der Ortsposten und bei der Kriminalpolizei jene des Ermittlungsdienstes und des Dienstes für Wirtschaftsdelikte. Die Mitarbeitenden tätigen solche Ermittlungen im Rahmen ihrer originären Tätigkeit.

Bei der Kriminalpolizei besteht aber ein Kompetenzzentrum "Cybercrime". Es besteht aus sechs Personen, davon zwei Kader, welche diese Funktion im Kompetenzzentrum als Nebentätigkeit ausüben. Aufgabe des Kompetenzzentrums ist es unter anderem, spezifisches Fachwissen aufzubauen, es intern zu multiplizieren und den Mitarbeitenden als Fachstelle zur Verfügung zu stehen. So wurde bereits eine interne Hotline eingerichtet, welche werktags und zu Bürozeiten für die Front-Mitarbeitenden zur Verfügung steht. Zudem wird das Netzwerk zu ausserkantonalen Fachstellen gepflegt und in verschiedenen Fachgremien mitgearbeitet. Letztlich soll das Kompetenzzentrum in besonderen Fällen von Cyberkriminalität die Ermittlungen sicherstellen.
Bei der Kantonalen Staatsanwaltschaft ist ein Staatsanwalt bei der Wirtschaftsabteilung tätig, welcher den Kanton Schwyz im Cyberboard, Teilbereich Cyber-CASE, vertritt.

2.2.2 Mit welchen Massnahmen wird die Schwyzer Polizei auf die markante Zunahme an Betrugsfällen im Bereich der Cyberkriminalität reagieren?

Die Delikte im Bereich Cyberkriminalität, insbesondere bei der digitalen Kriminalität, werden voraussichtlich weiter stark zunehmen. Dies bedeutet aber nicht automatisch, dass es auch zu einer bedeutenden Verlagerung der Anzahl Delikte kommen wird. Vielmehr ist davon auszugehen, dass durch die relative Einfachheit der Handhabung des Tatmittels sowie der Zunahme der Kom-

plexität in der Ermittlung der Gesamtumfang (Cyber- plus normale Kriminalität) der zu bewältigenden Arbeit zunehmen wird.

Die Kantonspolizei Schwyz arbeitet bereits heute, zusammen mit dem Zentralschweizer Polizeikonkordat, im Cyberboard und in NEDIK mit. Mit einem Fachgremium IT-Ermittlungen, in welchem auch die Kantonspolizei Schwyz mit einem IT-Spezialisten vertreten ist, wird in der Zentralschweiz unter anderem eine koordinierte Weiterbildung und eine fachliche Ermittlungsunterstützung wahrgenommen. Die Ausbildung der Mitarbeitenden im Sinne der Pyramidenstufen 1 bis 3 stellt eine weitere kurzfristige Massnahme dar, um die fachliche Kompetenz bei Delikten der Cyberkriminalität sicherzustellen und zu erhalten. Das Kompetenzzentrum Cybercrime schliesslich stellt den fachspezifischen Support sowie die Cyberermittlungen sicher. Des Weiteren wird ein enger Kontakt mit dem StA-SPoC der Staatsanwaltschaften des Kantons Schwyz gepflegt.

2.2.3 Welchen Bedarf sieht der Regierungsrat, die heute in diesen Bereichen eingesetzten Ressourcen zu verstärken, um für die neuen Herausforderungen der zunehmend digitalisierten Welt (Cyberangriffe und Cyberkriminalität) gewappnet zu sein?

Die Kantonspolizei Schwyz beabsichtigt, einen Fachbereich Cybercrime zu schaffen und diesen mit spezialisierten Mitarbeitenden zu besetzen. Konkret geplant sind einstweilen zwei Cyber-Ermittler und ein Cyber-Techniker, bei denen alle Delikte und grossmehrheitlich die in diesem Zusammenhang geführten Ermittlungen im Bereich Cyberkriminalität zusammenlaufen sollen. Der Fachbereich soll insbesondere auch die Koordination innerhalb der Kantonspolizei Schwyz sowie zu kantonalen und nationalen Drittbehörden sicherstellen. Von grosser Bedeutung wird aber auch die Zusammenarbeit mit der kantonalen Staatsanwaltschaft bzw. dem StA-SPoC der Staatsanwaltschaft sein.

Nachdem bei der Kantonspolizei in den letzten Jahren bereits verschiedene organisatorische Anpassungen zur Verstärkung bestimmter Fachbereiche im Rahmen des bestehenden Stellenetats vorgenommen worden sind, würde dieser ohne Verzichtsplanung bei anderen Feldern nicht mehr ausreichen, um auch noch den neuen bzw. zusätzlichen Fachbereich Cybercrime personell auszustatten. Aus diesem Grund beabsichtigt der Regierungsrat eine leichte Erhöhung der bewilligten Stellen um zwei FTE (Full Time Equivalent). Der restliche Bedarf dagegen soll durch Verzicht in anderen Bereichen kompensiert werden.

2.3 Schlussfolgerung

Nach dem oben Ausgeführten ist klar, dass sich mit der fortschreitenden Digitalisierung auch im Bereich der Kriminalität Herausforderungen stellen, denen die betroffenen Strukturen hierzulande teilweise noch nicht vollumfänglich gewachsen sind. Wertungsfrei muss festgehalten werden, dass die entsprechende Entwicklung aber verfolgt und mit ihr Schritt gehalten werden muss. Das vorliegend angesprochene Thema der Ermittlung und Verfolgung von Straftaten durch Polizei und Staatsanwaltschaften bezieht sich naturgemäss schwergewichtig auf in konkreten Fällen bereits erfolgte Missbräuche der IT-Technologie. Deren tatsächliche strafrechtliche Ahndung und Verurteilung gestaltet sich aber regelmässig als schwierig und aufwändig, nicht zuletzt mit Blick auf die Tatsache, dass die entsprechenden Handlungen häufig aus dem Ausland begangen werden. Umso essentieller ist nach dem Gesagten daher sowohl bei den privaten als auch den staatlichen Akteuren eine adäquate, sachgerechte Vorsorge im technischen Bereich (Cyber-Defence) einerseits und beim IT-basierten (persönlichen) Konsumverhalten jedweder Art andererseits.

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 (unter Rückgabe der Akten); Kantonspolizei.

Im Namen des Regierungsrates:

Dr. Mathias E. Brun, Staatsschreiber