



17.3507

**Motion Dittli Josef.
Ein Cyberdefence-Kommando
mit Cybertruppen
für die Schweizer Armee****Motion Dittli Josef.
Création d'un commandement
de cyberdéfense
dans l'armée suisse**

CHRONOLOGIE

STÄNDERAT/CONSEIL DES ETATS 25.09.17

Ordnungsantrag Hêche

Zuweisung der Motion 17.3507 an die zuständige Kommission zur Vorprüfung.

Motion d'ordre Hêche

Transmettre la motion 17.3507 à la commission compétente pour examen préalable.

Hêche Claude (S, JU): Je pars avec un handicap certain, puisque je n'ai pas réussi à convaincre l'auteur de la motion de suivre ma proposition. Je me permets tout de même de rappeler que, la semaine dernière, nous avons accepté une motion ayant pour but la création d'un centre de compétence fédéral pour la cybersécurité. En acceptant cette motion déposée par Monsieur Joachim Eder, notre conseil a poursuivi l'objectif de renforcer les capacités de la Confédération de résister à des cyberattaques. Tous les intervenants – sans exception – qui ont soutenu la motion ont insisté sur la question de la coordination. On ne veut pas une situation particulière, mais un centre de compétence au service des sept départements, auxquels j'ajouterai la Chancellerie fédérale. Le Conseil fédéral mentionne, dans son avis sur la motion Dittli, que "le DDPS a élaboré, dans le cadre de ses compétences et moyens, un plan d'action pour la cyberdéfense, dont il a informé le Conseil fédéral le 12 avril 2017". Si personne ne conteste que l'armée doive être dotée de moyens, de compétences et de capacités – je pense notamment à des experts adéquats –, le plan d'action du DDPS que je viens de citer doit être intégré dans une vision globale et coordonnée. C'est une question d'efficacité, de ressources, de compétences et, surtout, de coordination qui nous est posée.

La transmission de la motion à la commission, – je sou mets cette idée à votre appréciation – permettrait en outre à Monsieur le conseiller fédéral Parmelin de préciser les contours de son plan d'action, et ainsi de clarifier les situations actuelle et future en matière de cybersécurité.

Pour ces quelques raisons, je vous invite à accepter la transmission de la motion à la commission compétente.

AB 2017 S 701 / BO 2017 E 701

Dittli Josef (RL, UR): Ich bitte Sie, den Ordnungsantrag abzulehnen.

Ich muss Ihnen sagen: Wenn dieser Ordnungsantrag angenommen wird, weiss ich gar nicht, was wir in der Sicherheitspolitischen Kommission noch vorprüfen sollen, denn bis auf eine Ausnahme ist der Bundesrat mit den Forderungen grosso modo einverstanden. Er schreibt ja selber in seiner Antwort, dass die Forderungen der Motion mit dem, was er vorhat, zum grössten Teil erfüllt werden. Wenn also der Bundesrat schon selber sagt, dass er mit den meisten der Forderungen einverstanden ist, weiss ich nicht, was der Diskussionsbedarf in der Kommission noch sein soll.

Es gibt eine Ausnahme: Diese Ausnahme ist die Cyber-RS. Diese Forderung trägt der Bundesrat nicht mit. Er schreibt, dass aus Sicht des Bundesrates eine Cyber-RS "nicht zweckdienlich" sei, "da die Ausbildung der benötigten Spezialistinnen und Spezialisten mit den traditionellen Ausbildungsmodellen der Armee nicht zu





realisieren ist". Nicht nur, aber vor allem aus diesen Gründen lehnt der Bundesrat die Motion in der vorliegenden Form ab.

Dass sich der Bundesrat aber offenbar schon Gedanken gemacht hat, wie man die Rekrutierung und Ausbildung vorantreiben kann, und dass er offenbar eine Lösung hat, zeigt sich im allerletzten Satz seiner Antwort. Der Bundesrat schreibt nämlich in seiner Antwort auf die Motion, und das ist doch eher unüblich: "Wenn der erstbehandelnde Rat die Motion annimmt, hat das VBS die Möglichkeit, dem Zweitrat einen Änderungsvorschlag zu unterbreiten." Also gehe ich jetzt schon davon aus, dass der Sicherheitspolitischen Kommission des Nationalrates vom Departement her aufgezeigt wird, wie der Bundesrat die Ausbildung und Rekrutierung vornehmen will, wenn die Motion angenommen wird.

Vor diesem Hintergrund sehe ich wirklich keinen grossen Diskussionsbedarf in der Sicherheitspolitischen Kommission. Eigentlich ist diese Motion ja auch im Gesamtrahmen, also in Zusammenhang mit der Motion Eder 17.3508, "Schaffung eines Cyber-Security-Kompetenzzentrums auf Stufe Bund", die wir letzte Woche behandelt haben, zu verstehen. Jene Motion fordert, übergeordnet über alle Cyber-Security-Bereiche, ein Kompetenzzentrum, und meine Motion fokussiert in Ergänzung dazu speziell auf die Armee. Hier ist eine klare Abtrennung gegeben. Es liegt keine Vermischung zwischen der Motion Eder 17.3508 und meiner Motion vor; das möchte ich Herrn Hêche aufgrund der Bedenken, die er aufgeworfen hat, noch sagen.

Wir sollten jetzt unbedingt ein Zeichen setzen, dass der Ständerat auch bei der Armee der Auffassung ist, dass vorwärtsgemacht werden soll. Der Bundesrat will das ja auch. Wir sollten also heute entscheiden. Aus meiner Sicht steht dem nichts entgegen.

Ich bitte Sie also, den Ordnungsantrag Hêche abzulehnen.

Abstimmung – Vote

Für den Ordnungsantrag Hêche ... 10 Stimmen

Dagegen ... 28 Stimmen

(2 Enthaltungen)

Präsident (Bischofberger Ivo, Präsident): Wir kommen damit zur materiellen Behandlung des Vorstosses. Der Bundesrat beantragt die Ablehnung der Motion.

Dittli Josef (RL, UR): Wie in der Motion dargelegt, sind seitens der Armee die Mittel nicht in ausreichendem Masse vorhanden, um den aktuellen und zukünftigen Bedrohungen angemessen begegnen zu können. Wir haben zwar alle realisiert, dass sich das VBS intensiv damit auseinandersetzt, welches der Beitrag der Armee zur Cyberdefence sein soll. Was das VBS und der Bundesrat aber wirklich und konkret wollen, ist nach wie vor nicht klar; insbesondere ist unklar, wie die Stärken der Miliz einbezogen werden sollen.

In seiner Antwort schreibt der Bundesrat, dass das VBS im Rahmen seiner Kompetenzen und Mittel einen Aktionsplan Cyberdefence ausgearbeitet hat. Die meisten Forderungen seien darin abgedeckt. Der Bundesrat sei am 12. April dieses Jahres über diesen Aktionsplan informiert worden. Das ist sicher in Ordnung, aber weder das Parlament noch die Öffentlichkeit haben bisher nähere Kenntnisse über die Inhalte dieses Aktionsplanes. Selbst in der Sicherheitspolitischen Kommission wurde lediglich darüber orientiert, dass das VBS einen Aktionsplan Cyberdefence beschlossen hat, der bis 2020 umgesetzt werden solle, ohne aber auf die Inhalte einzugehen.

Es freut mich also, in der Antwort des Bundesrates nun feststellen zu können, dass die Motion in den meisten Punkten auf offene Ohren stösst. Bis auf eine Ausnahme ist der Bundesrat nämlich mit den Forderungen einverstanden. So sollen unter Einbezug der Miliz tatsächlich Cybertruppen in namhafter Stärke aufgebaut werden – das ist ja eigentlich die Hauptforderung. Es soll auch ein Cyberdefence-Kommando in einer noch zu klärenden Form geschaffen werden. Was die in der Motion angeführten Aufgaben betrifft, sollen grundsätzlich alle Forderungen abgedeckt werden können, nämlich vom Schutz der eigenen Systeme über die Befähigung zur Verteidigung des Cyberraumes bis hin zur subsidiären Unterstützung. Auf offene Ohren stösst die Motion auch, was die geforderte Zusammenarbeit mit den Hochschulen betrifft.

Nicht deckungsgleich ist der Bundesrat mit der Forderung nach einer Cyber-RS. Ich habe dies vorhin bereits erläutert, deshalb halte ich mich hier kurz. Ich bin aber schon etwas erstaunt, dass die Cyber-RS auf so massiven Widerstand stösst, denn ich habe ja in der Motion gar nicht gefordert, dass nur traditionelle Ausbildungsmodelle infrage kommen sollen. Da darf es auch andere Rekrutierungs- und Ausbildungsgefässe geben. Erwähnen möchte ich auch noch, dass die Medien im März dieses Jahres darüber berichtet haben, Herr Bundesrat Parmelin habe in einem Interview in der Zeitung "Schweiz am Wochenende" gesagt, dass er sich eine Art Cyber-RS gut vorstellen könne – das kann ich mir natürlich auch vorstellen. Was ihre Ausgestaltung betrifft, gibt es selbstverständlich diverse Möglichkeiten. Offenbar ist auch der Chef der Armee der Auffassung, dass



eine Cyber-RS nur noch eine Frage der Zeit ist. So hat er am Gewerbeabend der Thuner KMU Anfang September, also vor drei Wochen, in einem Referat gesagt: "Ein weiterer Schwerpunkt ist in Zukunft das Thema Cyber. Server und Rechenzentren von Armee und Bund müssen vor Angriffen und Attacken geschützt werden. Wir haben zwar eine Kompanie mit Fachleuten aus dem Milizdienst, aber noch keine entsprechende RS." Wie auch immer, ich kenne die Überlegungen nicht, wie das VBS die Rekrutierung und Ausbildung insbesondere der Miliz-Cybertruppen zu realisieren gedenkt. Es sollte aber immerhin möglich sein, interessierte und geeignete Stellungspflichtige frühzeitig zu erfassen und ihnen ein RS-Modul Cyber anzubieten. Dazu braucht es kein eigenes Schulkommando, man könnte beispielsweise im Schulkommando der Führungsunterstützungsbasis der Armee pro RS eine Klasse Cyberspezialisten führen.

Der Bundesrat empfiehlt also hauptsächlich wegen der Forderung nach der Cyber-RS, die Motion in der heutigen Form abzulehnen. Mit allen anderen Punkten ist er grossmehrheitlich einverstanden. Das andere habe ich bereits erläutert.

Der Bundesrat hat am Schluss seiner Stellungnahme folgende Formulierung angebracht: "Wenn der erstbehandelnde Rat die Motion annimmt, hat das VBS die Möglichkeit, dem Zweitrat einen Änderungsvorschlag zu unterbreiten." Das ist meines Erachtens ein Steilpass für uns. Wir sollten diese Chance nutzen und dem VBS die Gelegenheit geben, dann im Nationalrat, in der SiK des Nationalrates, dieses Thema einzubringen und allenfalls noch andere Punkte zu präzisieren. Damit wäre der Sache dann sehr gedient. Wir sollten diesen Steilpass also der Sache zuliebe aufnehmen, denn im Cyberbereich hat auch die Armee wirklich Nachholbedarf.

Ich empfehle Ihnen, die Motion anzunehmen.

Ettlin Erich (C, OW): Kollege Dittli hat das Wichtigste ausgeführt, weshalb ich nur punktuell ergänzen möchte. Auch mir ist in der Stellungnahme des Bundesrates aufgefallen, dass eine Cyber-RS offenbar nicht möglich sei. Dies wird damit begründet, dass eine Cyber-RS mit den traditionellen Ausbildungsmodellen der Armee nicht zu realisieren sei. Das ist schon eine spezielle Formulierung. Wenn man das nämlich weiterdenkt, so bedeutet das, dass man beim Auftauchen

AB 2017 S 702 / BO 2017 E 702

von neuen Waffen, wie das damals auch beim Flugzeug einmal der Fall gewesen ist, hätte sagen müssen, dass sich mit den traditionellen Ausbildungsmodellen keine entsprechende RS realisieren lasse, obschon die Gefahr bestand. So ist es auch im Cyberbereich: Die Gefahr ist da. Gerade heute habe ich gelesen, dass laut Experten rund 3000 Cyberangriffe monatlich auf die Schweiz einprasseln. Die Gefahr ist also real. Es handelt sich um eine andere Gefahr, um andere Waffen. Daher muss es einfach möglich sein, Ausbildungsmodelle zu schaffen.

Ergänzend möchte ich sagen, dass das ja auch eine Chance wäre. Wir haben eine Diskussion über Zivildienst und Militärdienst und darüber, dass der Militärdienst zu wenig attraktiv sei, sodass zu viele in den Zivildienst gehen. Hier könnte man doch eine Chance wahrnehmen, Leute, die potenziell zum Zivildienst neigen, für die Cyber-RS zu motivieren. Dann hätte man ein Zwischending, es gäbe zwischen dem Militärdienst in den üblichen Waffengattungen und dem Zivildienst mit Jobs im sozialen Bereich auch noch die Cybereinheit. Da würden sich, glaube ich, auch militärdienstuntaugliche Leute finden, die ja einen grösseren Anteil der Stellungspflichtigen ausmachen. Da könnte man vielleicht sagen, dass Leute, die heute nicht tauglich sind und auch keinen Zivildienst leisten, gewonnen werden könnten.

Es braucht talentierte Köpfe, die unbestrittenermassen vorhanden sind. Es braucht eine enge Zusammenarbeit mit den Hochschulen, was x-mal gesagt worden ist. Wir geben uns hier die Chance, Leute für die Armee zu gewinnen, indem wir, wie es Kollege Dittli gesagt hat, diese neue Einheit bilden und die Leute motivieren.

Deshalb empfehle auch ich Ihnen, diese Motion anzunehmen.

Parmelin Guy, conseiller fédéral: Jusqu'à présent, on pouvait penser que l'avis du Conseil fédéral en réponse à la motion Dittli signifiait une non-entrée en matière. Ce n'est pas du tout le cas, je crois que vous l'avez bien compris, Monsieur le conseiller aux Etats. Dans les faits, tous les services concernés approuvent l'idée générale de la motion. Il y a cependant deux éléments que le département ne souhaite pas reprendre in extenso, et c'est la raison pour laquelle le Conseil fédéral ne peut pas approuver cette motion dans sa teneur actuelle. La procédure étant ce qu'elle est, on ne peut pas modifier le texte maintenant. C'est pour cette raison que je suis obligé de combattre cette motion.

Tout d'abord, je parle de l'école de recrues et de l'organisation de bataillons de cyberdéfense composés de soldats de milice. Vous avez dit malicieusement, Monsieur Dittli, que j'avais dit dans une interview que je pouvais imaginer "eine Art Cyber-RS". Heureusement que vous avez dit "eine Art", "une sorte": cela laisse une



large place à l'interprétation.

Nous avons l'intention, c'est certain, de former des spécialistes pour l'armée de milice et nous souhaitons aussi que la formation qu'ils auront reçue leur soit utile dans leur carrière professionnelle, utile non seulement pour l'armée, mais aussi pour la société civile. Mais le modèle strict tel qu'il existe aujourd'hui, le modèle traditionnel, ne permet pas d'apprendre les métiers très pointus, très précis, très spécialisés dont nous avons besoin. Il s'agira donc pour nous de sélectionner des hommes et des femmes qui disposent déjà d'un niveau professionnel donné, sanctionné de préférence par un diplôme de la formation professionnelle initiale – un CFC – ou bien par un brevet de la formation professionnelle supérieure, voire par un diplôme universitaire du type bachelor, master ou doctorat. Il faudra construire sur des compétences qui sont déjà établies. Je pense que ce sera très important. Peut-être que nous soutiendrons aussi certains de ces développements. En tout cas, nous agissons comme nous le faisons déjà maintenant avec d'autres talents. Vous savez qu'il y a le sport, la musique, les langues même. C'est dans ce sens que nous travaillerons, c'est évident.

Pour cela, nous avons déjà initié le dialogue avec ICT Formation professionnelle – ICT Berufsbildung –, le Secrétariat d'Etat à la formation, à la recherche et à l'innovation, les hautes écoles, les universités et les écoles polytechniques. Nous discutons aussi avec les opérateurs d'infrastructures sensibles, qui ont les mêmes soucis de formation professionnelle en matière de défense. Un concept va d'ailleurs m'être présenté d'ici à la fin du mois d'octobre prochain déjà.

S'agissant ensuite des cyberbataillons, nous avons bien sûr, c'est évident, l'intention d'engager la milice. Elle est indispensable si on veut disposer de suffisamment de personnel. Nous devons en effet aussi pouvoir nous inscrire dans la durée, nous devons pouvoir alimenter les nombreuses positions qui vont se créer ces toutes prochaines années, et nous devons disposer d'une grande palette de compétences. Mais étant donné la sensibilité des différentes tâches, nous ne pouvons pas simplement – vous me passerez cette expression un petit peu osée – lâcher dans la nature des personnes sans contrôle étroit par des professionnels. Il est déjà aussi prévu que des militaires de milice soient partie du plan d'action que j'ai esquissé dans mes différentes interventions précédentes devant le Parlement. Ces personnes devront renforcer les effectifs et les structures existantes. Elles ne seront pas engagées comme l'infanterie ou comme les troupes mécanisées. Et puis, comme le Parlement l'a souhaité dans le cadre du développement de l'armée, nous avons initié ce qu'on appelle le projet "Commandement d'appui", "Unterstützungskommando". C'est dans ce cadre que nous souhaitons éprouver puis développer l'idée d'un cybercommandement spécifique. La structure actuelle de la Base d'aide au commandement dispose déjà d'une division qui s'appelle Centre des opérations électroniques. Cette division est responsable des questions liées à la guerre électronique dite classique, mais aussi des opérations cyber avec lesquelles les synergies sont toujours plus étroites. Ce centre est dans les faits déjà une partie conséquente de ce que d'autres armées nomment cybercommandement.

Les médias ont beaucoup parlé, ces derniers temps, du "Kommando Cyber- und Informationsraum" récemment créé en Allemagne, en le citant comme exemple à suivre. En Suisse, nous nous appuyons sur la Base d'aide au commandement, qui a été créée dans le cadre d'Armée XXI, et qui repose sur une structure professionnelle et de milice.

Nous estimons être sur le bon chemin. Nous poursuivons les mêmes objectifs que la motion. Toutefois, pour que nous puissions recommander son adoption, il suffirait de modifier la fin de son premier paragraphe en insérant une disposition qui dirait: "Pour l'instruction des forces cyber requises, des cursus adaptés vont être mis en place. La création d'un nouveau commandement cyber sera testée, réalisée dans le cadre de la création du commandement d'appui prévu par le développement de l'armée et comprendra au moins les capacités suivantes: ..." Les éléments nécessaires seraient énumérés ensuite.

Si votre conseil devait approuver la motion, c'est dans ce sens que nous proposerions au deuxième conseil d'adapter le texte proposé. Si la motion devait être adaptée telle quelle par les deux conseils, cela pourrait poser quelques difficultés vu la rigidité du passage en question. C'est pour cette raison formelle, et non pas par volonté de ne pas entrer en matière sur cette problématique dont il reconnaît l'existence, que le Conseil fédéral vous propose de rejeter la motion dans sa teneur actuelle.

Abstimmung – Vote

Für Annahme der Motion ... 34 Stimmen

Dagegen ... 7 Stimmen

(0 Enthaltungen)

AB 2017 S 703 / BO 2017 E 703

