Zwölfte Sitzung – Douzième séance

Dienstag, 13. März 2018
Mardi, 13 mars 2018

08.00 h

17.028

Informationssicherheitsgesetz

Loi sur la sécurité de l'information

Zweitrat – Deuxième Conseil

Ständerat/Conseil des Etats 04.12.17 (Erstrat – Premier Conseil)
Nationalrat/Conseil national 13.03.18 (Zweitrat – Deuxième Conseil)

Antrag der Mehrheit
Nichteintreten

Antrag der Minderheit
(Sommaruga Carlo, Flach, Fridez, Hardegger, Kälin, Mazzone, Munz, Quadranti)
Eintreten

Proposition de la majorité
Ne pas entrer en matière

Proposition de la minorité
(Sommaruga Carlo, Flach, Fridez, Hardegger, Kälin, Mazzone, Munz, Quadranti)
Entrer en matière

Gmür Alois (C, SZ), für die Kommission: Die Kommission befasste sich an zwei Sitzungen mit dem Informationssicherheitsgesetz. An der Januarsitzung wurde der Kommission von Nationalrat Pirmin Schwander der Mitbericht der Finanzkommission erläutert. Anlässlich dieser Sitzung wurde mit 21 zu 3 Stimmen bei 1 Enthaltung auf das Geschäft eingetreten. Es zeigte sich aber, dass bei den Kosten und dem zusätzlichen Personalbedarf grosse Unsicherheit herrscht und beides von der Verwaltung nur äusserst ungenau beziffert werden konnte. Es war die Rede von vier bis elf zusätzlichen Stellen, was grosse Ungenauigkeit bzw. fast einen Faktor 3 bedeutet.
Der Nationalrat ist Zweitrat. Der Ständerat hat bei der Beratung dieser Vorlage verlangt, dass er zu den Kosten dann nochmals konsultiert wird. Da die Kosten stark von den vorgesehenen Informationssicherheitsniveaus abhängen, wurde die Beratung des Gesetzes sistiert und die Verwaltung beauftragt, verschiedene aufgrund dieses Gesetzes mögliche Sicherheitsstandards zu beschreiben und möglichst genau die damit zusammenhängenden Kosten und den Personalbedarf aufzuzeigen.
An der Sitzung im Februar wurden der Kommission dann drei verschiedene Ambitionsniveaus präsentiert. Beim Ambitionsniveau 1, das gemäss Botschaft aktuell angestrebt wäre, hätten wir 9,5 bis 15,5 Stellen mehr und Kosten von 5 Millionen Franken. Das Ambitionsniveau 2 würde 42 Stellen und Betriebskosten von 33 bis 58 Millionen verursachen; das Ambitionsniveau 3 würde rund 78 Stellen und Kosten von 62 bis 87 Millionen Franken bedeuten. Der Bundesrat strebt momentan das tiefste Niveau, nämlich das Ambitionsniveau 1, an.
Es wurde auch erklärt, dass das Informationssicherheitsgesetz kein Informatiksicherheitsgesetz sei, das detaillierte Massnahmen der Informatiksicherheit beinhaltet, sondern dass diese Vorlage ein Informationssicherheitsmanagement-Gesetz sei. Dieses Informationssicherheitsmanagement beträfe die Informatiksicherheit, den Datenschutz, den Informationsschutz auch aus Sicht des Staatsschutzes, die Personensicherheitsprüfung und die Betriebssicherheitsverfahren sowie auch das Risikomanagement. Die Kosten von KMU für die Betriebssicherheitsverfahren könnten dem Bund in Rechnung gestellt werden. Die Kantone werden in dieses Informationssicherheitsmanagement mit einbezogen. Sie unterstützen dieses Gesetz, wollen aber nichts an die entstehenden Kosten bezahlen.
In der Kommission wurde dann der Mehrwert dieser Vorlage infrage gestellt. Es wurde festgestellt, dass der Aufwand bedeutend sei, daraus aber wenig Ertrag resultiere. Ein gewisser Handlungsbedarf bestehe, aber diesen Bedarf könne man mit einfachen Gesetzesanpassungen und bedeutend weniger Kosten abdecken. Die Mehrheit Ihrer Kommission kam zum Schluss, dass mit dem Gesetz ein zu grosser und zu komplexer Informationsschutzapparat aufgebaut würde, der hohe Kosten verursachen würde und eine Eigendynamik entfalten könnte und sich zunehmend der Kontrolle des Parlamentes entziehen würde. Eine hundertprozentige Sicherheit gäbe es auch mit diesem Gesetz nicht.
Die Minderheit hingegen sieht einen klaren Handlungsbedarf für einen gesamtheitlichen Ansatz, um die Informationssicherheit im Zuständigkeitsbereich des Bundes zu verbessern. Das vorgeschlagene Gesetz, das vom Ständerat mit nur wenigen Änderungen verabschiedet wurde, erlaube eine übersichtlichere Lösung als die heutigen Bestimmungen, die in verschiedenen Erlassen enthalten seien. Die Sicherheitslücken könnten geschlossen und die Koordination könnte stark verbessert werden. Die Kosten seien vertretbar. Die nötige Kontrolle durch das Parlament sei gewährleistet.
Ein Ordnungsantrag auf Rückkommen auf das Eintreten wurde in der Kommission mit 16 zu 9 Stimmen gutgeheissen. Es wurde dann nochmals über das Eintreten abgestimmt. Mit 16 zu 9 Stimmen wurde nicht auf die Vorlage eingetreten.
Deshalb beantrage ich Ihnen im Namen der Kommissionsmehrheit, nicht auf die Vorlage einzutreten.

Clottu Raymond (V, NE), pour la commission: Selon le Conseil fédéral, la sécurité de l'information au sein de la Confédération doit être adaptée aux défis actuels de la société d'information. Cette loi devrait créer, pour toutes les autorités fédérales, un cadre légal formel unique pour la protection de l'information et la sécurité des moyens informatiques. L'utilisation abusive d'informations, le vol de données ou la perturbation de systèmes d'informations sensibles peuvent nuire gravement aux intérêts de la Suisse et léser les droits de personnes physiques et morales. Le Conseil fédéral exige que ces menaces soient appréhendées et confrontées globalement et de manière coordonnée.
Cette exigence implique des mesures tant d'ordre juridique qu'organisationnel. Cette loi s'adresse en premier lieu aux autorités fédérales, y compris au Parlement, aux tribunaux fédéraux, au Ministère public de la Confédération et à la Banque nationale suisse. Les particuliers ainsi que les acteurs du secteur de l'économie ne sont concernés par cette loi que dans la mesure où ils exercent des activités sensibles sur mandat des autorités fédérales. Toutefois, le Conseil fédéral souhaite également améliorer la collaboration avec les cantons. Ceux-ci seront tenus d'assurer une sécurité égale à celle requise par la Confédération lorsqu'ils traitent des informations classifiées ou accèdent à des systèmes informatiques de la Confédération.
Notre commission s'est réunie les 22 et 23 janvier derniers et, dans un premier temps, est entrée en matière sur ce projet, par 21 voix contre 3 et 1 abstention. La majorité de la commission estimait que ce projet de loi pouvait contribuer à améliorer la sécurité de l'information relevant de la compétence de la Confédération.
Toutefois, notre commission s'interrogeait déjà sérieusement sur les conséquences de ce projet en termes de coûts. Afin de préparer la discussion par article, elle avait demandé au Département fédéral de la défense, de la protection de

la population et des sports de lui présenter une estimation plus précise des conséquences sur le plan des ressources financières et humaines, en tenant compte de différentes normes de sécurité possibles. Elle pensait poursuivre et clore l'examen de cet objet lors de sa prochaine séance en février dernier.

Ainsi, réunie les 19 et 20 février derniers, notre commission a poursuivi ses délibérations sur la base des informations complémentaires demandées au Département fédéral de la défense, de la protection de la population et des sports. Sur la base des informations reçues, la majorité de la commission est parvenue à la conclusion que cette loi mettrait en place un système de protection de l'information démesuré et beaucoup trop complexe qui ne générerait pas de valeur ajoutée déterminante. C'est la raison pour laquelle, par 16 voix contre 9, notre commission est revenue sur sa décision d'entrer en matière.

Pour la majorité de la commission, une telle loi ne ferait qu'alourdir la bureaucratie et ne pourrait que modestement contribuer à une mise en oeuvre uniforme des dispositions actuelles. Ce projet laisse aux autorités fédérale concernées, pour ce qui est de leur indépendance et de leur autonomie organisationnelle, un grand pouvoir d'appréciation dans la mise en oeuvre de cette loi, qui risquerait d'induire sa dynamique propre et de se soustraire peu à peu au contrôle du Parlement. La commission trouve particulièrement regrettable que, alors que l'élaboration de ce projet de loi a duré des années, les seules estimations disponibles concernant les conséquences financières soient sommaires et que les effets globaux de la loi, en termes de coûts et de personnel, ne pourront être évalués qu'à la lumière des ordonnances d'exécution.

Toujours selon la majorité de la commission, les problèmes signalés devraient être résolus dans le cadre des lois en vigueur et au moyen d'une meilleure coordination au sein de la Confédération et de ses services.

En conclusion, par 16 voix contre 9, la commission a décidé de ne pas entrer en matière, car ce projet de loi n'est pas une solution intelligible. La proposition de la minorité Sommaruga Carlo vise à entrer en matière; ses défenseurs estiment, au contraire, qu'il est évident que des mesures doivent être prises en vue d'une approche globale, afin d'améliorer la sécurité de l'information relevant de la compétence de la Confédération. Selon la minorité, la loi proposée constitue une solution plus intelligible que les dispositions actuelles, qui sont disséminées dans différents textes.

Sommaruga Carlo (S, GE): La profonde transformation du monde et de notre pays, provoquée par le développement rapide de l'informatique, de l'interconnexion digitale et du stockage numérique d'informations, place les autorités devant des défis majeurs. A côté des chances que la révolution numérique offre à notre économie et à notre population, il y a aussi des risques et des dangers majeurs. Ces dangers menacent notre pays. Il ne s'agit pas du risque d'invasion d'une armée d'infanterie bardée d'informatique ou de chars technologiquement ultrasophistiqués, mais de cyberattaques, d'intrusions sur les réseaux, de vols de données sensibles, de blocages d'installations sensibles. Cette menace n'est pas abstraite, elle est réelle et concrète, elle a déjà été mise à exécution contre le Département fédéral des affaires étrangères, contre Swisscom, qui s'est fait délester de dizaines de milliers de données personnelles, contre RUAG, l'entreprise d'armement de la Confédération, et contre des installations privées qui ont été infectées par le virus Wanna Cry, bien que dans une mesure moindre qu'en Grande-Bretagne. Il y a donc urgence à agir pour assurer une protection cohérente contre les cyberdangers et les risques qui pèsent sur les informations de masse ou les informations sensibles détenues ou gérées par nos institutions au sens large. Il s'agit également de protéger les infrastructures critiques dans les domaines de l'eau, de la santé, des transports, de l'énergie et de la défense, et d'éviter les risques liés aux personnes qui participent à la gestion de ces infrastructures et de l'Etat.

Aujourd'hui, le dispositif de sécurité de l'information est dispersé. Il se retrouve dans une multitude de lois, d'ordonnances qui couvrent des périmètres spécifiques, différents, et reposent sur des critères également divers. Il y a aussi des lacunes et des insuffisances notoires. Cette situation aboutit à des cas invraisemblables. Ainsi, lorsque la Banque nationale suisse veut se fournir en matériel informatique spécialisé, elle ne peut le faire seule. Elle doit passer, si elle veut un contrôle de sécurité, par le Département fédéral de la défense, de la protection de la population et des sports, car le dispositif légal actuel ne s'applique pas aux institutions étatiques externes. Les contrôles de sécurité des entreprises privées adjudicataires sur les marchés publics, dans les domaines sensibles, sont limités. Les contrôles de sécurité des personnes ne sont pas uniformes, ici, trop sévères, pour des postes à moindres risques, là, trop légers, lorsque les risques de sécurité sont importants.

Dans ce conseil, nous sommes largement d'accord sur le constat avec lequel le dispositif actuel est insuffisant et lacunaire puisque, en effet, nous submergeons le Conseil fédéral d'une multitude de motions, de postulats et d'interpellations visant au renforcement de la "IT security" de notre Etat.

Aujourd'hui, nous avons devant nous une proposition concrète du Conseil fédéral pour prendre des mesures importantes qui vont dans la bonne direction: c'est la loi sur la sécurité de l'information. Globalement, personne ne peut contester que cette loi apporte plus de cohérence et d'uniformité dans la mise en oeuvre de la sécurité numérique de nos autorités, qu'elle a un champ d'application plus large, qu'elle améliore le contrôle de sécurité des personnes et des entreprises soumissionnaires pour des infrastructures sensibles et qu'elle organise la collaboration avec les cantons. Même si nous pouvons avoir des divergences sur l'un ou l'autre point de la loi – et j'en ai personnellement plusieurs puisque j'ai déposé diverses propositions d'amendement –, la raison fondée sur la logique de protection de notre Etat et de nos infrastructures sensibles commande impérativement d'entrer en matière.

C'est ce qu'a fait le Conseil des Etats après l'audition en commission de représentants des cantons et de tous les secteurs touchés par la loi sur la sécurité de l'information. Aujourd'hui, sous prétexte d'objections financières, l'UDC, le seul parti à avoir manifesté son opposition frontale à cette loi en consultation, a réussi, de manière surprenante, à convaincre les groupes libéral-radical et PDC à ne pas entrer en matière.

Cette position est incompréhensible. Ce n'est pas moi qui le dis, c'est la "NZZ", qui, dans son édition du vendredi 9 mars 2018, écrit: "Mehr Konsequenz im Nationalrat, bitte!" La non-entrée en matière pour des raisons financières constitue, selon le même journal, "der falsche Weg".

L'argument financier ne résiste pas à l'examen. D'une part, la sous-commission de la Commission des finances a donné un préavis positif et la Commission des finances n'a pas contesté cette proposition. C'est donc assez piquant de voir la Commission de la politique de sécurité se substituer à la Commission des finances; d'ailleurs, le rapporteur de la Commission des finances auprès de la Commission de la politique de sécurité, au lieu de s'en tenir à la position de la Commission des finances, a savonné la planche pour que la Commission de la politique de sécurité laisse tomber le projet du Conseil fédéral.

D'autre part, le coût de la mise en oeuvre de la loi est fonction du degré de sécurité recherché. Selon le projet de loi, le degré de sécurité est fixé par le Conseil fédéral par ordonnance, après une procédure de consultation. Il est possible de modifier ce projet pour que le degré de sécurité soit fixé par le Parlement, mais, pour ce faire, il faut entrer en matière, et c'est ce que je vous invite à faire.

Il faut tenir compte aussi du fait que le coût articulé par le département oscille, selon le degré de sécurité visé, entre 5 et 20 millions de francs. Or, 5 millions de francs, c'est mille fois moins que le budget de l'armée – 5 milliards de francs – pour une année!

Gardons le sens des proportions, soyons raisonnables, entrons en matière et procédons à la discussion par article;

c'est ce que je vous demande au nom de la minorité de la commission.

Glanzmann-Hunkeler Ida (C, LU): Dem Rat liegt hier mit dem Informationssicherheitsgesetz ein Gesetz vor, das vieles beinhaltet, was vom Bund geregelt werden müsste. Während einigen Jahren wurde daran gearbeitet. Ich bin überzeugt: Heute könnte man in Bezug auf die ganze Cybersicherheit noch einiges anfügen und ergänzen.
Unbestritten ist, dass man die Grundlagen benötigt, um Informationen zu klassifizieren oder um Identitäten zu verwalten. Auch bei der Personensicherheitsprüfung, die in diesem Gesetz neu geregelt wird, gibt es Handlungsbedarf. Diese Personensicherheitsprüfung begleite ich seit mehreren Jahren in einer Subkommission der GPK. Dort haben wir schon lange Lücken aufgezeigt. Gerade diese hätte man sicher auch mit der Anpassung des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit schliessen können.
Es ist unverständlich, dass es bis heute noch keine einheitliche Verordnung über alle Departemente gibt, die regelt, wer geprüft wird, wie geprüft wird und wann eine Personensicherheitsprüfung stattfinden muss. Das EFD verfügt bis heute nicht mal über eine Verordnung zu dieser Frage. Allerdings frage ich mich, ob es dazu wirklich ein neues Gesetz braucht oder ob man Anpassungen im alten hätte vornehmen können.
Gesetzliche Anpassungen braucht es, ich glaube, das ist unbestritten. Was uns aber bei diesem neuen Gesetz fehlt, ist die Darstellung der Kosten respektive der neuen Stellen, die geschaffen werden, um dieses Gesetz umzusetzen; das ist etwas, was aus unserer Sicht eigentlich völlig normal sein sollte. In der Botschaft heisst es, dass die Kosten vollständig vom Sicherheitsniveau abhängen, welches die Behörden erreichen wollen. Dann heisst es, dass eine Reduktion bei der Personensicherheitsprüfung die anderen Stellen kompensieren würde. Aber bei der Personensicherheitsprüfung sind doch einige Stellen so oder so befristet; dies ist mir auf jeden Fall so bekannt, weil wir da auch schon nachgefragt haben, wie denn die Arbeitslast in Zukunft bewältigt werden könne. Wie kann man dann mit diesen Stellen noch etwas kompensieren? Irgendwie geht mir da die Rechnung nicht auf.
Auf die Nachfrage betreffend Kosten wurden wir mit neuen Stellen im Rahmen von 9,5 bis 78,5 Stellen konfrontiert. Dies ergibt sich, wenn man die drei verschiedenen Ambitionsniveaus, wie das so schön heisst, beachtet. Da reichen die Kosten von 1,5 bis 87 Millionen Franken und nicht, wie jetzt Herr Carlo Sommaruga gesagt hat, von 5 bis 20 Millionen Franken. Das sind nur die Umsetzungskosten, Herr Sommaruga, nicht die jährlichen Kosten, die dann entstehen.
Wir haben in der Kommission eine klare Kostenauflistung aufgrund der Beratung im Ständerat gefordert. Aber schon allein dies scheint wohl schwierig zu sein, weil viele offene Fragen bestehen mit Blick darauf, wie viele Stellen schlussendlich geschaffen werden sollen.
Bei der Betrachtung der nachgelieferten Informationen zu den Kosten kamen wir in der CVP-Fraktion zum Schluss, dass wir uns mit diesem neuen Gesetz und den nichtfestgehaltenen Kosten auf eine Blackbox einlassen, dies nur schon mal aus Sicht des Bundes. Wenn wir dann noch die Haltung der Kantone in der Vernehmlassung betrachten, die auch nicht mit zusätzlichen Kosten belastet werden möchten, dann ist diese Gesetzesvorlage so nicht zu unterstützen.
Die CVP-Fraktion hat dieses Gesetz zwar im Ständerat unterstützt, dies konnte uns aber nicht überzeugen. Auch die Ständeräte hatten dazu viele offene Fragen. Für uns ist es sehr wichtig, dass wir die Informationssicherheit auch mit einer gesetzlichen Grundlage abstützen können, aber dazu brauchen wir Fakten und klare Aussagen zu den Stellen und vor allem auch zu den Kosten. Aus unserer Sicht darf kein neues Gesetz geschaffen werden, wenn die Kosten so unklar sind. Nur Annahmen als Basis zu nehmen ist uns nicht seriös genug.
Die CVP-Fraktion hat darum klar entschieden, auf diese Gesetzesvorlage nicht einzutreten. Wir lassen uns nicht auf Experimente ein und fordern den Bundesrat auf, bestehende Gesetze anzupassen und so die Sicherheit zu gewährleisten.

Zuberbühler David (V, AR): Die uns vorliegende Botschaft zum Informationssicherheitsgesetz hat der Bundesrat am 22. Februar 2017 verabschiedet. Das Geschäft wurde anlässlich der Wintersession durch den Ständerat behandelt. Betrachtet man den Verlauf der Ständeratsdebatte, fällt umgehend auf, dass sich in der Kleinen Kammer lediglich drei Sprecher plus der Bundesrat zu Wort gemeldet haben. Die Gründe, weshalb sich sonst niemand an der Diskussion beteiligt hat, sind unbekannt, und man kann nur spekulieren.
Offensichtlich war der Ständerat aber bereit, einem umfassenden Gesetzeswerk zuzustimmen, das lediglich Scheinsicherheit vermittelt. Offensichtlich war er bereit, das Aufgabengebiet der öffentlichen Hand noch weiter auszubauen. Offensichtlich war er bereit, die Regulierungsdichte mit einem neuen Bürokratiemonster weiter auszubauen. Offensichtlich glaubte er, mit einem neuen Informationssicherheitsgesetz – einem einheitlichen Rahmengesetz – sei fortan sicherheitstechnisch alles in Butter. Offensichtlich glaubte er, mit einem neuen Einheitsgesetz wären nun alle Cyberattacken abgewehrt. Offensichtlich glaubte er, man könne mit einem neuen Einheitsgesetz sämtliche relevanten Lücken in Bezug auf die Informationssicherheit schliessen. Aber was ist schon sicher? Offensichtlich ist doch, dass nichts sicher ist, und nicht einmal das ist sicher!
Den Grundauftrag zum nun vorliegenden Entwurf erteilte der Bundesrat jedenfalls am 12. Mai 2010. Dass die Umsetzung eines Projektes bzw. die Ausarbeitung einer Vorlage satte sieben Jahre dauert, ist mehr als merkwürdig. Es scheint, als hätte sich mit diesem Gesetz jemand sehr schwergetan. Anders ist die lange Umsetzungszeit nicht zu erklären. Ob das nun ein gutes Zeichen ist, das wage ich an dieser Stelle zu bezweifeln.
Sie alle haben umfassende Unterlagen zum neuen Informationssicherheitsgesetz erhalten. Trotz dieser Fülle an Informationen, unverständlichen Begriffen und Abkürzungen oder eben gerade deswegen bleibt die Hauptfrage nach wie vor bestehen, die Frage nämlich, welchen besonderen Mehrwert dieses neue Gesetz bringt. Den entsprechenden Nachweis, dass das neue Gesetz tatsächlich einen zusätzlichen Nutzen bringt, konnten bis heute weder die Verwaltung noch der Bundesrat erbringen.
Es steht hingegen fest, dass seit Erteilung des Grundauftrags im Jahr 2010 der Überblick über das Ganze verlorenging. Ob es vielleicht daran liegt, dass in der Verwaltung heute zu viele Spezialisten sitzen, die spezifische Probleme möglichst perfekt beheben wollen? Ich weiss es nicht. Die Frage nach den finanziellen Auswirkungen bleibt ebenfalls ungeklärt.
Vielleicht hören Sie das Folgende heute erstmals. Die Vorlage sieht konkret drei Ambitionsniveaus vor. Ambitionsniveau 1 möchte die Sicherheit im Vergleich zu heute erhöhen, Ambitionsniveau 2 möchte die Informationssicherheit in Bezug auf heute deutlich erhöhen, und Ambitionsniveau 3 möchte eine sehr hohe Informationssicherheit. Die jährlich wiederkehrenden Kosten variieren je nach Ambitionsniveau zwischen 1,5 und 87 Millionen Franken. Die einmaligen Kosten für die Umsetzung des Projekts variieren innerhalb dieser Niveaus zwischen 5 und 20 Millionen Franken, und das Total der Vollzeitstellen variiert innerhalb der Niveaus zwischen 9,5 und 78,5 Stellen.
Mit dem Informationssicherheitsgesetz soll nun konkret Ambitionsniveau 1 angestrebt werden, was aber nicht heisst, dass es danach bei diesem Niveau bleibt. Das Gesetz hat den grossen Nachteil, dass es eine grosse Flexibilität in Bezug auf das jeweilige Ambitionsniveau bietet. Die entsprechende Regelung würde ausschliesslich in der Verordnung des Bundesrates erfolgen. Wenn also das Ambitionsniveau später erhöht werden sollte, müsste nicht das Gesetz geändert werden; es müsste lediglich die Verordnung angepasst werden. Das Parlament könnte seinen Einfluss dazu praktisch nicht mehr geltend machen. Glauben Sie mir: Sie gehen ja nicht wirklich davon aus, dass es bei diesem Ambitionsniveau 1 bleiben wird. Schliesslich will man doch eine hohe Informationssicherheit.
Ich fasse zusammen: Es ist brandgefährlich, auf ein Gesetz einzutreten, bei dem der konkrete Nutzen nicht nachvollziehbar ist. Es ist ebenso gefährlich, auf ein Gesetz einzutreten,

bei dem die Kostenfolge nicht absehbar ist bzw. bei dem nicht klar ist, wie viele zusätzliche Vollzeitstellen letztlich notwendig sind. Dies wäre gegenüber der steuerzahlenden Bevölkerung völlig unverantwortlich.
Auch schützt ein solches Gesetz – blickt man über die Landesgrenzen, sieht man das – nicht einmal ansatzweise vor Hackerangriffen. Mit dem Blick über die Landesgrenzen meine ich Folgendes: Trotz eines im Juli 2015 in Kraft getretenen IT-Sicherheitsgesetzes wurde das Datennetzwerk der deutschen Bundesregierung Ende Februar dieses Jahres gehackt. Die alte Weisheit aus der IT-Branche, wonach ein erfolgreicher Angriff immer nur eine Frage der Zeit und des Aufwands ist, hat sich wieder einmal bewahrheitet.
Die SVP-Fraktion ist überzeugt, dass mit einem neuen Bundesgesetz über die Informationssicherheit kein massgebender Mehrwert geschaffen wird. Das vorliegende Gesetz trägt kaum zu einer Effizienzsteigerung in Sachen Informationssicherheit bei. Es steigert auch nicht die Informationssicherheit selbst. Es erzeugt lediglich ein Gefühl von mehr Sicherheit, ein trügerisches Gefühl, das mit mehr Stellen bei der Bundesverwaltung bezahlt wird, die Sicherheit dieses Landes aber kaum voranbringt. Das vorliegende Gesetz bringt zusätzlichen bürokratischen Aufwand und noch mehr regulatorische Massnahmen, auch weil das Gesetz den jeweiligen Bundesbehörden im Rahmen ihrer Unabhängigkeit und Organisationsautonomie beim Vollzug viel Raum bietet. Darum ist es vorteilhafter, das derzeitige System beizubehalten und allenfalls gezielte Verbesserungen im Rahmen der bestehenden Strukturen anzubringen.
Aus diesen Gründen wird die SVP-Fraktion nicht auf das Geschäft eintreten, und ich bitte Sie, es ihr gleichzutun.

Eichenberger-Walther Corina (RL, AG): Im Namen der einstimmigen FDP-Fraktion beantrage ich Ihnen, nicht auf das Gesetz einzutreten. Dies bedeutet keineswegs, dass wir Sicherheit in der Datenverwaltung – die Sicherheit des Datenmanagements, das Management der Informationssicherheit – nicht befürworten oder sie nicht verbessern wollen. Allerdings ist in einem Verfahren des Zusammensetzens einzelner Teile ein riesiges, komplexes Gesetz entstanden, dessen Ausführlichkeit erstaunt. Nicht nur muss klar sein, wie die Sicherheit erhöht wird, vielmehr sind auch die finanziellen Konsequenzen dieses ausführlichen Gesetzeswerkes zu kennen. Aufgrund bestehender rechtlicher Grundlagen in Gesetzen und Verordnungen entsprach schon unsere jetzige Praxis dieser Sicherheit.
Die FDP-Fraktion hat grösste Bedenken, was die Kostenfolgen dieses Gesetzes anbelangt, ohne dass die Vorstösse betreffend eine Gesamt-Cyberstrategie schon darin integriert sind. Das Gesetz ist so konzipiert, dass verschiedene Ambitionsniveaus vom Bundesrat definiert und eingeführt werden können. Man spricht zurzeit vom Ambitionsniveau 1, das mehr Personal und Mehrkosten in überschaubarer Höhe, nämlich etwa 5 Millionen Franken zuzüglich 1,5 Millionen Franken für Betrieb und Personal, beinhaltet. Das wäre überschaubar. Sieht man sich die weiteren Ambitionsniveaus, die Niveaus 2 und 3, an, so stellt man fest, dass im Vollausbau Kosten von über 80 Millionen Franken dazukommen können. Der Bundesrat will sich diesbezüglich jedoch nicht festlegen und konnte keine konkreteren Angaben machen, bevor die Verordnungen vorliegen.
Diese Ambitionsniveaus sollen dann auch über Verordnungen bestimmt werden. Dies führt zu Zweifeln, ob das Gesetz in dieser Ausführlichkeit notwendig ist und ob die finanziellen Folgen tatsächlich genügend überlegt worden sind.
Die FDP-Liberale Fraktion ist von diesem Gesetz nicht überzeugt, zumal einige Abschnitte daraus in bestehenden Gesetzen sowie Verordnungen geregelt werden könnten. Aus diesem Grund beantragt sie Ihnen, auf das Gesetz nicht einzutreten.

Dobler Marcel (RL, SG): Die Vorlage des Bundesrates will einen einheitlichen, formell-gesetzlichen Rahmen für die Informationssicherheit beim Bund schaffen. Die FDP ist grundsätzlich auch der Meinung, dass gerade im Cyberbereich Koordination und zentrale Zuständigkeit sehr wichtig sind. Trotzdem muss man sich bei jedem Gesetz fragen, ob es dieses in allen Bereichen, die es regelt, wirklich braucht und ob die personellen und finanziellen Folgen wirklich abzuschätzen sind. Genau in diesem Bereich weist dieses Gesetz erhebliche Mängel auf.
1. An der Vorlage wurde über sieben Jahre gearbeitet, und das merkt man. Das Gesetz ist überladen. Hier ist dringend zu prüfen, welche Teile man entschlacken kann und ob das Verhältnis von Kosten und Nutzen wirklich stimmt.
2. Das Gesetz ist sehr unklar, was die personellen Ressourcen anbelangt. Ich würde sogar so weit gehen zu sagen, dass es in Bezug auf die Personalentwicklung ein Blindflug ist. Das konnte trotz mehreren Anläufen nicht genügend erklärt werden. Hier braucht es eine klare Ressourcenplanung mit einem Preisschild, und zwar jetzt und nicht erst im Rahmen der Ausführungsverordnung. Nur mit einer genauen Abschätzung der personellen Auswirkung jedes Bestandteils der Vorlage kann das Gesetz beraten und kann darüber entschieden werden.
3. Das Gesetz soll effizienzsteigernd sein. Von dieser Effizienzsteigerung und Zentralisierung ist immer wieder die Rede. Aber wo genau ist diese geschilderte Effizienz? Es sind weder Einsparungen von Geld noch Einsparungen von Personal ersichtlich, sondern nur Mehraufwand und Leistungsausbau.
Das Gesetz sieht die Dienstleistung einer Betriebssicherheitsprüfung vor. Die Nationalbank oder eine Grossbank könnte z. B. für ein internationales Projekt eine solche Prüfung beantragen. Der Bund würde dann eine Sicherheitsprüfung bescheinigen, was zum Vorteil und im Interesse des Auftraggebers wäre. Natürlich haben Firmen ein kommerzielles Interesse an solchen Überprüfungen. Doch warum macht dies nicht die Privatwirtschaft? Warum wird sie konkurrenziert? Warum braucht es diese Überprüfungen überhaupt in diesem Gesetz? Aus Sicht der FDP-Liberalen Fraktion gehört die personalintensive Betriebssicherheitsprüfung in die Privatwirtschaft.
Es gibt noch etliche weitere Punkte, in denen das Gesetz nicht stimmig ist. Einige Punkte, vor allem die Finanzierung, wurden bereits von Corina Eichenberger ausgeführt. An dieser Stelle möchte ich festhalten: Die Auswirkungen und der Nutzen des Gesetzes sind in der aktuellen Fassung noch zu ungenügend, um darauf eintreten zu können. Deshalb hat unsere Fraktion Nichteintreten beschlossen.
Im Namen der FDP-Liberalen Fraktion bitte ich Sie, nicht auf die Vorlage einzutreten.

Flach Beat (GL, AG): Können Sie mir erklären, wie ein privates Unternehmen eine Sicherheitsprüfung ohne das Wissen beispielsweise des Nachrichtendienstes oder anderer sicherheitsrelevanter Behörden vornehmen soll?

Dobler Marcel (RL, SG): Das ist zwar von der Kommission nicht zu Ende diskutiert, aber ein Ansatz wäre z. B., dass man nur den Standard definiert. Vertraulichkeit gibt es ja heute schon. Das Problem sehe ich also nicht wirklich.

Quadranti Rosmarie (BD, ZH): Die BDP-Fraktion wird eintreten. Weshalb wir das tun, begründe ich, doch zuerst eine Vorbemerkung: Das Gesetz ist hochkomplex, ja, und es überfordert uns Parlamentarierinnen und Parlamentarier sicher auch stellenweise. Wenn nun aber die Antwort auf hohe Komplexität Nichteintreten ist, dann erstaunt das die BDP doch sehr.
Was will das Gesetz, und weshalb meinen wir, dass es gute Gründe gibt, einzutreten und sich mit dem Gesetz auseinanderzusetzen?
Ich zitiere Professor Markus Müller, der die neutrale, externe Expertengruppe leitete. Auf die Frage, weshalb es das Gesetz brauche, antwortete er: "Weil die Bedrohung der Sicherheit durch die Digitalisierung massiv zugenommen hat. Man kann die Kernproblematik des Gesetzes mit den Begriffen 'E-Gov' oder 'Cyberadministration' auf den Punkt bringen." Das heisst, weil heute in wesentlichen Teilen nur noch elektronisch kommuniziert wird, wachsen die Herausforderungen an den Schutz. Es sind einheitliche und minimale Sicherheits-

standards für alle Beteiligten notwendig, und zwar nicht nur für den Bund, sondern eben auch für alle, die sich im Bereich des Bundes austauschen. Heute hat man unterschiedliche Schutzniveaus. Darunter aber leidet die Sicherheit. Heute hat jede Stelle, jedes Departement einen Informatik- und Datenschutzbeauftragen. Mit dem Gesetz sollen eine Konzentration und ein einheitlicher Schutzstandard garantiert werden. Parallelorganisationen, die nur viel kosten und wenig bringen, sollen ersetzt werden. Die Grunderkenntnis ist: Bei der Informationssicherheit hängt alles zusammen. Wenn man das nicht gesamtheitlich bewältigt, drohen Lücken.
Und jetzt wird es spannend: Auch Ihre SiK hat erkannt, dass es Lücken in der Informationssicherheit gibt. Die Antwort der Kommissionsmehrheit auf diese Erkenntnis ist Nichteintreten! Man hat nicht einmal – was, wenn schon, logischer gewesen wäre – Rückweisung mit einem klaren Auftrag beantragt. Das lässt sich aber erklären, denn eine Rückweisung würde wenig Sinn machen. Es wurde in den Anhörungen unserer SiK und in jenen der SiK-SR, deren Protokoll wir lesen konnten, erklärt, dass man Alternativen geprüft hätte, den Umfang diskutiert hätte usw. Deshalb würde eine Rückweisung wahrscheinlich auch nichts bringen.
Nichteintreten aber heisst Lücken Lücken sein lassen. Die BDP-Fraktion ist sich fast sicher: Diejenigen Parteien, die jetzt den Antrag auf Nichteintreten unterstützen, werden bei einem gravierenden Fall, der auf Sicherheitslücken zurückzuführen ist, nach sofortigem Handeln schreien und wohl auch mit Schuldzuweisungen nicht sparen.
Ja, das Gesetz ist umfangreich, hochkomplex. Als Politiker sind wir teilweise überfordert, doch das sollte eben auch heissen, Vertrauen zu haben in diejenigen, die dieses Gesetz erarbeitet haben. Das Gesetz ist so umfangreich, weil eigentlich vier Gesetze in eines verpackt wurden. Es regelt die Informationssicherheit, die Personensicherheit, das Betriebssicherheitsverfahren und die kritischen Infrastrukturen. Bei der Informationssicherheit hängt eben alles zusammen. Das Gesetz wäre schlanker, wenn man davon ausgehen würde, dass der Bundesrat den Vollzug einheitlich auf Verordnungsstufe regelt. Aber in der Vernehmlassungsantwort und in der Ämterkonsultation war es ein grosses Anliegen, dass man davon absehe.
Was sind die Alternativen, wenn man das Gesetz bachab schickt? Man könnte das Gesetz splitten, vier kleinere Gesetze machen. Die Resultate wären nach wie vor unübersichtlich, anfällig für Widersprüche, ineffizient und mit Vollzugsschwierigkeiten versehen. Das Ganze wäre nicht mehr kohärent. Man könnte – davon wurde beim Eintreten gesprochen – die bestehenden Gesetze ergänzen, so zum Beispiel das Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit, das Regierungs- und Verwaltungsorganisationsgesetz, das Militärgesetz, das Parlamentsgesetz oder das Bundesgerichtsgesetz. Doch auch das würde zu Doppelspurigkeiten, auch zu Ineffizienzen in der Umsetzung – eben wie heute – führen. Darum sind Alternativen weder sinnvoll noch machbar und bringen wenig bis nichts. Vor allem bringen sie nicht weniger Normen, sondern nur Inkohärenz.
Was sind die Risiken? Es gibt das rechtsstaatliche Risiko. Vieles ist nicht genügend abgestützt. Nehmen wir als Beispiel die Melde- und Analysestelle Informationssicherung (Melani). Die gesetzliche Grundlage ist ungenügend.
Der Handlungsbedarf besteht, das wurde mehrmals gesagt, eigentlich von allen bestätigt, doch Ihre SiK will in der Mehrheit kein neues Gesetz. Aber es besteht Handlungsbedarf. Jetzt mit dieser Ausgangslage nichts zu tun, erachten wir als fahrlässig. Die Bedrohungen sind vielfältig, und die Abwehrmechanismen müssen eben auch vielfältig sein – vielfältig, aber vor allem auch vernetzt. Mit dem Gesetz würde der Bund ein modernes, dem aktuellen Stand von Wissen und Technik entsprechendes Instrument sowie Informationen und eine Informatik erhalten, die letztlich den Staat vor vielfältigen Gefahren zu schützen vermögen – nicht zu hundert Prozent, hundertprozentige Sicherheit gibt es einfach nicht.

Der Ständerat hat das Gesetz durchberaten und nach Änderungen mit 39 zu 0 Stimmen bei 4 Enthaltungen angenommen. Die SiK-NR will mehrheitlich nicht eintreten und das Ganze an den Ständerat zurückschicken. Die BDP-Fraktion wird eintreten. Auch wenn es hochkomplex ist, sind wir bereit, das Gesetz zu beraten und eventuell Anpassungen vorzunehmen. Die BDP-Fraktion will nicht, dass wir in einem wichtigen Bereich weiterhin Sicherheitslücken zulassen. Natürlich wäre es uns lieber gewesen, man hätte die Kosten auf den Rappen genau beziffern können. Es ist uns aber klargeworden, dass das einfach noch nicht möglich ist. Für uns steht im Zentrum, dass erkannte Lücken geschlossen werden. Wir wollen nicht warten, bis uns ein Grossereignis diese Notwendigkeit vor Augen führt. In diesem Bereich ist Sicherheit grosszuschreiben. In der Informationssicherheit hängt alles zusammen. Wenn wir das nicht gesamtheitlich bewältigen, bleiben Lücken bestehen, die fatale Folgen haben können.
Warten wir also nicht, bis wir vor solchen Situationen stehen, treten wir auf dieses Gesetz ein.

Vitali Albert (RL, LU): Frau Kollegin, Sie haben jetzt sehr ausführlich über die sicherheitspolitische Ausgangslage informiert. Wir haben in der Finanzkommission des Nationalrates die finanzpolitische Ausgangslage beurteilt. Sie haben gesagt, man könne es nicht auf den Rappen beziffern. Wenn man den finanzpolitischen Spielraum betrachtet, so sieht man, dass wir über 2 bis 87 Millionen Franken diskutieren. Ich bin erstaunt, dass Sie darüber nichts gesagt haben. Können Sie dazu eine Aussage machen?

Quadranti Rosmarie (BD, ZH): Man kann keine Aussage über die genauen Kosten machen. Ich verstehe den finanzpolitischen Aspekt. Ich argumentiere aber mit einem sicherheitspolitischen Aspekt, und dieser lässt der BDP-Fraktion klarwerden, dass wir hier gravierende Lücken haben. Mit Verlaub, ja, es ist schade – das habe ich auch gesagt -: Die Kosten sind noch nicht genau zu definieren. Aber wenn wir nichts tun, was Sie mit dem Nichteintreten jetzt tatsächlich im Sinn haben, lieber Kollege Vitali, bin ich mir nicht sicher, ob uns das dann später nicht sehr viel mehr kosten wird. Auch diese Kosten können Sie im Moment nicht beziffern.

Seiler Graf Priska (S, ZH): Ich möchte gleich zu Beginn festhalten, dass die SP-Fraktion die Absicht und die Stossrichtung dieses Gesetzentwurfes gut findet. Wir finden, dieses Gesetz wird dringend benötigt, denn es würde einerseits verstreute Bestimmungen zusammenfassen und ein einheitlich hohes Cybersicherheitsniveau im Bereich der Informationssicherheit schaffen. Andererseits würde dieses Gesetz aber auch echte Fortschritte bringen, zum Beispiel mit der Schaffung einer behördenübergreifenden Fachstelle des Bundes für die Steuerung der erforderlichen Massnahmen zur Informationssicherheit.
Der vorliegende Entwurf des Bundesgesetzes über die Informationssicherheit beim Bund hätte nach unserer Ansicht einer integralen Informationssicherheit und dem gesellschaftlichen und technischen Wandel im Umgang mit Information angemessen Rechnung getragen. Stichworte sind Digitalisierung, Cyber, Big Data usw. Ich sagte "hätte", denn wir werden ja nicht auf dieses Gesetz eintreten, wenn Sie der Mehrheit der Kommission folgen, was ich jetzt mal annehme.
Die Frage nach den finanziellen Folgen dieses Gesetzes stand dermassen im Zentrum der Diskussionen in der SiK, dass alles andere in Vergessenheit geriet, zum Beispiel eben Sicherheitsfragen. Ich finde es fatal, wenn die SiK gar nicht richtig über Sicherheitsfragen diskutiert.
Es besteht dringender Handlungsbedarf im Bereich Informationssicherheit. Dieses Gesetz ist ein Vorschlag, ein komplexer Vorschlag, das gebe ich zu. Wir sind auch nicht mit allen Punkten einverstanden oder vollkommen glücklich – Stichworte sind Öffentlichkeitsprinzip und Klassifizierungen. Doch die Chance, dieses Gesetz materiell zu verbessern, vergeben Sie jetzt mit dem Nichteintreten. Ja, man könnte sogar sagen, die SiK begeht mit dem Nichteintretensantrag Arbeitsverweigerung. Wenn Sie dieses Gesetz tatsächlich so überladen, unberechenbar oder lückenhaft finden – ich habe alles gehört –, hätten Sie es ja in der Hand gehabt, es durch gezielte Streichungs-, Ergänzungs- oder Änderungsanträge zu entrümpeln, so wie das ja die Schwesterkommission getan hat. Aber diese Arbeit scheuen Sie offenbar. Ehrlich ge-

sagt, finde ich ein solches Verhalten in Anbetracht des akuten Handlungsbedarfs bei diesem Thema geradezu verantwortungslos. Ich könnte auch sagen: Man kapituliert halt.
Natürlich sind die Kosten ein wichtiges Argument. Dafür habe ich durchaus Verständnis. Aber wenn wir bei der Informationssicherheit jetzt nicht investieren und die verschiedenen daran beteiligten Stellen nicht besser koordinieren, als dies heute der Fall ist, löst dieses Versäumnis ebenfalls Kosten aus, und dies mit fatalen Folgen, da bin ich mir sicher. Das kommt uns unter dem Strich dann viel teurer als dieses Gesetz.
Ich bitte Sie darum wirklich eindringlich, den Minderheitsantrag Sommaruga Carlo auf Eintreten zu unterstützen.

Bendahan Samuel (S, VD): Madame Seiler Graf, je suis tombé de ma chaise en entendant tout à l'heure votre collègue de parti, Monsieur Sommaruga, porte-parole de la minorité, dire que le représentant de la Commission des finances avait sabordé cette loi – "savonné la planche" – lors de votre séance de commission. J'ai pourtant entre les mains le corapport de la Commission des finances, qui dit, en gros, qu'elle est tout à fait favorable à ce projet de loi. Pouvez-vous m'expliquer, alors que, selon son corapport, la Commission des finances est si favorable, ce qu'il s'est passé à la CPS qui explique le commentaire de Monsieur Sommaruga tout à l'heure?

Seiler Graf Priska (S, ZH): Merci pour cette question, Monsieur Bendahan. Der Vertreter der Finanzkommission, Pirmin Schwander, hat uns sehr lange und sehr ausführlich dargelegt, warum dieses Gesetz zu viele Kosten auslöst und dass das nicht verantwortbar sei. Ich war immer der Ansicht – und bin jetzt sehr erstaunt, etwas anderes zu hören –, dass das die Meinung der Mehrheit der Finanzkommission ist. Ich bin jetzt überrascht, dass dies offenbar nicht der Fall ist.

Crottaz Brigitte (S, VD): Nous abordons aujourd'hui un sujet qui ne laisse personne indifférent: la sécurité. Ce thème peut être traité de différentes manières, mais, aujourd'hui, nous l'abordons sous l'angle de la sécurité de l'information.
Le groupe socialiste vous propose d'entrer en matière sur ce projet de loi, comme l'a fait le Conseil des Etats en décembre dernier. Alors que la Commission de la politique de sécurité de notre conseil était entrée en matière sur le projet du Conseil fédéral en janvier, estimant que la loi contribuait à améliorer la sécurité de l'information relevant de la compétence de la Confédération, elle est revenue sur sa décision d'entrer en matière au mois de février dernier, argumentant que la loi mettrait en place un système de protection de l'information démesuré, trop complexe, et que les estimations disponibles en termes de conséquences financières étaient trop sommaires. Nous estimons que la position défendue par la majorité de la commission est incompréhensible et démontre une hiérarchisation des priorités erronée ainsi qu'un manque de prise de conscience de la nécessité de disposer d'instruments de cyberdéfense.
Cette loi mérite, à nos yeux, d'être soutenue pour différentes raisons, qui ont déjà été citées. Premièrement, l'évolution de notre société vers une hyperconnectivité conduit à des menaces différentes de celles auxquelles nous étions jusqu'alors confrontés. La digitalisation et l'interconnexion des systèmes rendent nécessaire une loi sur la sécurité de la cyberadministration. Deuxièmement, l'utilisation abusive d'informations, le vol de données ou la perturbation de systèmes d'informations sensibles peuvent nuire gravement aux intérêts essentiels de la Suisse. Ils peuvent mettre en péril l'accomplissement de tâches vitales de la Confédération et des cantons, voire léser la sécurité d'entreprises ou de particuliers.
Il est donc impératif, à nos yeux, d'assurer la sécurité de l'information, ce que propose la loi qui nous est soumise aujourd'hui. Elle établit une norme minimale de sécurité de l'information pour toutes les autorités fédérales, comblant ainsi de nombreuses lacunes en matière de sécurité.
Elle prévoit une protection des informations confidentielles et secrètes de la Confédération et gère les contrôles de sécurité concernant les personnes exerçant des fonctions qui nécessitent l'accès à des informations, à du matériel ou à des installations sensibles. Cette loi est un fondement indispensable de la cybersécurité et de la cyberdéfense. Elle établit, sur des critères reconnus internationalement, un cadre formel renforcé pour la mise en oeuvre de la sécurité de l'information de la Confédération et tient compte des recommandations des organes de surveillance parlementaire, en particulier des Commissions de gestion.
L'atteinte des objectifs fixés par cette loi dépendra des ressources financières et humaines allouées. Les coûts de la mise en oeuvre dépendront presque complètement du niveau de sécurité que les autorités fédérales voudront atteindre et qu'elles fixeront dans les ordonnances d'exécution. Le Conseil fédéral s'est d'ailleurs dit prêt à soumettre ces ordonnances à l'appréciation des deux conseils.
Comme dans le domaine médical, prévenir vaut mieux que guérir. La loi qui nous est proposée aujourd'hui fait office de prévention. Il est vrai que la prévention donne souvent l'impression de coûter cher, mais la perturbation de nos systèmes d'informations sensibles coûterait nettement plus cher et pourrait avoir des conséquences autrement plus graves.
En conclusion, nous estimons qu'il est évident que des mesures doivent être prises afin d'améliorer la sécurité de l'information. Nous vous invitons donc à suivre la minorité Sommaruga Carlo et à entrer en matière sur ce projet de loi afin de ne pas perdre davantage de temps dans la mise en application de mesures de cyberdéfense, sachant que le projet qui nous est soumis aujourd'hui a mis sept ans pour être élaboré. Nous ne pouvons pas nous permettre de perdre davantage de temps avant de mettre sous toit une loi sur la sécurité de l'information, sous peine de risquer des perturbations des systèmes d'informations sensibles, qui pourraient nuire gravement aux intérêts essentiels de notre pays.

Mazzone Lisa (G, GE): Le groupe des Verts a quelque peine à comprendre ce qui se joue dans notre Parlement. En principe, lorsqu'on utilise le mot "cybersécurité", cela agit comme une sorte de clé universelle qui pousse notre Parlement à se lever comme un seul homme – ou une seule femme – pour soutenir la proposition présentée. La semaine dernière encore, un postulat traitant de cybersécurité a été accepté à l'unanimité.
Ce n'est pas sans raison que notre Parlement agit de cette manière. En effet, les incidents se multiplient et la cyberattaque contre RUAG, qui nous a beaucoup préoccupés, n'en est qu'un exemple. Ce sont des risques qui sont réels et très actuels, et il est essentiel qu'on se donne les moyens de prévenir ces risques et qu'on garantisse la sécurité de l'information en Suisse, alors qu'en même temps on ne lésine pas sur les moyens alloués à l'armée. Ainsi, en principe, le mot "sécurité" est une clé pour obtenir des fonds. Dans ce dossier, force est de constater que ce mot ne suffit pas et qu'on est prêt à prendre des risques et à mettre la Suisse dans une situation périlleuse.
La sécurité de l'information, qu'est-ce que c'est? Cela consiste à assurer la confidentialité, la disponibilité et l'intégrité des informations, ainsi que le bon fonctionnement de nos systèmes informatiques. Cela englobe autant la sécurité informatique que la cybersécurité, donc que la sécurité sur Internet. Cette loi est essentielle à l'heure où le gouvernement recourt de plus en plus à Internet, est de plus en plus présent en ligne, et elle est essentielle pour offrir des bases légales à des mesures existantes. Nous pensons notamment à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information Melani, qui a besoin de cette loi pour disposer de bases légales pour pouvoir fonctionner.
Cette loi est aussi essentielle pour combler des lacunes en matière de sécurité de l'information, pour harmoniser, coordonner, renforcer la sécurité, pour mieux gérer les identités, les accès et les contrôles, pour régler les procédures de sécurité relatives aux personnes et aux entreprises. Bref, on a besoin de cohérence et de coordination. On a besoin d'étendre les compétences existantes, c'est essentiel pour garantir la sécurité de nos systèmes informatiques.

Dans le cadre de la consultation, le besoin de légiférer a été très largement reconnu, y compris d'ailleurs par deux des trois partis qui font aujourd'hui partie de la majorité. Les cantons soutiennent aussi la loi, et le Conseil des Etats l'a acceptée à l'unanimité, moins quelques abstentions. Bref, la loi a vraiment été plébiscitée, parce qu'il y a une reconnaissance du besoin d'agir.
Si on n'agit pas par ce biais, que se passera-t-il? De très nombreuses lois sectorielles devront être adaptées, et la pratique va continuer à être inefficace comme c'est le cas actuellement. Cela revient à de la bureaucratie: adapter chaque loi sectorielle représente réellement de la bureaucratie. C'est ce dont on doit se prémunir; nous ne devons pas nous engouffrer dans cette voie.
En ce qui concerne les coûts, on l'a entendu, les coûts de mise en oeuvre sont minimes. En fonction du développement de la loi, du degré de sécurité choisi, les coûts s'élèveraient, du niveau 1 au niveau 3, entre 5 et 20 millions de francs. Par ailleurs, les coûts, en termes d'équivalents temps plein pour la Confédération, représentent entre 3 et 10 personnes. Bref, au regard du budget de l'armée, par exemple, ces coûts sont des cacahuètes pour une amélioration essentielle de la sécurité.
On a eu également la garantie, lors des travaux de commission, que celle-ci serait consultée sur les ordonnances. Donc, si vous avez des doutes ou des craintes quant au niveau de sécurité ou à la manière dont les mesures seront mises en oeuvre, vous pourrez le dire puisque nous serons consultés sur les ordonnances. Mais, pour pouvoir être consultés et discuter du niveau de sécurité, nous devons entrer en matière aujourd'hui et aller de l'avant.
Enfin, pour notre place économique – et cela me semble important –, le contrôle de sécurité des entreprises représente un standard qui est parfois essentiel pour obtenir des mandats à l'étranger. Ne pas adopter cette loi, c'est aussi risquer de mettre l'économie dans une situation délicate, voire de passer à côté de mandats.
Aujourd'hui, pour toutes ces raisons, le groupe des Verts vous invite à soutenir la proposition de la minorité Sommaruga Carlo et à entrer en matière sur ce projet de loi.

Glättli Balthasar (G, ZH): Was ist schon sicher? Das ist eine Frage, die vorhin gestellt wurde, um zu rechtfertigen, dass man gar nicht erst in die Diskussion darüber einsteigen will, wie man die Informatiksicherheit beim Bund im Zusammenhang mit kritischen Infrastrukturen verbessern kann. Dieses Parlament oder zumindest diese Kommission hat schon ein wenig ein Problem mit der Abwägung. Wenn es darum geht, unbescholtene Schweizerinnen und Schweizer zu überwachen, den Internetverkehr einer Totalüberwachung zu unterziehen, wenn es darum geht, mit Netzsperren neue Märkte zu schaffen, dann ist keine technische Massnahme, keine Ausgabe gross genug. Wenn man dann jeweils sagt, die totale Sicherheit sei nicht erreichbar, wird einem entgegengehalten, man sei ein Träumer.
Hier ist ein Gesetz, das nicht totale Sicherheit will, nicht totale Sicherheit verspricht, sondern das umzusetzen verspricht, was in jedem anständigen Unternehmen in diesem Land Standard ist: dass man sich Richtlinien gibt, wie man die Informationssicherheit im eigenen Haus kohärent sicherstellt. Man weiss, dass es nichts bringt, wenn jeder für sich etwas bastelt. Man muss Kohärenz haben, weil die verschiedenen Einheiten ja auch miteinander verbunden sind, und wenn irgendwo ein Einfallstor ist, kann dort auch die stark befestigte Vordertür der anderen Abteilung umgangen werden.
Mir scheint auch, dass viele Kolleginnen und Kollegen die Grundlagen der parlamentarischen Mittel nicht ganz begriffen haben. Ich erkläre jeweils unseren neuen Ratsmitgliedern, was der Unterschied zwischen Nichteintreten und Rückweisung ist. Nichteintreten heisst, man sieht keinen Bedarf an Regulierung. Das ist das, was Sie uns jetzt in der Mehrheit beantragen, obwohl Sie gleichzeitig in Ihren Voten immer sagen: Natürlich, die Cybersicherheit, das ist ein grosses Problem.
Wenn Sie meinen, der Bundesrat habe untauglich legiferiert – das darf man ja meinen, ich bin nicht derjenige, der wie eine Salzsäule vor dem Bundesrat erstarrt –, dann geben Sie ihm mit einer Rückweisung einen klaren neuen Auftrag. So macht man das, sorry. Das andere ist einfach Dienstverweigerung.
Dann haben Sie gesagt, man regle die Frage besser in einzelnen Gesetzen. Ich muss Ihnen sagen, wenn Sie diese Vorlage – 99 Seiten – anschauen, sehen Sie, dass die Hälfte Änderungen in anderen Erlassen betrifft. Das ist genau das, was Sie verlangen: dass man in einzelnen Erlassen eben anpasst, was nötig ist.
Dann sagen Sie, man erteile einen Blankocheck. Überhaupt zielt die ganze Argumentation vor allem auf die Finanzen ab. Jetzt muss ich Ihnen sagen: Ein Informationssicherheitsleck kann nicht nur einen Reputationsschaden zur Folge haben, sondern ganz klar auch finanzielle Auswirkungen. Wir sprechen hier zum Beispiel von sogenannt kritischer Infrastruktur, also von Stromnetzen oder so. Ein Stromausfall ist dann also nicht einfach gratis. Mich würde es eigentlich noch interessieren, ob die ganze Finanzkommission das so sieht oder ob es nur der Vertreter der Finanzkommission war, der eigentlich meinte, man sollte hier im besten Falle keinen Franken investieren. Er hat überhaupt nicht davon gesprochen, dass hier nicht nur Sicherheitsrisiken, sondern auch finanzielle Risiken hintendran hängen, wenn wir keine einheitlichen Standards schaffen.
Es kann doch nicht sein, dass man hier jetzt sagt, man wolle schon im Detail wissen, was dann alles in den Verordnungen steht. Man hätte ja die Möglichkeit, die Verordnungen zu sehen – der Bundesrat nickt. Man könnte sogar sagen, man wolle, dass die Verordnungen durchs Parlament müssten. Das kann man. Das ist auch ein parlamentarisches Recht, von dem man Gebrauch machen kann, wenn man will.
Hier sagen Sie, dass wir nicht abstimmen, wenn wir nicht alles schon bis ins Detail wissen. Die Gleichen wollen dann vom Volk einen Blankocheck für 8 Milliarden Franken für Rüstungsgeschäfte, bei denen man nicht einmal weiss, wie viel für Flieger und wie viel für Luftverteidigung ausgegeben wird. Also, wenigstens ein bisschen Kohärenz möchte ich von Ihnen schon erwarten dürfen; das darf man in der politischen Auseinandersetzung. Ich muss Ihnen sagen: Wenn Sie hier jetzt nicht eintreten, dann möchte ich einmal ein Moratorium von einem halben Jahr und dass nicht alle immer sagen: Cybersicherheit, Cybersicherheit, Cybersicherheit, und der Bundesrat mache seine Aufgaben nicht.

Vitali Albert (RL, LU): Herr Glättli, Sie haben die Finanzkommission angesprochen. Ich sage gerne etwas dazu. Die Finanzkommission hat in einem Mitberichtsverfahren die finanzpolitische Ausgangslage beurteilt. Die SiK hat die sicherheitspolitische Ausgangslage beurteilt. Sie haben gesagt, die Finanzkommission habe im Mitberichtsverfahren gesagt, dass man da nichts investieren solle. Die Aussage der Finanzkommission im Mitbericht war, dass die Spannweite 2 bis 87 Millionen Franken betrage und dass man da mehr Genauigkeit wolle. Sie haben jetzt auch wieder zum Ausdruck gebracht, die Finanzkommission sage, man solle da nicht investieren. Aber es ist nicht so. Ich bitte Sie dementsprechend, den Mitbericht zu lesen. Darum meine Frage: Haben Sie den Mitbericht der Finanzkommission bekommen und gelesen?

Glättli Balthasar (G, ZH): Wir haben nicht nur den Mitbericht, sondern auch einen Sprecher der Finanzkommission bekommen. Wir wissen ja, Mitberichte sind am Schluss immer Kompromisswerke, bei denen versucht wird, die gemeinsame Haltung der Kommission oder der grossen Mehrheit der Kommission darzustellen. Die Art und Weise, wie der Sprecher der Finanzkommission diesen Mitbericht dargestellt hat – das, was wir vom Bericht durch die Livepräsenz mitgekriegt haben –, ist einer der wesentlichen Gründe dafür, dass jetzt alle so argumentieren, wie sie hier in den letzten 60 oder 65 Minuten argumentiert haben.
Es haben nämlich alle gesagt: Wir haben Angst vor den finanziellen Folgen. Sie haben aber jene Aufgabe, die Sie, Herr Kollege, zu Recht beschrieben haben, überhaupt nicht gemacht. Sie haben zu Recht gesagt, unsere Aufgabe als SiK sei die Prüfung, ob das aus sicherheitspolitischen Gründen notwendig sei. Da sage ich Ihnen: Ja, es ist aus si-

cherheitspolitischen Gründen notwendig, Mindeststandards im Bereich der Informatiksicherheit zu setzen. Wer das nicht will, der lebt wirklich auf einem anderen Planeten oder in einer anderen Zeit.

Arnold Beat (V, UR): Herr Kollege Glättli, Sie und auch Ihre Vorrednerin aus Ihrer Fraktion haben jetzt schön ausgeführt, was für Vorteile das Gesetz für die Informatiksicherheit bringt. Was sagen Sie denn zum Umstand, dass gerade Deutschland, das seit 2015 ein solches Gesetz hat, massiv angegriffen wurde und vermutlich massive Schäden davonträgt?

Glättli Balthasar (G, ZH): Wie Sie zu Recht sagen, ist ein Gesetz allein noch nicht die Lösung. Es wird ja darum gehen, jene Grundregeln, die im Gesetz sind – eben die Mindeststandards – dann auch einzuführen. Sie wissen, wie lange die Umsetzung von Gesetzen dauert. Das ist nicht mit unserer Schlussabstimmung gemacht. Sie wissen ja auch, wenn Sie es gelesen haben, dass es im Gesetz selber Übergangsfristen von fünf Jahren, zum Teil sogar noch längere, gibt. Auch bei uns wäre am Tag nach der Schlussabstimmung noch nichts gewonnen. Das Gesetz würde aber endlich einen klaren Auftrag erteilen, die zu erarbeitenden Sicherheitsstandards in allen Abteilungen umzusetzen.
Wenn Deutschland – es könnte auch die Schweiz sein – oder die Schweiz Ziel eines Anschlages durch einen anderen Staat wird, dann braucht es mehr als nur Minimalstandards. Deshalb hat dieses Gesetz verschiedene Sicherheitsniveaus: Man sagt, es gibt Sachen, die man gegen das alltägliche Unwetter schützt, gegen die Cyberkriminellen XY, und dann gibt es Sachen, für die es stärkere Sicherheitsbestimmungen und höhere Sicherheitsstandards braucht. Sie nicken jetzt; ich nicke auch. Ich verstehe bloss nicht, weshalb Sie dann dem Antrag auf Nichteintreten zustimmen.

Flach Beat (GL, AG): Die Grünliberalen treten ein und bitten Sie, auch einzutreten und damit der Minderheit zu folgen.
Worum geht es, und worum geht es nicht? Es geht nicht darum, ein neues Bürokratiemonster zu bauen, sondern es geht darum, ein Grundgesetz zu schaffen für die Koordination der Informationssicherheit im Bereich des Bundes, der Verwaltung und der nahestehenden wichtigen Betriebe und Organisationen des Bundes. Angriffe auf das EDA, den Nachrichtendienst des Bundes und zuletzt auf die Ruag haben, glaube ich, uns allen deutlich vor Augen geführt, dass in diesem Bereich Handlungsbedarf besteht. Es wurde schon mehrfach angetönt, dass sogar der Deutsche Bundestag offensichtlich ein Opfer eines solchen Internetangriffes war, eines Cyberangriffes, und dass dort wahrscheinlich über Monate hinweg ein riesiges Datenleck bestanden hat.
Es wurde jetzt in den Begründungen auch angeführt, dass genau das ein Grund sei, hier auf eine Gesetzgebung zu verzichten – einer der Vorredner hat das gerade gesagt -: Der Bundestag habe ja so ein Gesetz, und das habe ja dann auch nichts genützt. Ich muss Ihnen schon sagen: Das ist einfach komplett falsch! Das ist komplett falsch. Das föderalistische System in der Schweiz mit den verschiedenen Bundesämtern und angegliederten, teilweise sehr, sehr frei agierenden Organisationen ist keineswegs zu vergleichen mit der Bundesrepublik Deutschland und dem System des Deutschen Bundestages und den dort angegliederten Organisationen: Das ist etwas komplett anderes.
Worum geht es denn aber tatsächlich in unserer Vorlage? Sie ist relativ kompliziert. Es geht darin um Vertraulichkeit, es geht um Verfügbarkeit, es geht um Integrität, und es geht um Nachvollziehbarkeit von Informationen und um Informationssicherheit.
Sie müssen sich das einfach vorstellen: Die Regelungen, mit denen wir gedanklich noch leben, entstammen einer Zeit, in welcher man die Akten in Ordnern abgelegt hat, sie in einen Tresor oder in einen Aktenschrank gestellt und diesen abgeschlossen hat, einer Zeit, in welcher es ein Verzeichnis darüber gab, welche Informationen wo aufbewahrt werden, wer welche Kopien hat, wo die klassifizierten Dokumente und so weiter liegen. Diese Regelungen entstammen nicht einer Welt, wie wir sie heute haben, in der die Daten halt eben als Bits und Bytes auf einer Festplatte liegen, problemlos kopierbar, transferierbar, veränderbar und halt eben auch klaubar, entwendbar sind – und zwar, durch die Vernetzung, die wir heute in der Bundesverwaltung und in den angelehnten Betrieben haben, mit einfachsten Mitteln.
Es ist wichtig, dass wir hier eine koordinierte Sicherheit aufbauen, bei der alle Player entsprechend mitarbeiten können. Das ist auch der Grund, wieso es sieben Jahre dauerte, bis dieses Gesetz vorlag. Dass es sieben Jahre dauerte, bis die Vorlage da war, ist kein Grund zu sagen, das Gesetz sei schlecht. Wenn Sie ein Gesetz schaffen in einem Bereich, der sich ständig ändert wie die digitale Welt, in der Sie alle paar Wochen, alle paar Monate neue Erkenntnisse haben, dann kann es sein, dass Sie ein bisschen länger daran arbeiten müssen, weil ein Gesetz halt eben die Grundlagen dafür schaffen soll, dass es auch in der Zukunft funktioniert.
Ein wesentlicher Bestandteil bei der Erarbeitung dieses Gesetzes war es, dass die an den Bund, an das Parlament und an die Verwaltung angelehnten Betriebe in der Lage sind, entsprechend ihrem Sicherheitsbedürfnis ihre eigenen Regelungen zu treffen, und wir nur die Standards festhalten, wie das zu geschehen hat, inklusive halt eben der Nachvollziehbarkeit der Tätigkeiten, was einer der wichtigsten Bestandteile dieser ganzen Regelung ist. Damit Sie am Schluss wissen, dass etwas schiefgelaufen ist, müssen Sie nachvollziehen können, wie es funktioniert hat. Dieses Gesetz soll eben Lücken schliessen, Lücken, die heute bestehen.
Von allen Rednern habe ich immer wieder gehört, dass eigentlich Handlungsbedarf besteht. Man hat doch schon lange erkannt, dass im Bereich der Cybersecurity Handlungsbedarf besteht, auch bei uns in der Verwaltung. Trotzdem wollen Sie hier nicht auf dieses Gesetz eintreten. Das verstehe ich einfach nicht.
Es wurde in der Kommission ausgeführt, dass viele Dinge unklar seien. Es wurde insbesondere immer wieder die Frage der Kosten angeführt. Ja, es ist tatsächlich so, die Kosten belaufen sich auf irgendetwas zwischen 1,5 und 80 Millionen Franken. Es kommt aber darauf an, wie Sie das nachher im Detail umsetzen und wer dann was macht. Das können wir aber immer über das Budget steuern. Wir erlassen nicht ein Gesetz, und nachher fliesst das Geld in irgendeine Kasse oder kann einfach aus der Kasse genommen werden, sondern wir haben nach wie vor das Budget, das dann bestimmt, wie man das macht.
Wir wissen im Moment tatsächlich auch noch nicht, wo wir Einsparungen machen, denn ein grosser Teil der Massnahmen bei der Cybersecurity erfolgt im Moment in den Departementen. Sie treffen sie autonom, alleine. Und sie tun es eben unterschiedlich. Damit haben sie, sobald sie ein Netzwerk schaffen, eben auch unterschiedliche Standards und ein nichteinschätzbares Sicherheitsrisiko, weil sie nicht wissen, wie die Systeme und die Leute untereinander agieren.
Ich bitte Sie daher dringend, einzutreten. Und wenn Sie dann noch Fragen haben – das habe ich auch, denn auch ich habe das Gesetz noch nicht ganz verstanden; es sind über 90 Artikel mit Auswirkungen in sehr vielen Bereichen –, können Sie diese Fragen stellen und das bereinigen. Aber treten Sie doch bitte nicht einfach nicht ein, nachdem der Ständerat das Gesetz schon einmal durchberaten hat, und versenken Sie es nicht einfach. Es gibt Handlungsbedarf.
Ich bitte Sie, einzutreten, Ihre Kommission zu beauftragen, daran zu arbeiten, und nicht Arbeitsverweigerung zu betreiben, damit wir vorwärtsmachen können.

Parmelin Guy, conseiller fédéral: Je vous demande d'entrer en matière et, ainsi, de renvoyer le dossier à votre commission pour qu'elle étudie à fond le travail constructif que le Conseil des Etats a accompli, ce qu'elle n'a pas fait, elle, jusqu'ici. Où en sommes-nous aujourd'hui? Quel est le contexte dans lequel nous évoluons?
Pour mémoire, en 2009 a eu lieu la première attaque contre des systèmes informatiques au Département fédéral des affaires étrangères; en 2012, vol de données au sein du Service de renseignement de la Confédération; en 2016, attaque contre les réseaux de RUAG; en 2017, attaque contre les systèmes du Département fédéral de la défense, de la protection

de la population et des sports. Les attaques contre les institutions gouvernementales sont de plus en plus fréquentes dans le monde entier; c'est le cas, par exemple, en Allemagne. En 2015, il y a eu la fameuse attaque contre le Parlement allemand; des informations extrêmement sensibles ont été dérobées, y compris de services de renseignement. En 2018, il y a deux semaines, une attaque a visé l'administration fédérale allemande: le réseau de haute sécurité allemand a été piraté, et des informations sensibles ont été dérobées.
Ces incidents ne représentent que la pointe de l'iceberg. De très nombreux autres incidents de sécurité ne sont simplement pas communiqués ou médiatisés. La plupart des incidents graves de sécurité ne sont pas la conséquence exclusive d'une cyberattaque, mais ce sont aussi le résultat d'actes volontaires ou involontaires d'employés des entreprises ou des administrations. Toutes ces attaques ont comme objectif, en principe, d'accéder à des informations protégées. Les coûts de rétablissement de l'intégrité et de la sécurité des systèmes sont généralement bien supérieurs aux coûts des mesures qui permettent de réduire ces risques en amont.
Alors, face à ce tableau et aux menaces liées à la digitalisation, que fait, ou qu'essaie de faire, la Confédération?
Il y a premièrement la Stratégie nationale de protection de la Suisse contre les cyberrisques. Par ce biais, le Conseil fédéral veut renforcer la résilience des infrastructures critiques du pays face aux menaces issues d'Internet; il s'agit de la cybersécurité du pays. Il y a ensuite le projet de loi sur la sécurité de l'information, dont nous discutons l'entrée en matière aujourd'hui. Ce projet de loi vise à donner au Conseil fédéral les instruments nécessaires pour que, dans le secteur de la cybersécurité, dans le contexte de la digitalisation, les autorités fédérales soient mieux armées. Il s'agit de la sécurité propre des autorités fédérales, y compris de leur cybersécurité. Au niveau du Département fédéral de la défense, de la protection de la population et des sports, nous avons notre fameux plan d'action de cyberdéfense, qui vise à renforcer notre propre sécurité et à permettre d'être prêt à appuyer les autorités civiles et à défendre les infrastructures critiques en cas d'attaque.
Pourquoi avons-nous absolument besoin de cette loi? Cela a été dit par plusieurs intervenants, c'est une loi extrêmement technique, peut-être peu intéressante politiquement, mais elle répond à des besoins juridiques et sécuritaires clairs, liés à l'évolution que nous constatons en particulier dans le domaine de la digitalisation. Elle vise à assurer la sécurité des informations et de l'infrastructure TIC (Techniques de l'information et de la communication) de toutes les autorités fédérales, y compris du Parlement, des tribunaux fédéraux, du Ministère public de la Confédération et de la Banque nationale suisse. Elle vise à adapter les bases légales existantes de façon à tenir compte des besoins liés à la digitalisation, et elle rassemble dans un acte unique les bases légales prévoyant les principales mesures de sécurité, notamment le management de la sécurité, la classification des informations, la cybersécurité, la gestion des identités électroniques, le contrôle de sécurité relatif aux personnes, la sécurité dans le cadre de marchés publics sensibles, l'appui aux infrastructures critiques dans le domaine de la cybersécurité et, enfin, l'organisation transversale de la sécurité. C'est ce que vise cette loi.
Et cette loi impose à toutes les autorités fédérales la mise en oeuvre de mesures de sécurité minimales – j'y reviendrai puisqu'on a parlé des coûts tout à l'heure –, notamment d'un système de gestion de la sécurité selon des standards internationaux de référence. C'est nécessaire en raison des risques croissants liés à l'interconnexion des réseaux et à l'échange électronique d'informations protégées entre les différentes autorités. Elle va donc créer les bases légales pour des mesures existantes – aujourd'hui, les bases légales ne sont pas suffisantes – et pour permettre la facilitation de la conclusion d'accords internationaux par le Conseil fédéral.
En plus, cette loi tient compte des demandes et des recommandations des organes de surveillance que sont les Commissions de gestion et la Délégation des Commissions de gestion. Elle est absolument nécessaire parce que, aujourd'hui, de nombreuses mesures de sécurité ne sont plus adaptées aux besoins de la digitalisation en cours. Certaines informations et certains systèmes informatiques de la Confédération ont une importance vitale pour le bon fonctionnement du pays. La Confédération traite de très nombreuses informations sensibles de citoyens, d'entreprises, de nombreux partenaires internationaux. Elle investit un milliard de francs par an pour son informatique.
Quel lien y a-t-il entre la loi sur la sécurité de l'information et le plan d'action de cyberdéfense du Département fédéral de la défense, de la protection de la population et des sports? Il faut savoir que cette loi va assurer la fondation d'une cybersécurité efficace. Concrètement, la sécurité de l'information représente environ 80 à 90 pour cent de la cyberdéfense au sein du département que j'ai l'honneur de diriger. On peut mettre en oeuvre le plan d'action de cyberdéfense du DDPS, mais, si nous n'avons pas cette loi, il restera de très nombreuses lacunes. Premièrement, pour garantir la sécurité et les prestations essentielles, le département doit s'assurer que ses partenaires critiques fournissent eux aussi un niveau de sécurité suffisant. Et, pour cela, nous avons besoin de cette loi. Deuxièmement, les contrôles de sécurité relatifs aux personnes ne sont admissibles que pour le traitement d'informations classifiées et non pour l'exploitation de systèmes informatiques critiques. Troisièmement, la procédure de sauvegarde du secret est aujourd'hui limitée aux mandats militaires classiques et n'est donc applicable ni aux autorités civiles, comme le Service de renseignement de la Confédération, ni à l'acquisition de prestations liées aux systèmes informatiques critiques, et sans renforcement de la sécurité et de la résilience de ces partenaires essentiels pour nous – ce que prévoit la loi dont nous discutons aujourd'hui l'entrée en matière –, eh bien, la capacité de défense et d'action du département va rester extrêmement limitée.
Venons-en à l'application de la loi aux petites et moyennes entreprises. C'était une des inquiétudes formulées lors des discussions qui ont eu lieu au Conseil des Etats, mais elle a pu être dissipée. Les PME ne seraient touchées que dans le cadre de la procédure de sécurité relative aux entreprises. Concrètement, lorsque la Confédération confierait un mandat sensible à une entreprise, elle devrait contrôler que cette entreprise ne représente pas un risque pour notre sécurité. Il s'agirait en particulier de lutter contre l'espionnage au profit d'Etats étrangers. Une fois ceci fait, l'entreprise serait qualifiée de sûre, puis appliquerait les mesures de sécurité adéquates durant l'exécution du mandat. Elle pourrait être contrôlée par un service spécialisé prévu par cette loi. L'analyse du risque se ferait toujours en lien avec le mandat concret.
Pour les PME, les conséquences seraient minimes: il n'y aurait, en principe, aucun coût en relation avec la procédure puisque les coûts seraient reportés sur le prix des prestations offertes. En fin de compte, ce serait donc la Confédération qui en supporterait le coût. Aujourd'hui, nous connaissons ce système pour les mandats militaires classifiés. Ainsi, 500 entreprises, en grande majorité des PME, opèrent sous notre contrôle. Cela fonctionne très bien, c'est peu bureaucratique, mais cela ne s'applique pas aux mandats civils. Or, le projet de loi prévoit d'autoriser la Confédération à délivrer des attestations de sécurité aux entreprises qui souhaitent prendre part à des marchés classifiés d'autres Etats ou organisations internationales, des marchés à haute valeur ajoutée.
Vous nous avez demandé des exemples concrets de dommages subis par des entreprises exportatrices suisses; je vais donc vous en donner.
1. L'entreprise Trüb AG à Aarau: l'entreprise Trüb était spécialisée dans des solutions d'identification et de sécurité. En 2015, ses activités ont été reprises par une société néerlandaise. Trüb avait été contactée par plusieurs pays pour créer de nouveaux documents d'identité. Elle n'a pas pu prendre part à ces marchés parce que nous n'avons pas pu délivrer la déclaration de sécurité nationale. Voilà une conséquence concrète.
2. L'entreprise Orell Füssli Holding AG à Zurich: au début des années 2000, dans le cadre du projet Nouveau passeport suisse, le Département fédéral de justice et police s'est renseigné auprès du DDPS sur la possibilité de contrôler

et de certifier Orell Füssli, qui était l'entreprise chargée de l'élaboration et de l'impression du nouveau passeport. Cette entreprise imprime le passeport suisse depuis 1959 déjà. Or, faute de base légale, le DDPS n'a pas pu accéder à cette requête et, à défaut d'avoir cette déclaration de sécurité, Orell Füssli n'a pas pu soumissionner à plusieurs mandats conséquents dans le cadre international, entre autres par rapport à un marché à Singapour. Voilà les conséquences.

Concernant les coûts de la loi, puisque plusieurs d'entre vous se sont exprimés sur ce sujet – et là, vous faites un très mauvais procès au Conseil fédéral –, je confirme que, dans le projet dont il est question, nous vous parlons du niveau d'ambition 1, et c'est cela qui est visé par le Conseil fédéral: des coûts d'introduction uniques de 5 millions de francs et, après, des coûts tels qu'ils sont décrits dans le message. C'est naturellement dans les ordonnances que nous allons régler le niveau d'ambition voulu. Nous nous sommes engagés auprès du Conseil des Etats, et je me suis engagé, au nom du Conseil fédéral, auprès de la commission de votre conseil, à soumettre ces ordonnances à l'appréciation des Commissions de la politique de sécurité – c'était une demande du corapport de la Commission des finances, elle est désormais remplie.

Qu'est-ce qui se passe dans ces cas-là? On analyse – et ce n'est pas la première fois que cela se fait – les ordonnances, on peut les corriger – elles sont de la compétence du Conseil fédéral –, et si, par hypothèse, le Conseil fédéral ne suivait pas les recommandations du Parlement, il resterait plusieurs armes à ce dernier. Il resterait ainsi la voie de la motion qui permet, dans les deux chambres, de décréter que tel point de l'ordonnance, on n'en veut pas; il resterait aussi le budget: toute la procédure budgétaire vous permet de contrôler le niveau d'ambition que nous voulons atteindre et c'est là que vous avez la possibilité d'intervenir si nécessaire et de rappeler le Conseil fédéral à ses devoirs.

Que se passera-t-il si nous n'avons pas de loi sur la sécurité de l'information? De nombreuses lacunes dans la sécurité resteront ouvertes, notamment dans le domaine informatique et des risques qui y sont liés. La sécurité de l'information et la cybersécurité continueront à être mal coordonnées, à être peu efficientes. Les entreprises suisses n'auront toujours pas accès aux marchés étrangers qui nécessitent une attestation nationale de sécurité. De nombreuses mesures de sécurité actuelles n'auront pas les bases légales que la Constitution et la législation exigent.

Si je développe autant, c'est parce que, comme la commission a pris la décision de proposer au conseil de ne pas entrer en matière, je suis obligé de vous parler du contenu de ce projet de loi afin que vous puissiez prendre une décision tout à l'heure.

Je vous donnerai encore quelques exemples de risques concrets en cas de rejet du projet.

Premièrement, prenons les risques liés à la cyberadministration. La Stratégie suisse de cyberadministration du Conseil fédéral, comme vous le savez, précise que les autorités fédérales et cantonales communiquent entre elles par voie électronique. A cette fin, les autorités fédérales créent de plus en plus d'interfaces et de passerelles entre les différents systèmes informatiques. Le risque augmente ainsi de voir des attaques contre une autorité se répercuter dans les domaines de compétence d'autres autorités. C'est exactement ce qui est arrivé en 2015 lors de l'attaque contre le Parlement allemand: de nombreuses données extrêmement sensibles de l'administration fédérale allemande ont ainsi été dérobées. Sans loi sur la sécurité de l'information, nous renonçons à l'harmonisation et nous laissons ouvertes de très grandes lacunes dans la sécurité.

La deuxième difficulté, c'est l'utilisation des données biométriques. Lorsqu'une personne demande un accès à un système informatique, à une infrastructure, on contrôle son identité et l'étendue de l'accès. Plus le système informatique ou l'infrastructure est sensible, plus il faut procéder à une vérification pointue. Comme les données biométriques sont extrêmement sensibles, une base légale formelle est indispensable. Elle existe, mais dans le domaine militaire, elle n'existe pas dans le domaine civil. C'est la loi sur la sécurité de l'information qui nous la donnerait.

Voilà deux exemples concrets de problèmes que nous pourrions rencontrer. La problématique de la collaboration internationale subsistera. Nous collaborons sur le plan international; nous échangeons des informations classifiées. Les accords internationaux prévoient entre autres une concordance, une équivalence en matière de classification et une certaine harmonisation.

Pour cela, il faut créer une base formelle expresse, qui existe – je le répète – dans le domaine militaire, mais qui n'existe pas dans le domaine civil, et elle nous rendrait énormément service pour passer des accords sur le plan international.

Avant d'arriver à la conclusion, j'aimerais répondre encore à certaines interrogations. Certains d'entre vous ont dit qu'il suffisait de modifier un certain nombre de lois pour avoir le même résultat et que tout irait bien ainsi. Alors, sans entrer dans les détails, il faudrait au minimum modifier neuf lois, et encore, nous n'aurions pas la garantie d'avoir une vision d'ensemble. De ce côté, je pense que le risque pris est beaucoup trop important.

J'ai parlé du contrôle des ordonnances, je n'y reviendrai pas. Certains d'entre vous ont argué de la complexité de la loi, dit qu'elle était trop dense, qu'elle serait difficile à appliquer. C'est une loi-cadre qui, au contraire, apporte de la souplesse à un secteur en évolution extrêmement rapide. Au moyen des ordonnances, sous le contrôle du Parlement, nous pourrions, le cas échéant, adapter certaines choses extrêmement rapidement.

Certains d'entre vous ont dit qu'il fallait élaguer – "entschlacken" – cette loi, notamment Monsieur le conseiller national Dobler, mais pour savoir où il faut le faire, il vous faut entrer en matière et nous dire où vous voulez le faire. Ce n'est pas en refusant d'entrer en matière qu'on va arriver à faire avancer le projet.

J'aimerais encore lancer un appel à celles et ceux qui seraient hésitants. En particulier, je ne résiste pas à l'envie de vous lire la prise de position, lors de la procédure de consultation, du parti libéral-radical: "La Suisse doit renforcer sa sécurité dans ce domaine, comme l'ont montré certains incidents survenus ces dernières années. La gestion des risques liés à l'utilisation des TIC dans tous les secteurs de la Confédération est donc devenue une nécessité inhérente au développement de la société de l'information. Cette loi est en effet nécessaire pour combler les lacunes techniques de notre système de protection des informations – exécution, efficacité, rentabilité de l'ordonnance adoptée en 2007 par le Conseil fédéral –, mais également des lacunes organisationnelles. C'est pourquoi le PLR se prononce en faveur du rassemblement des mesures en matière de protection de l'information en une seule réglementation homogène concernant toutes les autorités fédérales et celles qui leur sont subordonnées. La plupart des conséquences économiques de cette loi vont dans le sens des exigences du PLR. Elles laissent en effet escompter un renforcement de la compétitivité des entreprises et une meilleure protection des secrets économiques qu'elles placeront sous la protection du gouvernement."

J'en arrive à la conclusion. Cette loi sur la sécurité de l'information est un des fondements, un des piliers de la stratégie de sécurité en matière d'information et de cyberdéfense de la Confédération. Durant ces derniers mois, cela a été rappelé par les personnes représentant la minorité de la commission, plusieurs interventions parlementaires ont exigé du Conseil fédéral qu'il renforce la sécurité du pays face aux nouveaux risques dans ce secteur qui, comme vous le savez, est en très rapide évolution, face aux défis posés par la digitalisation et aux lacunes qui pourraient être exploitées par des agresseurs potentiels. Il ne serait pas conséquent de votre part de refuser d'entrer en matière sur un projet essentiel sans même, et j'insiste là-dessus, que votre commission préparatoire ait pris la peine de l'étudier.

Je vous invite donc instamment à entrer en matière sur ce projet de loi, certes technique, nous l'avouons tous, certes difficile d'approche d'un point de vue politique, mais qui va permettre à notre pays, à ses autorités, et à ses entreprises

d'être bien mieux armés face à ces nouvelles menaces que nous devons affronter tous les jours.

Kiener Nellen Margret (S, BE): Monsieur le conseiller fédéral, vous vous êtes référé, comme d'autres, au corapport de la Commission des finances. Puisque j'étais présidente de la Commission des finances lors de l'examen de cet objet l'année dernière, je tiens à vous poser la question cruciale que la Commission des finances avait alors posée très clairement. Je vous prie, si possible, de me répondre en allemand, je vais également vous poser la question en allemand.

Für die Finanzkommission war es klar, dass die Entscheide darüber, welche Kosten generiert würden, auf Verordnungsebene fallen, weil in den Verordnungen die Sicherheitsstandards festgelegt werden. Wir aus der Finanzkommission haben gefordert, dass Sie diese Verordnungsentwürfe der Finanzkommission und natürlich auch der SiK zur Konsultation geben. Können Sie bestätigen, dass Sie diese Verordnungsentwürfe unserer Finanzkommission und unserer SiK zur Konsultation geben werden? Können Sie uns, wenn jetzt eingetreten wird, einen Zeithorizont nennen, wann ungefähr diese Verordnungsentwürfe in die Kommissionen kommen werden?

Parmelin Guy, Bundesrat: Ich habe mich im Namen des Bundesrates dafür engagiert, diese Verordnungen den Finanzkommissionen und den Sicherheitspolitischen Kommissionen beider Räte zu zeigen. Natürlich machen wir das, sobald das Gesetz angenommen ist. Bis jetzt ist es nicht möglich gewesen. Wir wollen nicht im Voraus daran arbeiten, ohne zu wissen, ob das Gesetz angenommen wird. Aber ich engagiere mich hier im Namen des Bundesrates dafür, das zu machen.

La sous-commission de la Commission des finances a proposé à cette dernière qu'elle demande à la Commission de la politique de sécurité que le Conseil fédéral lui soumette les ordonnances concernées pour consultation. Dans le corapport de la Commission des finances, il est indiqué que cette proposition de la sous-commission avait fait l'unanimité en son sein.

Je m'engage, je le répète, à soumettre les ordonnances à la Commission de la politique de sécurité.

Béglé Claude (C, VD): Monsieur le conseiller fédéral, il y a quelque chose que je ne comprends pas: personne ne semble remettre en cause la nécessité de moderniser notre cybersécurité, mais les objections portent essentiellement sur le flou quant aux coûts relatifs à la mise en oeuvre de la loi.

Sans parler des 5 millions de francs nécessaires pour garantir le niveau 1 de sécurité, comment évaluez-vous le rapport coût/bénéfice de cette loi, c'est-à-dire le rapport entre les montants à engager et les problèmes que nous pourrions potentiellement nous épargner? A combien évaluez-vous le surcoût qui serait occasionné en cas de report de la mise en oeuvre de la loi?

Parmelin Guy, conseiller fédéral: Monsieur Béglé, votre question est complexe et il est assez difficile d'y répondre. Dans le message, nous avons clairement dit que nous voulions atteindre le niveau d'ambition 1. Le niveau d'ambition 1 représente un coût unique de mise en oeuvre de la loi d'environ 5 millions de francs. Ensuite, des coûts d'exploitation vont s'ajouter. Déterminer le rapport coût/efficacité est extrêmement difficile.

Mais prenez l'exemple du Bundestag allemand, qui s'est fait pirater son système informatique et dérober des informations classifiées et confidentielles. L'infrastructure a dû être reconstruite de A à Z et, pourtant, les spécialistes ne sont pas allés au fond des choses puisque, quand ils ont redémarré le système, ils se sont aperçu qu'il y avait encore des résidus de l'attaque. Dérober des informations classifiées peut avoir des conséquences extrêmement graves pour la Confédération, mais aussi pour les entreprises qui sont concernées. C'est aussi pour cela que l'on a besoin de cette loi. Les coûts, je le crains, ne pourront malheureusement être précisés qu'au moment où on aura vraiment subi un gros dommage.

Clottu Raymond (V, NE), pour la commission: Je vais être relativement bref. La majorité de la commission propose de ne pas entrer en matière sur ce projet de loi, et ce pas uniquement pour des raisons financières, mais parce qu'elle a estimé qu'il ne générerait pas de valeur ajoutée déterminante – je vais m'expliquer. Au contraire, on a plutôt l'impression qu'une telle loi, ou plus exactement ce sac de noeuds – c'est un peu l'impression que nous donne ce projet –, ne ferait qu'engendrer beaucoup trop de bureaucratie et ne pourrait que modestement, voire pas du tout, contribuer à une mise en oeuvre uniforme, efficace et surtout efficiente, des dispositions visant à regrouper en une seule réglementation tous les éléments relatifs à la sécurité de l'information.

Nous avons passablement parlé ce matin de "cyber". Alors parlons-en encore. Pour lutter contre les cyberrisques, nous avons surtout besoin d'une meilleure coordination, ce qui peut être fait avec le système actuel en y apportant, au besoin, des améliorations ciblées dans le cadre des structures actuelles. Concernant les certificats de sécurité pour les entreprises, cela peut aussi se faire dans le cadre des lois, des bases légales en vigueur.

Nous avons vraiment l'impression, je le répète, qu'on a affaire, avec cette loi, à un sac de noeuds qui ne va rien résoudre, bien au contraire.

Brélaz Daniel (G, VD): Monsieur Clottu, j'ai l'impression que nous ne vivons pas dans le même univers informatique. Je ne savais pas, jusqu'à ce jour, qu'il y en avait deux. Ce que je veux dire, au nom de la Commission des finances – j'ai siégé dans la sous-commission compétente, je sais que ce n'est pas ce qui vous intéresse mais je tiens à le préciser –, c'est que, comme il s'agit de quelques millions de francs qui sont en jeu dans la loi sur la sécurité de l'information alors que les dégâts peuvent se chiffrer en milliards de francs en cas d'attaque contre les réseaux informatiques, nous avons estimé qu'il fallait aller de l'avant même s'il fallait préciser certains aspects financiers, ce qu'a fait le Conseil fédéral.

Mes questions sont les suivantes. Monsieur Clottu, la commission et votre majorité de droite pensent-elles qu'il vaut la peine de prendre un risque qui se chiffre en milliards de francs pour économiser quelques millions de francs? Ne craignez-vous pas que, dans quelques années, on parle de la Commission de la politique d'insécurité plutôt que de la Commission de la politique de sécurité?

Clottu Raymond (V, NE), pour la commission: Non, Monsieur Brélaz, je ne crois pas. Je considère, comme je l'ai dit, que nous disposons aujourd'hui des bases légales nécessaires et que nous pouvons être efficients. Il y a des améliorations à apporter, mais il n'y a pas besoin d'une usine à gaz pour être efficace.

Sommaruga Carlo (S, GE): Ma question portera sur les thèmes des bases légales et de l'usine à gaz. Dans le message du Conseil fédéral, à la page 2776, il est indiqué que, aujourd'hui, les bases légales sont disséminées dans les textes suivants: loi sur l'organisation du gouvernement et de l'administration, loi sur le Parlement, loi fédérale sur l'armée et l'administration militaire, Code pénal, loi fédérale instituant des mesures visant au maintien de la sûreté intérieure, loi sur le personnel de la Confédération, loi fédérale sur les marchés publics, loi fédérale sur l'archivage, loi fédérale sur la protection des données et loi sur la transparence. En d'autres termes, l'ensemble des dispositions relatives à la sécurité de l'information se répartissent dans plus de dix lois, et vous nous dites qu'il n'y a pas de plus-value à adopter une nouvelle loi organique qui soit également une loi-cadre. Ne commettez-vous pas une erreur d'appréciation lorsque l'on voit la complexité du dispositif juridique actuel?

Clottu Raymond (V, NE), pour la commission: Monsieur Sommaruga, tout comme moi, vous étiez présent aux séances de commission. Lors d'une de ces séances, un

membre a posé la question au juriste ayant participé à l'élaboration de la loi sur la sécurité de l'information. Les différences, par rapport aux bases légales actuelles, il y en a très peu, voire aucune; on nous a certifié qu'il y avait certaines améliorations à apporter. Je pense qu'on n'a pas eu la même écoute à ce moment-là.

Gmür Alois (C, SZ), für die Kommission: Aktuell gibt es zum Beispiel bezüglich Informationen drei Klassifikationsstufen, nämlich intern, vertraulich und geheim. Jetzt wird ein Gesetz geschaffen, um das zu managen. Die Mehrheit ist der Meinung, dass es, um die Informationssicherheit zu managen, nicht ein solch umfassendes Gesetz braucht, mit dem die Bürokratie massiv ausgebaut wird. Je nach Sicherheitsstandard verursacht das Gesetz Einführungskosten von 5 bis 20 Millionen Franken – nur Einführungskosten! – und nachher je nach Standard Betriebskosten von 1,5 bis 87,5 Millionen Franken. Es ist, das möchte ich hier erwähnen, kein Gesetz für die Informatiksicherheit, es ist ein Informationssicherheitsmanagement-Gesetz.
Die Mehrheit der Kommission fragt sich, wie ein Management mit mehr als 90 Gesetzesartikeln möglich ist. Ein solches Management wird tatsächlich aufwendig. Das beweisen die Kosten. Die Mehrheit ist nicht der Meinung, dass das Problem so akut ist, dass anfänglich 9 bis 15 Stellen, dann allenfalls 42 Stellen und beim Sicherheitsniveau 3 am Schluss 78 Stellen geschaffen werden müssen. Hundert Prozent Sicherheit gibt es auch mit diesem Gesetz nicht.
Die Kommission bittet Sie, nicht auf die Vorlage einzutreten.

Seiler Graf Priska (S, ZH): Es gab einige Verwirrung wegen der Finanzkommission. Sie sind ja in der komfortablen Lage, dass Sie sowohl in der SiK wie auch in der Finanzkommission sind. Können Sie nochmals klar darlegen, wie die Finanzkommission in Bezug auf dieses Geschäft entschieden hat? Wie genau war das Abstimmungsverhältnis?

Gmür Alois (C, SZ), für die Kommission: Die Finanzkommission hat mit Blick auf die Kosten so entschieden, dass sie nachher die Verordnung sehen will. Schon in der Finanzkommission herrschte also Unsicherheit bezüglich dieser Kosten. Das hat die SiK auch aufgenommen und deshalb gefordert, sie wolle erfahren, wie hoch die genauen Kosten sein werden. Diese Information über die Kosten haben wir dann an der zweiten Sitzung bekommen.
Aufgrund dieser Information hat die SiK entschieden, nicht auf die Vorlage einzutreten und ein Gesetz zu machen, das schlanker ist als jenes, das uns jetzt vorliegt.

Sommaruga Carlo (S, GE): Monsieur Alois Gmür, Madame Seiler Graf vous a posé la question suivante: Quelle a été la décision de la Commission des finances formellement? A-t-elle été prise à l'unanimité? Est-ce que cela a été du cinquante/cinquante, pour approuver le projet du Conseil fédéral? Quel a été le Stimmenverhältnis in der Finanzkommission?

Gmür Alois (C, SZ), für die Kommission: Das Stimmenverhältnis weiss ich nicht mehr ganz genau. Ich bin hier Berichterstatter der SiK und nicht der Finanzkommission. Ich weiss nur, in der Finanzkommission – das habe ich vorhin ja gesagt – hat man gesagt, ja, es brauche etwas, es brauche ein Gesetz. Aber die Kosten wurden massiv infrage gestellt.

Flach Beat (GL, AG): Herr Kollege Gmür, ich dachte eigentlich, dass Sie noch wissen, dass im Bericht der Finanzkommission stand, dass sie einstimmig auf das Geschäft eingetreten ist.

Gmür Alois (C, SZ), für die Kommission: Das weiss ich nicht mehr.

Kiener Nellen Margret (S, BE): Herr Kollege Gmür, Sie haben ja den Mitbericht sicher in Ihren Akten. Können Sie bestätigen, dass im Mitbericht der Finanzkommission Folgendes steht: "Die Subkommission ist sich einig, dass das Informationssicherheitsgesetz notwendig ist. Die Frage der Informationssicherheit ist heute zentral. Die Wichtigkeit dürfte eher noch zunehmen." Und dann noch ein letzter Satz: "Der Antrag der Subkommission fand in der Kommission einhellige Zustimmung." Es gab also keine Abstimmung.

Gmür Alois (C, SZ), für die Kommission: Genau deswegen sind wir ja in der SiK zuerst auf dieses Gesetz eingetreten. Als wir nachher dann die Kosten sahen, haben wir gesagt, das könne es ja nicht sein, da müsse ein schlankeres Gesetz gemacht werden. Wir sind in der SiK nicht der Meinung, dass nichts gemacht werden muss. Aber ein solches Gesetz mit über 90 Artikeln finden wir übertrieben. Es verursacht riesige Kosten und bedingt zusätzliche Stellen. Dahinter kann die Mehrheit der Kommission nicht stehen.

Le président (de Buman Dominique, président): Nous votons sur la proposition de non-entrée en matière de la majorité. Une minorité Sommaruga Carlo et le Conseil fédéral proposent d'entrer en matière.

Abstimmung – Vote
(namentlich – nominatif; 17.028/16709)
Für Eintreten ... 68 Stimmen
Dagegen ... 117 Stimmen
(8 Enthaltungen)

Le président (de Buman Dominique, président): L'objet retourne au Conseil des Etats.

17.051

Zur Förderung der Velo-, Fuss- und Wanderwege (Velo-Initiative). Volksinitiative

Pour la promotion des voies cyclables et des chemins et sentiers pédestres (initiative vélo). Initiative populaire

Schlussabstimmung – Vote final

Ständerat/Conseil des Etats 30.11.17 (Erstrat – Premier Conseil)
Nationalrat/Conseil national 01.03.18 (Zweitrat – Deuxième Conseil)
Nationalrat/Conseil national 13.03.18 (Schlussabstimmung – Vote final)
Ständerat/Conseil des Etats 13.03.18 (Schlussabstimmung – Vote final)
Nationalrat/Conseil national 16.03.18 (Schlussabstimmung – Vote final)
Ständerat/Conseil des Etats 16.03.18 (Schlussabstimmung – Vote final)

Le président (de Buman Dominique, président): Le Conseil national a traité cet objet le 1er mars 2018 et l'a adopté lors du vote sur l'ensemble. Nous allons procéder aujourd'hui au vote final sur ce contre-projet, selon l'article 101 alinéa 3 de la loi sur le Parlement.

2. Bundesbeschluss über die Velowege sowie die Fuss- und Wanderwege (direkter Gegenentwurf zur Volksinitiative "zur Förderung der Velo-, Fuss- und Wanderwege (Velo-Initiative)")
2. Arrêté fédéral concernant les voies cyclables et les chemins et sentiers pédestres (contre-projet direct à l'initiative populaire "pour la promotion des voies cyclables et des chemins et sentiers pédestres (initiative vélo)")