Beschluss Nr. 657/2026
Schwyz, 8. September 2026 / jh

Interpellation I 10/26: Ist die Kantonspolizei Schwyz für die Cyberkriminalität gewappnet?
Beantwortung

1. Wortlaut der Interpellation

Am 30. März 2026 haben Kantonsrat Karl Camenzind und drei Mitunterzeichner folgende Interpellation eingereicht:

«Die zunehmende Digitalisierung aller Lebensbereiche führt dazu, dass auch die Cyberkriminalität stetig an Bedeutung gewinnt. Laut Medienmitteilung der Kantonspolizei Schwyz vom 23. März 2026[1] nahmen die Straftaten der digitalen Kriminalität auch im vergangenen Jahr kontinuierlich zu. Sie stellt somit eine wachsende Bedrohung für Privatpersonen, Unternehmen und staatliche Institutionen dar. Straftaten wie Phishing, Ransomware-Angriffe, Identitätsdiebstahl oder Online-Betrug sind eine Herausforderung für die Strafuntersuchungsbehörden, der wirksam begegnet werden muss.

Die vorliegende Interpellation soll Klarheit über den aktuellen Stand im Kanton Schwyz schaffen und eine Grundlage für allfällige weitere Massnahmen bieten. Konkret stellen sich Fragen zur Organisation, Ressourcen sowie zur Aus- und Weiterbildung im Bereich Cyberkriminalität bei der Kantonspolizei Schwyz. Der Regierungsrat wird daher gebeten, folgende Fragen zu beantworten:

1. *Organisation und Ressourcen:*
   - *Über wie viele spezialisierte Stellen im Bereich Cyberkriminalität verfügt die Kantonspolizei Schwyz aktuell?*
   - *Wie haben sich diese Stellen in den letzten fünf Jahren entwickelt?*
   - *Ist ein weiterer Ausbau der Cybercrime-Einheiten geplant?*
2. *Fallzahlen und Entwicklung:*

[1] *https://www.sz.ch/verwaltung/sicherheitsdepartement/kantonspolizei/medienmitteilungen/detailseite.html/8756-8758-8802-9496-9613-10011-12161/news/24820*

- *Wie haben sich die Fallzahlen im Bereich Cyberkriminalität im Kanton Schwyz in den letzten Jahren entwickelt?*
- *Welche Deliktsarten stehen dabei im Vordergrund?*

3. *Zusammenarbeit:*
   - *Wie erfolgt die Zusammenarbeit mit anderen Kantonen, dem Bund (z. B. fedpol) sowie internationalen Behörden im Bereich Cyberkriminalität?*
   - *In welchen Netzwerken oder Kompetenzzentren ist der Kanton Schwyz eingebunden?*
4. *Ausbildung und Weiterbildung:*
   - *Wie wird das Thema Cyberkriminalität aktuell in der Grundausbildung der Polizistinnen und Polizisten im Kanton Schwyz vermittelt?*
   - *Welche spezifischen Weiterbildungsangebote bestehen für Mitarbeitende der Kantonspolizei im Bereich Cyberkriminalität?*
   - *Gibt es spezialisierte Ausbildungen für Cybercrime-Ermittlerinnen und -Ermittler?*
   - *Wie wird sichergestellt, dass das Wissen angesichts der rasanten technologischen Entwicklung laufend aktualisiert wird?*
5. *Prävention:*
   - *Welche Massnahmen ergreift die Kantonspolizei Schwyz zur Prävention von Cyberkriminalität in der Bevölkerung?*
   - *Gibt es gezielte Sensibilisierungskampagnen oder Kooperationen mit Schulen und Unternehmen?*
6. *Herausforderungen und Bedarf:*
   - *Wo sieht der Regierungsrat aktuell die grössten Herausforderungen im Bereich Cyberkriminalität?*

Wir bedanken uns für die Beantwortung der Fragen.»

2. Antwort des Regierungsrates

2.1 Allgemeine Bemerkungen

In den vergangenen Jahren sind die Fälle im Zusammenhang mit Digitaler Kriminalität massiv angestiegen. Auch im letzten Jahr nahm die Anzahl Fälle um sieben Prozent gegenüber dem Vorjahr zu. Nach einem Rekordjahr ging die angezeigte Schadenssumme im Zusammenhang mit Cybercrime im Kanton Schwyz im vergangenen Jahr zwar um 34 Prozent zurück, belief sich jedoch weiterhin auf hohen 14.4 Mio. Franken. Den grössten Anteil der registrierten Straftaten machte erneut die Cyber-Wirtschaftskriminalität aus. Besonders auffällig war dabei die Entwicklung im Bereich Phishing, welches mit einer Zunahme von 40 Prozent erneut deutlich hervorstach.

2.2 Beantwortung der Fragen

2.2.1 Organisation und Ressourcen

2.2.1.1 Über wie viele spezialisierte Stellen im Bereich Cyberkriminalität verfügt die Kantonspolizei Schwyz aktuell?

Die Kantonspolizei verfügt im Dienst Cyber- und Wirtschaftskriminalität im «Fachbereich Cybercrime» aktuell über drei Sachbearbeitende und ein Kader. Alle verfügen über eine Polizeiausbildung und haben sich im Bereich Cybercrime weitergebildet.

2.2.1.2 Wie haben sich diese Stellen in den letzten fünf Jahren entwickelt?

Bis ins Jahr 2019 verfügte die Kantonspolizei über keine speziell ausgewiesenen personellen Ressourcen, die sich ausschliesslich der Bekämpfung der Cyberkriminalität widmen konnten. Die Fälle wurden damals von den ordentlichen Mitarbeitenden der Sicherheits- und Kriminalpolizei bearbeitet. Bei der Sicherheitspolizei waren dies insbesondere die Mitarbeitenden der Ortsposten und bei der Kriminalpolizei jene des Ermittlungsdienstes sowie des ehemaligen Dienstes für Wirtschaftsdelikte. Bei der Kriminalpolizei existierte ein sogenanntes Kompetenzzentrum «Cybercrime». Dieses bestand aus sechs Personen, davon zwei Kader, welche die Bekämpfung von Cyberkriminalität als Nebentätigkeit ausübten.

Im Regierungsratsbeschluss Nr. 685/2018 vom 18. September 2018 (Beantwortung der Interpellation I 12/18) kam der Regierungsrat zu Schluss, dass die Cyberkriminalität, die Ermittlungskomplexität und die Arbeitslast stark zunehmen werden und bewilligte zwei Vollzeitstellen für den neu zu schaffenden Fachbereich «Cybercrime». Per 1. Oktober 2019 wurde innerhalb des damaligen Dienstes Wirtschaftsdelikte der «Fachbereich Cybercrime» geschaffen.

Mit Regierungsratsbeschluss Nr. 439/2021 vom 29. Juni 2021 nahm der Regierungsrat Bezug auf die erneute Zunahme der Fallzahlen, die professionellen Täterschaften und die internationalen Bezüge. Der Regierungsrat erkannte, dass der Cybercrime-Prävention künftig eine wichtige Rolle zukommen wird, was einen grossen Zusatzaufwand zur Folge haben würde. Entsprechend hiess der Regierungsrat eine weitere Aufstockung um zwei Vollzeitstellen per 1. Januar 2022 gut. Seither arbeiten vier Personen vollamtlich im «Fachbereich Cybercrime».

2.2.1.3 Ist ein weiterer Ausbau der Cybercrime-Einheiten geplant?

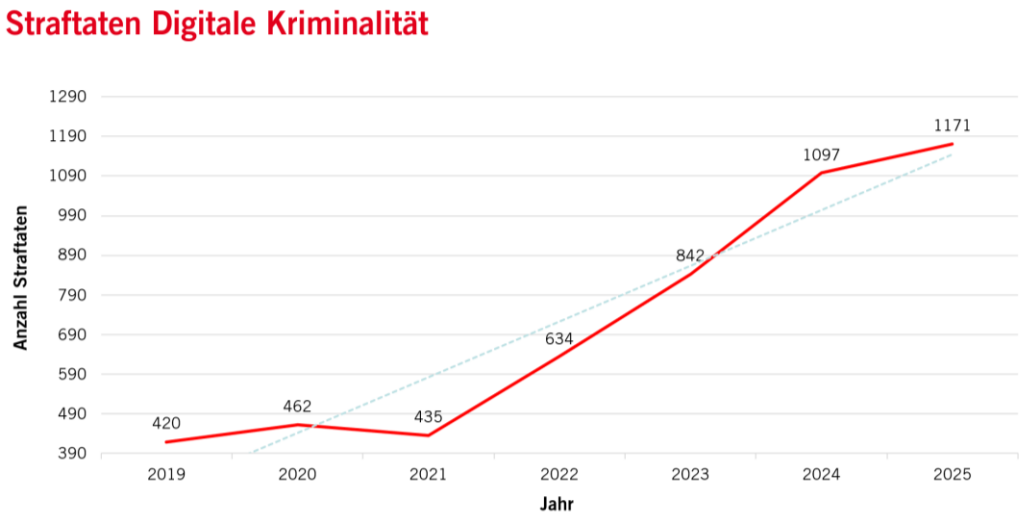
Die Kantonspolizei wird im «Fachbereich Cybercrime» per 1. Januar 2027 um eine weitere Vollzeitstelle verstärkt werden. Dies wird im Rahmen der ordentlich bewilligten Stellen und einer gezielten Prioritätensetzung geschehen. Dieser Bereich gehört damit zu den am stärksten zunehmenden Kriminalitätsbereichen, weshalb ein weiteres notwendiges «Schritt halten» zukünftig nicht ausgeschlossen werden kann.

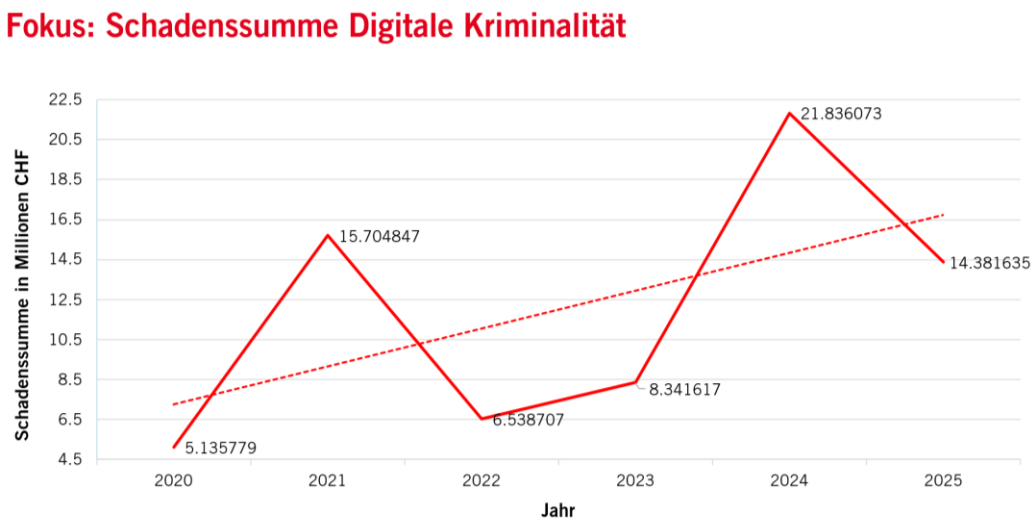
2.2.2 Fallzahlen und Entwicklung

2.2.2.1 Wie haben sich die Fallzahlen im Bereich Cyberkriminalität im Kanton Schwyz in den letzten Jahren entwickelt?

Seit dem Jahr 2020 werden in der polizeilichen Kriminalstatistik (PKS) explizit Straftaten in Zusammenhang mit der digitalen Kriminalität ausgewiesen. Diese Straftaten nahmen zwischen dem Jahr 2020 und 2025 im Kanton Schwyz erheblich zu:

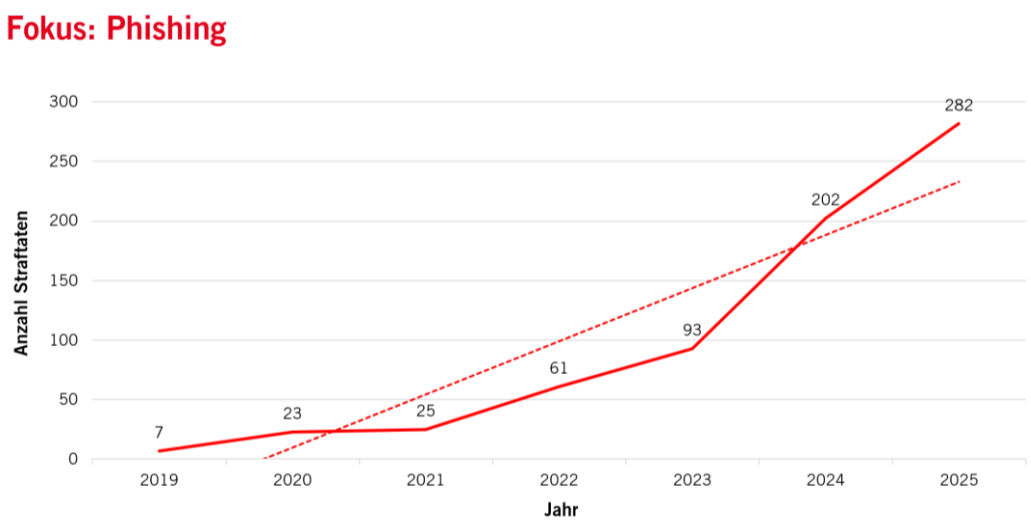
	2025	2024	2023	2022	2021	2020
Straftaten mit einem Modus Operandi der digitalen Kriminalität	1171	1097	842	634	435	462
Zunahme gegenüber Vorjahr	+ 7 %	+ 30 %	+ 33 %	+ 46 %	- 6 %	





2.2.2.2 Welche Deliktsarten stehen dabei im Vordergrund?

Im Vordergrund steht die Cyber-Wirtschaftskriminalität, insbesondere der Cyber-Betrug sowie das Phishing. Das nachfolgende Diagramm zeigt die Zunahme der Phishing-Straftaten von 2019 bis 2025 gemäss der kantonalen polizeilichen Kriminalstatistik:



2.2.3 Zusammenarbeit

2.2.3.1 Wie erfolgt die Zusammenarbeit mit anderen Kantonen, dem Bund (z. B. fedpol) sowie internationalen Behörden im Bereich Cyberkriminalität?

Die Zusammenarbeit im Bereich Cybercrime mit anderen Kantonen, dem Bund und internationalen Behörden verläuft erfolgreich. Alle zwei Wochen findet zwischen den Schweizern Polizeikorps ein virtuelles operatives Cybermeeting (OCM) statt. Dabei werden aktuelle Phänomene, neue Tatmuster und konkrete Schadensserien besprochen.

Zudem besteht eine enge Zusammenarbeit mit dem Netzwerk für die Ermittlungsunterstützung in der digitalen Internetkriminalität (NEDIK), welches unter anderem für die Sicherstellung von gegenseitigem Wissenstransfer zwischen den Kantonen verantwortlich ist und eng mit der Schweizerischen Kriminalprävention (SKP) und dem Bundesamt für Cybersicherheit (BACS) zusammenarbeitet.

Im Jahr 2023 arbeitete die Kantonspolizei beispielsweise mit der US-Justiz und der Joint Cybercrime Action Taskforce von Europol zusammen an einer Aktion gegen eine Ransomware-Gruppierung. Diese Gruppierung hatte zuvor auch Unternehmen im Kanton Schwyz geschädigt. Schliesslich konnte der Kopf der Gruppierung verhaftet werden.

2.2.3.2 In welchen Netzwerken oder Kompetenzzentren ist der Kanton Schwyz eingebunden?

Der Kanton Schwyz ist mit der Kantonspolizei in den beiden oben genannten Netzwerken (OCM und NEDIK) eingebunden. Darüber hinaus arbeitet der «Fachbereich Cybercrime» beim Gremium der IT-Ermittlungen des Zentralschweizer Polizeikonkordats, beim Informations- und Analysesystem zur Bekämpfung von Cyberkriminalität (PICSEL) sowie bei der nationalen Taskforce «TYR» – zur Bekämpfung von massenhaften Online-Falsch-Registrationen von Schweizer Mobiltelefonen und Bankkonten durch professionelle Täterschaften zwecks Betrugs – mit.

2.2.4 Ausbildung und Weiterbildung

2.2.4.1 Wie wird das Thema Cyberkriminalität aktuell in der Grundausbildung der Polizistinnen und Polizisten im Kanton Schwyz vermittelt?

Seit dem Jahr 2024 wurde die Cybercrime-Ausbildung an den Polizeischulen vertieft. Diese wird ergänzt durch E-Learnings des Schweizerischen Polizei-Instituts, durch interne Weiterbildungen, durch Beiträge auf dem Intranet sowie durch den Support des Fachbereichs Cybercrime.

2.2.4.2 Welche spezifischen Weiterbildungsangebote bestehen für Mitarbeitende der Kantonspolizei im Bereich Cyberkriminalität?

Geeignete Mitarbeitende der Kantonspolizei werden insbesondere in die Weiterbildung Cyber-Ermittlungen II des Schweizerischen Polizei-Instituts entsendet. Diese sind anschliessend die ersten Anlaufstellen auf den Polizeiposten für interne Fragen (sogenannte «Cyber-Satelliten») und können so den «Fachbereich Cybercrime» entlasten.

2.2.4.1 Gibt es spezialisierte Ausbildungen für Cybercrime-Ermittlerinnen und -Ermittler?

Es bestehen verschiedene spezialisierte Ausbildungen für Cybercrime-Ermittlerinnen und -Ermittler, die sowohl von staatlichen als auch von privaten Anbietern organisiert werden. Eine zentrale

Rolle spielt dabei NEDIK, welches diverse fachspezifische Weiterbildungen anbietet, beispielsweise in den Bereichen Open Source Intelligence (OSINT), Kryptowährungen und weiteren relevanten Themen. Darüber hinaus werden Weiterbildungen an verschiedenen Schulen absolviert. Dazu zählen unter anderem spezialisierte Lehrgänge wie das CAS Cyber Investigation and Digital Forensics. Ergänzend dazu werden auch Kurse von privaten Anbietern besucht, um sich spezifisches Fachwissen zu verwendeten Tools aneignen zu können.

2.2.4.2 Wie wird sichergestellt, dass das Wissen angesichts der rasanten technologischen Entwicklung laufend aktualisiert wird?

Die laufende Aktualisierung des Wissens im Bereich Cyberkriminalität ist eine Herausforderung und wird durch regelmässige und gezielte Weiterbildungen sichergestellt. Die Mitarbeitenden des «Fachbereichs Cybercrime» nehmen jährlich an unterschiedlichen Weiterbildungen teil, wobei auch internationale Angebote Teil davon sind, um von aktuellen Entwicklungen und Best Practices zu erfahren. Zusätzlich werden eigene Weiterbildungen organisiert. Diese stehen teilweise den anderen Zentralschweizern Polizeikorps offen.

2.2.5 Prävention

2.2.5.1 Welche Massnahmen ergreift die Kantonspolizei Schwyz zur Prävention von Cyberkriminalität in der Bevölkerung?

Die Kantonspolizei verfolgt im Zusammenhang mit der Cyberkriminalität ein seit mehreren Jahren etabliertes und kontinuierlich weiterentwickeltes Präventionskonzept. Dieses hat zum Ziel, die Bevölkerung, Unternehmen sowie Institutionen auf die Gefahren im digitalen Raum zu sensibilisieren und die Handlungskompetenzen im Umgang mit Cyberrisiken nachhaltig zu stärken.

Im Rahmen dieses Konzepts werden durch die Kantonspolizei jährlich rund 800 Arbeitsstunden gezielt in Cyber-Prävention investiert. Die Massnahmen sind vielfältig und umfassen unter anderem Informationsveranstaltungen, Standaktionen, Schulungen und Vorträge sowie Beratungen bei gemeldeten Verdachtsfällen. Ergänzend dazu werden in Zusammenarbeit mit nationalen und interkantonalen Partnern Sensibilisierungskampagnen durchgeführt, bei denen aktuelle Betrugsphänomene (z. B. Phishing, CEO-Fraud oder Romance-Scam) thematisiert und konkrete Verhaltenshinweise verbreitet werden. Die polizeilichen Cyber-Präventionsangebote stossen bei der Bevölkerung auf grosses Interesse, was sich in einer anhaltend hohen Nachfrage nach Veranstaltungen widerspiegelt.

2.2.5.2 Gibt es gezielte Sensibilisierungskampagnen oder Kooperationen mit Schulen und Unternehmen?

In der Zusammenarbeit mit den Schulträgern werden flächendeckende Präventionslektionen für die Zielgruppe Kinder und Jugendliche durchgeführt. Für Unternehmen und Vereine besteht das Angebot, polizeiliche Spezialisten für Referate oder Schulungen einzuladen. Für Unternehmen erfolgt die Sensibilisierung unter anderem über Drittpartner. Dabei werden beispielsweise Live-Events für die Mitarbeitenden organisiert, an denen aktuelle Cyberbedrohungen thematisiert und konkrete Handlungsempfehlungen vermittelt werden. Zudem erfolgt die Informationsverbreitung über bestehende Netzwerke, Verbände und Partnerorganisationen, wodurch eine breite Streuung relevanter Inhalte erreicht werden kann. Kontakte zu Unternehmen werden dabei gezielt branchenspezifisch gepflegt.

In den Volksschulen (Stufe Primar und Sek1) erfolgt die Präventionsarbeit flächendeckend im Rahmen des regulären Präventionsunterrichts, in der Sekundarstufe II auf Anfrage. Dabei werden Präventionsbotschaften mehrheitlich implizit vermittelt und zielen auf eine Sensibilisierung der Schülerinnen und Schüler ab.

Bei einer Häufung von ähnlich gelagerten Ereignissen informiert die Kantonspolizei die Bevölkerung zudem aktiv mittels Medienmitteilungen und Beiträgen auf den Social-Media-Kanälen über aktuelle Betrugsphänomene sowie die damit empfohlenen Verhaltensanweisungen. Insgesamt wird damit ein kombinierter Ansatz verfolgt, der sowohl breite, niederschwellige Sensibilisierung als auch gezielte, anlassbezogene Präventions-Vertiefungen umfasst.

2.2.6 Herausforderungen und Bedarf

2.2.6.1 Wo sieht der Regierungsrat aktuell die grössten Herausforderungen im Bereich Cyberkriminalität?

Der Regierungsrat sieht im Zusammenhang mit der Cyberkriminalität die grössten Herausforderungen insbesondere in den stetig steigenden Fallzahlen sowie in der zunehmenden Komplexität. Die Ermittlungsaufträge werden insgesamt aufwändiger und erfordern mehr Fachkenntnisse sowie einen erhöhten Ressourceneinsatz. Zur Bewältigung dieser Entwicklung wurden bei der Kantonspolizei verschiedene organisatorische und operative Massnahmen ergriffen. Dazu zählen unter anderem die Einführung eines strukturierten Cyber-Tagesdienstes, die systematische Kategorisierung von Cyber-Fällen sowie die Verwendung von Cyber-Musterrapporten zur Effizienzsteigerung. Zudem werden im «Fachbereich Cybercrime» Nebenämter reduziert und die Cyber-Fälle werden vermehrt auf die Polizeiposten verteilt.

Gleichzeitig müssen jedoch auch Einschränkungen vorgenommen werden. So können Cyber-Ermittlungen oftmals nicht mehr in der notwendigen Tiefe ausgeführt werden. Dies hat zur Folge, dass Zusammenhänge zwischen einzelnen Delikten teilweise nicht mehr erkannt werden und dadurch ein umfassendes Lagebild nur eingeschränkt erstellt werden kann. Mit der zusätzlichen Stelle bei der Kantonspolizei im «Fachbereich Cybercrime» per 1. Januar 2027 kann dem entgegengewirkt werden.

Beschluss des Regierungsrates

1. Erlass der vorliegenden Antwort zuhanden des Kantonsrates.

2. Zustellung: Mitglieder des Kantonsrates.

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

Im Namen des Regierungsrates:

Regierungsrat Kanton Schwyz

Dr. Mathias E. Brun
Staatsschreiber