



**Interpellation der CVP-Fraktion  
betreffend Sicherheit**

(Vorlage Nr. 2813.1 - 15643)

Antwort des Regierungsrats  
vom 26. Juni 2018

Sehr geehrter Herr Präsident  
Sehr geehrte Damen und Herren

Die CVP-Fraktion reichte am 19. Dezember 2017 eine Interpellation betreffend Sicherheit (Vorlage Nr. 2813.1 - 15643) ein. Der Kantonsrat überwies die Interpellation am 25. Januar 2018 an den Regierungsrat. Der Regierungsrat nimmt zu den in der Interpellation gestellten Fragen wie folgt Stellung:

**Einleitende Bemerkungen**

Die Interpellantin geht von einem umfassenden Verständnis von Sicherheit aus, das sich auf sämtliche Lebensbereiche erstreckt. Viele Bereiche fallen in die Zuständigkeit des Bundes, so beispielsweise die militärische Landesverteidigung (äussere Sicherheit), aber auch die meisten Sozialversicherungen (inkl. Altersvorsorge) und Teile der Finanz- und Wirtschaftspolitik. Der Kanton Zug kann diese Bereiche nicht direkt beeinflussen. Der Regierungsrat bringt seine Anliegen und seine Sichtweise aber aktiv beim Bund ein, namentlich im Rahmen von Vernehmlassungsverfahren und über interkantonale Konferenzen. Von besonderer Bedeutung ist hierbei der Sicherheitsverbund Schweiz (SVS), welcher alle sicherheitspolitischen Instrumente zwischen den verschiedenen Akteuren (Bund, Kanton, Gemeinden) koordiniert. Sein Fokus liegt bei der polizeilichen Gefahrenabwehr und der Wahrung der inneren Sicherheit, für welche grundsätzlich die Kantone zuständig sind.

Da die Behandlung sämtlicher sicherheitsrelevanter Belange den Rahmen einer Interpellation sprengt, nimmt der Regierungsrat zu ausgewählten Bereichen Stellung, welche für den Kanton Zug und dessen Bevölkerung aktuell und in absehbarer Zukunft von besonderer Bedeutung sind. Es handelt sich hierbei um die folgenden Bereiche:

- a) Bekämpfung von Radikalisierung und gewalttätigem Extremismus (Terrorismus)
- b) Schutz vor Cyberangriffen und Bekämpfung von Cyberkriminalität
- c) Sicherstellung des öffentlichen Gesundheitswesens.

*Frage 1: Für welche von solchen Veränderungen betroffenen Sicherheitsaufgaben erachtet sich der Regierungsrat als zuständig?*

**a) Bekämpfung von Radikalisierung und gewalttätigem Extremismus (Terrorismus)**

Die jüngere internationale Entwicklung, namentlich die Häufung von terroristischen Anschlägen in westlichen Ländern, zeigt die Notwendigkeit auf, die Sicherheitspolitik, die sicherheitsbezogenen rechtlichen Grundlagen und die Sicherheitsinstrumente an die aktuelle Lage anzupassen, damit zum Schutz der Bevölkerung adäquat auf Bedrohungen reagiert werden kann. Die Schweiz blieb bislang von terroristischen Anschlägen verschont, doch besteht auch hierzulande eine latente Gefahr von Anschlägen. Der Regierungsrat legt daher grossen Wert darauf, in Zusammenarbeit mit Bund, Kantonen und Gemeinden Massnahmen gegen Radikalisierung und gewalttätigen Extremismus zu ergreifen.

Der Bund hat zur Terrorismusbekämpfung drei Vorhaben lanciert. Ein erstes Vorhaben besteht aus Gesetzesänderungen im Strafrecht und in weiteren Gesetzen zur Strafverfolgung. Beabsichtigt ist die Aufnahme einer Strafbestimmung mit dem Verbot von Anwerbung, Ausbildung und Reisen zu terroristischen Zwecken (neu: Art. 260<sup>sexies</sup> StGB). Zudem soll die Bestimmung gegen kriminelle Organisationen (Art. 260<sup>ter</sup> StGB) überarbeitet und auf den Terrorismus ausgeweitet werden. Weitere Anpassungen umfassen das Rechtshilfegesetz, das Geldwäschereigesetz und das Nachrichtendienstgesetz. Der Regierungsrat hat am 19. September 2017 zu diesem Vorhaben Stellung genommen und die Gesetzesänderungen begrüsst. Da die Strafverfolgung im Bereich der Terrorismusbekämpfung im Wesentlichen in den Zuständigkeitsbereich des Bundes fällt, ergeben sich aus diesem Gesetzesvorhaben keine direkten Aufgaben für den Kanton Zug.

Das zweite Vorhaben ist das vom Bund geplante neue Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT). Es sieht verwaltungspolizeiliche Massnahmen gegen Gefährderinnen und Gefährder vor, beispielsweise eine regelmässige Meldepflicht. Weitere Massnahmen sind ein Ausreiseverbot, verbunden mit der Beschlagnahme des Reisepasses, ein Kontaktverbot sowie Ein- oder Ausgrenzungen. Letzteres bedeutet, dass eine Person ein bestimmtes Gebiet nicht verlassen darf oder dass ihr der Zugang zu einem bestimmten Gebiet oder Rayon verboten wird. Möglich ist auch ein Hausarrest (Eingrenzung auf eine Liegenschaft). Diese neuen Massnahmen werden ergänzt durch Kontroll- und Unterstützungsmassnahmen, beispielsweise durch Mobilfunklokalisierung und technische Ortungsgeräte wie die elektronische Fussfessel. Des Weiteren sieht der Gesetzesentwurf einen neuen Haftgrund im Hinblick auf die Landesverweisung von radikalisierten Ausländerinnen und Ausländern vor. Wer die innere oder äussere Sicherheit der Schweiz gefährdet, kann in Haft genommen werden, damit der Vollzug der Landesverweisung sichergestellt werden kann. Das PMT verbessert auch die Möglichkeiten von fedpol, Informationen zu beschaffen und diese mit den Kantonen auszutauschen. Schliesslich soll fedpol befugt werden, insbesondere im Internet und in elektronischen Medien verdeckt fahnden zu können, denn dies sind die bevorzugten Kommunikationskanäle krimineller Organisationen. Der Regierungsrat des Kantons Zug hat sich in seiner Vernehmlassung vom 20. März 2018 zum PMT grundsätzlich positiv geäussert, verlangt allerdings einige Ergänzungen, welche unter Frage 3 näher erläutert werden.

Als drittes Vorhaben hat der Sicherheitsverbund Schweiz (SVS) seit September 2016 einen nationalen Aktionsplan (NAP) erarbeitet. Der NAP ist Teil der Strategie der Schweiz zur Terrorismusbekämpfung, bei welcher die Prävention eine entscheidende Rolle spielt. Der NAP fördert das interdisziplinäre Vorgehen auf allen Ebenen des Staates gegen Radikalisierung und gewalttätigen Extremismus. Er schafft damit die Voraussetzungen dafür, dass Radikalisierung und gewalttätiger Extremismus in all ihren Formen erkannt und bekämpft werden können. Zu diesem Zweck sollen die heute schon unternommenen Anstrengungen gebündelt werden. Der NAP soll innerhalb von fünf Jahren umgesetzt und evaluiert werden. Die Umsetzung des NAP fällt zu einem wesentlichen Teil in den Zuständigkeitsbereich der Kantone. Der Regierungsrat verfolgt dieses Ziel aktiv und hat es deshalb auch in seiner Legislaturplanung berücksichtigt (vgl. hierzu die Antwort auf Frage 4). Der NAP orientiert sich am Grundgedanken, dass eine institutionalisierte interdisziplinäre Zusammenarbeit das wichtigste Element für eine wirkungsvolle Prävention ist. Diese sorgt für die Vernetzung der relevanten Akteurinnen und Akteure. Im Kanton Zug wurden die entsprechenden Fachstellen bezeichnet, die den lokalen Behörden und betroffenen Personen und Angehörigen für die Beratung und zur Vermittlung von Wissen zu Verfügung stehen. Zudem wurden Fachpersonen aus dem Erziehungs-, Sozial- und Jugendbereich sowie die Angehörigen der Zuger Polizei wie auch das Personal des Justizvollzugs für die Themen Radikalisierung und gewalttätigen Extremismus sensibilisiert und ausgebildet. So kön-

nen Anzeichen und Gefahren einer Radikalisierung frühzeitig erkannt und entsprechende Massnahmen eingeleitet werden.

Eine weitere Empfehlung des NAP hat den Aufbau eines behörden- und institutionsübergreifenden kantonalen Bedrohungsmanagements zum Gegenstand. Es soll von der Polizei geführt werden und ermöglichen, dass das Gefährdungspotenzial von Personen oder Gruppen, die der Polizei bereits bekannt sind, frühzeitig erkannt wird. Geeignete Instrumente sollen es erlauben, das Gefährdungspotenzial richtig einzuschätzen und mit geeigneten Massnahmen zu entschärfen. Zur Förderung des Ausstiegs und der Reintegration wurde ein Massnahmenkatalog nach interdisziplinärem Ansatz erstellt. Zudem wird empfohlen, dass jeder Kanton eine zuständige Behörde für die Betreuung radikalisierten Personen ausserhalb von Strafverfahren und Strafvollzug bezeichnet. Im Zusammenhang mit dem Entlastungsprogramm 2015–2018 muss im Kanton Zug zu jetzigen Zeitpunkt allerdings auf die Realisierung eines umfassenden Bedrohungsmanagements verzichtet werden. Auf der Basis der Erfahrungen anderer Kantone wären im Kanton Zug diesbezüglich zwei zusätzliche Personalstellen nötig. Die nunmehr vorgesehene redimensionierte Variante würde eine halbe Personalstelle benötigen, wobei die Zuger Polizei die neue Aufgabe indes mit den vorhandenen Personalressourcen umsetzen wird. Abstriche gegenüber dem empfohlenen Modell eines umfassenden Bedrohungsmanagements werden im Kanton Zug bei der konkreten Ausgestaltung von einzelnen Abläufen gemacht werden müssen. Die wesentlichen gesetzlichen Grundlagen eines kantonalen Bedrohungsmanagements werden jedoch durch die am 1. Januar 2019 in Kraft tretenden Anpassungen im Polizeigesetz (BGS 512.1) abgedeckt und erlauben auch den späteren Ausbau zu einem umfassenden Bedrohungsmanagement, falls sich die Bedrohungslage zukünftig ändern sollte.

#### **b) Schutz vor Cyberangriffen und Bekämpfung von Cyberkriminalität**

Die Digitalisierung verläuft mit hoher Geschwindigkeit und diese wird auch in Zukunft nicht abnehmen. Die Digitalisierung bietet der Gesellschaft und der Wirtschaft grosse Chancen, zugleich aber bestehen auch bedeutende Missbrauchsmöglichkeiten. Begriffe wie Spam, Trojaner, Cyberkrieg, Datendiebstahl und Cyberkriminalität stehen für immer grösser werdende Gefahren. Auf allen Ebenen werden Bestrebungen unternommen, um Schäden zu verhindern, sei es beim Bund, den Kantonen, Gemeinden oder bei Unternehmen. Dabei gilt es, die Missbrauchsmöglichkeiten zu minimieren, ohne die durch die Digitalisierung ermöglichten Freiräume und Innovationen zu beschränken. Zur Verhinderung von Cyberangriffen und Cyberkriminalität stehen nicht nur die Behörden auf allen staatlichen Ebenen, sondern auch die Unternehmen sowie die Bevölkerung in der Pflicht. Aufgrund von bisher entstandenen Schadenfällen und des zu erwartenden Schadenspotenzials haben die Unternehmungen in vielen Bereichen bereits stark investiert, um Cyberangriffe zu verhindern und Cyberkriminalität zu bekämpfen.

Die Bekämpfung der Cyberkriminalität und die Abwehr von Cyberangriffen werden sich weiterhin sehr dynamisch entwickeln. Auch für die öffentliche Hand stellt sich die Frage, in welchen Bereichen und auf welcher staatlichen Ebene Massnahmen sinnvoll oder gar rechtlich angezeigt sind. Da sich Cyberangriffe und -kriminalität nicht an staatliche Grenzen halten, die staatlichen Behörden, insbesondere die Strafverfolgungsbehörden hingegen territorial agieren, sollten nach Ansicht des Regierungsrats Massnahmen der öffentlichen Hand auf der obersten Staatsebene koordiniert werden. Dazu dient die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) 2018–2022. Um die unterschiedlichen Bestrebungen auf Bundes- und Kantonsebene abzustimmen, Doppelspurigkeiten zu vermeiden und gleichzeitig agil sowie effizient zu sein, braucht es auf nationaler Ebene eine ganzheitliche und vernetzte Herangehensweise der Strafverfolgung im Bereich der Cyberkriminalität. Polizei und Staatsanwaltschaften auf Bundes- und Kantonsebene haben sich daher geeinigt, ein Cyberboard als Koordinationsgremium für die Analyse der Ausgangslage und die Bearbeitung von Cybercrime-Meldungen zu schaffen. Zudem werden in der Schweiz im polizeilichen Bereich ein nationales und mehrere

regionale Kompetenzzentren geschaffen, die sich im «Netzwerk Ermittlungsunterstützung digitale Kriminalitätsbekämpfung» (NEDIK) zusammenschliessen. Damit sollen die Interoperabilität und die Reaktionsfähigkeit verbessert sowie fachliche, technische und personelle Kompetenzen aufeinander abgestimmt und gebündelt werden.

Da sich das Konzept Cyberboard derzeit in der Umsetzung befindet, wäre ein Vorpreschen eines einzelnen Kantons nicht zielführend. Der Regierungsrat erachtet sich daher vor allem zum Schutz der kantonalen Infrastrukturen vor Cyberangriffen und Cyberkriminalität als zuständig. So ist das Amt für Informatik und Organisation (AIO) verantwortlich für die Gewährleistung der Sicherheit, Verfügbarkeit und Integrität der kantonalen Informatik- und Kommunikationssysteme. Auf diese Systeme sind insbesondere die Notorganisationen des Kantons Zug, die Zuger Polizei und das Amt für Zivilschutz und Militär (AZM) sowie die relevanten Bundesstellen für die Bewältigung von Grossereignissen, Katastrophen oder Notlagen angewiesen. Auch haben sich im Sicherheitsverbund Schweiz (SVS) alle wichtigen Notorganisationen der Kantone und des Bundes organisiert, um im Verbund auch sicherheitspolitische Bedrohungen und Gefahren reagieren zu können. Dazu gehören auch Cyberangriffe. Im Bereich der Cyberkriminalität ist die Zuger Polizei sodann dafür zuständig und bestrebt, die entsprechenden Delikte zielgerichtet und wirksam aufzuklären zu können.

### **c) Sicherstellung des öffentlichen Gesundheitswesens**

Vom erweiterten Verständnis der Interpellantin des Begriffs Sicherheit wird auch das öffentliche Gesundheitswesen im Kanton Zug erfasst. Der Regierungsrat ist für dieses zuständig und übt die Oberaufsicht aus (§ 2 Abs. 1 des Gesetzes über das Gesundheitswesen im Kanton Zug [Gesundheitsgesetz, GesG; BGS 821.1]). Namentlich regelt er für die Berufe im Gesundheitswesen die fachlichen Voraussetzungen für die Erteilung der Berufsausübungsbewilligungen sowie die Berufsausübung (§ 6 Abs. 3 GesG). Zudem ist er zuständig für die Genehmigung von Tarifverträgen und die Festsetzung von Tarifen sowie die Spital- und Pflegeheimplanung (§ 3 Abs. 1 Bst. a und b des Einführungsgesetzes zum Bundesgesetz über die Krankenversicherung [BGS 842.1]). Bei der Sicherheit des Gesundheitswesens sind drei Dimensionen zu unterscheiden: Sicherheit bezüglich Angebot, Sicherheit bezüglich Qualität und Sicherheit bezüglich Bezahlbarkeit. Besonders letztere Dimension führt aufgrund stetig wachsender Kosten im Gesundheitswesen und ansteigender Krankenkassenprämien zu wachsender Besorgnis in der Bevölkerung.

*Frage 2: Wie beurteilt er die Risiken bezogen auf seine Zuständigkeiten?*

### **a) Bekämpfung von Radikalisierung und gewalttätigem Extremismus (Terrorismus)**

Terroranschläge können auch in der Schweiz nicht ausgeschlossen werden. Aktuell beurteilt der Bundesrat die Terrorrisiken als erhöht. Die Sicherheit der Schweiz wird laufend und umfassend auf Risiken und Verletzlichkeiten beurteilt. Es soll sichergestellt werden, dass entsprechende Vorzeichen früh erkannt und diesen mit geeigneten und wirkungsvollen rechtlichen Instrumenten begegnet werden kann.

Um in der Lage zu sein, terroristische Anschläge sowie andere ausserordentliche Ereignisse und deren Auswirkungen zu bewältigen, bedarf es eines etablierten Krisenmechanismus. Im Ereignisfall wäre mit mehreren Schadenplätzen und einer Gegenseite zu rechnen, die sehr schnell, spontan, teilweise auch unorganisiert und «zum Sterben bereit» handelt. Entsprechend wären die polizeilichen Interventionen mit einem sehr hohen Risiko für die eingesetzten Personen und einem massiven Mitteleinsatz verbunden. Um das Risiko, aufgrund einer mangelnden Einsatzerfahrung im Zusammenhang mit terroristisch motivierten Anschlägen den Einsatzerfolg

zu gefährden, möglichst zu minimieren, werden im Kanton Zug der kantonale Führungsstab und die Notorganisationen (Führungsorgane und Partnerorganisationen, wie der kantonale Führungsstab, die gemeindlichen Führungsstäbe, die Zuger Polizei, die Feuerwehren, das Gesundheitswesen, die technischen Betriebe sowie der Zivilschutz) regelmässig durch Ausbildung und wiederkehrende Übungen auf ihre Aufgaben im Verbund vorbereitet. Durch diese Stärkung der Widerstandsfähigkeit des Kantons Zug (Behörden, Gesellschaft, Infrastruktur etc.) wird sichergestellt, dass ein entsprechender Anschlag hinsichtlich der Ereignisbewältigung, Kommunikation und Betreuung der betroffenen Bevölkerung bewältigt werden könnte. Der Regierungsrat erachtet den Kanton Zug, insbesondere die Notorganisation und die Zuger Polizei, daher hinsichtlich der Risiken durch Terrorismus als gut vorbereitet, soweit dies bei solchen Ereignissen möglich ist.

#### **b) Schutz vor Cyberangriffen und Bekämpfung von Cyberkriminalität**

Cyberangriffe auf die Informatik- und Kommunikationssysteme des Kantons Zug erfolgen mehrmals täglich. Die am häufigsten attackierten Systeme sind Mail-, Web- und Extranet Server. Vielfältige und mehrschichtige Sicherheitsvorkehrungen verhindern, dass solche Angriffe erfolgreich sind. Die kantonalen Informatik- und Kommunikationssysteme werden durch technische und organisatorische Massnahmen mit erheblichem finanziellem und zeitlichem Aufwand vom AIO bezüglich Sicherheit und Verfügbarkeit betreut und gepflegt. Trotzdem kann eine hundertprozentige Sicherheit der Informatik- und Kommunikationsstruktur nicht garantiert werden. Deshalb hat das AIO im Rahmen der ISO 27001 Zertifizierung ein verbindliches Konzept eingeführt, das bei erfolgreichen Cyberangriffen zur Anwendung kommt. Dieser Prozess definiert das Vorgehen, die Zuständigkeiten und Kompetenzen im Notfall- und Krisenmanagement.

#### **c) Sicherstellung des öffentlichen Gesundheitswesens**

Der Regierungsrat beurteilt die Sicherheitssituation im Zuger Gesundheitswesen als sehr gut. Diese Einschätzung deckt sich weitgehend mit der Wahrnehmung der Bevölkerung. Das Sicherheitsgefühl der Bevölkerung bezüglich des Zuger Gesundheitswesens wurde 2014 in einer Befragung ermittelt. Demnach fühlen sich die Zugerinnen und Zuger hinsichtlich der Gesundheitsversorgung generell sicher. Das Sicherheitsgefühl bezogen auf einzelne Angebote ist ebenfalls gut. Kritisch wurde in der Umfrage hingegen die Verfügbarkeit von Plätzen in den Alters- und Pflegeheimen eingeschätzt. Zwischenzeitlich ist in diesem Bereich indes eine deutliche Entspannung eingetreten. Eine im September 2017 vorgelegte Studie des Schweizerischen Gesundheitsobservatoriums zeigt, dass die Alterung der Bevölkerung zwar auch im Kanton Zug einen erhöhten Pflegebettenbedarf mit sich bringt. Dieser kann jedoch mit den heute in den Zuger Pflegeheimen bestehenden Kapazitäten bis über das Jahr 2025 hinaus gedeckt werden, wenn Personen mit nur leichtem Pflegebedarf vermehrt ambulant betreut werden. Durchgehend erfreulich war die Einschätzung des Sicherheitsgefühls der Bevölkerung bezüglich der Qualität der Zuger Gesundheitsversorgung. Speziell gilt dies für die Qualität der Versorgung in Spitälern und im ärztlichen Bereich, aber auch in Apotheken, der Spitex sowie in Alters- und Pflegeheimen. Eine gewisse Unsicherheit besteht gemäss der Befragung hingegen bezüglich der Bezahlbarkeit des Gesundheitswesens. Der Aussage, dass bei der ärztlichen Behandlung die gesundheitlichen Bedürfnisse und nicht die Kosten im Zentrum stehen, wurde zugestimmt. Ebenso gilt dies für die Aussage, sich auch in Zukunft eine ausreichende Gesundheitsversorgung leisten zu können. Etwas tiefer war diese Überzeugung bei den Spitex-Diensten. Am tiefsten fiel die Beurteilung hinsichtlich der Bezahlbarkeit eines Alters- oder Pflegeheimplatzes aus. Der Regierungsrat nimmt diese Sorgen der Bevölkerung sehr ernst. Einerseits hat er eine Reihe von Massnahmen ergriffen, um das Kostenwachstum zu dämpfen, andererseits werden im Rahmen der Prämienverbilligung pro Jahr über 55 Mio. Franken eingesetzt, um die Gesundheitskosten von Haushalten in bescheidenen wirtschaftlichen Verhältnissen bedarfsgerecht zu reduzieren. In beiden Handlungsfeldern weist der Kanton Zug eine gute Erfolgsbilanz auf: Die Prämien gehören zu den tiefsten in der Schweiz und die Prämienverbilligung zu den besten.

*Frage 3: Macht der Regierungsrat einen Regelungsbedarf aus auf Stufe Kanton oder Bund, um allenfalls neuen Bedürfnissen im Bereich der Sicherheit Rechnung zu tragen und um insbesondere erkannten Risiken vorbeugend oder reagierend zu begegnen?*

**a) Bekämpfung von Radikalisierung und gewalttätigem Extremismus (Terrorismus)**

Auf Bundesebene befindet sich zurzeit das Bundesgesetz über polizeiliche Massnahmen zur Bekämpfung von Terrorismus (PMT) in Ausarbeitung. Mit diesem Gesetz will der Bundesrat dem fedpol die Kompetenz einräumen, im Internet und in elektronischen Medien auch ausserhalb eines Strafverfahrens verdeckt fahnden zu können, um terroristische Straftaten erkennen und bekämpfen zu können. Der Regierungsrat hat dieses Fahndungsmittel in seiner Vernehmlassung begrüsst und beantragt, dass eine verdeckte Fahndung auch ausserhalb des virtuellen Raums möglich sein soll.

Damit auch die Zuger Polizei im Rahmen ihrer präventiven Tätigkeit zur Erkennung und Verhinderung von Straftaten verdeckte Fahndungsmittel einsetzen kann, sieht der Regierungsrat vor, eine entsprechende Grundlage ins kantonale Polizeigesetz aufzunehmen. Da es sich hierbei nicht um strafprozessuale Massnahmen, sondern um präventive polizeiliche Tätigkeit handelt, liegt die Kompetenz zu ihrer Regelung bei den Kantonen.

Das PMT sieht weitere Massnahmen vor gegen Gefährderinnen und Gefährder, die auch nach Verbüsung einer Straftat eine Gefahr darstellen. Der Regierungsrat erachtet diese vorgeschlagenen Massnahmen als richtig und erforderlich, jedoch nicht als ausreichend. Er hat in seiner Vernehmlassung daher beantragt, dass im PMT die gesetzlichen Grundlagen geschaffen werden, damit gegen rechtskräftig verteilte Gefährderinnen und Gefährder nach Verbüsung ihrer Strafe gegebenenfalls eine gesicherte Unterbringung angeordnet werden kann. Dies soll dann möglich sein, wenn Gefährderinnen und Gefährder gemäss der kantonalen Risikoanalyse ein konkretes und ernsthaftes Rückfallrisiko für terroristische Straftaten aufweisen. Durch die gesicherte Unterbringung sollen weitere terroristische Straftaten durch diese Personen verhindert werden.

Der Regierungsrat hat zudem verlangt, dass im PMT der Informationsaustausch zwischen Bundesbehörden und kantonalen Organen ausdrücklich festzuhalten sei. Damit sollen gegenseitige Absprachen und die Koordination von Ermittlungen zur Abwehr von Gefährdungen im Bereich der inneren Sicherheit zwischen Bundesbehörden und den kantonalen Organen ermöglicht werden.

Regelungsbedarf sieht der Regierungsrat schliesslich im Bereich der Vernetzung von Datenbanken. Die föderalen Strukturen in der Schweiz mit lokal in den Kantonen gespeicherten Analysedaten verunmöglichen die schweizweite, effiziente und vernetzte Nutzung von kriminalistischen Analysetools und Datenbanken zur Früherkennung von potenziellen Straftäterinnen und Straftätern (unter anderem von hochseriellen reisenden Täterinnen und Tätern [Kriminaltourismus] und solchen mit erheblichem Schadenpotential). Aus diesem Grund ist eine schweizweite Vernetzung dieser Tools und Datenbanken aus Sicht des Regierungsrats erforderlich.

**b) Schutz vor Cyberangriffen und Bekämpfung von Cyberkriminalität**

Das sich derzeit in der parlamentarischen Beratung befindende neue Bundesgesetz über die Informationssicherheit beim Bund (ISG) verpflichtet die Kantone, eine gleichwertige Informationssicherheit wie der Bund zu gewährleisten. Die Kantone haben zudem die Umsetzung und Wirksamkeit der Massnahmen zur Sicherstellung der Informationssicherheit periodisch zu

überprüfen. Sobald das ISG verabschiedet ist und die bundesrechtlichen Vorgaben feststehen, wird der Regierungsrat prüfen, welche Änderungen der kantonalen Gesetzgebung zur Umsetzung dieser Vorgaben erforderlich sind, und diese Anpassungen in die Wege leiten.

**c) Sicherstellung des öffentlichen Gesundheitswesens**

Die gesetzlichen Grundlagen zur Gewährleistung der Sicherheit im Zuger Gesundheitswesen sind ausreichend. Ein zusätzlicher Regelungsbedarf besteht nicht.

*Frage 4: Was gedenkt der Regierungsrat in seiner Strategie ab 2019 zu berücksichtigen?*

**a) Bekämpfung von Radikalisierung und gewalttätigem Extremismus (Terrorismus)**

Der Regierungsrat hat die Bekämpfung von Radikalisierung und gewalttätigem Extremismus (Terrorismus) in seiner Strategie 2019–2026 unter dem Ziel «Kooperationen mit Gemeinden, angrenzenden Regionen, Kantonen und Bund festigen» aufgenommen und bei den Legislaturzielen 2019–2022 unter dem Thema «Mitwirkung bei koordinierter Verhinderung schwerer Straftaten» genauer definiert. Teilziel 1 des Legislaturziels besteht in der kantonalen Umsetzung des vom Bund, den Kantonen und den Gemeinden gemeinsam erarbeiteten Nationalen Aktionsplans (NAP). Die in fünf Handlungsfeldern zusammengefassten 26 Massnahmen des NAP sollen geprüft und im Verbund mit den betroffenen Ämtern und den Gemeinden realisiert werden. Damit sollen praxistaugliche Voraussetzungen für die frühzeitige Erkennung und Verhinderung von Radikalisierung und gewalttätigem Extremismus in all seinen Formen geschaffen werden. Das zweite Teilziel dient ebenfalls im Zusammenhang mit dem NAP und umfasst die Weiterentwicklung des Bedrohungsmanagements im Kanton Zug.

**b) Schutz vor Cyberangriffen und Bekämpfung von Cyberkriminalität**

Die Gewährleistung der Sicherheit, Verfügbarkeit und Integrität der Informatiksysteme ist ein strategisches Ziel der Informatikstrategie 2018–2022. Damit fliessen diese Aspekte indirekt auch in die Strategie 2019–2026 («Zuger Elan in anspruchsvollem Umfeld wahren») und in die Legislaturziele 2019–2022 ein, in welchen die Weiterentwicklung des E-Government und die Digitalisierung in der Verwaltung als Ziele genannt werden. Die Anforderungen in der Informatik bezüglich Sicherheit, Verfügbarkeit und Leistung bei gleichzeitiger Kosteneffizienz steigen, im Speziellen gilt dies für die Rechenzentren und Netzwerke. Ziel ist es, die IT-Infrastruktur möglichst störungsfrei zu betreiben. Im Bereich der Sicherheit gilt es, die Informatiksysteme permanent zu überwachen und gegen Bedrohungen und Risiken zu schützen. Für wichtige Kommunikations- und Informatiksysteme braucht es bei einem Totalausfall eine Rückfallebene (z.B. für Sprach- und Datenkommunikation). Das für die Notorganisationen bereitgestellte Zugernetz mit seinen Informatik- und Kommunikationssystemen soll redundant ausgelegt werden und es ist eine möglichst autonome Notstromversorgung zu gewährleisten als Schutz vor einem Stromausfall bei der öffentlichen Versorgung. Mittelfristig geht es primär darum, die Systemlandschaft zu konsolidieren und die Koordination bezüglich der Informations- und Kommunikationsmittel zu institutionalisieren. Im Fokus stehen Führungsinformatik- und Kommunikationsmittel im Verbund Kanton–Gemeinden oder im Verbund Kanton–Kanton. Auch müssen neue Informatik- und Kommunikationsmittel des Bundes für die schweizweite Ereignisbewältigung im Verbund berücksichtigt werden.

Ein weiteres Legislaturziel des Regierungsrats beinhaltet die Stärkung der Sicherheit im virtuellen Raum. Dieses Legislaturziel bildet Teil des Strategieziels «Erfolgsfaktoren im Fokus halten und stärken». Teilziel 1 betrifft die Verstärkung der Prävention im virtuellen Raum. Teilziel 2 befasst sich mit der Bekämpfung der zunehmend ansteigenden Cyberkriminalität. Die Anforderungen an die Cybercrime-Kompetenz der Strafverfolgungsbehörden und IT-Sicherheitsbeauftragten nehmen zu. Die Zusammenarbeit mit Forschungs- und Bildungseinrichtungen sowie

spezialisierten Zuger Firmen soll intensiviert werden mit dem Zweck, Informatikmittel sicher und kompetent zu nutzen, Schaden von Unternehmen und Privaten abzuwenden sowie bei Straftaten im virtuellen Raum zielgerichtet und wirksam aufklären zu können. Damit einhergehend soll der Bereich der Cyber-Ermittlung der Zuger Polizei personell durch Fachspezialisten verstärkt werden.

**c) Sicherstellung des öffentlichen Gesundheitswesens**

Die Sicherstellung der Gesundheitsversorgung gehört zu den Kernaufgaben des Kantons und hat dauerhaft oberste Priorität. Die bestehenden Risiken werden angemessen berücksichtigt. Eine Änderung oder Heraushebung einzelner Aspekte im Rahmen der Strategie des Regierungsrats ab 2019 ist daher nicht erforderlich.

**Antrag**

Kenntnisnahme.

Zug, 26. Juni 2018

Mit vorzüglicher Hochachtung

Regierungsrat des Kantons Zug

Die Frau Landammann: Manuela Weichelt-Picard

Die stv. Landschreiberin: Renée Spillmann Siegwart