

**Auszug aus dem Protokoll
des Regierungsrates des Kantons Zürich**

KR-Nr. 250/2017

Sitzung vom 22. November 2017

**1076. Anfrage (Cyber-Crime-Abteilung ist trotz 20 Stellen
relativ «ohnmächtig»)**

Kantonsrat Nik Gugger, Winterthur, Kantonsrätin Nina Fehr Düsel, Küsnacht, und Kantonsrat Thomas Marthaler, Zürich, haben am 11. September 2017 folgende Anfrage eingereicht:

Wir bitten den Regierungsrat mögliche Schritte aufzuzeigen, damit der Kanton Zürich gewährleisten kann, dass genügend Ressourcen und Möglichkeiten bestehen, um Cyber-Crime-Tatbestände effizienter zu verfolgen.

Die Unterzeichnenden wurden alle in den Sommerferien vom gleichen FB-Profil belästigt, welches bis heute nicht gelöscht wurde, trotz zahlreicher Anzeigen. In unserem Namen und mit Angabe unserer Funktion als Kantonsräte wurden Bettelemails an sämtliche Email-Kontakte verschickt, siehe Tagesanzeiger vom 23.8.2017.

Den Internet-Usern wird heutzutage bewusst, dass sie auch bei kritischem Überprüfen aller Anfragen und Emails nicht gegen Missbrauch gefeit sind. Betrugsfälle im Internet nehmen gemäss Kantonspolizei Zürich immer mehr zu und es kann uns alle treffen. Die Täter gehen immer subtiler vor. Solche und ähnliche Betrugsfälle häufen sich. Dabei machen sich die Täter u. a. des (versuchten) Betrugs nach Art. 146 StGB und der unbefugten Datenbeschaffung nach Art. 143 StGB strafbar. Die Kantonspolizei verfügt über eine spezielle Cyber-Crime-Abteilung und dennoch sind sie in den meisten Fällen machtlos. Denn heute ist es bei solchen international vernetzten Tatbeständen sehr schwierig, die Personen z. B. via IP-Adresse ausfindig zu machen.

Auch bei den Netzwerken und Providern wie Facebook, Google oder Windows gibt es nur allgemeine Meldeformulare und keine Kontaktpersonen. Man kann froh sein, wenn das Ganze überhaupt geprüft wird. Hier müsste die Cyber-Crime-Abteilung der Kapo Zürich rigorosere vorgehen können. Fakt ist: Die Tatbestände nehmen zu und können verheerende Ausmasse annehmen. Der Schaden kann immens sein. Umso wichtiger ist, dass die Legislative und die Gerichte diese zunehmende Gefahr erkennen und entsprechende Mittel bereitstellen. Sobald sich die Täterin oder der Täter im Ausland befindet, braucht es beispielsweise Rechtshilfesuche. Diese werden nach heutigem Gesetzesstand aufgrund des Aufwandes erst bei sehr grossem Schaden durchgesetzt. Es ist höchste Zeit, dass in Cyber-Crime-Fällen massiv strenger vorgegangen wird.

In diesem Zusammenhang bitten wir den Regierungsrat folgende Fragen zu beantworten:

1. An welche Stellen können sich Cyber-Crime-Opfer im Kanton Zürich wenden?
2. Welche Möglichkeiten gibt es, um bspw. der Kantonspolizei im Bereich Cyber-Crime mehr Ressourcen/Handlungsspielraum zu erteilen? Evtl. auch mittels Fachkräften aus der Armee? (Bundesrat Guy Parmelin hat auch schon Ähnliches gefordert, hier müsste bewusst besser vernetzt werden.)
3. Was gedenkt die Cyber-Crime-Abteilung in Zukunft zu tun, damit sie nicht ohnmächtig nur den verwischten IP-Spuren nachrennt?
4. Arbeitet die Kapo ZH mit den Banken und Telefonkonzernen zusammen, welche eigene, sehr gute Cyber-Crime-Abteilungen haben?

Auf Antrag der Sicherheitsdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Nik Gugger, Winterthur, Nina Fehr Düsel, Küsnacht, und Thomas Marthaler, Zürich, wird wie folgt beantwortet:

Bei der Internet-Kriminalität ist zu unterscheiden zwischen den Straftaten gegen das Internet und seine Instrumente als sogenannte Cyber-Kriminalität im engeren Sinn (beispielsweise Hacking) und den übrigen Straftaten unter Zuhilfenahme von Mitteln und Vorgehensweisen der Internettechnologie (beispielsweise Cybermobbing). Im Rahmen der Kriminalitätsentwicklung kommt der Internet-Kriminalität eine wachsende Bedeutung zu. Im Jahr 2009 hat der Regierungsrat deren Bekämpfung denn auch erstmals als einen der Schwerpunkte der Strafverfolgung definiert. In der Folge beschloss der Regierungsrat im Jahr 2012 die Bildung eines entsprechenden Kompetenzzentrums der Staatsanwaltschaften und der Kantonspolizei mit Einbezug der Stadtpolizei Zürich. Dieses Kompetenzzentrum nahm den Betrieb Ende 2013 auf. Bis heute ist der Kanton Zürich der einzige Kanton, der ein solches Kompetenzzentrum in der Zusammenarbeit zwischen Staatsanwaltschaften und Polizei betreibt. Die Bündelung der Kräfte ermöglicht ein koordiniertes Vorgehen in den aufwendigen Untersuchungen in einem ebenso dynamischen wie schwierigen Umfeld. Mit Beschluss Nr. 113/2017 bewilligte der Regierungsrat zudem die Schaffung von 20 zusätzlichen Stellen für die Bekämpfung der Internet-Kriminalität (Kantonspolizei, Staatsanwaltschaften). Auch diese

Stellenschaffung unterstreicht die Bedeutung, die der Regierungsrat der Bekämpfung der Internet-Kriminalität beimisst. Mit den zusätzlichen Stellen sollen die Mittel im Kampf gegen Internetkriminelle wirkungsvoll gestärkt werden.

Zu Frage 1:

Strafanzeigen können auf jedem Polizeiposten oder mittels E-Mail (cybercrime@kapo.zh.ch) direkt bei der Abteilung Cybercrime der Kantonspolizei Zürich erstattet werden. In dringenden Fällen ist eine Benachrichtigung der Polizei auch über die Telefonnummer 117 möglich. Im Rahmen eines spezifischen Ausbildungskonzepts hat die Kantonspolizei 2017 rund 500 Frontmitarbeitende in der Befähigung für erste Sicherungsmassnahmen nach Anzeigen geschult.

Zu Fragen 2 und 3:

Kantonspolizei und Staatsanwaltschaften koordinieren ihre Tätigkeit zur Bekämpfung der Internet-Kriminalität sowohl national als auch international. Die Abteilung Cybercrime steht dabei in einem engen und regelmässigen Austausch mit den Bundesbehörden, namentlich auch der Armee, sowie mit den schweizerischen und internationalen Partnerkorps. Eine Problemstellung für die Strafverfolgung liegt oft darin, dass schweizerische Tochtergesellschaften von internationalen Unternehmen, die Internet- und andere Kommunikationsdienstleistungen erbringen, Editionen und andere Auskunftsleistungen unter Hinweis auf ihre im Ausland registrierte Muttergesellschaft verweigern.

Die Bearbeitung der Fälle von Internet-Kriminalität kann nicht ausschliesslich dem Kompetenzzentrum als spezialisiertem Dienst überlassen werden. Vor diesem Hintergrund hat die Kantonspolizei das Ausbildungskonzept PACE (Polizeiliche Ausbildung für Computer-Ermittlungen) erarbeitet und bereits grösstenteils umgesetzt. Das Konzept besteht darin, sämtlichen Ermittlerinnen und Ermittlern der Kriminalpolizei das für die Verfolgung der Internet-Kriminalität notwendige IT-Knowhow, insbesondere Kenntnisse im Erkennen und Verfolgen digitaler Spuren, zu vermitteln. Damit kann die Abteilung Cybercrime den hierfür geschulten und spezialisierten Ermittlerinnen und Ermittlern der Kriminalpolizei je nach Komplexität Fälle zur Bearbeitung zuweisen. Dies verstärkt die Mittel und vergrössert den Handlungsspielraum bei der Bekämpfung der Internet-Kriminalität.

Die Kantonspolizei ist daran, gemeinsam mit anderen Polizeikorps Präventionskonzepte zur Sensibilisierung von Internetnutzerinnen und -nutzern sowie zur Verhinderung künftiger Delikte zu entwickeln. Sie steht dabei auch im Kontakt zu privatwirtschaftlichen Unternehmungen.

Zu Frage 4:

Die Kantonspolizei pflegt im Bereich der Bekämpfung der Internet-Kriminalität einen regen Austausch mit privaten Unternehmungen. Bei Bedarf kann sie über die Bundeskriminalpolizei auch auf das Netzwerk des Vereins «Swiss Cyber Experts» und damit auf das entsprechende Knowhow von privaten IT-Unternehmungen zurückgreifen. Zwischen Bund und Verein besteht ein Kooperationsvertrag im Rahmen einer Public Private Partnership.

II. Mitteilung an die Mitglieder des Kantonsrates und des Regierungsrates sowie an die Sicherheitsdirektion.

Vor dem Regierungsrat
Der Staatsschreiber:
Husi