17.3508

Motion Eder Joachim. Schaffung eines Cybersecurity-Kompetenzzentrums auf Stufe Bund

Motion Eder Joachim. Création d'un centre de compétence fédéral pour la cybersécurité

CHRONOLOGIE

STÄNDERAT/CONSEIL DES ETATS 19.09.17

Präsident (Bischofberger Ivo, Präsident): Der Bundesrat beantragt die Ablehnung der Motion.

Eder Joachim (RL, ZG): Der Bundesrat schreibt in seiner Stellungnahme vom 30. August 2017 unter anderem: "Der Bundesrat teilt die Ansicht des Motionärs, dass die zur Sicherstellung der Cybersecurity notwendigen Kompetenzen zu verstärken und bundesweit zu koordinieren sind. Er hat dazu mit der Melde- und Analysestelle Informationssicherung (Melani) ein Cybersecurity-Kompetenzzentrum auf Stufe Bund geschaffen."
Wenn man in der Stellungnahme weiterliest, ist man, Herr Bundesrat, eigentlich erstaunt, dass der Bundesrat als Gesamtgremium nicht die Annahme der Motion empfiehlt. Es fällt nämlich auf, dass die Landesregierung die Stossrichtung und Begründung des vorliegenden, immerhin von 22 Ständeratsmitgliedern unterstützten Vorstosses in jeder Beziehung akzeptiert, dass sie dann aber eine Schlussfolgerung zieht, die von niemandem, mit dem ich in Zusammenhang mit der Motion gesprochen habe, nachvollzogen werden kann. Ich übertreibe nicht. Es waren immerhin Cyberfachleute aus der Verwaltung, aus der Wirtschaft, von Infrastrukturbetreibern und aus der Wissenschaft. Ich erwähne dies speziell, weil der Kampf gegen und der Schutz vor Cyberrisiken eine gemeinsame Verantwortung von Wissenschaft, Wirtschaft, Gesellschaft und Staat ist.
Klar ist, dass es in der Bundesverwaltung viele gute Ansätze gibt, dass eifrig und nach bestem Willen gearbeitet wird, dass diverse Workshops und Veranstaltungen stattfinden – die nächste beispielsweise morgen zum Thema Cybersouveränität, organisiert von der Schweizerischen Akademie der technischen Wissenschaften in Zusammenarbeit mit dem VBS und seinem Cyberdefence-Beirat. Bundesrat Parmelin wird ebenfalls anwesend sein. Solche Foren sind gut und recht, sie reichen aber nicht, wenn man die grosse kriminelle Energie der potenziellen Angreifer in Betracht zieht. Der Handlungsbedarf ist deshalb unbestritten, ist es doch eine der Uraufgaben unseres Staates, der Bevölkerung die Sicherheit zu garantieren.
Dass die Bekämpfung von Cyberangriffen enorm wichtig ist, unterstreicht auch der kürzliche Angriff auf zwei Departemente. Er wurde am vergangenen Wochenende bekannt, wir haben bis heute inhaltlich nichts Näheres erfahren. Vielleicht kann der Herr Bundesrat uns dazu noch etwas sagen.
Unser Land ist also verwundbar. Die Bedrohungslage hat sich in letzter Zeit nicht nur deutlich verändert, sie hat sich auch intensiviert. Aus Sicht eines Verantwortlichen, der in der Bundesverwaltung mit seinen Leuten bereits jetzt gegen die zahlreichen und hochprofessionellen Cyberattacken kämpft, und zwar an vorderster Front, gibt es heute drei grosse Defizite:
1. Der Bund hat zu viele Koordinatoren und zu wenig Spezialisten – wenn ich die männliche Form nenne, meine ich selbstverständlich immer auch die Frauen. Er hat zu wenig Spezialisten, die wirklich etwas von der Sache verstehen.

AB 2017 S 662 / BO 2017 E 662

2. Die Cyberangriffe nehmen immer mehr zu, aber die Departemente haben noch keine Routine, wie sie damit umgehen sollen, das heisst, es wird noch zu viel improvisiert.
3. Das Thema Cyber hat beim Bund kein Gesicht, und das ist auch für die Öffentlichkeit schlecht.

Ich komme auf die vorliegende Stellungnahme des Bundesrates zurück. Melani wird kurzerhand als nationales Cybersecurity-Kompetenzzentrum bezeichnet. Nichts gegen die Melde- und Analysestelle Melani und nichts gegen die Personen, die dort arbeiten, sie machen einen guten Job, aber als eigentliches Cybersecurity-Kompetenzzentrum des Bundes wurde Melani bisher nicht wahrgenommen. In der 45-seitigen, noch gültigen nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken 2012–2017, die sechzehn konkrete Massnahmen entlang von sieben Handlungsfeldern vorschlägt, kommt das Wort Cybersecurity-Kompetenzzentrum nicht ein einziges Mal vor, geschweige denn im Zusammenhang mit Melani. Ich bitte Sie, Herr Bundesrat, um Verständnis für meine Einschätzung. Melani ist kein Cybersecurity-Kompetenzzentrum, sondern eine Plattform zum Informationsaustausch für kritische Infrastrukturen, das ist der geschlossene Kundenkreis, und für KMU, das ist der offene Kundenkreis.
Melani informiert und gibt in ihrer präventiven Rolle Empfehlungen ab. Auf der entsprechenden Website ist denn auch Folgendes zu lesen: "In der Melde- und Analysestelle Informationssicherung (Melani) arbeiten Partner zusammen, welche im Umfeld der Sicherheit von Computersystemen und des Internets sowie des Schutzes der schweizerischen kritischen Infrastrukturen tätig sind."
ETH-Professoren, die in der Vergangenheit von verschiedenen Bundesstellen in beratender Funktion zu Themen rund um die Cybersicherheit beigezogen wurden und somit die Strukturen in Bundesbern kennen, hielten mir gegenüber Folgendes fest: Das Thema Cybersecurity verlange zwangsläufig die Konsolidierung von zwei komplementären Betrachtungen, nämlich rückblickend, also reaktiv, und vorausschauend, also proaktiv. Rückblickende Aspekte umfassten die Feststellung und systematische Erfassung von erfolgten Angriffen und bekannten Sicherheitslücken sowie die Definition von Massnahmen. Vorausschauende Aspekte seien die systematische Erforschung von Sicherheitsrisiken, die Bereitstellung von Methoden für die Konstruktion sicherer Systeme, die Erforschung der Sicherheitstechnologie sowie die Bereitstellung eines umfassenden Aus- und Weiterbildungsangebots in all diesen Bereichen. Dieser Hinweis aus der Wissenschaft scheint mir wichtig, weil er aufzeigt, dass die Antwort des Bundesrates unter Verweis auf Melani zu kurz greift.
Ich gebe mich deshalb, das wird Sie nicht erstaunen, mit dem bundesrätlichen Standardsatz – "Wir verstehen zwar den Motionär, lehnen das Anliegen aber ab" – nicht zufrieden und beantrage Ihnen Annahme der Motion. Damit können wir einen wesentlichen Beitrag zur Verbesserung der Situation in unserem Land leisten. Das müsste eigentlich auch im Interesse des Bundesrates sein, denn der Zeitpunkt ist günstig. Gegenwärtig wird die nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS) überarbeitet und für die Jahre 2018 bis 2022 neu verabschiedet. Eine Möglichkeit wäre, den Aufbau des Kompetenzzentrums als Massnahme in die Weiterführung der NCS aufzunehmen. Insbesondere muss der Bundesrat aber dafür sorgen, dass die vorgesehenen und notwendigen Aktivitäten koordiniert und die Kräfte gebündelt werden.
Ein übergeordnetes, mit Weisungsbefugnis ausgestattetes Kompetenzzentrum, in das alle Departemente einbezogen sind, bietet dafür Gewähr. Es garantiert auch, dass Vertreter des Staates, der Wissenschaft bzw. der Hochschulen, der IT-Wirtschaft und der Betreiber der potenziell gefährdeten Infrastrukturen – ich denke an Energie, Verkehr und Banken – direkt in alle wichtigen Aktivitäten, Massnahmen und Entscheide einbezogen sind.
Beide Eidgenössischen Technischen Hochschulen in unserem Land, die anerkanntermassen internationale Leuchttürme sind, stimmen der Wichtigkeit eines Kompetenzzentrums bei und sind auch bereit, einen wesentlichen Beitrag für den Erfolg der Verteidigung des schweizerischen Cyberraums zu leisten. Ich sage dies nicht nur, sondern war diesbezüglich auch in direktem Kontakt mit den Herren Präsidenten Lino Guzzella von der ETH Zürich und Martin Vetterli von der EPF Lausanne, welche den Vorstoss unterstützen.
Abschliessend halte ich Folgendes fest: Herr Bundesrat, Ihre Kollegin, Frau Bundespräsidentin Doris Leuthard, hat in diesem Rat am 7. Juni 2017 anlässlich der Beratung des Geschäftsberichtes des Bundesrates 2016 in aller Offenheit betont – das haben wir geschätzt –, dass das Thema Cybersicherheit "vielleicht eine Zeit lang unterschätzt wurde oder nicht auf Stufe Gesamtbundesrat eingehend diskutiert wurde" (AB 2017 S 426).
Wenn Sie, geschätzte Kolleginnen und Kollegen, die Motion annehmen und Sie, Herr Bundesrat, die damit verbundene Forderung umsetzen, kommen wir auf dem Weg zu einer agilen, erfolgreichen, souveränen Schweiz im globalen Cyberraum einen wesentlichen Schritt weiter. Ich danke Ihnen für die Unterstützung.

Hêche Claude (S, JU): Le Conseil fédéral nous indique dans son avis: "Plus les menaces augmentent et visent des groupes larges, plus s'accroissent les exigences auxquelles doivent satisfaire les services compétents pour résister en cas d'incidents. En fonction de ces exigences, il faudra donc poursuivre le renforcement de Melani sur les plans technique et humain." Aujourd'hui, le besoin d'agir est indéniable, cela a été confirmé – cela vient d'être rappelé par Monsieur Eder – à la session d'été déjà lors du débat sur le rapport de gestion du Conseil fédéral, y compris par Madame Leuthard, présidente de la Confédération. Il y a donc urgence à agir,

la situation l'exige et les avis du Conseil fédéral ne sont pas pleinement satisfaisants.
En effet, on donne le sentiment que Melani, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information, va tout régler. Ce centre de compétence est un bon outil, mais ses effectifs, moins de vingt personnes, sont insuffisants. De plus, et c'est une de ses faiblesses, son mandat est limité. Par exemple, Melani n'est pas habilitée à donner des instructions aux autres départements et à la Chancellerie fédérale, elle ne peut véritablement jouer son rôle de coordinateur. A cela s'ajoute que la gestion des interfaces, notamment entre l'armée, dont l'organe de tutelle est le Département fédéral de la défense, de la protection de la population et des sports, et les six autres départements, n'est pas clarifiée. En clair, les compétences et les missions sont trop diluées.
Il y a donc lieu de créer un véritable centre de compétence fédéral pour la cybersécurité, qui aurait notamment pour mission et comme responsabilité de donner des instructions, d'assurer le rôle de coordinateur, l'élaboration d'une stratégie de prévention sur la base des expériences vécues, la formation, la collaboration et la communication auprès des instances civiles, militaires et économiques. Ainsi, cette nouvelle structure serait la véritable instance centralisée qui collaborerait avec les milieux académiques, les acteurs économiques, les exploitants des infrastructures importantes et sensibles et, c'est mon voeu, également avec les cantons.
Il y aurait lieu aussi de porter une attention renforcée aux acteurs économiques et à la relation avec ceux-ci. Je pense en particulier aux établissements bancaires, car ils sont régulièrement exposés. Ils ont donc de l'expérience et des compétences à partager.
Considérant que nous sommes dans le domaine de la sécurité, les moyens humains et financiers à engager devraient être pris en charge par le budget du Département fédéral de la défense, de la protection de la population et des sports. Il va de soi que l'objectif n'est pas de créer un doublon avec Melani, mais au contraire de l'intégrer dans la nouvelle structure. Une certaine légèreté et la limitation des moyens ne sont plus de mise, car il en va de la sécurité de la population, des infrastructures de base et de notre économie.
Par conséquent, je vous invite à soutenir la motion.

Savary Géraldine (S, VD): Comme Monsieur Hêche, je voudrais apporter moi aussi un soutien à cette motion. Aujourd'hui, nous avons le plaisir de profiter de la présence de Monsieur le conseiller fédéral Maurer, ministre des

finances. Pour examiner cette motion, il aurait été toutefois souhaitable que soient parmi nous Monsieur le conseiller fédéral Schneider-Ammann, qui s'occupe de la recherche, Monsieur le conseiller fédéral Parmelin, qui est en charge de la défense, Madame Leuthard, présidente de la Confédération, responsable du domaine des télécommunications, Madame la conseillère fédérale Sommaruga, qui s'occupe du secteur de la protection des données et le ou la successeur de Monsieur le conseiller fédéral Burkhalter pour la question des relations avec l'étranger.
Notre collègue Eder pointe du doigt un problème que le Conseil fédéral connaît. En matière de sécurité, il y a des systèmes et une structure qui fonctionnent sans doute par beau temps. De nombreuses séances ont lieu. Beaucoup de groupes, de structures et de collaborations entre les départements existent. Il y a des coopérations entre cantons, entre différents échelons de responsabilité dans notre pays. Mais, en cas de mauvais temps, de grain, de crise ou de menace potentielle ou réelle, notre système risque de s'enrayer. Hormis les menaces potentielles ou réelles, je pense que déjà aujourd'hui la multiplicité des compétences et des responsabilités empêche que des projets intéressants et novateurs soient financés, avancent ou soient mis en oeuvre. Ou les départements se renvoient la balle lorsqu'il s'agit du financement – "ce n'est pas mon domaine, ce n'est pas ma tâche, donc ce n'est pas à moi de financer cette prestation" –, ou ils considèrent que le département qui souhaite lancer un projet novateur n'est pas compétent et le projet est bloqué.
Je suis particulièrement sensible au domaine de la recherche, qui a été évoqué par Monsieur Eder, en particulier dans les hautes écoles. Je pense qu'on a là un immense potentiel à faire fructifier en matière de compétences sur les questions de cybersécurité, en particulier au sein des Ecoles polytechniques fédérales. Ces deux écoles polytechniques, à Lausanne et à Zurich, souhaitent avancer sur ce thème et mettre leurs compétences et leurs forces en commun. Un centre de compétence, tel qu'il a été présenté par Monsieur Eder, permettrait à ces écoles de travailler en collaboration avec la Confédération, et la Suisse pourrait devenir une référence reconnue en matière de recherche et de formation sur les cyberrisques.
Je conclurai en partageant avec vous un souvenir qui date d'il n'y a pas si longtemps, quatre ou cinq ans. J'étais à un débat sur les failles en matière de cybersécurité, et un responsable de la Confédération, je ne dirai pas de quel département, nous a dit que le meilleur moyen de détruire un ordinateur, c'est encore d'utiliser

un marteau. C'était il y a quatre ou cinq ans, cela veut dire que les discussions au sein de la Confédération avancent, mais parfois peut-être un peu trop lentement, vu les développements actuels et les cyberrisques qui menacent sans doute la Suisse.
Je crois que nous devons maintenant donner un coup d'accélérateur à ce dossier, et un des moyens qui, à mes yeux, seraient des plus efficaces, c'est un centre de compétence tel que celui qui est proposé par la voie de cette motion. Je vous demande donc de l'accepter.

Janiak Claude (S, BL): Ich weiss nicht, ob Sie die heutige "NZZ" gelesen haben. Darin ist ein interessanter Artikel eines Mitarbeiters von Herrn Bundesrat Maurer mit dem Titel "Der Aufbau einer Cyberforce ist dringlich". Ich zitiere daraus kurz: "Lange herrschte die Meinung vor, bei Krieg handle es sich um eine bewaffnete Auseinandersetzung zwischen Armeen. Die jüngsten Erfahrungen vor allem im Cyberbereich zeigen jedoch, dass es sich bei Krieg um ein Ereignis handelt, das weiter gefasst werden muss, nämlich, wie bereits von Clausewitz definiert, als die Weiterführung der Politik mit anderen Mitteln. Damit erhält auch die Armee als Mittel des Bundes zur Kriegsverhinderung und Landesverteidigung ein weiteres Aufgabenspektrum."
Ich bin ein bisschen stolz, dass ich vor zwei Jahren im Rahmen des Wahlkampfs folgenden Slogan verwendete – Slogans sind immer ein bisschen provokativ, aber das dürfen sie ja sein -: "Die neuen Kaliber unserer Bedrohung erkennen. Also mehr Informatiker im Sicherheitsbudget. Und weniger Infanteristen." Das war noch vor der Verabschiedung der Weiterentwicklung der Armee.
In einer von Globalisierung und Wettbewerb geprägten Welt ist die Schweiz Ziel von Spionageaktivitäten, die von privaten und staatlichen Akteuren, zunehmend unter Nutzung des Cyberraums, ausgehen. Sie kennen alle Fälle, die passiert sind. Ich kann Ihnen sagen: Als Mitglied der Delegation der GPK erfahre ich da relativ viel und darf sicher so viel sagen, dass ich beunruhigt bin. Neben systemrelevanten Unternehmen im Finanzsektor beherbergt die Schweiz ja auch noch internationale Organisationen sowie Handels-, Produktions- und Dienstleistungsunternehmen, die volkswirtschaftlich bedeutend sind.
Ich glaube, Handlungsbedarf ist erkannt; aber wenn ich zurückblicke, habe ich den Eindruck, dass wir bei diesem Thema schon ein bisschen ein langsames Tempo anschlagen. 2012 wurde die erste Strategie des Bundesrates verabschiedet. Sie war darauf ausgerichtet, Cyberrisiken frühzeitig zu erkennen, die Widerstandsfähigkeit der kritischen Infrastrukturen zu erhöhen und die Abwehr von Cyberspionage, Cybersabotage und Cybercrime zu stärken. Die Zielvorgaben waren sehr offen formuliert. Wie bereits erwähnt: Vorfälle in den letzten Jahren haben gezeigt, dass auch vieles nicht umgesetzt worden ist.
Der Nachrichtendienst hat seinen Grundauftrag 2015 neu formuliert. Im Vordergrund steht dort eben neu auch das Erkennen und Bekämpfen von Cyberattacken auf wichtige Infrastrukturen. Der Bundesrat hat ja, das hat Kollege Eder auch schon dargelegt, inzwischen auch beschlossen, eine neue Strategie ausarbeiten zu lassen. Der Beschluss datiert vom 26. April dieses Jahres. Ich habe einfach etwas Mühe mit dem Zeitplan, der uns da vorgeschlagen wird. Sie haben es damals auch von Bundespräsidentin Leuthard gehört, das war ja bei der Debatte über den Geschäftsbericht auch ein Thema. Da liest man, dass bis 2018 ein Kompetenzzentrum eingerichtet sein soll und dass die Mittel dann zur Verfügung gestellt werden müssen.
In der Stellungnahme heisst es am Schluss, man müsse es weiterentwickeln, man müsse darauf hinarbeiten, man müsse diese Punkte berücksichtigen, optimieren und wenn nötig ausbauen. Ich habe, wenn ich die Stellungnahme lese, einfach den Eindruck, dass man hier nach dem Grundsatz "Nume nid gsprängt!" geht. Meines Erachtens muss man hier eindeutig das Tempo erhöhen. Das ist auch der Grund, weshalb ich die Motion unterschrieben habe und sie auch unterstütze. Wenn ich daran denke, was alles gemacht wird, sehe ich einfach niemanden, der letztlich die Verantwortung trägt und den Überblick über alles hat, was in diesem Bereich in der Bundesverwaltung passiert. Unsere Nachbarn im Norden haben übrigens schon 2011 durch einen Kabinettsbeschluss ein Nationales Cyberabwehrzentrum geschaffen, also jemanden als Hauptverantwortlichen bezeichnet.
Ich denke, das Anliegen der Motion ist berechtigt. Ich bitte Sie, diese zu unterstützen.

Fetz Anita (S, BS): Ich möchte auf einen bestimmten Aspekt der Motion hinweisen. Ich unterstütze sie ebenfalls, möchte aber die Debatte nicht in dieser Unverbindlichkeit belassen. Ich glaube, darüber, dass wir mehr Cybersecurity brauchen und dass dafür ein Kompetenzzentrum mit der Teilnahme des Bundes, der IT-Wirtschaft und der Hochschulen sinnvoll und nötig ist, besteht Einigkeit. Ich frage: Wie wird das Ding finanziert? Das ist nämlich die entscheidende Frage! Darum "hötterlet" die Sache bis jetzt so dahin, mit Melani, mit hier ein bisschen, da ein bisschen, hinten noch ein bisschen. Das hat natürlich mit mangelnden Finanzen zu tun.
Jede relevante Nation hat heute in ihrem Militärbudget substanzielle Beiträge, um die IT-Forschung und die IT-Security zu sichern. Ich kann mir diese Motion, die Umsetzung des Cybersecurity-Kompetenzzentrums, nur

innerhalb des VBS-Budgets vorstellen, und zwar aus folgenden Gründen: Es ist sinnvoll, es dort anzusiedeln. In der IT-Forschung sind übrigens sehr spannende Innovationen aus der militärischen Forschung erfolgt. Mehrere Bausteine von Google kommen von dort, auch der Touchscreen der Smartphones, die wir jeden Tag benutzen, ist ein klassisches militärisches

Forschungselement. Ich habe nichts dagegen, wenn die Armee auch solche substanziellen Sachen erforscht und finanziert, weil es nämlich dazu dient, die Sicherheit zu erhöhen. Was ich mir auf keinen Fall vorstellen kann – einfach, damit dies einmal ausgesprochen ist –, ist, dass ein solches Zentrum dann auch noch über die Bildungsausgaben finanziert wird. Das möchte ich Ihnen einfach mitgeben. Bei einem Cybersecurity-Center, das seinen Namen verdient, gehen wir von mehreren Hundert Millionen Franken aus.
Es wäre also sehr viel vernünftiger gewesen, die 400 Millionen Franken, die wir in die Mörserabwehr oder Mörserhalbabwehr investiert haben – die wir brauchen, wenn wir schon besetzt und wenn unsere Infrastrukturen für Verkehr, Energie und Banken längstens gehackt sind –, in dieses Cybersecurity-Kompetenzzentrum zu investieren, das wir als Basis brauchen. Dem werde ich in dieser Form zustimmen. Aber die weitere Verfolgung und Umsetzung werde ich davon abhängig machen, dass diese Gelder dann innerhalb des VBS-Budgets organisiert werden. Das passt auch zum Auftrag einer Armee, die einen Verteidigungsauftrag hat, und ein Verteidigungsauftrag im 21. Jahrhundert ist es nun einmal, IT-Attacken abzuwehren und nicht unbedingt Lastwagen für eine halbe Milliarde in der Gegend herumzufahren und zu renovieren. Ich werde dem also zustimmen und nachher genau schauen, woher bzw. aus welchem Budget das Geld kommt.

Ettlin Erich (C, OW): Es ist ja schon fast langweilig: Es sind alle dafür, ich auch. Ich möchte aber noch etwas ergänzen, auch zum Votum von Frau Fetz. Madame Savary hat es schon gesagt, und auch ich glaube, dass wir in der Schweiz mit der ETHZ und der EPFL zwei tolle Institutionen haben. Es geht nicht darum, jetzt bezüglich Budget die Verteidigung gegen Bildung und Wissenschaft auszuspielen. Vielmehr muss man in der Konsequenz diese beiden Bereiche nahe zusammenführen. Meines Erachtens muss es das Kompetenzzentrum geben, das ist die einhellige Meinung. Es hat mit Sicherheit zu tun, aber nicht nur mit militärischer Abwehr. Es gibt ja auch die Industrie, auch der Datenschutz wurde erwähnt. Wir müssen das Kompetenzzentrum haben, aber es braucht eine enge Zusammenarbeit mit der Wissenschaft – das ist dann auch der Gewinn, den wir haben.
Was Start-ups betrifft, so machen es uns andere Länder vor; das wurde erwähnt. Da entstand aus dieser Zusammenarbeit von Verteidigung und Wissenschaft eine veritable Start-up-Szene. Hier müssen wir dann den Hebel ansetzen. Es ist ganz wichtig, jetzt nicht die Budgets gegeneinander auszuspielen, sondern das Kompetenzzentrum zu schaffen, und dann folgt die enge Zusammenarbeit, wie es Kollege Eder auch gesagt hat. Die Präsidenten der beiden Hochschulen sind enorm interessiert, und die Studenten sind es sicher auch. Wir müssen dieses Know-how aufnehmen und stärken.
Deshalb müssen wir zustimmen und dann für Lösungen offenbleiben, die nicht nur auf das VBS konzentriert sind.

Maurer Ueli, Bundesrat: Ich habe hier offensichtlich einen schweren Stand mit der Haltung des Bundesrates. Ich möchte aber doch einiges zu unserer aktuellen Situation sagen, denn ich bin klar der Meinung, dass Sie das, was wir machen, massiv unterschätzen. Dass wir so schlecht sind und nichts machen – so tönte es jetzt ein bisschen –, trifft nicht zu. Nehmen wir Melani: Das ist zwar ein harmloser Name, aber im Grunde genommen ist Melani der Kern eines Kompetenzzentrums. Hier ist sehr viel Erfahrung zusammengekommen. Wir müssen uns schon im Klaren darüber sein: In der Cyberabwehr geht es nicht um Quantität, sondern um Qualität. Selbstverständlich gehört es zu unserem Alltag, dass wir täglich irgendwo gehackt werden, und zwar nicht nur einmal, sondern unsere Systeme werden laufend angegriffen, wie das in der Privatwirtschaft auch der Fall ist. Die Tatsache, dass wenig passiert, ist auch ein Zeichen dafür, dass unsere Abwehr und unsere Leute nicht so schlecht sein können.
Zur Frage der Zusammenarbeit mit den Hochschulen, die Sie aufgeworfen haben, muss ich Ihnen sagen, dass sie im Alltag funktioniert: Auf dieser Stufe haben wir, wenn auch vielleicht nicht mit den beiden Rektoren, eine ordentliche Zusammenarbeit. Wir haben auch eine entsprechende Arbeitsgruppe, die Sie damals mit der Motion Rechsteiner Paul 13.3841 bewilligt haben. Hier sind sämtliche technischen Hochschulen und Universitäten dabei. Mit diesen erarbeiten wir zurzeit Massnahmen in Bezug auf die Sicherheit. Da sind wir daran, und der Bericht wird Anfang des nächsten Jahres abgeliefert.
Wir haben diese Expertengruppe auch in Bezug auf die Prüfung unserer Abwehrmassnahmen nach erfolgten Hackerangriffen einbezogen. Wir haben also diesen Experten unterbreitet, was wir gemacht haben, und die

kamen zusammengefasst zum Schluss: Okay, das habt ihr gut gemacht! Sie haben unsere Empfehlungen nur in einigen Punkten noch etwas präzisiert. Diese Zusammenarbeit mit den Hochschulen, die Sie bemängeln, funktioniert meiner Meinung nach recht gut. Auch ich habe Kontakte mit entsprechenden Leuten der Hochschulen, um mich auszutauschen.
Auch wenn ich es international vergleiche, komme ich zum Schluss, dass wir nicht so schlecht sind. Ich war vor zwei Wochen in Israel und habe mir die Sache angeschaut. Dort ist die Zusammenarbeit mit der Armee ein wesentliches Element. Da müssen wir uns nicht verstecken, habe ich das Gefühl. Ich werde in zwei Wochen in Estland sein und mir die Sache anschauen. Dort findet eine Konferenz statt, auch ein Austausch mit anderen. Wir kommen eigentlich immer wieder zum Schluss, wenn wir uns international vergleichen, dass wir zwar eine beschränkte Zahl an Leuten haben, dass wir aber im internationalen Vergleich eine gute Qualität in dieser Abwehr haben.
Es ist eine Tatsache, dass hier auf der Gegenseite aufgerüstet wird, und es ist auch eine Tatsache, dass wir versuchen, damit Schritt zu halten. Wir haben aber vor einigen Jahren auch in unserer Cyberstrategie, in unserer Sicherheitsstrategie gesagt, dass wir zwischen der zivilen Informatik und der militärischen Informatik unterscheiden, weil wir uns gesagt haben: Das ist kein Krieg, und die Armee hat hier nicht zivile Informatik zu verteidigen; vielmehr sind das zwei unterschiedliche Dinge.
Wir haben im Bereich der Armee ein entsprechendes Abwehrsystem, das meiner Meinung nach eigentlich auch gut funktioniert. Aber was Herr Eder gesagt hat – dass wir der Bevölkerung die Sicherheit garantieren sollen –, können Sie vergessen. Im Cyberbereich gibt es keine Garantien. Wir können alles vorkehren, damit wir sicher sind, aber Garantien gibt es nicht. Das ist ein zu interessanter Bereich, als dass die Gegenseite nicht entsprechend aufrüsten würde.
Melani hat Weisungsbefugnis über alle Departemente. Es ist also nicht so, dass da irgendwo im stillen Kämmerlein gewirkt wird, sondern immer wenn wir etwas feststellen und Massnahmen zur Verbesserung beschliessen, hat Melani eine direkte Weisungsbefugnis. Auch in Bezug auf die Ausbildung der entsprechenden Leute sind wir meiner Meinung nach auf einem recht guten Stand. Auch in Bezug auf neue Informatikprogramme hat schon bei der Bedürfnisabklärung und der Erstellung solcher neuen Programme die Sicherheit einen ganz entscheidenden Stellenwert. Das haben wir verbessert. Früher kam das ganz am Schluss: Man hat ein Programm gebaut und hat es dann geprüft. Jetzt ist die Sicherheit in diesen Programmen von Anfang an entsprechend integriert. Damit ist das, was diese Motion fordert, eigentlich bereits in einen laufenden Prozess der Verwaltung integriert. Aber selbstverständlich haben wir hier durchaus noch Bedarf, das weiter zu verbessern.
Unser Problem ist vielleicht, dass die EDV beim Bund in den letzten Jahrzehnten etwas organisch gewachsen ist. Wir haben gegen 3000 Anwendungen; etwa 20 Prozent der Leistungen sind standardisierte, die übrigen sind individuelle Anwendungen. Damit ist es auch ausserordentlich schwierig, in diesen Bereichen die Sicherheit zusammenzuführen. Das haben wir anerkannt. Ich habe Ihnen aber vorhin bei einem anderen Geschäft schon gesagt, dass der Bundesrat anlässlich einer Klausur erklärt habe, die Digitalisierung, die EDV, werde zur Chefsache und müsse "top-down" angeordnet werden. Damit werden wir in der Verwaltung da und dort noch auf Granit stossen. Hier sind eine gewisse Weisungsbefugnis von oben und eine gewisse Konzentration einfach notwendig, damit wir auch die Sicherheit besser im Griff haben.

AB 2017 S 665 / BO 2017 E 665

Ich glaube, Sie rennen offene Türen ein, wenn Sie die Motion annehmen. Wir arbeiten in diesen Bereichen – ob Sie dem dann Melani oder Kompetenzzentrum sagen. Das weiter auszubauen, haben auch wir im Sinn: Wir verfolgen die gleichen Ziele.
Aus unserer Sicht ist es nicht notwendig, dass Sie die Motion annehmen, weil wir eigentlich alles, was Sie gesagt haben, auch unterstützen und im Alltag umsetzen. Es gibt keine Bundesratssitzung, an der die Cybersicherheit kein Thema ist. Sie ist es aufgrund aktueller Vorfälle, aber auch sonst. Wir beschäftigen uns tatsächlich damit, ich kann Ihnen das einfach versichern. Das ist etwas, das wir wirklich ernst nehmen, etwas, das zuoberst auf unserer Traktandenliste steht. Wenn Sie Ihr Gewissen beruhigen wollen, dann können Sie diesen Vorstoss annehmen. Wir werden das Thema selbstverständlich noch ernster nehmen als jetzt, aber es ist eine Daueraufgabe, mit der wir uns auseinandersetzen.
Noch einmal möchte ich sagen: Unterschätzen Sie uns nicht! Unterschätzen Sie Melani nicht, denn die Leute, die dort arbeiten, die Kontakte und das Netzwerk sind gut! Selbstverständlich kommt nicht jede Erfolgsmeldung dann in den Medien, weil solche Dinge meist vertraulich behandelt werden. Es hat niemand Interesse, öffentlich zu erklären, er sei jetzt angegriffen worden, denn das schadet dem Ruf der Firmen und der Leute, die uns das melden. Ich bin aber überzeugt, und auch Ihre GPK hat diesbezüglich Einsicht nehmen können: So schlecht, wie das jetzt anscheinend dargestellt wurde, sind wir nicht. Wir sind auch noch nicht so gut, wie wir es einmal

sein müssen, aber wir sind auf dem Weg dorthin.
Zusammengefasst meine ich also, dass wir im Sinne der Motion arbeiten. Aus unserer Sicht ist es nicht mehr notwendig, dass Sie uns dabei noch mehr anfeuern.

Abstimmung – Vote
Für Annahme der Motion ... 41 Stimmen
Dagegen ... 4 Stimmen
(0 Enthaltungen)