

*Logistik – Logistique**Abstimmung – Vote*(namentlich – nominatif: Beilage – Annexe 10.028/4736)

Für den Antrag der Mehrheit/Minderheit I ... 97 Stimmen

Für den Antrag der Minderheit II ... 73 Stimmen

*Mobilität (Kauf von GMTF)**Mobilité (achat de GMTF)**Abstimmung – Vote*(namentlich – nominatif: Beilage – Annexe 10.028/4737)

Für den Antrag der Mehrheit ... 95 Stimmen

Für den Antrag der Minderheit II ... 76 Stimmen

*Mobilität (Kompensation von 122 Millionen Franken)**Mobilité (compensation de 122 millions de francs)**Abstimmung – Vote*(namentlich – nominatif: Beilage – Annexe 10.028/4738)

Für den Antrag der Mehrheit ... 116 Stimmen

Für den Antrag der Minderheit I ... 58 Stimmen

*Ausgabenbremse – Frein aux dépenses**Abstimmung – Vote*(namentlich – nominatif: Beilage – Annexe 10.028/4739)

Für Annahme der Ausgabe ... 120 Stimmen

Dagegen ... 36 Stimmen

*Das qualifizierte Mehr ist erreicht**La majorité qualifiée est acquise***Art. 2–4***Antrag der Kommission*

Zustimmung zum Beschluss des Ständerates

Proposition de la commission

Adhérer à la décision du Conseil des Etats

*Angenommen – Adopté**Gesamtabstimmung – Vote sur l'ensemble*(namentlich – nominatif: Beilage – Annexe 10.028/4740)

Für Annahme des Entwurfes ... 117 Stimmen

Dagegen ... 37 Stimmen

10.3625

**Motion SiK-NR.
Massnahmen gegen Cyberwar
Motion CPS-CN.
Mesures contre la cyberguerre**

Einreichungsdatum 29.06.10

Date de dépôt 29.06.10

Nationalrat/Conseil national 02.12.10

Antrag der Mehrheit

Annahme der Motion

Antrag der Minderheit

(Müller Geri, Lachenmeier, Lang)

Ablehnung der Motion

Proposition de la majorité

Adopter la motion

Proposition de la minorité

(Müller Geri, Lachenmeier, Lang)

Rejeter la motion

Schlüer Ulrich (V, ZH), für die Kommission: Mit dieser Kommissionsmotion beantragt Ihnen die SiK-NR, die Rechtsgrundlagen zu schaffen, damit der Bundesrat gegen mögliche Formen von Cyberwar oder schädlichen Cyberaktivitäten angemessen vorgehen kann.

Es geht hier nicht um Alarmismus. Wir müssen uns nicht so benehmen, als würden morgen sämtliche Netzwerke, die es auf dieser Welt gibt, lahmgelegt. Aber wir müssen uns mit der Tatsache befassen, dass man mit feindseliger Absicht in Netzwerke eindringen kann und dass solches Eindringen in Netzwerke ausserordentlichen Schaden verursachen kann. Wir sind darüber orientiert worden, dass es im VBS verschiedene sensible Systeme und Netzwerke gibt, die als gegen Cyberbedrohung unzureichend geschützt eingestuft werden. Wir sind im Weiteren darüber orientiert worden, dass der Schutz, der solchen Netzwerken im VBS zukommt, im Durchschnitt besser ist als im zivilen Bereich der Bundesverwaltung. Wir wissen aber selbstverständlich auch, dass Netzwerke der zivilen Bundesverwaltung anfällig sind und Schutzwürdiges, allenfalls Geheimes enthalten, das nicht jedermann zugänglich sein soll.

Von gewissen Systemen sagt man, dass sie besser geschützt seien als andere. Es ist unbefriedigend, dass der Schutz für verschiedene Netzwerke unterschiedlich ist. Es gibt keine einheitliche Strategie, kein einheitliches Vorgehen zum Schutz sämtlicher Netzwerke des Bundes. Es gibt auch keine einheitliche Ausbildung für jene, die im Rahmen dieser Netzwerke arbeiten. Die Sensibilität der Mitarbeiter insgesamt wird deshalb als unterschiedlich, als heterogen bezeichnet, was als zunehmend problematisch eingestuft wird. Wir sind gegenwärtig Zeugen eines Angriffs auf ein Netzwerk der USA, der dramatische Dimensionen annimmt. Betroffen ist nicht ein militärisches Netzwerk, vielmehr ein ziviles Netzwerk; aber der Schaden für die amerikanische Diplomatie kann kaum abgeschätzt werden. Es ist vorzubeugen, dass Gleiches nicht auch uns geschieht.

Auf der anderen Seite ist es auch eine Tatsache, dass die Schweiz von Cyberaktivitäten betroffen ist. Insbesondere im EDA wurde ein Angriff verzeichnet, dessen Dimension man erst allmählich abzuschätzen in der Lage ist; diese ist jedenfalls dramatisch. Noch aber weiss man nicht, woher die Attacke kam, was damit bezweckt wurde, was für Motive dahinterstehen.

In der Diskussion um diese Entwicklung wurde von der Bundesverwaltung übereinstimmend darauf hingewiesen, dass die heutigen Rechtsgrundlagen ungenügend sind oder überhaupt fehlen, damit man angemessen gegen Cyberaktivitäten mit feindlicher Absicht vorgehen kann. Es geht heute nicht um konkretes Vorgehen: Es geht heute nur darum, den Auftrag zur Schaffung von Rechtsgrundlagen zu geben, damit man vorgehen kann! Dazu ist die Kommission der Meinung – gerade auch, nachdem ein Angriff stattgefunden hat –, dass Schritte zu ergreifen sind, bevor wir in schwerwiegendem Ausmass Opfer solcher Aktivitäten werden. Es ist insofern höchste Zeit, dass etwas getan wird.

Wir müssen uns damit befassen, dass es nicht bloss um Hacker geht. Man hat zeitweise im Zusammenhang mit feindseliger oder feindselig motivierter Cyberaktivität regelmässig von Hackern gesprochen, die irgendwo eindringen können. Es geht darum, dass auch in ganze Netzwerke eingedrungen werden kann, dass Netzwerke manipuliert werden können, sodass Selbstverständliches plötzlich nicht mehr funktioniert. Wir haben beispielsweise die Frage aufgeworfen: Ist es möglich, dass jenes ganze System, das die AHV-Zahlungen in diesem Land garantiert, das dafür sorgt, dass alle Rentner Anfang Monat ihre Renten bekommen, angegriffen und lahmgelegt werden kann? Wir bekamen zur Antwort, das sei tatsächlich möglich. Da zeichnen sich Di-

mensionen ab, die zumindest dazu veranlassen müssen, die Bundesverwaltung in die Lage zu versetzen, Schritte vorzusehen, damit gegen Cyberbedrohung vorgegangen werden kann.

Wir unterschätzen nicht, dass sich im Rahmen solcher Cyberbedrohung auch heikle Fragen stellen, weil die Abgrenzung schwierig und die Grenze zwischen Sicherungshandlungen, zwischen Verteidigungshandlungen und aktiven Massnahmen, also Angriffsmassnahmen, fließend ist. Es ist nicht genau abgrenzbar, was wie einzuschätzen ist. Deshalb ist es notwendig, dass die Rechtsgrundlagen jetzt sauber ausgearbeitet werden, dass alle Fragen umfassend diskutiert und Normen festgelegt werden, damit die Landesregierung im Ernstfall, wenn sie darauf angewiesen ist, auf der Grundlage der entsprechenden Kompetenzen, der entsprechenden Kompetenzverteilung und der entsprechenden Aufgabenverteilung agieren kann.

Das ist der Zweck dieser Kommissionsmotion. Ich bitte Sie im Namen der Kommission, sie zu unterstützen. Sie wurde von der SiK im Verhältnis von 20 zu 3 Stimmen bei 1 Enthaltung angenommen.

Voruz Eric (S, VD), pour la commission: Le 29 juin dernier, la Commission de la politique de sécurité a analysé la motion 10.3625 faisant suite à l'information, suivie d'une discussion nourrie, sur un rapport intitulé «Guerre virtuelle. Analyse des dangers et contre-mesures. Armée et sécurité des données».

Le texte de la motion qui vous est soumise demande au Conseil fédéral de créer des bases légales permettant de prendre des mesures de défense active et passive efficaces pour sauvegarder les réseaux de données qui revêtent une grande importance pour la Suisse et pour les installations suisses.

Il faut rappeler que dans un passé récent, trois cas d'attaques ont retenu notre attention. D'abord en Suisse, il y a eu une attaque sur la page Internet du DFAE, qui a conduit à une paralysie de plusieurs semaines. A l'étranger, il y a eu également des attaques massives portées par des hackers russes contre les pays baltes, leurs autorités et leurs infrastructures, produisant une paralysie de ces Etats. De plus, lors de la guerre du Caucase, il y a eu également des attaques informatiques sur le réseau de l'Etat-major de l'armée géorgienne.

Pour revenir à l'attaque sur la page Internet du DFAE, des doutes sont portés sur un Etat étranger qui voulait connaître les rapports que la Suisse entretenait avec l'Iran, étant entendu que notre pays représente les intérêts américains dans ce pays. Il en est de même concernant la Géorgie où des inconnus ont voulu connaître les rapports qu'a la Suisse avec ce pays. Il est évident qu'il s'agissait d'attaques très ciblées et hautement professionnelles.

Ainsi, suite à ces événements, le Conseil fédéral a constitué une «task force» en vue de découvrir les causes et un projet de plan directeur est en élaboration. Des mesures de protection des données ont également été prises pour l'ensemble de l'administration fédérale. Le gouvernement travaille aussi dans le domaine des systèmes militaires à l'amélioration de la sécurité.

Il n'existe pas aujourd'hui dans le système de l'armée de protections efficaces contre les menaces cybernétiques car actuellement, on ne connaît pas encore suffisamment ce type de menaces. Toutefois, il nous a été expliqué que les systèmes militaires bénéficiaient d'un niveau de protection supérieur aux systèmes dits civils. Il est probable toutefois que des systèmes achetés à des tiers auraient pu être manipulés. Il faut donc le savoir et s'en préoccuper pour ne pas payer les conséquences.

Cependant, il y a un paradoxe car dans le rapport sur la sécurité dont le Parlement vient d'être saisi, il est dit «que la Suisse n'envisage pas de protections particulièrement importantes contre des menaces notoires sur l'informatique et le renseignement, mais que le Conseil fédéral se concentre sur l'élaboration d'une stratégie propre à contrer ce type d'attaques».

Cette contradiction ne plaît pas à la commission qui a déposé une motion pour que le Conseil fédéral crée les bases légales permettant les mesures de défense passive mais aussi active pour le cas où cela serait nécessaire. La motion étant formulée en termes généraux, au Conseil fédéral de voir sous quelle forme il entend formuler les bases légales en la matière.

La minorité de la commission n'est pas convaincue que de telles bases légales puissent garantir la sécurité informatique de l'administration. Elle pense que cette proposition donne l'air de faire quelque chose sans pour autant connaître les buts, les principes. La minorité pense également qu'une protection élevée est importante et elle part du principe que la Suisse fait le maximum et qu'il faudrait d'abord investir dans l'information, à commencer chez les enfants, pour qu'ils comprennent qu'Internet et les téléphones mobiles ne sont pas sécurisés. La minorité pense aussi que si l'on veut vraiment un dispositif sécurisé, il faudrait alors quitter le domaine informatique.

Enfin, tant la majorité que la minorité estiment qu'il manque dans le rapport présenté en commission la reconnaissance de moyens de désinformation car c'est l'un des instruments de la guerre cybernétique. De fausses informations sur les déplacements de troupes ont transité et, du coup, de fausses mesures militaires ont été prises. Ce fut le cas dans la guerre d'Irak et également dans le conflit russo-géorgien.

Pour conclure, un postulat Recordon a été déposé au Conseil des Etats qui soulève la même problématique et demande que des mesures soient prises.

En définitive, convaincue que nous devons prendre au sérieux les dangers d'attaques de systèmes informatiques tant civils que militaires, la commission vous propose, par 20 voix contre 3 et 1 abstention, d'approuver la motion 10.3625, «Mesures contre la cyberguerre».

Müller Geri (G, AG): Es sind erstaunlich wenige Leute im Saal, gemessen an der «Gefährlichkeit» des Themas, das wir hier zu behandeln haben. Und es ist auch erstaunlich, dass wir nur vom «rapporteur de langue française» gehört haben, was die Minderheit in der Kommission gesagt hat. Herr Ueli Schlüer hat vor Schreck vollkommen vergessen, die ganze Kommission zu vertreten.

Ueli Schlüer hat Alarmismus verneint. Es ist aber von Alarmismus gesprochen worden angesichts der Vielzahl der Vorstösse, die in diesem Bereich gemacht worden sind, und angesichts des Vorschlags, der jetzt auf dem Tisch liegt. Wir unterliegen hier einem grossen Alarmismus. Die SVP produziert ja ein Gesetz nach dem andern. Das ist bekannt. Wir verabschieden auch immer wieder solche Gesetze. Und jetzt will sie ein Gesetz auf Vorrat schaffen. Sie will dem Bundesrat jetzt schon sagen, er solle sich gesetzliche Möglichkeiten schaffen, um dem Cyberwar entgegenzutreten zu können.

Ich erinnere Sie, wir haben diese Diskussion schon einmal gehabt, sie liegt ein paar Jahrzehnte zurück: Das Produkt war am Schluss die Fichenaftäre. Ausnahmsweise, so müsste man sagen, hat der Bundesrat bis jetzt die richtigen Sachen gemacht. Er hat eine Analyse vorgenommen, und zwar nicht nur über das VBS, sondern über alle Departemente hinweg, und er hat diese Analyse auch mit ausländischen Stellen zusammen gemacht. Man darf wahrscheinlich sagen, dass man heute beim jetzigen Stand des Irrtums wahrscheinlich am besten weiss, was zu tun ist. Der Bundesrat hat der Analyse auch Vorschläge folgen lassen, und über diese Vorschläge haben wir in der Kommission diskutiert.

Jetzt geht es darum, Vorschlag für Vorschlag genau anzuschauen, um zu prüfen, ob er implementierbar ist. Was meines Erachtens aber nicht möglich ist, ist der Umstand, Vorschläge zu machen, die die persönlichen Freiheiten der Bürgerinnen und Bürger einschränken. Gerade dahin aber geht unsere Befürchtung; wir befürchten, dass wir irgendwelche Gesetze machen, dass sämtliche Laptops, die jetzt hier aufgeklappt sind, plötzlich in dem Sinn offen wären, dass man von überall her auf sie zugreifen und sie kontrollieren könnte. Die Absicht, eine gesetzliche Vorlage zu machen, geht in diese Richtung. Wir aber möchten zuerst

Massnahmen auf dem Tisch haben, die uns aufzeigen, was man effektiv machen müsste. Sie sehen, dies ist ein Angriff auf den liberalen Staat, der Gesetze erst dann macht, wenn er keine anderen Möglichkeiten mehr hat. Aber wir sind jetzt erst im Aufbau der Abwehr oder der Idee, wie man gegen Cyberwar kämpfen müsste. Die Grünen haben nicht gesagt, sie seien gegen Massnahmen, sondern sie haben klar gesagt, sie seien gegen das Produzieren von Gesetzen, ohne zuerst zu schauen, wie es weitergeht. Wir sind also gegen Gesetze auf Vorrat.

Was können wir aber heute schon als Konklusion daraus ziehen? Vorhin wurde Wikileaks genannt. Wikileaks ist in diesem Zusammenhang vielleicht ein bisschen ein falsches Beispiel. Es wurden dort Dinge öffentlich gemacht, die in der internationalen Diplomatie schon lange öffentlich waren, aber einfach nicht auf diese Art und Weise schriftlich festgelegt waren. Im Übrigen hat die Schweiz dabei gut abgeschnitten. Unsere Aussenministerin hat von den Amerikanern ein hervorragendes Zeugnis erhalten; immerhin hat Wikileaks auch Vorteile.

Aber im Ernst: Wir werden mit einem Gesetz nie und nimmer verhindern können, dass Leute, die die entsprechende Intelligenz und die entsprechenden Fähigkeiten haben, in die Systeme einbrechen. Was wollen Sie mit diesem Gesetz machen? Wollen Sie dann wieder irgendwelche Leute ausschaffen, die in ein System eingebrochen sind? Solche Überlegungen werden der Sache nicht gerecht. Wir müssen uns überlegen, wie wir die Systeme schützen könnten. Die Tatsache ist die, dass wir heute quasi von Kindsbeinen an das Gefühl haben, dass Elektronik absolut kein Problem ist, sei es beim Umgang mit dem Handy oder mit Computer oder Internet. Dort müsste man ansetzen, dort bräuchten wir wahrscheinlich auch sehr viel an Finanzen, um unsere Jugendlichen zu befähigen, mit diesen Medien umzugehen. Da steht uns ausgerechnet wieder eine Partei im Weg, die praktisch in allen Kantonen versucht, Bildungsmassnahmen zu verhindern, die dort ergriffen werden sollen. Diese Partei findet, es müsse im Bildungsbereich gespart werden.

Was müssten wir sonst noch machen? Alle Systeme, die es heute auf Bundes-, Kantons- und Gemeindeebene gibt, sind elektronisch unterstützt. Ich habe es bei der vorherigen Vorlage gesagt: Sie können ohne Elektronik heute nicht einmal mehr ein Auto starten. Elektronik ist überall, und wir denken nur noch an diese Elektronik. Das heisst, dass wir einen anderen Weg gehen müssten, wo die Mechanik wieder berücksichtigt würde. Das gäbe uns bestimmt mehr Sicherheit, als wenn übers Ganze irgendein Gesetz gemacht würde, in dem stünde, was verboten sein sollte.

Zusammenfassend bitte ich Sie, den Prozess, den der Bundesrat über alle Departemente hinweg eingeleitet hat, zu unterstützen – er wird dies mit oder ohne diese Motion weiter tun –, keine Gesetze auf Vorrat zu schaffen und in dem Sinne das abzulehnen, was hier vorgeschlagen wird.

Maurer Ueli, Bundesrat: Der Bundesrat beschäftigt sich seit Längerem mit dem Thema dieser Motion und ist daher auch bereit, sie entgegenzunehmen. Einige Bemerkungen dazu: Es geht zunächst einmal darum zu klären, was man unter Cyberwar überhaupt versteht. Wir verstehen darunter nicht die allgemeine Kriminalität im Internet; dafür ist die Fedpol zuständig. Da haben wir, so meine ich, recht gute Mittel und bekämpfen diese Kriminalität auch. Pornografie, Missbrauch von Kindern im Internet, Missbrauch in anderen Bereichen – das sind Dinge, mit denen wir uns seit Längerem beschäftigen, dafür sind wir recht gut gerüstet. Cyberwar ist ein neuer Begriff für Angriffe im System, und zwar nicht unbedingt von einzelnen Hackern, sondern von Organisationen, die versuchen, ganze Systeme zu stören. Herr Schlüer hat das AHV-Auszahlungssystem angesprochen. Das wäre als Ziel von Angriffen durchaus denkbar. Angriffe auf Werke, auf die Stromversorgung, Abhörattacken, wie wir sie beim EDA hatten – das sind neue Dimensionen. In diese Richtung geht die Motion, die Ihre SiK unterbreitet. Der Bundesrat beschäftigt sich damit. Er wird an einer der nächsten Sitzungen eine

Aussprache darüber führen und Massnahmen an die Hand nehmen, um konzeptionell an das Problem heranzugehen.

Es stellen sich drei grundsätzliche Fragen. Erstens geht es um die Strategie: Was will die Schweiz, was will der Staat hier erreichen? Sind wir defensiv tätig? Defensiv nur für die Bundesverwaltung? Wieweit sind die Kantone einzubeziehen? Wieweit sind Werke, ist die Versorgung einzubeziehen? Wieweit ist mit der Wirtschaft zusammenzuarbeiten? Wo darf die Schweiz allenfalls angreifen, wenn das legal überhaupt geht? Hier besteht keine Gesetzesgrundlage, das wurde angesprochen. Das ist also die ganze Frage, welche Strategie die Schweiz in diesem Bereich mittel- und längerfristig verfolgt. Das muss erarbeitet werden, das muss abgezwungen werden, da müssen Vergleiche angestellt werden. Daraus ergibt sich dann die zweite Frage: Was ist technisch vorzukehren, damit wir in diesem Bereich operativ werden können?

Und als Drittes stellt sich die operative Frage: Wer betreibt das?

Es gibt also drei Ebenen: Welche Strategie wollen wir? Was braucht es technisch dazu? Wer ist operativ tätig? Darüber führt der Bundesrat eine Aussprache. Er wird Massnahmen dazu treffen. Wir sprechen davon, dass wir einen Beauftragten einsetzen, denn in der Verwaltung ist hier etwas und dort etwas organisch gewachsen, und das muss zusammengeführt werden. Die Kräfte müssen gebündelt werden. Sollte daraus eine Gesetzesänderung entstehen oder was auch immer, haben Sie selbstverständlich wieder die Möglichkeit mitzusprechen.

Die Fragen, die Sie mit dieser Motion ansprechen, beschäftigen auch den Bundesrat. Wir gehen davon aus, dass es doch einige Zeit braucht, um hier Klarheit zu schaffen. Vieles ist diffus, vieles erfährt man erst, wenn man Opfer einer Attacke wird, anderes kann man erahnen, aber eine wirkliche Übersicht besteht heute nicht, weder bei uns noch – so würde ich jetzt einmal sagen – irgendwo sonst. Vieles ist noch im grauen Bereich. Das möchten wir aufklären und analysieren.

Vielleicht gestatten Sie mir noch eine Bemerkung: Herr Geri Müller hat gesagt, der Bundesrat hätte ausnahmsweise das Richtige gemacht. Dem würde ich widersprechen: Der Bundesrat macht immer das Richtige, ausnahmsweise kann einmal ein Schuss danebengehen.

Wir beantragen Ihnen also, die Motion anzunehmen.

Müller Geri (G, AG): Mit dem letzten Satz kann ich gut leben, aber dennoch eine Frage: Sie haben gesagt, der Bundesrat habe sich ausführlich auch mit dieser Motion beschäftigt und damit auch mit den gesetzlichen Grundlagen. In welche Richtung geht denn der Bundesrat? Geht es darum, die Leute wieder mehr zu überwachen, beispielsweise den ganzen Internetverkehr, oder geht es darum, gesetzliche Grundlagen zu schaffen, um jemanden zu bestrafen? In welche Richtung geht Ihre Tendenz?

Maurer Ueli, Bundesrat: Ich glaube, im Bereich der Internetkriminalität bestehen die gesetzlichen Grundlagen, da gibt es das Strafgesetzbuch. Da besteht meiner Meinung nach kaum Handlungsbedarf. Die Frage, die Sie mit Ihrer Motion aufwerfen und die der Bundesrat prüfen wird, ist eigentlich die folgende: Welche Strategie verfolgen wir hinsichtlich Cyberwar? Cyberwar bedeutet ja Krieg, und in einem Krieg muss man allenfalls auch angreifen. Wir verwenden im Moment eher den Begriff Cyberdefence, also Abwehr von Angriffen. Dazu bräuchte es kaum neue gesetzliche Grundlagen, aber wir werden das noch prüfen. Der Bundesrat hat sich noch keine Meinung gebildet; er wird jetzt dann eine Arbeitsgruppe einsetzen, einen Delegierten. Wir sind der Meinung, dass wir in den nächsten ein, zwei Jahren zusammentragen können, was vorhanden ist und was es braucht. Wir werden Ihnen dies in Erfüllung der Motion unterbreiten und dann in einer Vorlage, sofern wir das als notwendig erachten. Es sind demnach keine Vorentscheide gefällt. Wir sind daran, Fakten zusammenzutragen, um etwas Licht in die Grauzonen zu bringen.

Schlüer Ulrich (V, ZH), für die Kommission: Wir sind eigentlich der Auffassung, dass sich der Gegensatz in etwas seltsamem Raum bewegt: Die Kommissionsmehrheit und die Kommissionsminderheit sind offensichtlich gleichermassen der Meinung, dass im Bereich Cyberwar, Cyberaktivitäten nicht nur sehr vieles geschieht, sondern sehr vieles auch unkontrolliert geschieht. Wir meinen auch, dass vieles, was da geschieht, heikle Bereiche betrifft. Eigentlich ist es doch unser Grundsatz, dass sich staatliches Handeln im Rahmen der Gesetzlichkeit bewegen soll. Nichts anderes als das soll der Bundesrat aufgrund der SiK-Motion im Zusammenhang mit dem, was sich abspielt, jetzt prüfen.

Welchen Vorteil der Verzicht auf solche Prüfung bezüglich zu schaffender gesetzlicher Festlegungen bringen soll, ist wirklich schwer vorzusagen. Wenn der Bundesrat in dieser Hinsicht einmal reagieren müsste, dann müsste er das mehr oder weniger anarchisch tun, ohne dass Klarheit bestünde, wer welche Kompetenzen dazu besitzt.

Ich glaube, der Vorstoss ist gut fundiert. Das Interesse daran, dass für staatliches Handeln ein gesetzlicher Rahmen bestehen soll, ist breit abgestützt. In diesem Sinn bitte ich Sie, der Mehrheit zu folgen.

Voruz Eric (S, VD), pour la commission: Je pense qu'il faut effectivement faire confiance au Conseil fédéral dans le cadre de cette étude.

Nous avons examiné cette motion le 29 juin dernier et plusieurs attaques se sont produites depuis, pas seulement contre l'administration fédérale, mais également contre les partis politiques. Pour cette raison, je crois que l'examen que va faire le Conseil fédéral nous permettra de voir comment il faudra procéder par la suite. Je pense que cette motion peut amener de l'eau au moulin du Conseil fédéral qui, le moment venu, nous dira s'il faut une base légale ou pas. Pour l'heure, nous sommes persuadés qu'une base légale est nécessaire.

Abstimmung – Vote

(namentlich – nominatif: Beilage – Annexe 10.3625/4742)

Für Annahme der Motion ... 104 Stimmen

Dagegen ... 25 Stimmen

09.478

**Parlamentarische Initiative
Hurter Thomas.
Gewissensprüfung
bei der Rekrutierung
für den Zivildienst**

**Initiative parlementaire
Hurter Thomas.
Service civil.
Réintroduire l'examen
du conflit de conscience**

Vorprüfung – Examen préalable

Einreichungsdatum 14.09.09

Date de dépôt 14.09.09

Bericht SiK-NR 11.10.10

Rapport CPS-CN 11.10.10

Nationalrat/Conseil national 02.12.10 (Vorprüfung – Examen préalable)

10.481

**Parlamentarische Initiative
SiK-NR.
Revision
des Zivildienstgesetzes.
Erste Phase**

**Initiative parlementaire
CPS-CN.
Révision de la loi
sur le service civil.
Première phase**

Vorprüfung – Examen préalable

Einreichungsdatum 24.08.10

Date de dépôt 24.08.10

Bericht SiK-NR 11.10.10

Rapport CPS-CN 11.10.10

Nationalrat/Conseil national 02.12.10 (Vorprüfung – Examen préalable)

09.478

Antrag der Mehrheit

Der Initiative Folge geben

Antrag der Minderheit

(Lachenmeier, Allemann, Birrer-Heimo, Chopard, Galladé, Streiff, Lang, Müller Geri, Voruz)

Der Initiative keine Folge geben

Proposition de la majorité

Donner suite à l'initiative

Proposition de la minorité

(Lachenmeier, Allemann, Birrer-Heimo, Chopard, Galladé, Streiff, Lang, Müller Geri, Voruz)

Ne pas donner suite à l'initiative

10.481

Antrag der Mehrheit

Der Initiative Folge geben

Antrag der Minderheit

(Lachenmeier, Allemann, Birrer-Heimo, Chopard, Galladé, Lang, Müller Geri, Voruz)

Der Initiative keine Folge geben