Regierungsrat des Kantons Uri

Auszug aus dem Protokoll
9. Februar 2021

Nr. 2021-74 R-540-19 Interpellation Michael Arnold, Altdorf, zur Cyberfitness der Kantonspolizei Uri; Antwort des Regierungsrats

I. Ausgangslage

Am 11. November 2020 reichte Landrat Michael Arnold, Altdorf, zusammen mit einem Mitunterzeichner eine Interpellation zur Cyberfitness der Kantonspolizei ein.

Der Interpellant erkundigt sich nach der Cyberfitness der Kantonspolizei Uri respektive nach deren Möglichkeiten zur Bekämpfung der Cyberkriminalität. Er verweist auf die Kriminalstatistik und den Rechenschaftsbericht über die kantonale Verwaltung und über die Rechtspflege des Kantons Uri, worin auf die Zunahme von Straftaten im Bereich Cyberkriminalität hingewiesen wird.

In diesem Zusammenhang wendet sich der Interpellant mit sieben Fragen an den Regierungsrat.

II. Vorbemerkungen

1. Begriffliche Definition

Die zahlreichen Themenfelder rund um die Cyberkriminalität bedürfen einer begrifflichen Definition. Von Cyberkriminalität wird gesprochen, wenn Straftaten unter Nutzung von Informations- und Kommunikationstechnologien begangen werden. Dabei sind verschiedene Erscheinungsformen auszumachen. Cyberkriminalität wird unterteilt in «Cyberkriminalität im engeren Sinn» und in «digitale Kriminalität». Bei ersterer sind Schwachstellen der Informations- und Kommunikationstechnologien das Angriffsziel (z. B. Phishing) und damit das Tatobjekt, während bei der digitalen Kriminalität diese lediglich als Tatmittel zur Zielerreichung dienen (z. B. digitale Erpressung, Kinderpornografie).

Eine Cyberattacke oder ein Cyberangriff sind der gezielte Angriff auf grössere für spezifische Infrastrukturen wichtige Rechnernetze von aussen (z. B. zur Informationsgewinnung oder Sabotage). Die Angriffe erfolgen computerbasiert via Informations- und Kommunikationstechnologie. Betroffen sind Staaten, die Wirtschaft oder die Gesellschaft. Die Angriffe können persönlich, politisch oder gesellschaftlich motiviert sein.

Als Cyberwar wird die kriegerische Auseinandersetzung im und um den virtuellen Raum mit Mitteln

vorwiegend aus dem Bereich der Informations- und Kommunikationstechnologie verstanden. Cyberwar wird von Staaten und deren Institutionen geführt.

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

2. Bekämpfung von Cyberkriminalität in der Schweiz

2.1 Säulenmodell

In der Schweiz stützt sich die Bekämpfung von Cyberkriminalität im Bereich der Strafverfolgung grundsätzlich auf drei Säulen, namentlich

- das Cyberboard,
- das Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung (NEDIK) sowie auf
- das Vier-Stufen-Ausbildungsmodell (Pyramidenmodell).

Eine vierte Säule bilden die spezialisierten Ermittlungsdienste im Bereich Cyberkriminalität bei grossen kantonalen Polizeikorps (Cybercrime-Kompetenzzentren) sowie der Bundeskriminalpolizei (Cyber Competence Center).

2.2 Cyberboard

Das Cyberboard ist eine Plattform mit verschiedenen Vertretern der Strafverfolgungsbehörden von Kantonen und Bund. Jeder Kanton ist im Teilbereich «Cyber-CASE» durch einen Staatsanwalt vertreten. Dieses Gremium bezweckt vor allem die Erstellung und Führung einer nationalen Fallübersicht, die Sicherstellung einer koordinierten Beratung sowie die Pflege eines Erfahrungsaustauschs zu aktuellen Fällen bzw. Phänomenen.

2.3 NEDIK

NEDIK besteht aus den regionalen Cybercrime-Kompetenzzentren und dem durch das Bundesamt für Polizei (fedpol) geführten nationalen Cyber Competence Center. Ziel dieses Netzwerks 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. Die effektive Fallbearbeitung zählt nicht zu den Aufgaben von NEDIK.

2.4 Vier-Stufen-Ausbildungsmodell

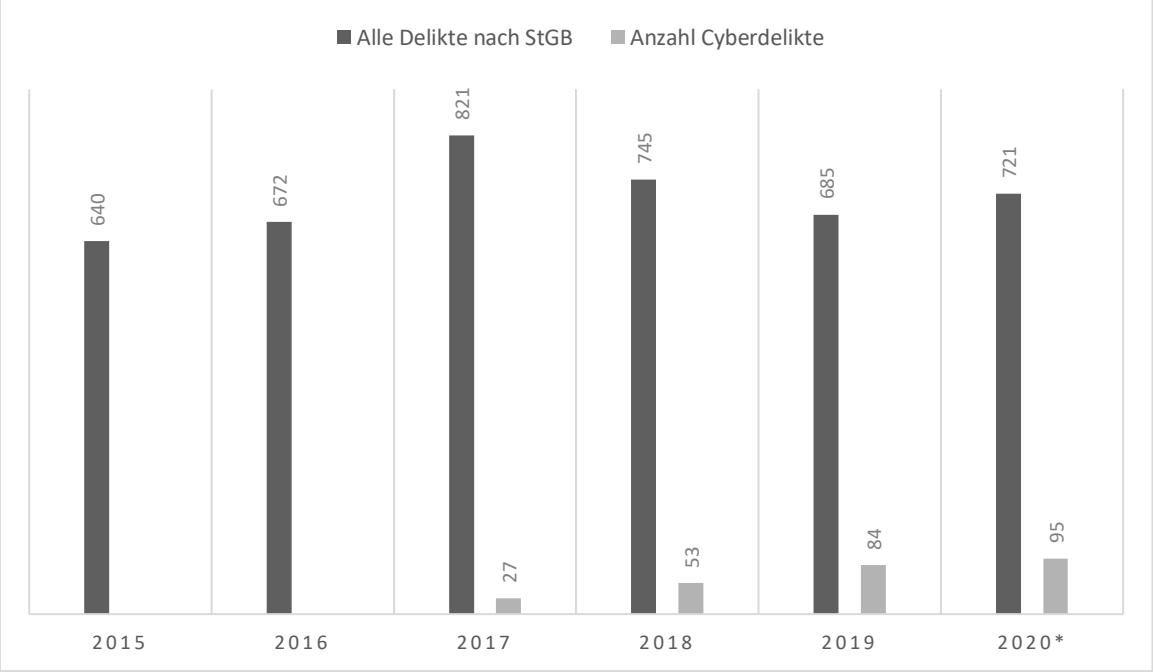
Im Bereich der Strafverfolgung stützt sich die Ausbildung auf das Vier-Stufen-Ausbildungsmodell (Pyramidenmodell).

- Stufe 1: Ausbildung aller Polizisten mittels eines E-Learning-Programms.
- Stufe 2: Weiterbildung der Mitarbeitenden der Kriminalpolizei mittels eines Ausbildungskurses am Schweizerischen Polizei-Institut (SPI).
- Stufe 3: Weiterbildung von ausgewählten und spezialisierten Ermittlerinnen und Ermittlern der Polizeikorps mittels einer externen Weiterbildung an Fachhochschulen.
- Stufe 4: Anstellung von extern ausgebildeten Spezialistinnen und Spezialisten (Fachhochschulen, Universitäten) im nationalen und in den regionalen Kompetenzzentren.

III. Antwort des Regierungsrats

1. Was sagt die Urner Kriminalstatistik aus, zur Abnahme der physischen Verbrechen und der Zunahme der «Cyberverbrechen»? Können die verschiedenen Verbrechen in Zahlen genannt werden resp. wie sind die Verbrechen anteilsmässig verteilt?

In der nationalen Kriminalstatistik des Bundesamts für Statistik (BFS) werden Cyberdelikte bislang nicht ausgewiesen. Sie werden jedoch seit dem Jahr 2017 separat erfasst. Auch wenn die definitiven Zahlen für das Jahr 2020 noch nicht vorliegen (die Statistik des BFS wird erst Ende März 2021 präsentiert), kann bereits heute gesagt werden, dass sich der Trend, der während der letzten Jahre feststellbar war, deutlich fortgesetzt hat. Während die Anzahl aller Delikte gemäss Strafgesetzbuch als volatil, aber stabil bezeichnet werden kann (Durchschnitt von 714 Delikten zwischen 2015 bis 2020), steigt die Zahl der Cyberdelikte weiterhin deutlich an. Im Kanton Uri hat sich ihre Zahl in der Zeit von 2017 bis ins Jahr 2020 mehr als verdreifacht. Die nachfolgende Tabelle zeigt die Entwicklung der Cyberdelikte im Verhältnis zur Anzahl aller Deliktsarten.



*) Zahlen berücksichtigt bis 9. Dezember 2020

Informatikmittel spielen heute praktisch bei sämtlichen Straftaten, angefangen bei Strassenverkehrsdelikten, bei Ehrverletzungsfällen, bei häuslicher Gewalt, bei Delikten gegen die sexuelle Integrität, bei Delikten gegen das Ausländer- und Integrationsgesetz bis hin zum Cyberdelikt im engeren Sinne,

eine zentrale Rolle.

In früheren Jahren war die Polizei im Rahmen von Strafverfahren damit beschäftigt, grosse Papiermengen sicherzustellen und auszuwerten (Agenden, Notizen, Buchhaltungen, Fotos usw.). Heute sieht dies ganz anders aus. Praktisch bei sämtlichen Deliktskategorien sind es vorwiegend elektronische Daten, die im Rahmen der digitalen Ermittlungen strafprozessual korrekt sichergestellt werden müssen, die anschliessend lesbar zu machen sind und schliesslich auch ausgewertet werden müssen. Diese Arbeiten sind deutlich komplexer und zeitaufwändiger als die frühere Arbeit mit Papier. Insbesondere die Systemvielfalt, Verschlüsselungen sowie die meist grossen Datenmengen sorgen dafür, dass Ermittlungen an Komplexität deutlich zugelegt haben.

Im Fall von Cyberdelikten im engeren Sinn hat die Täterschaft ihre Spur zudem oftmals durch den Einsatz von mehreren Servern, in unterschiedlichen Ländern platziert, verschleiert. Die meist sehr langen Wartefristen im Rahmen der internationalen Rechtshilfe spielen der Täterschaft in die Hände. Die Ermittlung der Verantwortlichen ist in grenzüberschreitenden Fällen leider die Ausnahme. Kommt dazu, dass laufend neue Phänomene feststellbar sind. Die Täter sind äusserst agil unterwegs, ändern ihr Vorgehen laufend und erschweren damit die Ermittlungen zusätzlich.

Aufgrund des anhaltenden Trends zur Digitalisierung dürfte sich die Zahl der Cyberdelikte in den nächsten Jahren noch einmal deutlich erhöhen. Cyberdelikte sind für die Täterschaft (leider) bequem begehbar. Die kriminellen Machenschaften können von überall auf der Welt, unabhängig von der Tageszeit, betrieben werden, das Risiko, in flagranti erwischt zu werden, ist dabei gering, und es ist relativ einfach, im Cyberspace seine Spuren zu verwischen.

2. *Mit einem wie grossen Graubereich, sogenannten nicht gemeldeter Fälle, in der Internetkriminalität muss gerechnet werden?*

Es muss von einer sehr hohen Dunkelziffer ausgegangen werden. Die Kantonspolizei schätzt diese auf gegen 80 Prozent. Oftmals werden die Opfer auf perfide Art und Weise um ihre Ersparnisse gebracht. Es ist anzunehmen, dass häufig aus Scham keine Anzeige bei der Polizei erstattet wird. So zum Beispiel, wenn ein junger Mann durch das Phänomen Sextortion (Androhung der Veröffentlichung von Nacktfotos) zu Geldüberweisungen genötigt wird. In solchen Fällen ist den Opfern das eigene Verhalten nachträglich oft sehr unangenehm und peinlich, sodass sie von einer Anzeigeerstattung absehen. Auch haben viele Opfer das Gefühl, dass sie selber Schuld seien an ihrer Situation, da sie auf E-Mails, Anrufe oder dergleichen hereingefallen sind und sich so selber in eine solche Lage gebracht haben.

3. *Ist das Korps sensibilisiert auf heikle und persönliche Fälle einzugehen?*

Ja. Die Kantonspolizei verfügt über gut geschulte Mitarbeitende, die es verstehen, auf heikle und persönliche Fälle einzugehen. Einfühlungsvermögen mit den Opfern ist bei sämtlichen Deliktsarten gefragt, nicht nur im Fall von Cyberkriminalität.

4. Ist das Know How bei der Bekämpfung von Cyberverbrechen genügend vorhanden oder gibt es einen Bedarf an Ausbildung innerhalb des bestehenden Korps resp. müsste über eine Aufstockung des Stellenetats diskutiert werden?

In den letzten Jahren hat die Kantonspolizei viel in ihre Cyberfitness investiert. Sämtliche Mitarbeitenden mit Polizeistatus haben die Ausbildung Stufe 1 durchlaufen. Zudem absolvieren alle Mitarbeitenden der Abteilung Kriminalpolizei die Ausbildung Stufe 2. Diese Ausbildungen sind bis heute noch nicht abgeschlossen, da bei den schweizerischen Kursen Kapazitätsengpässe bestehen.

Das Polizeikommando hat, nicht zuletzt aufgrund der Zunahme der Cyberfälle, per 1. Januar 2021 die Struktur der Abteilung Kriminalpolizei angepasst und acht Fachbereiche geschaffen. Dem Fachbereich «Cyberdelikte + IT-Ermittlung» sind drei (von total zwölf) Ermittler zugewiesen. Bei diesen Mitarbeitenden handelt es sich um kriminalpolizeiliche Allrounder mit einem Flair für IT-Belange. Es gilt jedoch darauf hinzuweisen, dass die betreffenden Mitarbeitenden auch Fälle ausserhalb des Bereichs Cyber zu bearbeiten haben. Aufgrund der aktuellen Ressourcensituation ist es nicht möglich, dass sich diese Mitarbeitenden ausschliesslich auf den Bereich Cyber konzentrieren können.

Bis heute haben keine Mitarbeitenden der Kantonspolizei die Ausbildungsstufe 3 durchlaufen. Mittel- bis langfristig ist geplant, dass ausgewählte Mitarbeitende der Kantonspolizei auch auf dieser Stufe eine Weiterbildung in Angriff nehmen. Eine Weiterbildung bis auf Stufe 4 ist bei der Kantonspolizei nicht vorgesehen. Diese Stufe ist ausschliesslich für jene Organisationen vorgesehen, die über Cyber-Kompetenzzentren verfügen (Kantonspolizei Bern, Genf und Zürich sowie Bundeskriminalpolizei).

Aufgrund des agilen Umfelds ist es wichtig, dass die Ausbildungen sämtlicher Mitarbeitenden laufend aufgefrischt werden und sich die Kantonspolizei den neu auftretenden Deliktsphänomenen anpasst. Der Ausbildungsaufwand im Bereich Cyber ist hoch und wird auch künftig hoch bleiben.

Das aktuelle Ermittlungsniveau der Kantonspolizei, bezogen auf den Bereich der digitalen Ermittlungen, ist knapp genügend. Der grösste Teil dieser Arbeiten kann das Polizeikorps mit eigenen Mitteln erledigen. Teilweise muss fallbezogen die Unterstützung anderer Korps beigezogen werden. Ungenügend ist das Niveau im Bereich der komplexeren Cyberdelikte im engeren Sinn. Bei diesen Delikten ist das Urner Polizeikorps zu grossen Teilen auf Unterstützung aus anderen Kantonen angewiesen.

Die heutigen Ressourcen im Bereich Cyber sind zu knapp bemessen. Im Rahmen der erfolgten Strukturanpassung innerhalb der Abteilung Kriminalpolizei hat sich gezeigt, dass die vorhandenen Personaleinheiten künftig nicht genügen. Das Urner Polizeikorps ist mittelfristig auf Mitarbeitende angewiesen, die sich ausschliesslich um Cyberfälle kümmern können und die im Fachbereich über die Ausbildungsstufe 3 verfügen. Der entsprechende zusätzliche Personalbedarf wird auf mindestens zwei Vollzeitstellen geschätzt. Die Zahl der Delikte und auch deren Komplexität werden, wie aufgezeigt, weiter deutlich ansteigen. Bei der Bearbeitung dieser Fälle wird sich der Kanton Uri nicht auf die Unterstützung durch Dritte verlassen können. Der Beizug von Spezialisten anderer Polizeikorps darf nicht zur Regel werden. Vor diesem Hintergrund ist eine Investition in zusätzliche Stellen zu prüfen.

Es wird zudem nicht genügen, einzig die Kapazitäten der Polizei im Bereich Cyber zu erhöhen. Im Gleichschritt wird es auch notwendig sein, aufseiten der Staatsanwaltschaft eine spezialisierte Stelle

zu schaffen, die über ein tiefgehendes technisches Verständnis verfügt und die Vorarbeiten der Polizei erfolgreich zum Abschluss bringen kann.

5. *Da der Datenschutz und auch die globale Verteilung der Betrüger eine Strafverfolgung erschweren, muss viel in die Prävention investiert werden, damit es möglichst wenige Betroffene gibt. Sind im Kanton Uri dazu genügend Ressourcen vorhanden?*

Die Kantonspolizei engagiert sich heute im Bereich der Prävention stark, einerseits mit Referaten an Schulen zum Umgang mit Sozialen Medien, andererseits auch mit Elternvorträgen zu dieser Thematik und zudem auch mit regelmässigen Warnmeldungen im Rahmen von Medienmitteilungen.

Trotz des betriebenen Aufwands werden Urnerinnen und Urner regelmässig Opfer von Cyberdelikten. Dies insbesondere deshalb, weil die Täterschaft äusserst raffiniert vorgeht und den Modus Operandi aus ihrer Optik laufend optimiert. Vor diesem Hintergrund muss auch der Bereich der Prävention verstärkt werden (z. B. Intensivierung Referate bei verschiedenen Altersgruppen, Präventionsveranstaltungen mit Finanzdienstleistern usw.). Die künftige Generation der potenziellen Opfer hält sich heute im Bereich der Sozialen Medien (Instagram, Tiktok, Facebook, Twitter u.a.m.) auf. Diese Kanäle können aus Kapazitätsgründen nicht bewirtschaftet werden. Um die Präventionsarbeit erfolgreicher zu gestalten, ist auch in diesem Bereich eine Investition in zusätzliche Stellenprozente unumgänglich.

6. *Bestehen Kooperationen mit anderen Zentralschweizer Korps? Gibt es allenfalls ein Kompetenzzentrum für entsprechende Anfragen (Prävention und Bekämpfung) oder regionale Zusammenarbeiten?*

Wie einleitend erwähnt, arbeiten die Polizeikorps zur Bekämpfung der Cyberkriminalität schweizweit im Rahmen von NEDIK zusammen. Auch auf Stufe Zentralschweiz besteht ein regelmässiger und sehr guter Austausch zwischen den Polizeikorps. Zudem kann in komplexen Verfahren fallweise die Unterstützung eines der vier existierenden schweizerischen Kompetenzzentren beigezogen werden.

Im Bereich der IT-Forensik besteht seit dem Jahr 2016 eine Verwaltungsvereinbarung mit der Zuger Polizei. Durch die Kantonspolizei bzw. die Staatsanwaltschaft sichergestellte elektronische Datenträger werden durch die Spezialisten der Zuger Polizei gesichert, ausgelesen und aufbereitet. Die Auswertung der Daten muss aber nach wie vor durch Mitarbeitende der Kantonspolizei Uri erfolgen.

7. *Wie können betroffene Unternehmen und Private im Bereich Cyber-Crime mit Unterstützung seitens der Polizei rechnen?*

Betroffene Unternehmen und Private können sich jederzeit persönlich, schriftlich oder per E-Mail an die Kantonspolizei wenden. Die angezeigten Straftaten werden entgegengenommen, bearbeitet und/oder die betroffenen Unternehmen/Personen bezüglich der nötigen Massnahmen beraten.

IV. Fazit

Auch wenn die Deliktszahlen in ihrer Gesamtheit in den vergangenen Jahren praktisch gleichgeblieben sind, ist der Aufwand zur kriminalpolizeilichen Bearbeitung der Fälle deutlich gestiegen. Die digitalen Ermittlungen sind anforderungsreicher und zeitintensiver als die bisherige Arbeit mit physisch vorliegendem Beweismaterial. Bei Cyberdelikten im engeren Sinn ist zudem ein hohes technisches Verständnis Voraussetzung dafür, dass die Täterschaft überführt werden kann. Vor diesem Hintergrund wird der Kanton Uri prüfen, ob die Cyberfitness mittelfristig verbessert werden muss, zumal davon auszugehen ist, dass die Anzahl der Cyberdelikte noch deutlich ansteigen wird.

Mitteilung an Mitglieder des Landrats (mit Interpellationstext); Mitglieder des Regierungsrats; Rathauspresse; Standeskanzlei; Amt für Kantonspolizei; Direktionssekretariat Sicherheitsdirektion; Landammannamt und Sicherheitsdirektion.

Im Auftrag des Regierungsrats
Standeskanzlei Uri
Der Kanzleidirektor