zurück, sind aber an anderen Hotspots in dieser Welt sehr stark engagiert, beispielsweise Frankreich in der Sahelzone, wo es eine sehr, sehr schwierige Situation gibt und wo es, kann man sagen, brennt. Frankreich ist sehr stark in der Sahelzone engagiert. Es ist auch, wie Sie richtig sagen, im Interesse der Schweiz, wenn dort etwas zur Beruhigung beigetragen werden kann. Darum, denke ich, ist es wichtig, dass auch die Schweiz ihren Beitrag zur internationalen Sicherheit leistet, und dies eben im Kosovo, wo wir allgemein anerkannte gute Leistungen erbringen können.

Pointet François (GL, VD), pour la commission: L'augmentation d'effectifs demandée doit être considérée en tenant compte du contexte. La situation change vite, même entre la discussion en commission et celle en plénum. Nous faisons partie du système, nous participons à l'analyse de la situation, nous collaborons à la définition des besoins et nous sommes prêts à prendre nos responsabilités.
L'analyse de la situation et des besoins a convaincu la commission que cette augmentation, qui est un plafond, est nécessaire. Elle vous propose donc de suivre le Conseil fédéral sur l'augmentation de l'effectif, par 14 voix contre 10.
Pour ce qui est de la deuxième minorité Heimgartner, la réserve demandée par le Conseil fédéral est à destination de la Swisscoy et non de la Kfor. C'est aussi un signal en direction de nos troupes sur place qui indique que leur sécurité sera assurée en cas de dégradation de la situation et qu'elles pourront continuer à remplir leur mission. La commission le comprend ainsi.
Elle vous propose de suivre le Conseil fédéral, par 14 voix contre 10, en rejetant la deuxième minorité Heimgartner.

Marti Min Li (S, ZH), für die Kommission: Bei diesen beiden Minderheiten Heimgartner geht es jeweils um den Bestand. Die erste Minderheit Heimgartner möchte den Maximalbestand auf 165 Angehörige der Armee beschränken. Der zweite Antrag möchte Artikel 2 ganz streichen. Diese Bestimmung gibt dem Bundesrat die Kompetenz, das Kontingent kurzfristig zu verstärken, mit 50 Personen für maximal acht Monate zur Instandhaltung und mit 20 Personen für längstens vier Monate bei erhöhter Bedrohung. Die Minderheit ist der Meinung, dass diese Aufstockungsmöglichkeiten nicht benötigt werden.
Die Mehrheit beantragt, beide Anträge abzulehnen. Die Aufstockung auf 195 Militärangehörige wird für Genieleistungen gebraucht, wir haben das schon in der Eintretensdebatte gehört, um allfällige Strassensperren wieder abzubauen und die Mobilität und die Bewegungsfreiheit zu gewährleisten. Ein Teil der Aufstockung betrifft Nachrichtenoffiziere, und ein Teil soll die Präsenz in Mitrovica verstärken, wo die Lage weiterhin sehr angespannt ist.
Die Mehrheit ist auch der Meinung, dass die Lage fragil ist und sich immer wieder verändert, sodass es sinnvoll ist, dass der Bundesrat hier eine gewisse Flexibilität erhalten soll. Sie glaubt nicht, dass der Bundesrat diese ohne Not in Anspruch nehmen würde.
Die Kommission hat mit 14 zu 10 Stimmen diese beiden Anträge abgelehnt. Zudem hat sie der Vorlage mit 16 zu 8 Stimmen zugestimmt. Ich bitte Sie im Namen der Kommission, es ihr gleichzutun.

Art. 1

Abstimmung – Vote
(namentlich – nominatif; 19.082/20444)
Für den Antrag der Mehrheit ... 102 Stimmen
Für den Antrag der Minderheit ... 80 Stimmen
(3 Enthaltungen)

Art. 2

Abstimmung – Vote
(namentlich – nominatif; 19.082/20445)
Für den Antrag der Mehrheit ... 103 Stimmen
Für den Antrag der Minderheit ... 81 Stimmen
(3 Enthaltungen)

Art. 3–5
Antrag der Kommission
Zustimmung zum Entwurf des Bundesrates
Proposition de la commission
Adhérer au projet du Conseil fédéral

Angenommen – Adopté

Gesamtabstimmung – Vote sur l'ensemble
(namentlich – nominatif; 19.082/20446)
Für Annahme des Entwurfes ... 105 Stimmen
Dagegen ... 77 Stimmen
(5 Enthaltungen)

17.028

Informationssicherheitsgesetz
Loi sur la sécurité de l'information

Differenzen – Divergences

Ständerat/Conseil des Etats 04.12.17 (Erstrat – Premier Conseil)
Nationalrat/Conseil national 13.03.18 (Zweitrat – Deuxième Conseil)
Ständerat/Conseil des Etats 26.09.18 (Differenzen – Divergences)
Nationalrat/Conseil national 04.06.20 (Differenzen – Divergences)

Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
(= Eintreten)

Proposition de la commission
Adhérer à la décision du Conseil des Etats
(= Entrer en matière)

Fridez Pierre-Alain (S, JU), pour la commission: Après une première tentative manquée en mars 2018, notre conseil, second conseil sur cet objet, a enfin l'occasion d'entrer en matière sur cette loi sur la sécurité de l'information, un texte important comme en témoigne le libellé de son article 1 alinéa 1: "La présente loi vise à garantir la sécurité du traitement des informations relevant de la compétence de la Confédération et la sécurité de ses moyens informatiques." A l'alinéa 2, il est précisé qu'elle vise ainsi à protéger les intérêts publics suivants: la capacité de décision et d'action des autorités et organisations de la Confédération; la sécurité intérieure et extérieure de la Suisse; les intérêts de la politique extérieure de la Suisse; les intérêts économiques, financiers et monétaires de la Suisse; l'accomplissement des obligations légales et contractuelles des autorités et organisations de la Confédération en matière de protection des informations.
Après un premier passage au Conseil des Etats, qui a accepté le projet du Conseil fédéral, sous réserve de différentes modifications, par 39 voix sans opposition et 4 abstentions, notre conseil a refusé d'entrer en matière le 13 mars 2018, par 117 voix contre 68 et 8 abstentions. L'opposition de la majorité de la Commission de la politique de sécurité de notre conseil, puis de notre conseil, s'appuyait sur des arguments qui avaient trait à la crainte d'un surcroît de bureaucratie et de conséquences financières trop importantes.
Le Conseil des Etats a maintenu sa position déterminée et notre conseil est à nouveau saisi de ce texte. Cette fois, cependant, l'approche de votre Commission de la politique de sécurité est très différente. Lors de sa séance des 8 et 9 octobre 2018, elle est entrée en matière par 17 voix contre 8. Par la suite, elle a décidé d'une interruption transitoire du traitement de l'objet jusqu'à l'été 2019, le temps d'obtenir un rapport complémentaire permettant de répondre à quelques interrogations et craintes portant en particulier sur l'adéquation des mesures proposées ainsi que les coûts supplémentaires

susceptibles d'être induits par la loi pour les entreprises privées qui obtiendraient un mandat de la Confédération.

Rassurée par l'ensemble des informations obtenues, la commission a procédé à la discussion par article lors de ses séances d'août et octobre 2019.

La loi sur la sécurité de l'information vise à renforcer et à sécuriser le fonctionnement de l'Etat à un moment où nous prenons toutes et tous conscience de l'importance de la problématique cyber et où différentes attaques contre les systèmes d'information de la Confédération ont démontré des lacunes dans nos systèmes actuels de sécurisation, des systèmes disparates et régis par différentes bases légales.

Cette loi vise à regrouper dans un acte législatif unique les bases légales régissant le traitement de la sécurité de l'information et des moyens informatiques de la Confédération. Il est appelé à devenir la base de référence unique pour l'ensemble des autorités et organismes de la Confédération pour élever le standard de sécurité. La liste de ces autorités et organismes est longue: l'Assemblée fédérale, le Conseil fédéral, les tribunaux fédéraux, le Ministère public de la Confédération, la Banque nationale, les Services du Parlement, l'Administration fédérale ou encore l'Armée.

Cette loi fixe le cadre de la règlementation dans différents domaines sensibles: la gestion des risques, la classification des informations, la sécurité des moyens informatiques, les contrôles de sécurité relatifs aux personnes – un domaine particulièrement sensible qui se doit d'être, vu les enjeux, suffisamment efficace, tout en respectant le droit des personnes –, ou encore la protection physique des informations et des moyens informatiques.

L'esprit de la loi vise à assurer le niveau de protection des informations en fonction des impératifs et des atteintes potentielles aux intérêts supérieurs des différentes structures de l'Etat, sur la base de principes essentiels. Premièrement, la confidentialité: les informations ne doivent être accessibles qu'aux personnes autorisées selon les échelons de classification "interne", puis "confidentiel" et ensuite "secret". Deuxièmement, la disponibilité: des données accessibles en cas de besoin en tout temps. Troisièmement, l'intégrité: pas de modification possible sans droit ou par mégarde. Quatrièmement, la traçabilité.

Sont également abordées dans ce texte les procédures de sécurité de l'information lors de l'exécution de mandats publics par des entreprises ou des sous-contractants, dans la mesure où ces mandats impliquent l'exercice d'une activité sensible.

Un autre point sensible est celui des infrastructures critiques. Vu leur importance dans toute une série de prestations essentielles offertes à la population et permettant le bon fonctionnement de l'Etat, une des tâches de la Confédération est de leur apporter un soutien pour assurer la poursuite en tout temps du service public. Ces moyens seraient les suivants: l'identification et l'évaluation précoces des dangers, des menaces, des vulnérabilités et des failles de sécurité; la gestion des situations extraordinaires par un service national d'alerte et un service d'assistance; l'appui des services compétents de la Confédération pour des conseils et des échanges d'informations avec les responsables des infrastructures critiques.

La question des coûts a été débattue de façon approfondie au sein de la commission. Les coûts engendrés par la réforme et l'incidence sur le nombre de postes de travail ont été des points longuement discutés. Dans le message du Conseil fédéral, cette question est abordée de manière pragmatique. Les coûts dépendront de ce que l'on aura l'intention de faire en pratique. Des mesures minimales, la correction des lacunes essentielles, une certaine harmonisation des pratiques et des moyens, pourraient être intégrés dans le budget normal, donc sans frais notables supplémentaires. En revanche, des mesures plus ambitieuses, par exemple obliger l'ensemble des autorités et organisations soumises à la loi à se conformer pour leur système de gestion de la sécurité de l'information à la norme ISO 27 001 reviendrait à 8 à 12 millions de francs, essentiellement pour des charges de conseil.

Au niveau des postes de travail, on parle de 15 postes au maximum. Tant les coûts que les postes supplémentaires dépendront de la mise en musique de cette loi par le Conseil fédéral, en particulier en fonction de la réglementation de l'organisation interne. Ce sujet est essentiel pour notre pays en termes de sécurité, dans le contexte des menaces "cyber", sujet récurrent et prioritaire. Les moyens nécessaires mériteraient d'être engagés.

Autre point important: sécurité de l'information ne veut pas dire opacité de l'information. A l'article 4 de la loi, il est rappelé que "la loi du 17 décembre 2004 sur la transparence prime la présente loi".

Lors de son traitement au Conseil des Etats, le projet du Conseil fédéral a été largement amendé. Pour l'essentiel, notre commission s'est alignée sur le Conseil des Etats. Les débats ont porté principalement sur la liste des infrastructures critiques concernées, avec une proposition d'y ajouter les installations hospitalières de base. Une proposition a été faite de s'aligner sur des normes reconnues sur le plan international pour réaliser les différentes améliorations au niveau de la sécurité. La commission a examiné le fait d'utiliser le numéro AVS pour identifier les personnes dont les données sont traitées. Elle a statué sur le fait de savoir s'il faudrait que les responsables d'une infrastructure critique communiquent la survenue d'un éventuel incident. Ces divers points seront débattus lors de la discussion par article, puisqu'ils font l'objet de propositions de minorité.

Votre commission a décidé, presque sans contestation, de modifier certaines dispositions, qui représentent dès lors autant de divergences avec le Conseil des Etats. Par exemple, à l'article 7 alinéa 3, le Conseil fédéral devra consulter les Commissions de politique de sécurité sur ses objectifs en matière de sécurité de l'information et les coûts afférents. Cette proposition a été acceptée par 20 voix contre 2.

A l'article 23 alinéa 2, il est proposé, dans les zones de sécurité, d'interdire plutôt que de soumettre à autorisation certains objets, en particulier les appareils de prises de vue et de son.

A l'article 30 alinéa 4 lettre g, relatif aux personnes soumises ou non à un contrôle de sécurité, il est proposé de remplacer le texte initial "membre d'un gouvernement cantonal et juge auprès d'un tribunal cantonal" par "magistrat cantonal élu par le peuple ou par le parlement du canton concerné". Cette proposition a été acceptée à l'unanimité.

Au vote sur l'ensemble, la commission a approuvé le projet par 16 voix contre 1 et 5 abstentions.

Je vous remercie de bien vouloir entrer en matière.

Gmür Alois (M-CEB, SZ), für die Kommission: Ihre Kommission befasst sich schon seit mehr als zwei Jahren mit dem Informationssicherheitsgesetz. Der Ständerat ist Erstrat und hat das Gesetz in der Wintersession 2017 beraten. Er hat damals dem Entwurf des Bundesrates mit nur wenigen Änderungen zugestimmt. In der Frühjahrssession 2018 ist dieser Rat Ihrer Kommission gefolgt und damals nicht auf das Gesetz eingetreten. Der Ständerat hat das Gesetz dann in der Herbstsession 2018 ein zweites Mal traktandiert und an seinem Beschluss festgehalten. Infolgedessen liegt es jetzt an unserem Rat, das Geschäft wieder zu behandeln.

An der Sitzung vom 8./9. Oktober 2018 entschied Ihre Kommission mit 17 zu 8 Stimmen bei 1 Enthaltung, auf das Geschäft einzutreten. An dieser Sitzung beschloss die Kommission dann aber mit 17 zu 9 Stimmen eine Sistierung und beauftragte das VBS, bis Mitte 2019 aufzuzeigen, wie die Vorlage verbessert werden kann. Die Kommission verlangte Verbesserungen unter anderem bezüglich der Kosten für die öffentlichen und privaten Unternehmen bzw. wie die Bestimmungen zu überarbeiten sind, damit diese Kosten für die Unternehmen keine Belastung darstellen. Weiter verlangte sie, das Gesetz zu konkretisieren, zu vereinfachen und zu straffen. Auch wollte die Kommission eine verstärkte Kontrolle des Parlamentes bei der Anwendung und Überwachung des Gesetzes und eine Abklärung, ob der Bereich Personensicherheitsprüfung in einem vom ISG getrennten, separaten Erlass geregelt werden könnte. Es wurde auch gefordert, aufzuzeigen, inwieweit das ISG auf die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken abgestimmt ist.

Fristgerecht wurde der Kommission vom VBS das entsprechende Zusatzdokument in Erfüllung des Auftrags zugestellt. Im August letzten Jahres diskutierte die Kommission die umfangreichen Zusatzinformationen. Im Lichte dieser Informationen nahm die Kommission die Detailberatung auf.
Im Namen der Kommissionsmehrheit bitte ich Sie deshalb, jetzt auf das Gesetz einzutreten und anschliessend die Detailberatung aufzunehmen.

Zuberbühler David (V, AR): Sie befassen sich zum zweiten Mal mit dem Informationssicherheitsgesetz. Mit diesem will der Bundesrat die Informationssicherheit beim Bund an die Herausforderungen der Informationsgesellschaft anpassen. Für alle Bundesbehörden soll ein formell einheitlicher gesetzlicher Rahmen für den Schutz von Informationen und die Sicherheit beim Einsatz von Informatikmitteln geschaffen werden. Es geht hauptsächlich um die Themen Risikomanagement, Klassifizierung von Informationen, Informatiksicherheit, Personensicherheitsprüfungen, Sicherheit bei sensitiven Beschaffungen oder die Unterstützung der Betreiber von kritischen Infrastrukturen im Bereich der Informationssicherheit durch den Bund.
Das Gesetz soll nach Inkrafttreten nicht nur die Bundesbehörden verpflichten, sondern auch, und das ist ganz wichtig, weite Teile der Wirtschaft. Alle Organisationen des öffentlichen und privaten Rechts, die kritische Infrastrukturen betreiben, werden sich nach der neuen Rechtsnorm zu richten haben.
Nachdem der Ständerat in der Wintersession 2017, obwohl es praktisch keine Wortmeldungen gab, auf das Geschäft eingetreten ist, hat der Nationalrat eine ganz andere Haltung eingenommen. Die grosse Kammer ist der vorberatenden Kommission gefolgt und hat damals Nichteintreten beschlossen. Als Argument wurde unter anderem angeführt, dass mit dem Gesetz ein zu grosser und komplexer Informationsschutzapparat aufgebaut würde, der eine Eigendynamik entfalten und sich zunehmend der Kontrolle des Parlamentes entziehen könnte. Ausserdem war einer Ratsmehrheit nicht klar, welchen Mehrwert das neue Gesetz bringen sollte.
Den Ständerat liess dies kühl. Um sein Gesicht zu wahren, ist er nach dem Nichteintretensentscheid des Nationalrates wieder auf die Vorlage eingetreten. Den Rest kennen Sie: Nachdem unsere Sicherheitspolitische Kommission zusätzliche Abklärungen in Auftrag gegeben hatte, ist auch sie mehrheitlich auf das Geschäft eingetreten und hat sich danach mit der Detailberatung auseinandergesetzt.
Den Grundauftrag zur nun vorliegenden komplizierten Vorlage des Bundesrates erteilte dieser übrigens bereits am 12. Mai 2010. Die Umsetzung dauert somit bereits zehn Jahre. In Zeiten von Cyberwar mag es sich unheimlich gut anhören, wenn der Bundesrat die Informationssicherheit anpassen will. In Tat und Wahrheit wird mit dieser Vorlage aber ein umfangreiches und komplexes Bürokratiemonster erschaffen.
Vonseiten des Bundesrates heisst es zwar, dass angesichts der zunehmenden Vernetzung eine Harmonisierung der Sicherheitsniveaus zwischen den Bundesbehörden, den Kantonen und den internationalen Partnern der Schweiz dringend sei. Zusätzlich sei das Gesetz – auch wenn, mit Verlaub, in den letzten zehn Jahren nicht wirklich jemand danach geschrien hat – notwendig für die Schweiz und insbesondere auch für die Wirtschaft. Interessanterweise ist aber ausgerechnet die Wirtschaft gegen dieses Gesetz, weil unklar ist, was es überhaupt will.
In erster Linie will das Gesetz die Informationssicherheit beim Bund stärken, doch es verspricht auch, die Informationssicherheit der Schweizer Wirtschaft zu erhöhen. Dabei lässt das Gesetz aber offen, wie das geschehen soll. Interessant ist auch, dass die Botschaft einhellig zum Schluss kommt, dass es bereits viele, teilweise parallele Strukturen gibt und dass sehr viel Fachwissen vorhanden ist, dieses aber teilweise wenig genutzt wird. Auch erstaunt es nicht, dass die bundesrätliche Botschaft rund ein Dutzend Mal von möglichen Synergien spricht und diese mit diesem Gesetz auch realisieren will. Es erstaunt dann aber doch, dass man trotz Realisierung von Synergien insgesamt eben mehr Verwaltungsstellen schaffen will. Offenbar ist man sich bewusst, dass die Informationssicherheit des Bundes bereits heute erstens dem Stand der Technik entspricht, zweitens durch Fachleute des Bundes laufend koordiniert und drittens durch Experten laufend überprüft und angepasst wird.
Ich komme zu den finanziellen Auswirkungen der Vorlage. Die Vorlage sieht drei sogenannte 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. Die zusätzlich benötigten Vollzeitstellen variieren innerhalb der Niveaus zwischen 9,5 und 78,5 Stellen. Noch nicht berücksichtigt wurden die Zusatzkosten für die Schweizer Wirtschaft, welche das Gesetz generiert.
Die Botschaft zum vorliegenden Gesetz enthält keine Einschätzung zu den durch das Gesetz generierten Regulierungskosten und beachtet gar nicht, was die Akkreditierungs- und Zertifizierungserfordernisse für die betroffenen Unternehmen bedeuten. Der Schweizerische Gewerbeverband rechnet, und diese Zahl lässt doch aufhorchen, mit 500 Millionen Franken, welche die Schweizer Wirtschaft bei einer Annahme zusätzlich zu tragen hätte.
Mit dem Informationssicherheitsgesetz soll nun konkret das Ambitionsniveau 1 angestrebt werden. Wenn dieses Ambitionsniveau später erhöht werden soll, muss das Gesetz nicht geändert werden. Dies würde in der Kompetenz des Bundesrates liegen, der lediglich die Verordnung anpassen müsste. Das Parlament könnte seinen Einfluss praktisch nicht mehr geltend machen. Daran ändert auch der neue Absatz 3 in Artikel 7 nichts, der den Bundesrat verpflichtet, seine Ziele und die Kosten für die Informationssicherheit den Sicherheitspolitischen Kommissionen zur Konsultation vorzulegen. Wenn Sie diesem Gesetz heute zustimmen, können Sie folglich mit grösstmöglicher Sicherheit davon ausgehen, dass die Kosten in Zukunft steigen werden.
Das vorliegende Gesetz trägt wohl kaum zur 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 unseres Landes aber kaum voranbringt. Unter anderem auch deshalb sind der Schweizerische Gewerbeverband, welcher 230 Verbände und gegen 500 000 Unternehmen vertritt, sowie auch Suisse Digital als Verband der betroffenen Unternehmen gegen die Vorlage.
Anlässlich ihrer Fraktionssitzung hat die SVP-Fraktion aus all den erwähnten Gründen beschlossen, dieses Gesetz abzulehnen. Es ist nach wie vor nicht sonnenklar, welchen Mehrwert dieses Gesetz bringen wird. Es ist völlig unklar, wie hoch die Folgekosten sein werden, und die Schweizer Wirtschaft hätte mit einer massiven finanziellen und regulatorischen Mehrbelastung zu rechnen. Zudem ist die SVP-Fraktion überzeugt, dass mit einem neuen Bundesgesetz über die Informationssicherheit wohl kaum ein massgebender Mehrwert geschaffen wird.
Ich bitte Sie deshalb im Namen der SVP-Fraktion, dieses Bürokratiemonster abzulehnen.

Seiler Graf Priska (S, ZH): Dieses Gesetz ist dringend notwendig, gerade in Zeiten von Cyberbedrohung, aber auch für alle unsere international tätigen Firmen. Es fasst einerseits bestehende verstreute Bestimmungen zusammen und schafft ein einheitliches hohes Cybersicherheitsniveau im Bereich der Informationssicherheit. Andererseits bringt es aber auch echte Fortschritte, wie zum Beispiel mit der Schaffung einer behördenübergreifenden Fachstelle des Bundes für die Steuerung der erforderlichen Massnahmen für die Informationssicherheit. Der vorliegende Entwurf des Bundesgesetzes trägt einer integralen Informationssicherheit und dem gesellschaftlichen und technischen Wandel im Umgang

mit Informationen angemessen Rechnung; Stichworte sind Digitalisierung, Cyber, Big Data und Open Data.
Cybersicherheit ist die grosse Herausforderung, und Informationssicherheit ist ein zentrales Element davon. Andere Staaten investieren über 10 Prozent des IKT-Budgets in die Sicherheit, die Banken sogar 10 bis 12 Prozent. Aus SP-Sicht ist es sogar falsch, nur das absolute Minimum zu tun, wie wir das jetzt hier machen und wie das der Bundesrat auch vorgesehen hat. Wir wären hier auch für ein höheres Ambitionsniveau zu haben gewesen, denn es handelt sich um Risiken mit sehr hoher Eintretenswahrscheinlichkeit und einem sehr grossen Schadensausmass bei gleichzeitig im Verhältnis überblickbaren Kosten. Selbst bei einem hohen Ambitionsniveau werden sich die Kosten insgesamt bei verantwortbaren etwa 100 Millionen bewegen. Dass dies gar nichts nützt, wie jetzt die SVP sagt, das ist einfach so behauptet.
Die Fragen nach den finanziellen Folgen dieses Gesetzes standen bei den Diskussionen in der SiK-N denn auch dermassen im Vordergrund, dass, wir haben es jetzt wieder gemerkt, ganz in Vergessenheit geriet, wofür dieses Gesetz eigentlich benötigt wird und dass im Bereich Informationssicherheit tatsächlich dringender Handlungsbedarf besteht. Man könnte das Verhalten des Nationalrates und der SiK-N sogar als Arbeitsverweigerung bezeichnen. Zuerst wurde gar nicht erst auf das Gesetz eingetreten, obwohl man ja die Möglichkeit gehabt hätte, das Gesetz zu konkretisieren und zu verbessern. Nachdem der Ständerat wieder auf das Gesetz eingetreten war, wurde es in der SiK-N einmal mehr mit einer Sistierung verschleppt. Nun kann ich es kaum glauben, dass ich jetzt wirklich hier stehe und wir dieses Gesetz nun endlich beraten.
Für die SP-Fraktion war der akute Handlungsbedarf von Anfang an ausgewiesen. Ich hoffe sehr, dass wir durch all die diversen Pirouetten nicht allzu viel wertvolle Zeit verloren haben. Die SP-Fraktion wird ihre eigenen Minderheitsanträge in der Detailberatung begründen. Den beiden Minderheitsanträgen Glättli zu den Artikeln 6a und 86 werden wir zustimmen. Sie tragen dazu bei, dass die Standardanforderungen genug hoch sind und auf international anerkannten Standards beruhen. Die Anträge der Minderheit I (Flach) und der Minderheit II (Keller-Inhelder) zu den Artikeln 20 und 26 werden wir ablehnen. Wir sind der Ansicht, dass die vom Bundesrat vorgeschlagene Kann-Formulierung bei der Verwendung der AHV-Nummer als Personenidentifikator am vernünftigsten ist. In der Detailberatung wird das noch genauer begründet werden. Insgesamt wird die SP-Fraktion aber in der Gesamtabstimmung klar und überzeugt dem Gesetz zustimmen.

Glanzmann-Hunkeler Ida (M-CEB, LU): Das Informationssicherheitsgesetz zeigt eigentlich, wie man nicht mit Vorlagen umgehen sollte. Seit mehr als drei Jahren ist dieses Gesetz nun in den Räten unterwegs. Damit wird der landläufigen Meinung, dass die Mühlen in Bern langsam mahlen, entsprochen. Diese Botschaft wurde nämlich schon am 22. Februar 2017 vom Bundesrat verabschiedet.
Der Ständerat ist auf die Vorlage eingetreten und hat ihr zugestimmt. Anschliessend ist der Nationalrat im März 2018 nicht eingetreten. Im November 2019 haben wir die Vorlage in der Sicherheitspolitischen Kommission, nach einer erneuten Zustimmung im Ständerat, nochmals beraten; wir sind dann ebenfalls eingetreten und haben die Vorlage vorberaten.
In den letzten Wochen und Monaten hat sich in unserer Wirtschaft einiges verändert. Die Digitalisierung hat einen riesigen Schub erfahren. Wir alle haben im Parlament erlebt, dass die Informationssicherheit bei uns schlecht gewährleistet werden kann und ganz besonders nicht auf Gesetzen basiert, die der heutigen Zeit angepasst sind. Diese Vorlage gibt uns die Möglichkeit, die Informationssicherheit des Bundes und der Verwaltung anzupassen. Ich möchte daher meinem Vorredner, Herrn Zuberbühler, widersprechen, der sagte, dass das gar nicht nötig sei.
Der Bundesrat verfolgt mit dieser Vorlage zwei ambitiöse Ziele. Er will die Rechtsgrundlagen für die Sicherheit von Informationen und Informatikmitteln des Bundes in einen einzigen Erlass zusammenführen. Dabei sollen Lücken des geltenden Rechts geschlossen sowie zahlreiche Anliegen der parlamentarischen Aufsichtsbehörden berücksichtigt werden. Die Regelung soll für Behörden und Organisationen des Bundes gelten. Damit soll ein möglichst einheitliches Sicherheitsniveau erreicht werden. Die Vorlage basiert auf anerkannten, in der Praxis erprobten internationalen Standards. Sie schafft einen formell-gesetzlichen Rahmen, auf dessen Grundlage die jeweiligen Bundesbehörden auf Verordnungs- und Weisungsebene die Informationssicherheit konkretisieren können.
Mit diesem Gesetz soll der Geltungsbereich des militärischen Betriebssicherheitsverfahrens auf zivile Beschaffungen erweitert werden. Und was ganz besonders jetzt für die Wirtschaft wichtig ist: Es soll eine Grundlage für die Abgabe von Sicherheitserklärungen zugunsten von Schweizer Unternehmen geschaffen werden, die sich um ausländische Aufträge bewerben und dafür eine nationale Sicherheitserklärung benötigen. Das betrifft zum Teil auch KMU, die ebenfalls und ganz besonders auf diese Sicherheitserklärung angewiesen sind. Im Umfeld der und ganz besonders im Nachgang zur Corona-Krise ist dies für unsere Firmen, die international tätig sind, relevant.
Ein nicht unwesentlicher Teil dieses Gesetzes befasst sich mit der Regelung der Personensicherheitsprüfung. Diese war bis jetzt im BWIS geregelt, sollte schon längere Zeit überarbeitet werden und wird jetzt in diesem Gesetz geregelt. Der Bundesrat will die Personensicherheitsprüfung reduzieren, aber trotzdem das Mindestmass, welches zur Identifizierung von erheblichen Risiken erforderlich ist, im Gesetz festhalten.
Umstritten waren das letzte Mal beim Nichteintreten des Nationalrates die Umsetzungskosten. Diese hängen weitgehend vom Sicherheitsniveau ab, das die Bundesbehörden erreichen wollen, und dann selbstverständlich auch vom entsprechenden Ausführungsrecht. Der Mehraufwand soll unter anderem durch die Reduktion bei den Personensicherheitsprüfungen kompensiert werden.
Für uns war die Beantwortung der Frage wichtig, ob das vorliegende Gesetz auf der nationalen Cyberstrategie basiert. Alles andere wäre unverständlich. Zudem wird die Fachstelle des Bundes für Informationssicherheit ins Kompetenzzentrum für Cybersicherheit integriert.
Die Mitte-Fraktion CVP-EVP-BDP wird auf diese Vorlage eintreten, überall der Mehrheit zustimmen, ausgenommen bei Artikel 20 Absatz 3, wo wir zusammen mit der Minderheit I (Flach) den Beschluss des Ständerates unterstützen. Dazu werde ich mich dann gerne in der Detailberatung noch äussern.
Unsere Fraktion stimmt für Eintreten auf dieses Gesetz und befürwortet die Behandlung dieser Vorlage.

Hurter Thomas (V, SH): Geschätzte Kollegin Glanzmann, Sie haben jetzt gesagt, das Parlament habe eine Verweigerungshaltung eingenommen, das haben Sie hier auch erwähnt. Sie haben von Verzögerungstaktik usw. gesprochen, der Bundesrat habe schnell gearbeitet, dabei war dieses Gesetz ein Jahrzehnt in der Verwaltung. Aber nun zu meiner Frage: War es nicht gerade ein Mitglied Ihrer Fraktion, welches den Rückweisungsantrag gestellt hat? Soweit ich mich erinnere, war das so.

Glanzmann-Hunkeler Ida (M-CEB, LU): Von Verweigerungshaltung des Parlamentes habe ich nichts gesagt. Ich habe gesagt, dass wir nicht eingetreten sind. Uns fehlte die Grundlage. Wir wussten zu wenig Bescheid über die Finanzen. Diese Auskunft haben wir bei der letzten Detailberatung erhalten, und darum unterstützen wir jetzt die Vorlage.

Glättli Balthasar (G, ZH): Endlich biegen wir in die Zielgerade ein. Ich hoffe, dass wir den Einlauf auch schaffen. Sie haben die Geschichte gehört. Ich habe meinen Kollegen und Kolleginnen die Vorlage vereinfacht erklärt. Vermutlich hat der Ständerat von diesem Gesetz nicht wahnsinnig viel verstanden und in seiner staatsgläubigen Art einfach gesagt: Okay, wir stimmen dem Bundesrat zu. Beim Nationalrat ging es eigentlich gleich. Wir brauchten in der Kommission auch

ein paar Anläufe, bis wir das Konzept verstanden hatten; nur lief es in der Eigendynamik des Nationalrates dann auf eine Ablehnung hinaus. Das ist das, was man auch bedauern muss, weil wir dadurch durchaus Zeit verloren haben. Wir haben aber hoffentlich auch ein wenig an Erkenntnis gewonnen, weshalb es dieses Gesetz überhaupt braucht.

Ich möchte einleitend auch kurz sagen, dass es in diesem Gesetz ganz verschiedene Elemente gibt. Sie haben es gehört, ich muss es nicht noch einmal von der Personensicherheitsprüfung bis zur Informationssicherheit im IT-Bereich aufdröseln. Wir haben uns in der Kommission überlegt, ob man das nicht allenfalls in unterschiedliche Gesetze aufteilen könnte, und haben auch über entsprechende Anträge debattiert. Wir sind dann aber zum Schluss gekommen, dass es von allen schlechten Lösungen die am wenigsten schlechte ist, das Gesetz als Ganzes zusammenzubehalten. Es ist jedoch nicht so, dass Sie das Gesetz als einheitliches Gesetz lesen können. Es sind wirklich ganz unterschiedliche Teile, die geregelt werden und im groben Ganzen die Informationssicherheit betreffen.

Ganz wichtig scheint mir: Wenn Sie gewissen Minderheitsanträgen noch zur Mehrheit verhelfen, haben Sie mit diesem Gesetz die Möglichkeit, zu verhindern, dass das passiert, was wir jetzt in einem anderen Bereich leidvoll erlebt haben, wo man versucht hat, mit Plänen für künftige Krisen vorzusorgen. Wir alle haben den Pandemieplan in den letzten Monaten vermutlich viel näher kennengelernt, als uns allen lieb ist. Wir haben gemerkt, wie nützlich oder nutzlos ein Plan ist, wenn er nur ein Plan bleibt und es keine verbindlichen Vorgaben gibt. Es ist gerade im Bereich der IT auch das Ziel, konkrete Vorgaben zu machen. Das soll, um den Vergleich zu bemühen, nicht im Sinne einer Vorgabe geschehen, welche Anzahl Masken in der Verantwortung von dieser oder jener Organisationseinheit vorzubereiten oder auf Vorrat zu halten seien, sondern vielmehr ist die Verantwortung klar festzuschreiben, dass es Informationssicherheits-Managementsysteme braucht.

Es macht keinen Sinn, ganz konkrete Sicherheitsanforderungen auf Gesetzes- oder meinetwegen Verordnungsstufe festzuschreiben. Das Wichtige ist, dass alle sicherheitsrelevanten Bereiche gezwungen sind, ein solches Informationssicherheits-Managementsystem einzuführen. Das heisst, dass anerkannte Prozesse da sind, wo man die Risiken identifiziert, mögliche Reaktionen abwägt, das Gewicht definiert, mit wie viel Aufwand man auf welches Risiko vorbereitet sein will, und dann auch Pläne B in petto hat für den Fall, dass es wirklich mal südwärts geht.

Ich spreche dann in der Detailberatung nochmals kurz zum Minderheitsantrag, aber ich lege Ihnen schon jetzt wirklich ans Herz: Wenn Sie schon dieses Gesetz beschliessen, dann geben Sie ihm auch Zähne, denn sonst riskieren wir tatsächlich, dass es sich nur um ein Bürokratiegebilde, um einen Papiertiger handelt.

Porchet Léonore (G, VD): La loi sur la sécurité de l'information a une longue histoire derrière elle. Le message du Conseil fédéral date du 22 février 2017, et compte tenu de la vitesse à laquelle évolue la société de l'information, on pourrait presque se demander si la loi n'est pas déjà complètement dépassée. Heureusement, le Conseil fédéral a résisté à la tentation d'inscrire certaines normes techniques dans la loi, mais s'est plutôt limité à créer un cadre légal unique pour toutes les autorités fédérales, afin de garantir la protection de l'information et la sécurité des moyens informatiques.

L'idée est d'utiliser des normes et des méthodes reconnues dans le monde professionnel, qui correspondent à l'état actuel des connaissances. Il ne s'agit donc pas pour la Confédération de réinventer la roue. Il s'agit plutôt de s'engager à donner à la sécurité de l'information le poids nécessaire, comme le font tous les grands acteurs économiques et aussi de nombreux petits.

La minorité Glättli qui propose un nouvel article 6a, il faut le souligner dès maintenant, vise exactement ce but: que la Confédération ne fasse pas le long et inutile travail de réinventer la roue, tout en garantissant que la gestion de la sécurité de l'information repose sur des normes et des standards internationalement reconnus.

Ces dernières semaines, nous avons vu à quel point le fonctionnement de l'informatique, au niveau de l'infrastructure et au niveau des applications, est central, et à quel point un système informatique fonctionnel peut nous aider à surmonter une crise. Inversement, il est difficile d'imaginer à quel point non seulement les activités de l'administration elle-même, mais aussi celles de la population et de l'économie, seraient affectées si les autorités fédérales n'étaient plus en mesure de fonctionner, ou en tout cas pas correctement, en raison de problèmes de sécurité dans le domaine de l'informatique.

C'est pourquoi les Verts se réjouissent que cette loi semble aujourd'hui avoir une seconde chance dans notre conseil, après la décision de ce dernier de ne pas entrer en matière en 2018.

La raison du rejet lors du premier débat était d'abord la crainte que la loi ait des conséquences financières incontrôlables.

Franchement, notre crainte était toute autre, et plutôt le contraire. Les coûts des incidents qui pourraient être évités avec un système de gestion de la sécurité de l'information opérationnel, et la gestion appropriée des risques qui y est associée, sont autrement plus inquiétants.

Néanmoins, nous nous rallions à la commission qui demande que les Commissions de la politique de sécurité soient consultées par le Conseil fédéral sur les objectifs concrets et les coûts. Bien qu'il soit assez inhabituel de consigner ainsi cela dans un texte législatif, si cela sert à créer la confiance nécessaire et à éviter un rejet définitif de la loi, nous nous y rallions volontiers.

Je ne veux pas conclure sans évoquer la minorité à l'article 86 alinéa 3 que les Verts vous recommandent vivement d'accepter. Il n'est pas contesté par la commission que la Confédération doit fixer des exigences de sécurité standardisées. Mais le Conseil fédéral propose que ces exigences aient en principe purement valeur de recommandations. La crise du coronavirus a malheureusement prouvé à quel point les normes et plans de sécurité fonctionnent mal et ne sont pas respectés s'ils ne sont pas contraignants.

Notre minorité propose donc que les exigences standard soient en principe contraignantes, tout en laissant une certaine flexibilité, puisque notre proposition stipule que les autorités peuvent définir ces exigences comme non contraignantes pour leur propre domaine, en donnant des raisons spécifiques à ce choix.

En vous demandant de prendre en considération ces remarques, le groupe des Verts vous recommande d'entrer en matière sur ce projet de loi.

Dobler Marcel (RL, SG): Die FDP-Liberale Fraktion empfiehlt Ihnen einstimmig, auf das heute unumstrittene Informationssicherheitsgesetz einzutreten. Ich werde mich jetzt in meinem Eintretensvotum auch gleich zur Detailberatung äussern und nachher nicht mehr sprechen.

Aufgrund von mehreren Angriffen auf Informationssysteme des Bundes hat sich gezeigt, dass der Schutz von Informationen beim Bund Lücken aufweist. Daher sollen für die Bundesbehörden minimale Sicherheitsstandards gelten, die mit diesem Gesetz definiert werden. Das Gesetz soll die Sicherheit von Informationen in der Bundesverwaltung verbessern und einen Mindeststandard schaffen. Es regelt einheitlich die Personensicherheitsprüfungen, die für die Schweiz sicherheitsrelevanten Informationen und die Betriebssicherheitsprüfungen für kritische IKT-Beschaffungen.

Wie Sie wissen, haben wir am 13. März 2018 im Nationalrat Nichteintreten beschlossen. Die Ablehnung bei uns ist aus zwei Gründen erfolgt: Erstens beinhaltet das Gesetz drei verschiedene Ambitionsniveaus, das haben wir schon gehört. Diese verursachen sehr unterschiedliche Kosten. Das Ambitionsniveau 1, die tiefste Sicherheitsstufe, verursacht Kosten von geschätzten 5 bis 12 Millionen Franken, und das im Moment sicherste Ambitionsniveau verursacht Kosten von 87 Millionen Franken. Da die Verwaltung ungenügend erklären konnte, wie genau sich diese Kosten bei den Ambitionsniveaus 2 und 3 zusammensetzen, und auch noch selber

das Ambitionsniveau wechseln konnte, blieb uns nichts anderes übrig, als nicht auf dieses Gesetz einzutreten. Zweitens war zu diesem Zeitpunkt unklar, welche Kosten für die Wirtschaft aufgrund der Betriebssicherheitsprüfungen entstehen werden.

Was sind jetzt nun die Gründe, warum genau wir dieses Gesetz heute gutheissen?

Die Notwendigkeit des Gesetzes und die Einführung eines Mindeststandards bei den Informationssystemen des Bundes sind aus unserer Sicht unbestritten. Die Sicherheit und die Resilienz werden erhöht. Auch waren das Ambitionsniveau 1 und die damit verbundenen Kosten und Massnahmen aus unserer Sicht nicht bestritten. Aufgrund dieser Situation hat sich der Bundesrat dann bereit erklärt, bei einem Wechsel des Ambitionsniveaus die Sicherheitspolitische Kommission erneut zu konsultieren. Weiter haben wir in der Beratung eine detaillierte Prüfung der konkreten Kosten anhand praktischer Fälle seitens der Firmen bei den Betriebssicherheitsprüfungen vorgenommen. Diese Kosten sind verhältnismässig tief und zumutbar.

Aus den genannten Gründen empfehlen wir, die FDP-Liberale Fraktion, einstimmig, auf dieses Gesetz einzutreten.

Ich komme jetzt zur Detailberatung und zu den verbleibenden sechs Differenzen und den Minderheiten.

Bei Artikel 5 Litera c geht es um die Definition der kritischen Infrastrukturen. Die Formulierung des Ständerates entspricht der Formulierung der Strategie der kritischen Infrastrukturen des Bundes. In dieser Formulierung ist es keine abschliessende Liste, und sie stützt sich auf eine bestehende Definition ab. Die Minderheit Sommaruga Carlo führt als Unterschied lediglich die Spitaleinrichtungen explizit zusätzlich auf. Diese sind aber auch bei der Formulierung des Ständerates nicht ausgeschlossen. Bitte folgen Sie der Mehrheit und führen Sie nicht neue Definitionen bei den kritischen Infrastrukturen ein, die sich inhaltlich nicht unterscheiden.

Bei Artikel 6a will die Minderheit Glättli die Behörden und Organisationen dazu verpflichten, ein System zum Informationssicherheitsmanagement, das auf international anerkannten Standards basiert, zu definieren und zu betreiben. Dem ist bereits so, deshalb hat die Redaktionskommission bewusst darauf verzichtet. Aus unserer Sicht ist dieser Artikel somit unnötig. Deshalb beantragen wir Ihnen, der Mehrheit zuzustimmen.

Die Minderheitsanträge zu Artikel 20 Absatz 3 und zu Artikel 26 sind die grösste Differenz, die in diesem Gesetzentwurf noch besteht. Dabei geht es um die Verwendung der AHV-Versichertennummer als Personenidentifikator. Es liegen uns sozusagen drei verschiedene Konzepte vor: Die Mehrheit der Kommission steht hinter dem Entwurf des Bundesrates und will, dass für die Personenidentifikation einmalig die AHV-Versichertennummer verwendet werden kann und dass diese AHV-Versichertennummer nach der Erzeugung einer nicht zurückrechenbaren Personennummer zu löschen ist. Die Minderheit I (Flach) folgt dem Ständerat und will, dass die AHV-Versichertennummer als systematischer Personenidentifikator verwendet werden kann. Die Minderheit II (Keller-Inhelder) will, dass die AHV-Versichertennummer gar nicht verwendet werden kann.

Aus unserer Sicht ist die Einschränkung oder das Verwendungsverbot der AHV-Versichertennummer unverhältnismässig und nicht zielführend. In Artikel 20 ist streng geregelt, wer genau Zugang zu diesem System erhält; die Verwendung ist somit gesetzlich eingeschränkt, und es ist ein geschlossenes System. Bei diesem Gesetz geht es um die Sicherheit unseres Landes sowie darum, wer Zugriff auf geheime und streng geheime Informationen erhalten soll. Durch dieses Gesetz wird es ermöglicht, biometrische Daten der Personen zu erfassen und zum Beispiel Steuerunterlagen der zu prüfenden Personen einzusehen. Das war in der Beratung nie bestritten, es geht ja schliesslich auch um die Sicherheit unseres Landes. Jetzt wollen einzelne Kreise eine effiziente Identifikation erschweren. Das Verbot der Verwendung der AHV-Versichertennummer als Ausnahme in diesem Gesetz ist in diesem Zusammenhang nicht nachvollziehbar. Der einzige Grund wäre, wenn man die Verwendung der AHV-Versichertennummer generell verbieten und keine Ausnahmen zulassen wollte, die jetzt aber schon bestehen.

Ich beantrage Ihnen im Namen der FDP-Liberalen Fraktion, im Grundsatz der Mehrheit der Kommission wie auch dem Minderheitsantrag I (Flach) zuzustimmen.

Artikel 77 Absatz 3 und Artikel 81 hängen zusammen. Die Kommissionsmehrheit will die Möglichkeit schaffen, bei der Zusammenarbeit im Inland bei bestimmten Vorfällen Daten weiterzugeben. Es ist eine Kann-Formulierung. Die Minderheit will eine Meldepflicht bei bestimmten erheblichen Vorfällen einführen. Bloss, was sind "bestimmte erhebliche Vorfälle"? Die Definition ist unklar. Sie ist eine Ermessenssache der Betreiber von kritischen Infrastrukturen und schlussendlich des Bundesrates, an den die Definition delegiert wird. Das schafft neue Unklarheiten. Aus diesem Grund bitte ich Sie, bei Artikel 77 Absatz 3 und Artikel 81 der Mehrheit zu folgen.

Ich komme zum letzten Artikel, Artikel 86. Es geht um die Standardanforderungen und Massnahmen. Die Mehrheit will, dass diese einen empfehlenden Charakter haben, sofern sie von den verpflichteten Behörden für nicht verbindlich erklärt werden. Die Minderheit Glättli will, dass sie immer verpflichtend sind, ausser sie werden von den verpflichteten Behörden als nicht verpflichtend deklariert. Der Antrag der Mehrheit entspricht der Regelung in anderen Bereichen und stellt die Unabhängigkeit der Behörden sicher. Ich bitte Sie, auch in diesem Fall der Mehrheit zu folgen.

Ich fasse nochmals kurz zusammen: Die FDP-Liberale Fraktion empfiehlt Ihnen einstimmig, immer der Mehrheit zu folgen, ausser bei den Artikeln 20 und 26, wo es um die AHV-Versichertennummer geht. Dort unterstützen Sie bitte die Minderheit I (Flach).

Flach Beat (GL, AG): Eigentlich hätte ich einfach mein Votum vom 13. März 2018 noch einmal hervorholen und Ihnen noch einmal genau dasselbe vortragen können, denn an der Haltung der grünliberalen Fraktion hat sich nichts geändert. Die Rückweisung damals war nicht gerechtfertigt. Auch die Begründung, mit der diese Rückweisung gemacht wurde und mit der sie nun als berechtigt dargestellt wird, ist einfach nicht richtig.

Wenn Sie in den Protokollen nachlesen, dann sehen Sie, dass die Informationen, die wir zusätzlich noch einmal bekommen haben, eigentlich schon da waren. Wir haben die Grössenordnung gekannt. Es war uns auch bekannt, dass es um ein Gesetz geht, das aus verschiedenen anderen Gesetzen zusammengegossen wird und das in Bereiche hineingeht, die kompliziert nachzuvollziehen sind. Vielleicht ist es aber auch richtig, dass wir bei diesem Gesetz, das ein Rahmengesetz ist und einen ganz, ganz sensiblen Bereich unserer heutigen Staatsführungs-, Verwaltungs-, Justiz- und Sicherheitsstruktur beinhaltet, sehr genau vorgehen und versuchen, zu verstehen, wie Informationssicherheit in Zukunft gewährleistet werden muss.

Es ist eine integrale Aufgabe, und es ist auch nicht so, dass man einfach ein Gesetz mit Bestandteilen aus formalen Vorgängen schreiben kann, die wie früher Aktenschränke, Aktenkärtchen, Ordner oder vielleicht Unterlagen, die in einem Tresor gelagert werden, Personenkontrollen, die Prüfung von Personen, die Zutritt zu irgendwelchen Archiven haben, oder Ähnliches beinhalten. Das neu auf einer digitalen Ebene zu organisieren, ist nicht einfach, und es ist eben auch nicht abschliessend. Es ist nicht so, dass wir heute umschreiben können, wie die Informationssicherheit zu gewährleisten ist, wer wann wo Zugriff hat und wie wir diese Strukturen, vor allen Dingen die Infrastruktur, auszubilden haben.

Wir bewegen uns in einer technologischen Entwicklung, die rasant voranschreitet. Mit dem Gesetz heute ist dies nicht fertig, sondern es wird weitere Schritte brauchen. Darum ist es wichtig, dass wir den Rahmen schaffen, damit sich der Bund und die ihm nahestehende Verwaltung in Sachen Sicherheitsinfrastruktur bis hin zur Infrastruktur der Hardware usw. auf einem gemeinsamen Level befinden, und dies kontrollierbar, der für uns nachvollziehbar sicher ist. Wir brauchen die Sicherheit in den Systemen, nicht im Ausdeutschen dessen, was es denn genau ist, sondern in der Kontrolle und

dem Management dieser Informationssicherheit. Informationen sind heute nicht nur ein Nervenstrang unserer Gesellschaft, unseres Staates, der Staatssicherheit und unserer gesamten Wirtschaft, sondern sie sind das Rückgrat. Ohne die Informationstechnologie und die Sicherheit dieser Informationen sind wir schlicht und ergreifend verloren. Darum ist es wichtig.

Es ist denn auch eine Gratwanderung. Es gibt einerseits Ansprüche auf Sicherheit, die dann auch teuer und einschränkend ist, bis in die Privatwirtschaft hinein. Wenn die Privatwirtschaft im Rahmen von Aufträgen des Staates tätig wird, muss sie selbstverständlich dieselben Standards erfüllen, wie wenn der Staat selber diese Tätigkeit ausüben würde, ja vielleicht sogar noch ein bisschen mehr, weil man halt eben im privaten Bereich ist und nicht überall ein staatliches Aufsichtsorgan mit dabei ist oder dahintersteht. Es ist deshalb wichtig, dass man diese Gratwanderung definiert und sagt, wo sie wie aussehen soll. Darum sind auch die Ambitionen, die dieses Gesetz vorgibt, richtig. Es ist sinnvoll, dass man die entsprechenden Ebenen vorgibt, aber noch nicht endgültig definiert.

Der Geheimhaltung von Informationen steht auf der anderen Seite die Öffentlichkeit gegenüber, die einen Anspruch darauf hat, Informationen zu erhalten. Das ist dann das andere. Das ist schwierig zusammenzubringen, aber in diesem Gesetz hat man dies nun einigermassen versucht. Es ist jetzt seit mittlerweile zehn Jahren unterwegs, und wie gesagt, es ist vielleicht nicht der Weisheit letzter Schluss. Es ist tatsächlich sehr schwierig zu lesen. Einer meiner Vorredner hat gesagt, es sei sehr schwierig, sich in diesem Gesetz zurechtzufinden. Das ist tatsächlich so. Sie brauchen dazu noch etwa drei oder vier weitere Gesetze, damit Sie überhaupt wissen, worauf sich die Referenzen beziehen. Aber es ist wichtig und richtig, dass wir jetzt eintreten. Ich bitte Sie, dies zu tun. Ich werde mich dann zu den Anträgen der Minderheiten noch äussern und hoffe, dass wir hier und jetzt auf dem richtigen Wege sind.

Amherd Viola, Bundesrätin: Vor etwas über zwei Jahren sass ich nicht in diesem, aber im Nationalratssaal im Bundeshaus und habe als Nationalrätin mit Ihnen über das Eintreten auf dieses Gesetz debattiert. Obschon zu diesem Zeitpunkt bereits weitgehend unbestritten war, dass es dieses Gesetz braucht, dass es Handlungsbedarf gibt, waren wir vom Entwurf des Bundesrates für ein Informationssicherheitsgesetz nicht überzeugt. Daher sind wir damals, wie es die Sicherheitspolitische Kommission empfohlen hat, nicht auf das Gesetz eingetreten.

Nachdem der Ständerat die Notwendigkeit des Gesetzes nochmals ohne Gegenstimme bestätigt hatte, eben aus der Überzeugung, dass es das Gesetz braucht, und nicht etwa einfach, um das Gesicht zu wahren, konnte die Sicherheitspolitische Kommission des Nationalrates mit neuen Argumenten, mit neuen Informationen und in intensiven Diskussionen von der Notwendigkeit des Gesetzes ebenfalls überzeugt werden. Das Informationssicherheitsgesetz wird dem Bund einen modernen, wirksamen und entwicklungsfähigen Rahmen geben, einen Rechtsrahmen im Cyberbereich. Es wird zahlreiche wesentliche Sicherheitslücken schliessen, Einheitlichkeit schaffen und gleichzeitig die Effizienz und Wirksamkeit der bestehenden Sicherheitsmassnahmen erhöhen. Die Erfahrung zeigt, dass eine Harmonisierung des Sicherheitsniveaus zwischen Bundesbehörden, Kantonen, Industrie und Wirtschaft notwendig ist. Mit diesem Gesetz haben wir das.

Wichtig ist auch eine Harmonisierung mit den internationalen Partnern. Entsprechende Massnahmen brauchen aber eine gesetzliche Grundlage, die wir heute nicht haben.

Das Informationssicherheitsgesetz ist auf die Cyberstrategie des Bundes abgestimmt. Es schafft eine erste rechtliche Grundlage für bestimmte Massnahmen der Strategie und ist flexibel genug, weitere Entwicklungen aufzunehmen.

Die Kosten für die Umsetzung des Gesetzes sind im Verhältnis zu dessen Nutzen gering und gerechtfertigt. Das gilt insbesondere auch für die Wirtschaft. Die Cyberbedrohung ist Tatsache, weshalb ich die Cybersicherheit zu einer der Prioritäten in meinem Departement erklärt habe.

Ich bin überzeugt, dass dieses Informationssicherheitsgesetz für die Sicherheit des Bundes und für unsere international tätige Wirtschaft notwendig ist. Hierzu möchte ich sagen, dass die international tätige Wirtschaft im sicherheitsrelevanten Bereich auf dieses Gesetz explizit angewiesen ist. Wenn es abgelehnt wird, können sich diese Unternehmen nicht mehr zertifizieren lassen und verlieren damit internationale Aufträge in diesem wichtigen Bereich, in dem die Schweiz sehr stark ist. Das wäre dann der Schaden für die Wirtschaft, nicht die etwas vermehrten Kosten, die sich durch dieses Gesetz ergeben.

Ich bitte Sie also, auch im Interesse der Wirtschaft, der SiK Ihres Rates zu folgen und auf die Vorlage einzutreten. Eine Ablehnung wäre in höchstem Grade wirtschaftsfeindlich.

La présidente (Moret Isabelle, présidente): Les rapporteurs renoncent à reprendre la parole.

Eintreten wird ohne Gegenantrag beschlossen
L'entrée en matière est décidée sans opposition

Bundesgesetz über die Informationssicherheit beim Bund
Loi fédérale sur la sécurité de l'information au sein de la Confédération

Detailberatung – Discussion par article

Titel und Ingress, Art. 1–4
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Titre et préambule, art. 1–4
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 5
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Sommaruga Carlo, Crottaz, Fridez, Glättli, Mazzone, Seiler Graf)
Bst. c
c. ... Informations-, Kommunikations- und Transportinfrastrukturen sowie grundlegende Spitaleinrichtungen und weitere Prozesse ...

Art. 5
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Sommaruga Carlo, Crottaz, Fridez, Glättli, Mazzone, Seiler Graf)
Let. c
c. ... de communication et de transport ainsi que les installations hospitalières de base et d'autres installations, processus ...

La présidente (Moret Isabelle, présidente): La proposition de la minorité Sommaruga Carlo sera présentée par Mme Seiler Graf.

Seiler Graf Priska (S, ZH): Bei Artikel 5 Buchstabe c beantragt die SP-Fraktion, dass grundlegende Spitaleinrichtungen unbedingt als Teil der kritischen Infrastrukturen betrachtet werden müssen und darum in dieser Aufzählung auch explizit erwähnt werden sollen. Das hätte dann auch Konsequenzen für Artikel 6 des Nachrichtendienstgesetzes und

Artikel 1 des Militärgesetzes. Dort werde ich nicht mehr dazu sprechen.
Wie vom Bundesrat und nachher auch noch vom Ständerat weiter ausgeführt, enthält der Artikel in der geänderten Fassung eine konkrete Auflistung mit einem allgemeinen Aspekt. Diese Auflistung im ersten Teil befasst sich mit den Themen Trinkwasser, Energie, Information, Kommunikation und Verkehrsinfrastruktur. In einem zweiten Teil des Artikels ist von zusätzlichen anderen Einrichtungen die Rede. Wir schlagen deshalb vor, dass wir hier auch die grundlegende Gesundheitsinfrastruktur, nämlich die Krankenhäuser, erwähnen sollten. Wir haben während des Angriffs durch das "Wanna Cry"-Virus gesehen, dass auch Krankenhäuser gerne angegriffen werden. Das ist gefährlich, da durch die mögliche Blockierung von medizinischen Geräten Leben gefährdet sein könnten. Eine sehr schnelle Reaktion ist also erforderlich. Ich denke, es wäre angebracht, dem Verkehr, der Kommunikation und dem Trinkwasser auch die grundlegende Krankenhausausstattung hinzuzufügen.
Die Liste kann wahrscheinlich niemals wirklich abschliessend geführt werden, aber Spitäler als grundlegende Gesundheitsinfrastruktur müssen hier eindeutig speziell erwähnt werden. Nach der Corona-Krise erhält dieser Punkt eine noch grössere Dringlichkeit und ist noch offensichtlicher.
Ich bitte Sie darum, diesem Minderheitsantrag zuzustimmen.

Hurter Thomas (V, SH): Ich erlaube mir, für die SVP-Fraktion zu den ersten beiden Minderheiten zu sprechen, weil es ja hier um die allgemeinen Bestimmungen und die allgemeinen Massnahmen geht.
Meine Vorrednerin hat es gesagt: Sie möchte hier gerne die Spitaleinrichtungen als kritische Infrastrukturen aufnehmen. Ich glaube, das ist nicht sinnvoll. Auch wir finden, dass das tatsächlich kritische Infrastrukturen sind. Aber wenn Sie beginnen, hier eine Aufzählung zu machen, und eine bestimmte Gruppe explizit erwähnen, machen Sie auch automatisch eine Priorisierung, und dann kann es durchaus sein, dass andere Dinge, die auch wichtig sind, vergessen gehen. Deshalb enthält der Entwurf des Bundesrates die absolut richtige Priorisierung: Er nennt nämlich die Infrastrukturen, die für das Funktionieren von Gesellschaft, Wirtschaft und Staat unerlässlich sind. Da sind auch die Spitäler mit eingeschlossen, und deshalb braucht es hier keine explizite Erwähnung. Deshalb werden wir diese Minderheit ablehnen.
Ich nutze die Zeit auch gerade für die zweite Minderheit, dann muss ich das nächste Mal nicht mehr sprechen. Die Minderheit Glättli möchte die internationalen Standards anwenden. Auch diese Erwähnung ist nicht notwendig: Das hat der Bundesrat in seiner Vorlage bereits vorgesehen, nämlich im folgenden Artikel 7. Dort wird gesagt, dass die Informationssicherheit auf dem neusten technologischen Wissen und den neusten Erkenntnissen der Wissenschaft beruht. Damit ist eigentlich klar, dass auch die internationalen Standards umgesetzt werden. Die SVP-Fraktion wird auch diese Minderheit ablehnen.
Lassen Sie mich hier zum Schluss noch einen Hinweis machen, weil es vielleicht noch ein paar Stimmen der SVP-Fraktion geben wird, die für das Gesetz sind. Bei Artikel 7 hat es einen neuen Absatz 3 gegeben. Sie haben jetzt von allen Vorrednern von diesen Ambitionsniveaus gehört, und es wurden auch Ausführungen zu den Kosten und den benötigten Stellen für die Umsetzung dieses Gesetzes gemacht. Dieser Absatz 3 verlangt vom Bundesrat – ich hoffe, dass Bundesrätin Amherd trotz allem auch noch dazu reden wird –, dass die Sicherheitspolitischen Kommissionen informiert und in die Diskussion mit einbezogen werden, wenn das Ambitionsniveau erhöht werden müsste oder dies verlangt würde. Damit kann verhindert werden, dass dieses Gesetz ausufert und schlussendlich sehr, sehr teuer wird. Das ist ein wesentliches Element, das neu in diese Vorlage eingebracht worden ist.
Wenn Sie, Frau Seiler Graf, als Vertreterin der linken Seite uns sagen, es sei Arbeitsverweigerung gewesen, muss ich sagen: Genau aufgrund dieser "Arbeitsverweigerung" wurden diese Niveaus aufgezeigt, und genau deshalb konnte man eben hier eine Entschärfung, eine Verbesserung erreichen! Es war also überhaupt keine Arbeitsverweigerung. Man könnte sich sowieso fragen, ob ein Gesetz, das über Jahre vorbereitet werden muss, überhaupt besser werden kann.
Zusammenfassend bitte ich Sie also, die beiden ersten Minderheiten abzulehnen.

Crottaz Brigitte (S, VD): Je ne reviendrai pas sur l'importance de cette loi qui contribue à améliorer la sécurité de l'information relevant de la compétence de la Confédération.
L'évolution de notre société vers une hyperconnectivité conduit en effet 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.
L'utilisation abusive d'informations, le vol de données ou la perturbation de systèmes d'informations sensibles peuvent en effet nuire gravement aux intérêts essentiels de la Suisse, voire léser la sécurité d'entreprises ou de particuliers.
A son article 75, la loi précise que: "La Confédération apporte un soutien aux exploitants d'infrastructures critiques pour garantir que les interruptions de réseau et de système et les utilisations abusives soient rares, de courte durée, maîtrisables et peu dommageables."
L'article 5 lettre c définit quant à lui les infrastructures critiques qui sont concernées par cette loi. Dans sa stratégie nationale de protection des infrastructures critiques 2018–2022, le Conseil fédéral définit neuf secteurs comme infrastructures critiques, dont celui de la santé. Or celui-ci ne figure pas nommément dans la liste définissant les infrastructures critiques à cet article 5 lettre c. Même si M. Hurter pense qu'il n'est pas nécessaire de tous les citer, il faut bien dire que la plupart des autres secteurs définis comme infrastructures critiques sont cités dans cet article.
La minorité Sommaruga Carlo, reprise par Mme Seiler Graf, qui vous est soumise propose donc que les installations hospitalières de base soient ajoutées à cette liste d'infrastructures critiques. Rien de bien révolutionnaire vous en conviendrez, et, de plus, dans les circonstances très particulières que nous vivons depuis le début de l'année, il n'échappera à personne que nos hôpitaux sont des infrastructures critiques, autant que celles concernant l'approvisionnement en eau potable ou en énergie, les transports ou d'autres système essentiels au fonctionnement de l'économie.
Les hôpitaux, sous forte tension à cause de la pandémie, en ce temps de crise mondiale, ont vu des pirates sans scrupules profiter de l'épidémie de coronavirus pour les attaquer et exiger des rançons ou voler des documents. Plusieurs cyberattaques viennent ainsi de se dérouler à l'étranger.
La menace numéro un, ce sont les "ransomwares", ou "rançongiciels", ces programmes qui paralysent les systèmes informatiques. Pour rendre l'accès aux ordinateurs, les pirates exigent une rançon. En 2019, pour les seuls Etats-Unis, 764 établissements hospitaliers ont été ciblés par de telles attaques, avec comme conséquences des patients redirigés vers d'autres hôpitaux, des dossiers inaccessibles et parfois détruits.
D'autres méthodes sont employées par les pirates, comme l'attaque par déni de service constatée au mois de mai de cette année à Paris. Ce sont des attaques qui saturent les serveurs. L'Assistance publique-Hôpitaux de Paris a ainsi dû couper temporairement l'accès externe aux mails et à des outils de télétravail en raison d'une surcharge du système.
Avant la pandémie, en octobre 2019, l'hôpital de Wetzikon, dans le canton de Zurich, avait également subi une attaque par "ransomware" et avait dû débrancher du système central plusieurs dispositifs médicaux. Ces quelques éléments vous convaincront, je l'espère, de la nécessité de considérer les installations hospitalières comme des infrastructures critiques et de les inscrire clairement, à l'article 5 lettre c.
Je vous remercie donc de soutenir la proposition de la minorité Sommaruga Carlo, défendue par Mme Seiler Graf.

La présidente (Moret Isabelle, présidente): Le groupe du centre PDC-PEV-PBD soutient la proposition de la majorité.

Glättli Balthasar (G, ZH): Es ist wirklich nicht zentral – das ist das Wichtigste, das man auch zuhanden des Amtlichen

Bulletins festhalten muss: Es ist nicht zentral, wie Sie hier entscheiden. Was zentral ist, und das war das, was für uns auch etwas schwierig war, ist, dass man in der ganzen Verwendung des Begriffs der kritischen Infrastruktur über die Bundesverwaltung und über die verschiedenen Gesetze hinweg ein wenig eine einheitliche Formulierung findet.
Das schaffen, mit Verlaub gesagt, weder die erste noch die zweite, noch die dritte Möglichkeit, die heute zur Debatte stehen. Der Bundesrat selbst schafft es nicht. Die Variante des Ständerates lehnt sich zwar an die Formulierung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken an, aber ich finde, dass dort zum Beispiel die wesentlichen staatlichen Organe nicht als kritische Infrastruktur festgehalten sind. Es ist eigentlich eine schlechte Definition. Deshalb ist es eher Ihrem politischen Ermessen überlassen, ob Sie die Spitäler jetzt noch hineinnehmen wollen oder nicht.
Wir empfehlen Ihnen, das zu tun. Wir haben in den letzten Wochen und Monaten erlebt, wie stark die Spitäler leider auch kritische Infrastrukturen sind. Wir wissen auch, und das ist vielleicht ein zweiter Grund, weshalb es sinnvoll ist, die Spitäler explizit zu nennen, dass gerade im Bereich der Spitäler sehr oft unheimlich veraltete Systeme im Einsatz sind, auch Betriebssysteme, die Sie schon lange nicht mehr auf Ihren Computern haben. Damit werden Systeme, die für den Bereich der Gesundheit ganz wichtig sind, gesteuert. Dass man sich dort die nötige Mühe nimmt, eben auch gewisse Sicherheitsstandards einzuführen, und zwar nicht nur im Ausnahme-, sondern auch im Normalzustand, ist doch sehr wichtig.
Sie wissen auch, dass Spitäler im Ausland, aber auch in der Schweiz immer wieder Zielscheibe von Cyberattacken sind. Deshalb ist es aus meiner Sicht, bei aller Imperfektion einer nicht geschlossenen Aufzählung, sinnvoll, die Spitäler im Sinne des Minderheitsantrages auch explizit anzuführen. Aber es ist klar, wenn dieser Antrag keine Mehrheit findet, bleiben die Spitäler mitgemeint.

Amherd Viola, Bundesrätin: Es wurde gesagt: Artikel 5 Buchstabe c des Gesetzes definiert, was unter dem Begriff "kritische Infrastrukturen" zu verstehen ist. Diese Definition muss mit Artikel 6 des Nachrichtendienstgesetzes und Artikel 1 des Militärgesetzes übereinstimmen, die beide ebenfalls den Begriff der kritischen Infrastrukturen enthalten.
Die Nationale Strategie zum Schutz kritischer Infrastrukturen 2018–2022 unterscheidet neun kritische Sektoren, unterteilt in insgesamt 27 Teilsektoren. Artikel 5 des vorliegenden Entwurfs hält in Übereinstimmung mit Artikel 6 des Nachrichtendienstgesetzes eine allgemeine Definition der kritischen Infrastrukturen sowie beispielhaft vier der kritischen Sektoren fest. Es ist aber, wie bereits gesagt wurde, keine abschliessende Aufzählung.
Der Ständerat fügt in seiner Variante zusätzlich den Teilsektor Trinkwasserversorgung ein und passt die allgemeine Definition an die nationale Cyberstrategie an. Diese Lösung ist praktikabel. Die Kommissionsminderheit will ergänzend zur Variante des Ständerates noch die grundlegenden Spitaleinrichtungen nennen, die weder ein Sektor noch ein Teilsektor sind, sondern dem Teilsektor medizinische Versorgung angehören. Diese Aufzählung ist nicht nötig und würde die in der Cyberstrategie enthaltene Ordnungsstruktur durchbrechen.
Ich bitte Sie entsprechend, den Minderheitsantrag abzulehnen.

Fridez Pierre-Alain (S, JU), pour la commission: A l'article 5 lettre c, une proposition de minorité vise à ajouter à la liste des infrastructures critiques les installations hospitalières de base. Dans le projet du Conseil fédéral, ces installations sont implicitement comprises dans le libellé à la fin de l'article, où il est précisé "ou autre indispensable au fonctionnement de la société civile, de l'économie et de l'Etat."
Sur cette base, la commission s'est opposée à cette minorité par 18 voix contre 6.

Gmür Alois (M-CEB, SZ), für die Kommission: In Artikel 5 Buchstabe c auf Seite 5 der Fahne geht es darum, welche kritischen Infrastrukturen von diesem Gesetz betroffen sind. Eine Minderheit Sommaruga Carlo, übernommen von Priska Seiler Graf, will, dass auch Spitaleinrichtungen als kritische Infrastruktur aufgeführt werden. Die Mehrheit ist der Meinung, dass diese Liste fast endlos würde, wenn wir alle kritischen Infrastrukturen, die in unserem Land existieren, aufführen würden. Dies kann in der Verordnung geregelt werden. Der Ständerat lehnt sich mit seiner Aufzählung an die nationale Cyberstrategie an. Diese Aufzählung unterstützt auch die Mehrheit der Kommission. Diese Regelung betrifft auch die Aufzählung in Artikel 6 des Nachrichtendienstgesetzes und in Artikel 1 des Militärgesetzes.

La présidente (Moret Isabelle, présidente): Le vote vaut également pour le chiffre 2 article 6 alinéa 1 lettre a et chiffre 11 article 1 alinéa 2 lettre c.

Abstimmung – Vote
(namentlich – nominatif; 17.028/20449)
Für den Antrag der Mehrheit ... 117 Stimmen
Für den Antrag der Minderheit ... 68 Stimmen
(0 Enthaltungen)

Art. 6
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 6a
Antrag der Minderheit
(Glättli, Crottaz, Flach, Fridez, Mazzone, Sommaruga Carlo)
Titel
Informationssicherheitsmanagement
Text
Die verpflichteten Behörden und Organisationen definieren und betreiben ein System zum Informationssicherheitsmanagement, das auf international anerkannten Standards basiert.

Art. 6a
Proposition de la minorité
(Glättli, Crottaz, Flach, Fridez, Mazzone, Sommaruga Carlo)
Titre
Gestion de la sécurité de l'information
Texte
Les autorités et organisations soumises à la présente loi définissent et exploitent un système de gestion de la sécurité de l'information fondé sur des normes reconnues sur le plan international.

Glättli Balthasar (G, ZH): In der Botschaft zum Informationssicherheitsgesetz wurde immer wieder erwähnt und bekräftigt: Man will das Rad nicht neu erfinden, sondern internationale Standards anwenden. Zu den wohl bekanntesten Standards in diesem Bereich gehört die Norm ISO/IEC 27001, und die verlangt eben gerade die Umsetzung eines Informationssicherheits-Managementsystems.
In der Kommission wurde in der Diskussion meines Antrages erwähnt, in Artikel 7 Absatz 1 sei eigentlich auch irgendwie mitgemeint, man solle ein solches Informationssicherheits-Managementsystem umsetzen. Die Begründung, weshalb man das nicht geschrieben hat, war, dass die Redaktionskommission dieses Wort etwas kompliziert findet. Jetzt muss ich Ihnen sagen: Ich habe mit verschiedensten Experten aus dem Bereich gesprochen, ich bin ja selbst keiner, zum Beispiel mit Experten verschiedener Computer Emergency Response Teams. Niemand hat das in diesen Text hineingelesen! Es gilt eben auch in jeder Fachsprache: Ein Apfel ist ein Apfel. Wenn man einfach sagt: "Gib mir eine runde Frucht, die mal rot, mal grün und mal gelb ist", dann versteht man das nicht. Wenn man aber einen Apfel einen Apfel nennt, dann versteht man es. Ich finde, dass wir als Gesetzgeber es uns doch schuldig sind, wenn wir meinen, es brauche ein Informationssicherheits-Managementsystem,

auch zu schreiben, dass es ein Informationssicherheits-Managementsystem braucht. Es ist nicht das komplizierteste Wort.
Zum Ort, wo das festgelegt werden soll: Die Auskunft der Verwaltung war, man habe das in Artikel 7 aufgenommen. Dort geht es aber um die Führung und die Führungsverantwortung. Innerhalb eines Informationssicherheits-Managementsystems sind die Führung einerseits und das Risikomanagement andererseits zwei systematisch klar getrennte Bereiche. Für Leute, die sich mit diesen Systemen auskennen, leuchtet das eine grün und das andere rot, weil es unterschiedliche Rollen sind. Deshalb ist es falsch, wenn man das nur in Artikel 7 erwähnt. Man muss die Verpflichtung zum Betrieb eines solchen Informationssicherheits-Managementsystems als grundsätzlichen Auftrag in Artikel 6a schreiben.
Sie könnten jetzt sagen, das sei "l'art pour l'art". Es ist insofern "l'art pour l'art", als ich in den Debatten in der Kommission zum Schluss gelangt bin, dass die Bundesverwaltung effektiv das meint, was ich beantrage. Das Problem ist einfach, dass ich finde, dass Gesetze so formuliert sein sollten, dass das geschrieben steht, was man meint.
In diesem Sinne empfehle ich Ihnen, immer noch überzeugt, bei Artikel 6a dem Antrag meiner Minderheit zuzustimmen.

La présidente (Moret Isabelle, présidente): Le groupe socialiste et le groupe des Verts renoncent à prendre la parole.

Amherd Viola, Bundesrätin: Es wurde begründet: Eine Kommissionsminderheit will im Gesetz eine explizite Pflicht zur Definition und zum Betrieb eines Systems zum Informationssicherheitsmanagement verankern.
Inhaltlich-materiell haben wir keine Differenz dazu. Es ist für uns, für den Bundesrat, und auch für die Mehrheit der Kommission klar, dass ein solches System definiert und eingesetzt werden muss. Es muss aber aus unserer Sicht nicht explizit in einem speziellen Absatz eines Artikels erwähnt werden, weil es bereits in Artikel 7 Absatz 1 enthalten ist. Dieser Artikel schreibt vor, dass die Informationssicherheit nach dem Stand der Wissenschaft und Technik organisiert, umgesetzt und überprüft wird. Stand der Wissenschaft und Technik ist eben, dass man ein solches Managementsystem für die Informationssicherheit hat. Deshalb ist es unnötig, dies nochmals explizit festzuhalten.
Ich bin gleicher Meinung: Das Gesetz muss sagen, was es meint. Man muss aber im Gesetz auch nicht wie in einem Kochrezept jedes Detail anführen. Es ist hier enthalten, die Definition genügt. Der Betrieb und die Definition des Systems sind somit im heutigen Gesetzestext eingeschlossen. Im Übrigen können auch bei der Interpretation eines Gesetzes die Materialien zu Hilfe genommen werden. Aus den Materialien, die sich auch aus dem Amtlichen Bulletin und aus der Botschaft ergeben, ist klar ersichtlich, dass in Artikel 7 Absatz 1 ein Managementsystem für die Informationssicherheit mitgemeint ist.
Ich bitte Sie deshalb, das Gesetz nicht durch noch mehr Artikel zu belasten und diesen Minderheitsantrag abzulehnen.

Fridez Pierre-Alain (S, JU), pour la commission: La proposition de la minorité Glättli à l'article 6a prévoit que "les autorités et organisations soumises à la présente loi définissent et exploitent un système de gestion de la sécurité de l'information fondé sur des normes reconnues sur le plan international".
Dans le message du Conseil fédéral, il est question de respecter de tels standard, et on cite la possibilité de respecter la norme ISO 27 001. Cependant, leur mise en oeuvre pourrait générer des frais, comme cela a été abordé dans mon rapport lors du débat d'entrée en matière.
Les règlements d'application auront le dernier mot. Mais rappelons encore que, à l'article 7 alinéa 1, il est demandé aux autorités soumises à la présente loi de veiller "à ce que la sécurité de l'information soit organisée, mise en oeuvre et contrôlée conformément à l'état des connaissances scientifiques et techniques".
La commission a refusé la proposition défendue par la minorité Glättli par 16 voix contre 7 et aucune abstention.

Gmür Alois (M-CEB, SZ), für die Kommission: Sie haben es gehört: Die Minderheit Glättli will ein Informationssicherheitsmanagement einführen, das auf internationalen Standards basiert. Die Mehrheit ist der Meinung, dass das Anliegen der Minderheit Glättli mit Artikel 7 Absatz 1 erfüllt ist. Dort wird erwähnt, dass die Informationssicherheit nach dem Stand von Wissenschaft und Technik organisiert, umgesetzt und überprüft wird. Mit 16 zu 6 Stimmen wurde der Antrag Glättli abgelehnt.

Abstimmung – Vote
(namentlich – nominatif; 17.028/20450)
Für den Antrag der Minderheit ... 78 Stimmen
Dagegen ... 106 Stimmen
(0 Enthaltungen)

Art. 7
Antrag der Kommission
Abs. 1, 2
Zustimmung zum Beschluss des Ständerates
Abs. 3
Der Bundesrat legt seine Ziele und die Kosten für die Informationssicherheit den Sicherheitspolitischen Kommissionen zur Konsultation vor.

Art. 7
Proposition de la commission
Al. 1, 2
Adhérer à la décision du Conseil des Etats
Al. 3
Le Conseil fédéral consulte les Commissions de politique de sécurité sur ses objectifs en matière de sécurité de l'information et les coûts y afférents.

La présidente (Moret Isabelle, présidente): Mme la conseillère fédérale souhaite s'exprimer sur l'alinéa 3.

Amherd Viola, Bundesrätin: Zu diesem Artikel gibt es zwar keinen Minderheitsantrag, ich möchte mich aber trotzdem dazu äussern. Das wurde auch von Herrn Nationalrat Hurter so gewünscht. Leider werde ich mich wahrscheinlich nicht in dem Sinne äussern, wie er sich das wünschen würde.
Aber trotzdem: Mit diesem Antrag soll der Bundesrat verpflichtet werden, den Sicherheitspolitischen Kommissionen seine Ziele und die Kosten für die Informationssicherheit zur Konsultation vorzulegen. Wir lehnen diesen Antrag ab, nicht weil wir nicht Rechenschaft ablegen wollen, sondern weil die Bestimmung überflüssig ist. Das Parlamentsgesetz gibt den Kommissionen umfassende Kontrollrechte über den Bundesrat und die Verwaltung. So können Sie bereits heute jederzeit vom Bundesrat verlangen, dass er Sie über seine Ziele und die Kosten der Cybersicherheit informiert und auch eine Konsultation dazu bei Ihnen macht.
Zudem wird der Bundesrat gemäss Artikel 89 des Gesetzentwurfes den zuständigen parlamentarischen Kommissionen regelmässig Bericht über die Umsetzung, die Zweckmässigkeit, die Wirksamkeit und die Wirtschaftlichkeit dieses Gesetzes erstatten. Mit dieser Bestimmung wird sichergestellt, dass das Parlament frühzeitig Einfluss auf Ziele, Risiken, Massnahmen und Kosten nehmen kann. Der Bundesrat sieht keinen Grund, für die Kosten der Informationssicherheit eine Sonderregelung einzuführen, die es sonst in keinem Bereich gibt.
Ich bitte Sie deshalb, den Antrag Ihrer Kommission abzulehnen, das heisst, der Variante Bundesrat zuzustimmen.

Fridez Pierre-Alain (S, JU), pour la commission: Je vous dis juste que c'est à une très large majorité, par 20 voix contre 2, que la commission a accepté cette proposition.

La présidente (Moret Isabelle, présidente): Mme la conseillère fédérale propose de biffer l'alinéa 3.

Abstimmung – Vote
(namentlich – nominatif; 17.028/20455)
Für den Antrag der Kommission ... 158 Stimmen
Für den Antrag des Bundesrates ... 22 Stimmen
(6 Enthaltungen)

Art. 8–19
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 20
Antrag der Mehrheit
Abs. 1, 2
Zustimmung zum Beschluss des Ständerates
Abs. 3
Streichen

Antrag der Minderheit I
(Flach, Cattaneo, Dobler, Glanzmann, Gmür Alois, Quadranti)
Abs. 3
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit II
(Keller-Inhelder, Addor, Amstutz, Clottu, Golay, Umbricht Pieren, von Siebenthal, Zuberbühler)
Abs. 3
Streichen

Art. 20
Proposition de la majorité
Al. 1, 2
Adhérer à la décision du Conseil des Etats
Al. 3
Biffer

Proposition de la minorité I
(Flach, Cattaneo, Dobler, Glanzmann, Gmür Alois, Quadranti)
Al. 3
Adhérer à la décision du Conseil des Etats

Proposition de la minorité II
(Keller-Inhelder, Addor, Amstutz, Clottu, Golay, Umbricht Pieren, von Siebenthal, Zuberbühler)
Al. 3
Biffer

Flach Beat (GL, AG): In Artikel 20 Absatz 3 des Informationssicherheitsgesetzes, das wird Sie jetzt überraschen, reden wir plötzlich über die AHV-Nummer. In diesem Gesetz kommt wirklich einiges vor. Es ist wirklich ein Rahmengesetz und eine Umschreibung dessen, was der Bund, die Kantone und die Behörden tun können müssen, um die Sicherheit der Informationen zu gewährleisten. Einer der Punkte, die hier vorkommen, ist, wie man eine Person genau identifiziert, also wie man feststellt, dass Beat Flach auch wirklich der Beat Flach ist und nicht einer, der vielleicht ähnlich oder gleich heisst oder nur vorgibt, dieser zu sein.
Das sicherste Mittel, das wir bei uns kennen, ist die Personenidentifikationsnummer der AHV. Die Nummer ist ganz genau auf die einzelne Person zugeschnitten. Die Mehrheit will hier, dass sie nicht verwendet wird, um Personen zu identifizieren, obwohl die Identifikation einer Person via AHV-Nummer gemäss meiner Minderheit I nur so läuft: Die Person wird identifiziert, und nachher wird die AHV-Nummer vernichtet, gelöscht, weggetan, das heisst, sie kann nicht weiterverwendet werden.
Wie ist das überhaupt in dieses Gesetz hineingekommen? Es ist so entstanden: Als man das Gesetz beraten hat, meldeten sich die kantonalen Datenschutzbeauftragten und haben ganz generell moniert, dass die Verwendung der AHV-Nummer als Identifikationsmittel für Personen mittlerweile sehr verbreitet sei und man da ein bisschen aufpassen sollte. Natürlich ist das tatsächlich so. Die AHV-Nummer ist als universelles Mittel auch einfach universell verwendbar, um Personen genau zu identifizieren, Verwechslungen zu vermeiden und festzustellen, wer jemand ist.
Aber es geht dabei nicht um die Verwendung der AHV-Nummer selbst. Die Nummer selbst gibt auch nichts mehr preis; wir haben heute keine AHV-Nummer mehr, die einen Rückschluss auf den Geburtsort, den Namen, das Alter usw. zulässt. Es ist eine anonymisierte Nummer. Wie gesagt: Die Nummer wird nur zur Identifikation verwendet, dann wird sie wieder gelöscht und nicht weiterverbreitet oder gebraucht. Wir schaffen damit keine Lücken im Sicherheitssystem. Wir schaffen auch datenschutzrechtlich kein Problem, das ist mittlerweile ganz klar.
Ich bitte Sie, hier der Minderheit I zu folgen.

La présidente (Moret Isabelle, présidente): La proposition de la minorité II (Keller-Inhelder) ne sera pas présentée.

Hurter Thomas (V, SH): Wie es die Präsidentin ausgeführt hat, begründen wir hier den Minderheitsantrag nicht direkt. Ich übernehme das gerade als Vertreter der Fraktion.
Wie Sie alle wissen, kommen wir hier zu einem heiklen Punkt, nämlich zur Verwendung der AHV-Nummer. Sie kennen auch die Diskussionen, die wir immer wieder haben, auch im Zusammenhang mit Datenschutzbeauftragten. Übrigens sind auch der Hauseigentümerverband und der Gewerbeverband sehr kritisch. Deshalb ist das eigentlich eines der Kernelemente dieser Gesetzesvorlage. Wichtig sind also nicht nur der Nutzen und die Kosten, sondern auch die Frage, wie man auf diese Daten zugreifen kann. Hier geht es um Artikel 20, aber auch um Artikel 26.
Hinter den Minderheiten stehen eigentlich drei Konzepte. Jene Minderheit, die ich Sie zu unterstützen bitte und die die SVP unterstützen wird, ist die Minderheit II (Keller-Inhelder). Sie will eine komplette Streichung, das heisst keine Verwendung. Weiter gibt es die Variante des Bundesrates, die mit den Worten "kann" und "vorübergehend" formuliert ist. Dann gibt es die noch etwas stärkere Verwendung des Ständerates. Ich bitte Sie wirklich, unsere Minderheit zu unterstützen. Wenn Sie dann halt zwischen der Variante des Ständerates und jener des Bundesrates wählen müssen, bitte ich Sie, auf die Variante des Bundesrates einzuschwenken.
Hier eine kleine Anmerkung, und das vielleicht auch an die Adresse des Bundesrates: Bei diesem Gesetz wollte der Bundesrat ursprünglich keine Verwendung der AHV-Nummer vorsehen, weil er genau wusste, dass es ein sehr kritisches Thema betrifft. Jetzt ist er aber eingeschwenkt und will die Verwendung trotzdem. Ich finde, das ist ziemlich brisant, aber man sieht hier, wie schwierig und heikel dieses Thema ist.
Deshalb bitte ich Sie, unbedingt die Minderheit II (Keller-Inhelder) zu unterstützen, die die Verwendung der AHV-Nummer nicht will.

Roth Franziska (S, SO): Ich spreche zu den Artikeln 20 und 26. Grundsätzlich geht es bei beiden Artikeln um die Regelung der Frage, wie sich Personen authentifizieren können, die berechtigt sind, sich in ein System des Bundes einzuloggen. Es geht also darum, ein System zu definieren, das eine eindeutige Identifikation der zugangsberechtigten Person erlaubt. Rein technisch gibt es mehrere Möglichkeiten, die Identität einer Person festzustellen. Die bei Weitem einfachste und – es ist so! – effizienteste Lösung ist hier wohl die Verwendung der AHV-Nummer. Sie ermöglicht auch eine effiziente Zusammenarbeit mit den Kantonen. Die AHV-Nummer ist aber entsprechend zu schützen. Sowohl in der Bundesverwaltung wie in der Armee bestehen hierzu Standards. Umstritten ist namentlich die Anschlussfrage, ob die AHV-Nummer systematisch verwendet werden muss oder bei Bedarf verwendet werden kann. Der Ständerat hat bei Artikel 20 einen zusätzlichen Absatz 3 eingefügt, der ermöglicht, die AHV-Nummer als Personenidentifikator zu verwenden. Inhaltlich verlangen Bundesrat und Ständerat zwar dasselbe.

Indem der Ständerat aber parallel die Streichung der Kann-Bestimmung in Artikel 26 fordert, bedeutet dies doch, dass die AHV-Nummer in der Fassung des Ständerates systematisch verwendet werden muss. Das lehnt die SP-Fraktion zusammen mit der Mehrheit der Kommission und dem Bundesrat ab.
Die SP-Fraktion findet es richtig, dass Artikel 26 eben nicht gestrichen wird. Die Verwendung der AHV-Nummer soll nicht über Artikel 20 geregelt werden. Das System gemäss Artikel 26 ist nämlich absolut geschlossen. Die AHV-Nummer darf nur an Systeme weitergeleitet werden, die über eine Rechtsgrundlage für die Bearbeitung der AHV-Nummern verfügen. Lassen wir Artikel 26 stehen, so ist die Verwendung der AHV-Nummern also rechtlich eingeschränkt. Wir sind der Ansicht, dass die vom Bundesrat in Artikel 26 verwendete Kann-Formulierung bei der Verwendung der AHV-Nummer als Personenidentifikator am vernünftigsten ist. Weder soll sie systematisch verwendet werden müssen, noch soll die Verwendung grundsätzlich ausgeschlossen werden.
Die Minderheit I (Flach) und die Minderheit II (Keller-Inhelder) zu den Artikeln 20 und 26 lehnen wir ab.

Glanzmann-Hunkeler Ida (M-CEB, LU): Bei diesem Artikel unterstützt die Mitte-Fraktion CVP-EVP-BDP den Minderheitsantrag Flach und hält damit an der Version des Ständerates fest.
Der Ständerat hat hier festgehalten, dass die AHV-Versichertennummer als Personenidentifikator verwendet wird. Uns scheint dies richtig und sinnvoll zu sein. Die Verwendung der AHV-Versichertennummer in diesem Sinn ist aus unserer Sicht effizient und die Vereinheitlichung des Gebrauchs, wie dies der Ständerat mit der Aufnahme dieses Artikels vorsieht, angemessen. Wenn wir im Zusammenhang mit der Verwendung der AHV-Versichertennummer Angst haben, dass ein Datenschutzproblem vorliegt, dann sollten wir uns wohl alle in unserem persönlichen Umfeld und in einem riesig grossen Umfeld mit ganz vielen Daten auseinandersetzen, die wir heute auch so weitergeben. Die AHV-Versichertennummer ist ein klarer Identifikator und kann so gebraucht werden. Sie kann für alle sicher gehandhabt werden.
Wie wir in der Kommission gehört haben, wird die AHV-Versichertennummer schon heute im Militärbereich zur Identifikation verwendet. Wir unterstützen dies, wir unterstützen auch, dass dies mit diesem Gesetz auch der Fall sein kann.
Ich bitte Sie, die Minderheit I (Flach) und damit den Ständerat zu unterstützen. Die Minderheit II (Keller-Inhelder) lehnen wir ab.

Glättli Balthasar (G, ZH): Vorab: Ich gehöre nicht zu jenen, die aus der AHV-Nummer einen heiligen Gral machen. Manchmal hat man ein wenig das Gefühl, der Schutz der AHV-Nummer käme gewissermassen dem Schutz der Seele des Schweizers gleich und alles andere sei dann unproblematisch. Nur um ein Beispiel zu nennen: In diesem Gesetz wird auch die Personensicherheitsprüfung geregelt. Da werden Informationen von Leuten gespeichert, die sehr, sehr tief in die Persönlichkeitssphäre, in die Intimsphäre hineingehen, weil man eben schauen muss, ob jemand eine Flanke aufweist, die allenfalls missbraucht werden kann. Wenn man von Risiken spricht, sind diese also an einem anderen Ort zu suchen.
Dennoch empfehlen wir Grünen Ihnen, mit der Mehrheit zu gehen, dies aus dem folgenden Grund: Wir sollten die AHV-Nummer nur dort verwenden, wo sie wirklich nötig ist, dort, wo es darum geht, aus unterschiedlichen Systemen Daten miteinander abzugleichen – und zwar je Daten, die gemäss diesen Systemen gespeichert werden dürfen – und sicherzustellen, dass man von derselben natürlichen Person spricht. Auf der anderen Seite aber sollte man es so machen, wie es grundlegend Standard ist: Man soll nicht die AHV-Nummer selbst speichern, sondern einen von ihr unumkehrbar abgeleiteten Code. Das heisst, es gibt eine mathematische Operation, die aus der AHV-Nummer etwas anderes macht, was zwingend einmalig ist und von dem man zwingend nicht mehr auf die AHV-Nummer zurückschliessen kann. Das ist meines Erachtens die richtige technische Antwort auf das Problem.
Der Ständerat ist auch etwas weltfremd, indem er die AHV-Nummer quasi im Plaintext als das Hauptidentifikationsmerkmal schafft. Ich würde mich dann schon lieber mit einem Login einloggen, statt mich jeweils mit meiner AHV-Nummer einloggen zu müssen. Das ist etwas weltfremd.
Zur Minderheit II: Für uns ist es klar – wenn die Mehrheit nicht durchkommt, werden wir trotz allem, obwohl es technische Erschwerungen gibt, eher mit der Minderheit II (Keller-Inhelder) gehen als mit der Minderheit I (Flach).

Amherd Viola, Bundesrätin: Sie haben es gehört, es geht hier um die viel diskutierte Verwendung der AHV-Nummer. Die Kommissionsmehrheit will bezüglich der Verwendung der AHV-Nummer die Fassung des Bundesrates. Die Minderheit I will dem Beschluss des Ständerates folgen. Die Minderheit II ist grundsätzlich gegen die Verwendung der AHV-Nummer.
Weit mehr als 100 000 Angestellte von Bund, Kantonen und Wirtschaft sowie Angehörige der Armee benötigen aus verschiedenen Gründen ein Benutzerkonto beim Bund. Der Bund muss diese Personen klar identifizieren, bevor er ihnen einen Zugriff auf seine Informatiksysteme erteilt. Wird dies nicht gemacht, ist das Missbrauchspotenzial gross. Ohne einen eindeutigen Identifikator ist es sehr aufwendig, die Benutzerinnen und Benutzer fehlerfrei zu identifizieren. Entweder werden zusätzliche Daten erhoben, oder der Kontrollvorgang erfolgt manuell. Beide Varianten sind fehleranfällig.
Ganz konkret: In der Schweiz leben Tausende von Personen, die Meier, Müller oder Schmid heissen. Ohne eindeutigen Identifikator müssen deren Benutzerkonten alle manuell überprüft werden. Der beste Personenidentifikator für eine fehlerfreie Identifizierung ist die AHV-Nummer. Deshalb wollen sowohl der Bundesrat, in Artikel 26, als auch der Ständerat, in Artikel 20, den Bund ermächtigen, die AHV-Nummer dafür zu verwenden; beide Bestimmungen sehen im Übrigen eine Kann-Formulierung vor. Wird Artikel 20 im Sinne des Beschlusses des Ständerates angepasst, so kann der ganze Artikel 26 gestrichen werden. Es geht hier nicht darum, Personendaten von Bürgerinnen und Bürgern zu vernetzen oder Profile zu erstellen. Die AHV-Nummer dient lediglich der fehlerfreien Identifizierung der Informatikbenutzerinnen und -benutzer des Bundes.
Der Bundesrat hat in seiner Botschaft einen ziemlich restriktiven Vorschlag gemacht: Die AHV-Nummer soll nur in speziellen Systemen verwendet werden, die ausschliesslich der Kontrolle der Identitäten dienen. Die Regelung des Ständerates geht leicht weiter: Die AHV-Nummer soll nicht nur für diese speziellen Kontrollsysteme verwendet werden, sondern allgemein für die Identitätskontrolle beim Zugang zu den Systemen des Bundes. Bei beiden Varianten wird die AHV-Nummer sehr gut geschützt. Die etwas weiter gehende Lösung des Ständerates bietet dem Bund mehr Sicherheit gegen missbräuchlichen Zugriff. Sie entspricht der Regelung, die heute für militärische Systeme bereits gilt.
Der Bundesrat hat am 30. Oktober letzten Jahres eine Botschaft zur Änderung des AHV-Gesetzes verabschiedet. Neu sollen Behörden generell die AHV-Nummer verwenden dürfen. Strikte Regelungen stellen sicher, dass der Datenschutz und die Informationssicherheit gewährleistet sind. In der Vernehmlassung zu dieser Revision sprach sich eine deutliche Mehrheit für diese Änderung aus.
Die Formulierung des Ständerates übernimmt die Absicht des Bundesrates bereits für das vorliegende Gesetz. Die Regelung im Informationssicherheitsgesetz ist nötig, weil sie dem Bund für laufende und geplante Projekte bis zum Inkrafttreten der Änderung des AHV-Gesetzes klare Sicherheits- und Effizienzgewinne bietet.
In diesem Sinne, weil dieses Gesetz – wir haben es gehört – ja schon seit zehn Jahren in Diskussion ist und weil man jetzt mit der Revision des AHV-Gesetzes in Richtung der Lösung des Ständerates gehen will, bitte ich Sie, dem Antrag der Minderheit I zuzustimmen.

Fridez Pierre-Alain (S, JU), pour la commission: A l'article 20, qui est en lien avec l'article 26, nous sommes saisis de trois concepts. Le premier concept est celui de la majorité

de la commission, qui propose d'accepter le projet du Conseil fédéral, à savoir une utilisation temporaire du numéro AVS dans le système de gestion des données d'identification des personnes pour générer un numéro personnel dérivé du numéro AVS selon un processus unidirectionnel et irréversible. Le numéro AVS est effacé dès la création du numéro personnel dérivé. Le deuxième concept est celui de la minorité I (Flach), qui correspond à la version du Conseil des Etats. Il prévoit l'utilisation du numéro AVS comme identificateur de personnes. Le troisième concept est celui de la minorité II (Keller-Inhelder), qui ne prévoit aucune utilisation du numéro AVS.
Lors du premier vote en commission, le projet du Conseil fédéral a été opposé à la version du Conseil des Etats et a été accepté par 17 voix contre 6 et aucune abstention. Lors du second vote, qui a opposé le projet du Conseil fédéral à la proposition défendue par Mme Keller-Inhelder, la version du Conseil fédéral a été acceptée par 14 voix contre 8 et 1 abstention.

Gmür Alois (M-CEB, SZ), für die Kommission: In Artikel 20 Absatz 3 und in Artikel 26 geht es um die Verwendung der AHV-Nummer als Personenidentifikator. Der Ständerat hat eine systematische Verwendung der AHV-Nummer beschlossen. Der Bundesrat will biometrische Verifikationsmethoden verwenden und die AHV-Nummer allenfalls vorübergehend zulassen.
Es gibt in dieser Angelegenheit zwei Minderheitsanträge. Die Minderheit I (Flach) will die AHV-Nummer systematisch verwenden, wie das der Ständerat will. Sie ist der Ansicht, dass das eine effiziente und günstige Lösung sei. Die Minderheit II (Keller-Inhelder) will die Verwendung der AHV-Nummer grundsätzlich nicht ermöglichen.
Mit 14 zu 8 Stimmen bei 1 Enthaltung wurde der Beschluss des Ständerates, der jetzige Antrag der Minderheit I, abgelehnt. Mit dem gleichen Stimmenverhältnis wurde auch der Antrag, der jetzt als Antrag der Minderheit II vorliegt, abgelehnt. Die Mehrheit der Kommission will damit die Wichtigkeit des Persönlichkeitsschutzes in den Vordergrund stellen und möglichen Missbrauchsgefahren, namentlich bei einer allfälligen Verknüpfung von Datenbanken, vorbeugen. Die Mehrheit ist deshalb für die Lösung des Bundesrates.

La présidente (Moret Isabelle, présidente): Le vote vaut également pour l'article 26.

Erste Abstimmung – Premier vote
(namentlich – nominatif; 17.028/20451)
Für den Antrag der Mehrheit ... 120 Stimmen
Für den Antrag der Minderheit I ... 68 Stimmen
(0 Enthaltungen)

Zweite Abstimmung – Deuxième vote
(namentlich – nominatif; 17.028/20452)
Für den Antrag der Mehrheit ... 137 Stimmen
Für den Antrag der Minderheit II ... 52 Stimmen
(0 Enthaltungen)

Art. 21, 22
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 23
Antrag der Kommission
Abs. 1, 3, 4
Zustimmung zum Beschluss des Ständerates
Abs. 2
Zustimmung zum Beschluss des Ständerates
(die Änderung betrifft nur den französischen Text)

Art. 23
Proposition de la commission
Al. 1, 3, 4
Adhérer à la décision du Conseil des Etats
Al. 2
...
a. interdire certains objets, en particulier les appareils de prises de vue et de son;
...

Angenommen – Adopté

Art. 24, 25
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 26
Antrag der Mehrheit
Zustimmung zum Entwurf des Bundesrates

Antrag der Minderheit I
(Flach, Cattaneo, Dobler, Glanzmann, Gmür Alois, Quadranti)
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit II
(Keller-Inhelder, Addor, Amstutz, Clottu, Golay, Umbricht Pieren, von Siebenthal, Zuberbühler)
Zustimmung zum Beschluss des Ständerates

Art. 26
Proposition de la majorité
Adhérer au projet du Conseil fédéral

Proposition de la minorité I
(Flach, Cattaneo, Dobler, Glanzmann, Gmür Alois, Quadranti)
Adhérer à la décision du Conseil des Etats

Proposition de la minorité II
(Keller-Inhelder, Addor, Amstutz, Clottu, Golay, Umbricht Pieren, von Siebenthal, Zuberbühler)
Adhérer à la décision du Conseil des Etats

La présidente (Moret Isabelle, présidente): Nous nous sommes déjà prononcés sur les propositions des minorités à l'article 20.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Art. 27–29
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 30
Antrag der Kommission
Abs. 1–3
Zustimmung zum Beschluss des Ständerates
Abs. 4
...
g. Kantonale Magistratsperson, die vom Volk oder vom kantonalen Parlament gewählt wird.

Art. 30
Proposition de la commission
Al. 1–3
Adhérer à la décision du Conseil des Etats

Al. 4
Les candidats aux fonctions suivantes ne sont pas soumis à un contrôle de sécurité:
...
g. magistrat cantonal élu par le peuple ou par le parlement du canton concerné.

Angenommen – Adopté

Art. 31–76
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 77
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Seiler Graf, Arslan, Crottaz, Fridez, Glättli, Masshardt)
Abs. 3
Die Betreiberinnen von kritischen Infrastrukturen sowie die Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten geben den Stellen nach Artikel 75 Absatz 5 Daten, einschliesslich Personendaten, die sich auf einen bestimmten erheblichen Vorfall beziehen, bekannt. ...

Art. 77
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Seiler Graf, Arslan, Crottaz, Fridez, Glättli, Masshardt)
Al. 3
Les exploitants d'infrastructures critiques, de même que les fournisseurs et les exploitants de services informatiques et de communication, communiquent aux services visés à l'article 75 alinéa 5 des données liées à des incidents considérables, y compris des données personnelles. ...

Seiler Graf Priska (S, ZH): Ich spreche zu meinem Minderheitsantrag zu Artikel 77 und auch gleich zu meinem Minderheitsantrag zu Artikel 81, da die beiden Anträge inhaltlich zusammengehören und auch voneinander abhängig sind.
Der SP-Fraktion war es immer wieder ein wichtiges Anliegen, dass die Meldepflicht für kritische Infrastrukturen endlich einmal gesetzlich verankert wird. Wir haben schon versucht, sie ins Bevölkerungs- und Zivilschutzgesetz aufzunehmen. Da wurde wahrscheinlich zu Recht moniert, dass das nicht der richtige Ort sei. Ich bin nun aber klar der Ansicht, dass eine Meldepflicht für kritische Infrastrukturen sicher in ein zweckmässiges Informationssicherheitsgesetz gehört. In Artikel 77 Absatz 3 ist ja bereits ein Melderecht aufgeführt, das aber unserer Meinung nach zu defensiv ist und das Sicherheitsniveau darum nicht wirklich erhöht.
Frau Bundesrätin Amherd erwähnte in der Kommission, dass im Rahmen der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken geprüft wird, ob eine Meldepflicht für Betreiber von kritischen Infrastrukturen eingeführt werden soll. Das eine schliesst aber das andere unserer Meinung nach nicht aus. Eine Meldepflicht muss jetzt endlich einmal gesetzlich festgelegt werden, und ich denke, in diesem Gesetz wäre der richtige Ort, hier sollte es erwähnt sein.
Ich bitte Sie darum, unserem Minderheitsantrag zuzustimmen.

La présidente (Moret Isabelle, présidente): Le groupe UDC, le groupe socialiste et le groupe des Verts renoncent à prendre la parole.

Amherd Viola, Bundesrätin: Artikel 77 Absatz 3 sieht vor, dass die Betreiberinnen von kritischen Infrastrukturen sowie die Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten auf freiwilliger Basis mit dem neuen Nationalen Zentrum für Cybersicherheit Informationen und Daten über Bedrohungen und Vorfälle austauschen können. Mit dem Minderheitsantrag zu den Artikeln 77 und 81 soll nun eine Meldepflicht bei erheblichen Cybervorfällen eingeführt werden. Ein ähnlicher Antrag wurde bereits im Rahmen der Beratung des Bevölkerungs- und Zivilschutzgesetzes gestellt und in dieser Kammer abgelehnt.
Der Bundesrat prüft zurzeit im Rahmen der Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken, ob er eine solche Meldepflicht einführen will. Der Regelungsbedarf für die Umsetzung der neuen Strategie soll gesamtheitlich beurteilt und dann dem Parlament unterbreitet werden. Wenn man so etwas einführen will, müsste man sich dann auch noch näher darüber unterhalten, was ein "erheblicher Cybervorfall" ist. Auch das ist ein sehr unbestimmter Begriff, und es wäre schwierig, jetzt hier so etwas einzuführen, zumal die Umsetzung unklar wäre.
Ich bitte Sie deshalb, den Minderheitsantrag zu den Artikeln 77 und 81 abzulehnen, damit man das eben im Rahmen der Cyberstrategie genau anschauen und überlegen kann, wie so etwas, wenn man es denn will, formuliert werden muss, damit es auch umsetzbar ist.

Fridez Pierre-Alain (S, JU), pour la commission: Cette minorité traite de la question de la transmission d'informations par les exploitants d'infrastructures critiques aux instances fédérales chargées de les appuyer et de les conseiller, soit un service national d'alerte et un service d'assistance.
Dans le texte du Conseil fédéral, il est prévu que les exploitants d'infrastructures critiques, de même que les fournisseurs et les exploitants de services informatiques et de communication, peuvent communiquer des données liées à des incidents. La minorité Seiler Graf propose une communication d'office pour des données liées à des incidents considérables; cette minorité est accompagnée d'un ajout à l'article 81 lettre e qui donne mandat au Conseil fédéral d'édicter les modalités de cette communication d'informations.
En commission, la proposition défendue par la minorité Seiler Graf a été rejetée, à l'article 77 alinéa 3 par 16 voix contre 6, et à l'article 81 lettre e par 15 voix contre 6.

Gmür Alois (M-CEB, SZ), für die Kommission: In Artikel 77 Absatz 3 und Artikel 81 Buchstabe e möchte die Minderheit Seiler Graf eine Meldepflicht für Betreiberinnen von kritischen Infrastrukturen sowie für Anbieterinnen und Betreiberinnen von Informatik- und Kommunikationsdiensten einführen. Die Mehrheit der Kommission lässt hier eine Abwägung mit entsprechender Freiwilligkeit der Meldung zu.
Mit 16 zu 6 Stimmen bei Artikel 77 Absatz 3 und mit 15 zu 6 Stimmen bei Artikel 81 Buchstabe e wurden die entsprechenden Anträge Seiler Graf in der Kommission abgelehnt.

Abstimmung – Vote
(namentlich – nominatif; 17.028/20453)
Für den Antrag der Mehrheit ... 116 Stimmen
Für den Antrag der Minderheit ... 68 Stimmen
(0 Enthaltungen)

Art. 78–80
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 81
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Seiler Graf, Arslan, Crottaz, Fridez, Glättli, Masshardt)
Bst. e
e. die Bekanntgabe von Informationen an die Stellen nach Artikel 75 Absatz 5 durch die Betreiberinnen von kritischen Infrastrukturen nach Artikel 77 Absatz 3.

Art. 81
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Seiler Graf, Arslan, Crottaz, Fridez, Glättli, Masshardt)
Let. e
e. les modalités de la communication d'informations aux services visés à l'article 75 alinéa 5, par les exploitants d'infrastructures critiques conformément à l'article 77 alinéa 3.

La présidente (Moret Isabelle, présidente): La proposition de la minorité Seiler Graf a déjà été rejetée à l'article 77.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Art. 82–85
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 86
Antrag der Mehrheit
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Glättli, Arslan, Crottaz, Fridez, Masshardt, Seiler Graf)
Abs. 3
Die verpflichteten Behörden können mit einer konkreten Begründung die Standardanforderungen als nicht verpflichtend deklarieren.

Art. 86
Proposition de la majorité
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Glättli, Arslan, Crottaz, Fridez, Masshardt, Seiler Graf)
Al. 3
Les autorités soumises à la présente loi peuvent déclarer non contraignantes les exigences standards; elles motivent concrètement leur décision.

Glättli Balthasar (G, ZH): Wir haben es extra schon in den einleitenden Voten unserer Fraktion erwähnt, Léonore Porchet und ich: Hier geht es aus Sicht der Minderheit tatsächlich um noch mehr als nur um eine ästhetische Konkurrenz. Hier geht es darum, ob diese ganze Geschichte mit den Mindeststandards auch Biss hat oder nicht.
Es macht wenig Sinn, zwar mühsam grundlegende Sicherheitsstandards festzulegen, die dann auch flächendeckend gelten sollen, diese aber gleichzeitig für vollkommen freiwillig zu erklären. Die Formulierung des Bundesrates hat nichts anderes zur Folge als das. Es heisst nämlich: "Die Standardanforderungen und -massnahmen haben empfehlenden Charakter, sofern sie von den verpflichteten Behörden nicht für verbindlich erklärt werden." Normalerweise werden die, die den Auftrag haben, doch nicht gefragt, ob sie diese Empfehlungen umsetzen wollen oder nicht, sondern die Empfehlungen gelten und müssen überall umgesetzt werden. Wir wollen das umdrehen, dass es so ist, wie es normalerweise sein muss: Standards sind Standards, sie müssen nicht hoch sein, aber sie müssen gelten – und sie müssen verbindlich gelten. Da wir uns auch bewusst sind, dass es Einzelfälle geben kann, bei denen dann selbst diese minimalen Standards vielleicht doch zu hoch oder zu aufwendig sind, möchten wir mit unserer Minderheit den verpflichteten Behörden, welche die Grundstandards eigentlich umsetzen müssen, die Möglichkeit eines Opt-out geben. Das Opt-out kann aber nur dann gemacht werden, wenn es mit einer konkreten Begründung versehen ist. Das heisst, ich kann immer noch unter die Minimalstandards gehen, dann muss ich aber begründen, dass das kein Risiko ist.
Der Bundesrat sagt: Wir geben euch Empfehlungen für Minimalstandards, wenn ihr wollt, könnt ihr Opt-in machen.
Wenn Sie wirklich mehr Sicherheit wollen, dann folgen Sie in Artikel 86 Absatz 3 der Minderheit Glättli. Es geht wirklich nicht um die Frage, welchen Begriff man jetzt hier mit oder ohne Segen der Redaktionskommission ins Gesetz schreibt, hier geht es um den Kern, dass nur verbindliche Mindeststandards auch brauchbare Mindeststandards sind.
Ich verwende nochmals das Beispiel aus dem Eintretensvotum: Wir wären sehr froh gewesen, wenn wir in unserem Pandemieplan keine Verantwortungsdiffusion gehabt hätten, wenn gewisse Zuständigkeiten nicht einfach empfohlen, sondern vorgeschrieben gewesen wären. Machen wir hier nicht den gleichen Fehler.

Hurter Thomas (V, SH): Ich bitte Sie, diesen Minderheitsantrag abzulehnen. Es geht ja hier um die Frage, ob die sogenannt verpflichteten Behörden, also z. B. die Armee, die Parlamentsdienste oder das Parlament, diese Regelung und diese Standardanforderungen übernehmen sollten oder nicht. Es ist doch völlig richtig, dass der Bundesrat definiert, welche zu übernehmen sind und welche nicht. Es kann ja nicht sein, dass dann diese Behörden eigentlich im Nachhinein sagen müssen, warum sie welche nicht übernehmen. Das ist, glaube ich, der falsche Weg. Deshalb müssen wir hier bei der Mehrheit bleiben.
Erlauben Sie mir zum Abschluss, wir sind ja am Ende dieser Beratung, noch eine Bemerkung: Dieses Gesetz ist kein grosser Wurf. Es ist zehn Jahre her, dass man mit dem Gesetz begonnen hat. Man hat eine Vernehmlassung gemacht, über 500 Antworten sind eingetroffen, und wir haben uns an mehreren Sitzungen darüber unterhalten. Das Gesetz wurde zurückgewiesen, unter anderem aufgrund eines Antrages aus der CVP. Wir haben dann die Sicherheitsniveaus definieren können, und dann wurde endlich klar, um welche Kosten es geht. Es geht zunächst um mehrere Millionen bis zu fast 100 Millionen Franken, je nachdem, was man da alles einrechnet.
Deshalb ist natürlich auch dieser Artikel 7 Absatz 3 ganz wichtig. Ich möchte hier noch einmal darauf hinweisen: Es ging eigentlich die ganze Zeit auch um die Frage, was der wirkliche Mehrwert dieses Gesetzes ist. Hier ist auch bei uns in der Fraktion noch etwas Unzufriedenheit da. Man spürt es auch in der Industrie: Es sind nicht alle so glücklich, wie Sie, Frau Bundesrätin, sagen. Vor allem dann, wenn Sie dann bezüglich höherer Kosten oder höherer Sicherheitsniveaus die Konsultation nicht wollen, läuten schon etwas die Alarmglocken, wenn wir das so sagen dürfen.
Das Gesetz ist also ganz klar kein grosser Wurf. Es enthält sehr viele Inputs, deren Nutzen teilweise sehr fraglich ist. Die Kosten hat man zwar dank diesem Artikel 7 etwas besser in den Griff gekriegt. Ich sage nicht, dass ich hier warnen will. Wenn aber der Ständerat bei Artikel 7 diesen Absatz 3 bezüglich Konsultation herausnimmt, dann bin ich überzeugt, dass dieses Gesetz keine Chance haben wird.

Flach Beat (GL, AG): Wir sind hier bei der letzten Minderheit, die noch verblieben ist, und ich bitte Sie, diese abzulehnen.
Herr Glättli hat vorhin ausgeführt, dass er eigentlich das System umkehren will. Er will, dass der Bund die Minimalstandards, die er festlegt, immer als verbindlich betitelt, das heisst, sie müssen eingehalten werden, es sei denn, es bestehen konkrete Anhaltspunkte, dass das nicht notwendig wäre. Das ist einfach systematisch falsch, wenn es in diesem Sinne um Minimalstandards geht, weil man in einem Bereich tätig ist, in dem wir verschiedene Sicherheitslevels haben, verschiedene Techniken, verschiedene Infrastruktu-

ren, verschiedene EDV-Systeme; das alles ist im Wandel, das wird alles ständig von Neuerungen umgewälzt. Wenn wir jetzt darauf vertrauen, dass der Bund bei allen Systemen jeweils sagt: "Das ist der Standard, und es darf nichts anderes sein", und alles andere verboten ist, dann führt das nicht zu mehr Sicherheit, sondern höchstens zu einer Verknöcherung der Systeme, weil man dann immer sagen muss: "Wir müssen warten, bis der Bund sagt, dass wir hier auch etwas anderes machen können", obwohl die Sicherheit vielleicht sogar besser gewährleistet ist, als wenn man es macht.
Ich glaube, letztlich ist es mehr als Wortklauberei, was man hier tut, da hat Herr Glättli vollkommen recht, aber es ist wichtig, dass wir es als Rahmengesetz und auch als Managementsystem der Infrastrukturen für die Sicherheit bei den Informationen verstehen.
Vielleicht noch ein letztes Wort: Herr Hurter hat zum Abschluss gesagt, dass es quasi der Tod des Gesetzes sei, wenn die Konsultation fehle. Ich glaube, wir müssen uns einfach im Klaren sein, dass wir jederzeit über das Budget steuern können, wie viel wir für was ausgeben. Das brauchen wir nicht in jedes Gesetz hineinzuschreiben. Wir haben im Rahmen der Budgetberatungen alle diese Möglichkeiten. Ich glaube, das ist dann wirklich das Falsche.
Es ist eine komplizierte Geschichte, die wir hier zusammengenommen haben. Ich bitte Sie aber, letztlich dem Gesetz zuzustimmen, damit wir etwas haben, womit wir weiterarbeiten können.

Glättli Balthasar (G, ZH): Kollege Flach, Sie haben jetzt gesagt, man müsse dann, wenn man sich mit Begründung nicht an diese Minimalstandards halten wolle, eine Bewilligung abwarten. Können Sie bestätigen, dass das nicht Gegenstand meines Minderheitsantrages ist, mit dem der verpflichteten Behörde bloss eine Begründungspflicht auferlegt werden soll, aber keine Pflicht, eine Bewilligung einzuholen?

Flach Beat (GL, AG): Das ist prinzipiell richtig, Herr Kollege Glättli. De facto ist es natürlich aber so, dass der Systembetreiber jeweils nachfragen muss, ob er etwas anderes unternehmen könne, denn er hat keine konkrete vorausschauende Beurteilung, in der es heisst, da könne er etwas anderes machen. Vielleicht muss sich der Ständerat noch einmal über diese Frage beugen, ich habe es eben nicht Wortklauberei genannt, und das noch einmal genauer anschauen. Ich bin aber nach wie vor der Überzeugung, dass wir mit Ihrem Minderheitsantrag nicht mehr Sicherheit schaffen.

Amherd Viola, Bundesrätin: Die Sicherheitsstandards des Bundesrates werden für alle Behörden, die ihm unterstellt sind, verpflichtend sein. Dies betrifft vor allem die Bundesverwaltung und auch die Armee. Vom Bundesrat unabhängige Behörden wie das Parlament oder die Bundesgerichte dürfen hingegen nicht zur Übernahme des Standards verpflichtet werden, weil diese Behörden laut Verfassung eben unabhängig sind. Die Standards dürfen hier lediglich empfehlenden Charakter haben. Das ist im Gesetz so vorgesehen. Dies hat nichts mit Biss und auch nichts mit höheren oder tieferen Standards zu tun, sondern mit Verfassungsrecht, an das wir uns halten wollen und müssen. Deshalb geht es hier tatsächlich um den Kern, nämlich um den Kern der Gewaltentrennung.
Ich bitte Sie, den Antrag der Minderheit abzulehnen.

Fridez Pierre-Alain (S, JU), pour la commission: A l'article 86 alinéa 1, il est écrit: "Le Conseil fédéral fixe des exigences standard en matière de sécurité et définit des mesures standard en matière d'organisation, de personnel et de construction, de même que sur le plan technique, pour assurer la sécurité de l'information; il suit à cet effet l'avancement des connaissances et de la technique." A l'alinéa 3, il est précisé: "Les exigences et mesures standard du Conseil fédéral ont valeur de recommandations, sauf si les autorités soumises à la présente loi les déclarent obligatoires." L'obligation n'est donc pas la règle, mais l'exception.
La minorité Glättli propose de rédiger l'alinéa 3 ainsi: "Les autorités soumises à la présente loi peuvent déclarer non contraignantes les exigences standards; elles motivent concrètement leur décision." L'obligation devient la règle et la "non-obligation" l'exception.
Cette proposition a été rejetée par 15 voix contre 6 et 1 abstention.

Gmür Alois (M-CEB, SZ), für die Kommission: Bei Artikel 86 Absatz 3 sieht der Bundesrat die Standardanforderungen und Standardmassnahmen in erster Linie als Empfehlung an, die aber von den verpflichteten Behörden für nicht verbindlich erklärt werden können. Die Minderheit Glättli will, dass diese Anforderungen und Massnahmen grundsätzlich verbindlich sein sollen und nur mit einer konkreten Begründung als nicht verpflichtend erklärt werden können.
Mit 15 zu 6 Stimmen bei 1 Enthaltung hat die Kommission der Fassung des bundesrätlichen Entwurfes zugestimmt.
Ich komme zum Schluss: In der Gesamtabstimmung wurde mit 16 zu 1 Stimmen bei 5 Enthaltungen dem Informationssicherheitsgesetz zugestimmt. Die Kommission will die Umsetzung des Gesetzes und namentlich die Entwicklung der Kosten weiterhin aufmerksam verfolgen und sich zu den Verordnungsanpassungen, die sich in der Folge der jetzt behandelten Gesetzesvorlage ergeben, konsultieren lassen.
Im Namen der Kommissionsmehrheit bitte ich Sie, dem Gesetz zuzustimmen.

Abstimmung – Vote
(namentlich – nominatif; 17.028/20454)
Für den Antrag der Mehrheit ... 122 Stimmen
Für den Antrag der Minderheit ... 66 Stimmen
(0 Enthaltungen)

Art. 87–91
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Art. 91a
Antrag der Kommission
Titel
Koordination mit dem Strafregistergesetz
Text
1. Tritt das Strafregistergesetz vom 17. Juni 2016 (StReG) vor dem vorliegenden Gesetz in Kraft, entfallen die im vorliegenden Gesetz enthaltenen Änderungen von Artikel 365 Absatz 2 Buchstabe d sowie 367 Absätze 2 Buchstabe i, 2bis Buchstabe b und 4 StGB. Stattdessen sind Artikel 46 Absatz 6 Buchstabe a ISG, Artikel 46 Buchstabe e, Artikel 51 Buchstabe f StReG und Artikel 59 StReG mit Inkrafttreten des vorliegenden Gesetzes wie folgt zu ändern:
Art. 46 Abs. 6 Einleitung ISG
Die Daten nach Absatz 4 können automatisch und systematisch durch Abfrage der folgenden Informationssysteme erhoben werden:
Art. 46 Abs. 6 Bst. a ISG
a. Strafregister-Informationssystem Vostra nach dem Strafregistergesetz vom 17. Juni 2016;
Art. 46 Einleitung StReG
Folgende angeschlossene Behörden können durch ein Abrufverfahren in alle im Behördenauszug 2 erscheinenden Daten (Art. 38) Einsicht nehmen, soweit dies für die Erfüllung der nachstehend genannten Aufgaben notwendig ist:
Art. 46 Bst. e StReG
e. die Fachstellen für Personensicherheitsprüfungen nach Artikel 32 Absatz 2 des Informationssicherheitsgesetzes vom ... (ISG):
1. für die Beurteilung des Risikos im Rahmen von Personensicherheitsprüfungen nach dem ISG,
2. für Beurteilungen des Gefährdungs- und Missbrauchspotenzials nach dem Militärgesetz vom 3. Februar 1995,
3. für weitere Beurteilungen des Risikos im Rahmen der in der Spezialgesetzgebung vorgesehenen Prüfungen;

Art. 51 Bst. f StReG
Aufheben
Art. 59 Titel StReG
Meldungen an die Gruppe Verteidigung
Art. 59 Abs. 1 StReG
Die registerführende Stelle meldet der Gruppe Verteidigung zu den in Absatz 2 erwähnten Zwecken unverzüglich folgende neu in Vostra eingetragenen Daten von Stellungspflichtigen und Angehörigen der Armee:
a. schweizerische Grundurteile wegen eines Verbrechens oder Vergehens;
b. ausländische Grundurteile;
c. freiheitsentziehende Massnahmen;
d. Entscheide betreffend Nichtbewährung.
Art. 59 Abs. 2 StReG
Die Gruppe Verteidigung darf die gemeldeten Daten für folgende Zwecke verwenden:
a. Prüfung einer Nichtrekrutierung, einer Zulassung zur Rekrutierung, eines Ausschlusses aus der Armee, einer Wiederzulassung zur Armee, einer Degradation oder der Eignung für eine Beförderung oder Ernennung nach dem MG;
b. Prüfung von Hinderungsgründen für die Überlassung der persönlichen Waffe nach dem MG.
Art. 59 Abs. 3 StReG
Die Meldung erfolgt über eine elektronische Schnittstelle zwischen dem Personalinformationssystem der Armee und des Zivilschutzes (PISA) und Vostra. Die Aufbereitung der Daten nach Absatz 1 erfolgt automatisiert und unter Verwendung der Versichertennummer.
2. Tritt das Strafregistergesetz nach dem vorliegenden Gesetz in Kraft, so sind Artikel 46 Absatz 6 Buchstabe a ISG, Artikel 46 Buchstabe e StReG, Artikel 51 Buchstabe f StReG und Artikel 59 StReG gemäss oben stehendem Wortlaut zu ändern. Hingegen entfällt die im Strafregistergesetz vorgesehene Änderung von Artikel 20a BPG; die nach dem vorliegenden Gesetz vorgesehene Änderung von Artikel 20a BPG bleibt also in Kraft.

Art. 91a
Proposition de la commission
Titre
Coordination avec la loi sur le casier judiciaire
Texte
1. Si la loi sur le casier judiciaire (LCJ) entre en vigueur avant la présente loi, les modifications des articles 365 alinéa 2 lettre d et 367 alinéa 2 lettre i, 2bis lettre b et 4 CP prévues par le présent projet seront caduques. L'article 46 alinéa 6 lettre a LSI, l'article 46 lettre e LCJ, l'article 51 lettre f LCJ et l'article 59 LCJ devront alors être modifiés comme suit:
Art. 46 al. 6 introduction LSI
Les données visées à l'alinéa 4 peuvent être collectées automatiquement et systématiquement en ligne dans les systèmes d'information suivants:
Art. 46 al. 6 let. a LSI
a. casier judiciaire informatique au sens de la loi du 17 juin 2016 sur le casier judiciaire;
Art. 46 introduction LSI
Les autorités raccordées suivantes peuvent consulter en ligne toutes les données figurant sur l'extrait 2 destiné aux autorités (art. 38), lorsqu'elles leur sont nécessaires pour accomplir les tâches mentionnées ci-après:
Art. 46 let. e LSI
e. les services spécialisés qui mènent les contrôles de sécurité relatifs aux personnes au sens de l'article 32 alinéa 2, de la loi du ... sur la sécurité de l'information (LSI):
1. pour évaluer le risque dans le cadre de contrôles de sécurité relatifs aux personnes au sens de la LSI,
2. pour évaluer le potentiel d'abus ou de dangerosité au sens de la loi du 3 février 1995 sur l'armée,
3. pour évaluer le risque dans le cadre d'autres contrôles prévus dans la législation spéciale;
Art. 51 let. f LCJ
Abroger
Art. 59 titre LCJ
Communication au Groupement Défense
Art. 59 al. 1 LCJ
Le Service du casier judiciaire communique sans délai au Groupement Défense, aux fins énumérées à l'alinéa 2, les données suivantes concernant des conscrits et des militaires, dès leur saisie dans Vostra:
a. les jugements suisses pour crime ou délit;
b. les jugements étrangers;
c. les mesures entraînant une privation de liberté;
d. les décisions relatives à l'échec de la mise à l'épreuve.
Art. 59 al. 2 LCJ
Le Groupement Défense peut utiliser les données communiquées:
a. pour prendre les décisions de non-recrutement, d'admission au recrutement, d'exclusion de l'armée ou de réintégration dans l'armée, de dégradation, et pour examiner l'aptitude à une promotion ou une nomination, en application de la LAAM;
b. pour examiner les motifs empêchant la remise de l'arme personnelle, en application de la LAAM.
Art. 59 al. 3 LCJ
La communication a lieu par une interface électronique entre le système d'information sur le personnel de l'armée et de la protection civile (SIPA) et Vostra. Les données visées à l'alinéa 1 sont sélectionnées et transmises de manière automatisée sur la base du numéro AVS de la personne concernée.
2. Si la LCJ entre en vigueur après la présente loi, l'article 46 alinéa 6 lettre a, LSI et les articles 46 lettre e, 51 lettre f, et 59 LCJ seront modifiés comme ci-dessus. En revanche, la modification de l'article 20a LPers prévue par la LCJ sera caduque; en d'autres termes, la modification de l'article 20a LPers prévue par le présent projet restera en vigueur.

Angenommen – Adopté

Art. 92
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Änderung anderer Erlasse
Modification d'autres actes

Ziff. 1
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. 1
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Ziff. 2
Antrag der Mehrheit
Art. 6 Abs. 1 Bst. a Ziff. 4; 51 Abs. 4 Bst. d
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Sommaruga Carlo, Crottaz, Fridez, Glättli, Mazzone, Seiler Graf)
Art. 6 Abs. 1 Bst. a Ziff. 4
4. ... Informations-, Kommunikations- und Transportinfrastrukturen sowie grundlegende Spitaleinrichtungen und weitere Prozesse ...

Ch. 2
Proposition de la majorité
Art. 6 al. 1 let. a ch. 4; 51 al. 4 let. d
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Sommaruga Carlo, Crottaz, Fridez, Glättli, Mazzone, Seiler Graf)
Art. 6 al. 1 let. a ch. 4
4. ... de communication et de transport ainsi que les installations hospitalières de base et d'autres installations, processus ...

La présidente (Moret Isabelle, présidente): La proposition de la minorité Sommaruga Carlo a déjà été rejetée à l'article 5 de la loi sur la sécurité de l'information.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. 3–10
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. 3–10
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Ziff. 11
Antrag der Mehrheit
Art. 1 Abs. 2 Bst. c; 14; 113 Abs. 6; 150 Abs. 4
Zustimmung zum Beschluss des Ständerates

Antrag der Minderheit
(Sommaruga Carlo, Crottaz, Fridez, Glättli, Mazzone, Seiler Graf)
Art. 1 Abs. 2 Bst. c
c. ... Informations-, Kommunikations- und Transportinfrastrukturen sowie grundlegende Spitaleinrichtungen und weitere Prozesse ...

Ch. 11
Proposition de la majorité
Art. 1 al. 2 let. c; 14; 113 al. 6; 150 al. 4
Adhérer à la décision du Conseil des Etats

Proposition de la minorité
(Sommaruga Carlo, Crottaz, Fridez, Glättli, Mazzone, Seiler Graf)
Art. 1 al. 2 let. c
c. ... de communication et de transport ainsi que les installations hospitalières de base et d'autres installations, processus ...

La présidente (Moret Isabelle, présidente): La proposition de la minorité Sommaruga Carlo a déjà été rejetée à l'article 5 de la loi sur la sécurité de l'information.

Angenommen gemäss Antrag der Mehrheit
Adopté selon la proposition de la majorité

Ziff. 12, 13
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. 12, 13
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Ziff. 14
Antrag der Kommission
Art. 20a Abs. 1
Personen, die von der nationalen Netzgesellschaft in kritischen oder höchstkritischen Funktionen eingesetzt werden, werden zur Beurteilung des Sicherheitsrisikos periodisch auf ihre Vertrauenswürdigkeit hin geprüft.
Art. 20a Abs. 2, 3
Zustimmung zum Beschluss des Ständerates
Art. 20a Abs. 4
Die nationale Netzgesellschaft ersucht um Durchführung der Prüfung. Das Ergebnis ist ihr mitzuteilen und kurz zu begründen.

Ch. 14
Proposition de la commission
Art. 20a al. 1
Les personnes auxquelles la société nationale du réseau de transport attribue des fonctions critiques ou extrêmement critiques sont périodiquement soumises à un contrôle de loyauté visant à évaluer le risque pour la sécurité.
Art. 20a al. 2, 3
Adhérer à la décision du Conseil des Etats
Art. 20a al. 4
La société nationale du réseau de transport demande que le contrôle soit effectué. Le résultat du contrôle lui est communiqué et brièvement expliqué.

Angenommen – Adopté

Ziff. 15, 16
Antrag der Kommission
Zustimmung zum Beschluss des Ständerates

Ch. 15, 16
Proposition de la commission
Adhérer à la décision du Conseil des Etats

Angenommen – Adopté

Gesamtabstimmung – Vote sur l'ensemble
(namentlich – nominatif; 17.028/20456)
Für Annahme des Entwurfes ... 131 Stimmen
Dagegen ... 53 Stimmen
(1 Enthaltung)

Schluss der Sitzung um 17.50 Uhr
La séance est levée à 17 h 50