16.3561

Interpellation Dittli Josef. Erklärung der Nato. Hackerangriffe können einen Bündnisfall auslösen

Interpellation Dittli Josef. Elargissement de la clause de défense mutuelle de l'OTAN aux cyberattaques. Et la Suisse?

CHRONOLOGIE

STÄNDERAT/CONSEIL DES ETATS 21.09.16

Le président (Comte Raphaël, président): L'interpellateur s'est déclaré partiellement satisfait de la réponse écrite du Conseil fédéral. Il demande l'ouverture de la discussion. – Ainsi décidé.

Dittli Josef (RL, UR): Auch hier danke ich dem Bundesrat für die sorgfältige und ausführliche Beantwortung der Fragen. Mit dem Nato-Gipfel dieses Jahr in Warschau wurde im Bereich der Verteidigungsdoktrin Geschichte geschrieben – und niemand hat es bemerkt, zumindest in der Öffentlichkeit nicht. Offenbar interessierte es hierzulande auch niemanden. Selbst unsere Medien haben kaum darüber berichtet.
Wovon spreche ich? Bisher kannten moderne Streitkräfte grosser Nationen drei Operationsräume: Luft, Boden, Meer. Nun hat die Nato den Cyberspace zu einem vierten, eigenständigen Operationsgebiet erklärt. Das ist eigentlich

revolutionär. Nato-Länder und Nato werden nun also einen neuen Operationsraum ausgestalten mit allem, was dazugehört: mit einer eigenen Doktrin, mit einer eigenen Strategie, eigenen Mitteln wie Cybertruppen, Nachrichtendiensten, Infrastruktur usw. Es ist spürbar: Da wird etwas gehen – aber nicht nur dies, sondern noch viel mehr.
Die Nato-Verteidigungsminister haben an derselben Konferenz beschlossen, dass Angriffe auf Datennetze gleich zu behandeln sind wie Angriffe durch Land-, See- und Luftstreitkräfte und dass sie den Bündnisfall gemäss Artikel 5 des Nordatlantikvertrages auslösen. Anders ausgedrückt: Wenn ein Nato-Land durch ein Land, das nicht in der Nato ist, im Cyberraum angegriffen wird, sind die anderen Nato-Länder in der Pflicht zu helfen, im Extremfall bis hin zu kriegerischen Handlungen auch in den anderen Operationsräumen Boden, Luft und Meer. In meiner Beurteilung ist dieser historische Entscheid der Nato auch für die neutrale Schweiz, unsere Sicherheitspolitik und unsere Verteidigung von enormer Tragweite.
Mit dem Einreichen meiner Interpellation habe ich auf die Verantwortung der Schweiz für ihre Sicherheitspolitik und damit für unsere Sicherheit hinweisen wollen. Ich bin mir aufgrund der Antwort des Bundesrates und der aufgeführten schweizerischen Massnahmen aber nicht sicher, ob die Brisanz dieses Nato-Beschlusses wirklich in der richtigen Dimension erkannt worden ist. Da kann der Bundesrat in seiner Antwort schon schreiben, dass solche Nato-Beschlüsse keine direkten Auswirkungen auf die Schweiz haben würden – das trifft zu –, aber indirekte Auswirkungen haben sie alleweil. Wenn fast alle Länder um uns herum Massnahmen für einen neuen Operationsraum hochfahren, mit Cybertruppen usw., können wir uns doch nicht einfach zufriedengeben mit der Umsetzung des Nachrichtendienstgesetzes, das am Sonntag hoffentlich durchkommt, und mit der Umsetzung der Weiterentwicklung der Armee und glauben, dass es damit dann schon getan sei. Hier sind wir also noch gefordert. Dies zum Bereich des Nato-Beschlusses.
Ich begrüsse es aber sehr, dass sich der Bundesrat der sicherheitspolitischen Bedeutung des Cyberraums grundsätzlich bewusst ist, zumal gerade auch der hochentwickelte Finanz-, Werk- und Denkplatz Schweiz von der Cybersicherheit abhängt.

Damit bin ich bei der Cyberabwehr. Die uns bekannten Hackerangriffe auf die Ruag und das VBS waren alarmierend. Obwohl wir uns als neutraler Staat an unsere Verfassung halten müssen, ist eine internationale Zusammenarbeit in diesem Sicherheitsbereich für die Schweiz bedeutungsvoll. Da macht das VBS auch gute Arbeit. Generell möchte ich aber den Bundesrat auffordern, noch grössere Anstrengungen zu unternehmen, die Prioritäten zu überprüfen und Investitionen zu tätigen, wo dies notwendig ist.
Zum Schutz der Systeme der Armee, zum Schutz der Einrichtungen des Bundes und für Cyberoperationen ist auch die Einführung einer Cybertruppe in Erwägung zu ziehen. Gerade die schnelle Digitalisierung, die rasante IT-Entwicklung, aber auch der Bildungsstand und die Kenntnisse der Bevölkerung in der Schweiz machen es notwendig und auch möglich, unsere Sicherheitspolitik angemessen auf die modernste Bedrohung, die Bedrohung aus dem Cyberraum, auszurichten.
Ich lade deshalb den Bundesrat ein, der Cyberdefence noch mehr Beachtung zu schenken und ein neues sicherheitspolitisches Bewusstsein zu bilden in diesem Bereich, ganz nach dem Motto "Gouverner, c'est prévoir".

Parmelin Guy, conseiller fédéral: Monsieur Dittli, je vais commencer par la fin. Vous demandez au Conseil fédéral de faire davantage d'efforts dans le secteur de la cyberdéfense. Nous sommes parfaitement conscients de ce problème. Le Conseil fédéral avait déjà pris conscience auparavant de ces nouveaux défis. Ces dernières années, plusieurs mesures ont été prises pour renforcer la protection de ce qu'on appelle en anglais le "cyberspace" ou le cyberespace en français. En 2012, la Stratégie nationale de protection contre les cyberrisques a été mise en oeuvre; les cybercompétences au niveau des services de renseignement de la Confédération et de l'armée ont été renforcées; des collaborations avec les cantons et les exploitants d'installations critiques, dans le cadre du Réseau national de sécurité, ont été mises en place. Il y a eu, ce qu'on peut appeler, une prise de conscience de ce nouveau défi.
Dans le rapport sur la politique de sécurité de la Suisse, qui vient d'être adopté par le Conseil fédéral, ce sujet est traité en détail. C'est votre conseil, je crois, qui sera le premier conseil à se pencher sur ce rapport. Nous aurons certainement l'occasion de nous en entretenir en commission tout prochainement. Effectivement, ces dernières années, les risques de ce type ne sont pas allés en diminuant mais plutôt en augmentant. Il n'y a aucun doute pour nous qu'il faut accroître la collaboration ainsi que la formation à tous les niveaux et mettre en place les mesures correspondantes. Cela implique de revoir la Stratégie nationale de protection contre les cyberrisques, ce que la Confédération va faire.
Concernant mon département en particulier – parce que plusieurs départements sont concernés par la Stratégie nationale de protection contre les cyberrisques –, nous allons exposer d'ici la fin de l'année, en collaboration avec les autres départements, quels sont nos moyens défensifs, offensifs, les compétences de la Confédération, de quoi elle devrait disposer de nouveau ou de mieux en matière de cyberdéfense afin de protéger notre pays de la meilleure des façons. Cela fera l'objet d'une note de discussion d'ici la fin de l'année au sein du Conseil fédéral.
Dans ce cadre, nous nous intéressons naturellement à tout ce qui se passe à l'étranger, que ce soit dans des Etats membres de l'OTAN ou dans d'autres Etats. Quand je me rends à l'étranger ou lorsque je rencontre des homologues étrangers, comme j'ai eu l'occasion de le faire avec mon homologue suédois, mon homologue français ou avec mon homologue autrichien que j'ai reçu en Suisse, ou dans le cadres des conférences internationales comme le Dialogue Shangri-La à Singapour, on aborde le problème de la cyberdéfense. Il est très intéressant de voir comment cette question est abordée dans d'autres pays. Je remarque que depuis les années 2008 à 2010, en tout cas dans les pays qui nous entourent, on prend conscience du problème et que des stratégies sont mises en place. On procède de façon différente; ce n'est pas la même chose en France ou en Suède par exemple. Il est intéressant de voir les différentes approches, car celles-ci peuvent nous être utiles pour nos travaux.
Il est aussi juste, Monsieur Dittli, que l'OTAN a formellement défini la cyberdéfense comme étant le quatrième domaine d'opération militaire en plus des domaines terrestres, aériens, maritimes, et qu'elle l'a officiellement déclarée comme étant un domaine stratégique. Jusqu'à il y a peu de temps, l'OTAN s'était limitée à tout faire pour protéger ses propres réseaux informatiques. C'est une méthode similaire à ce que nous faisons chez nous, qui consiste à faire d'abord de l'ordre chez nous, à nous protéger d'abord, avant d'envisager les prochaines étapes.
On voit donc que l'OTAN, d'une manière générale, mène aussi une réflexion sur ce sujet. Dans certains Etats, c'est déjà le cas, mais l'OTAN en tant qu'organisation poussera sa réflexion plus loin quant aux conséquences que la problématique "cyber" peut avoir dans le cadre d'opérations militaires. On parle de guerre hybride: cela préoccupe non seulement l'armée suisse, mais aussi toutes les armées du monde. Vous avez rappelé le cas qui nous touche depuis que nous l'avons découvert au mois de janvier dernier. Il est clair que, si des

attaques d'une certaine envergure devaient toucher un Etat membre de l'OTAN, c'est par ricochet que, en vertu des traités conclus, tous les Etats membres de l'Alliance atlantique seraient touchés. Pour l'alliance, cela équivaudrait à une attaque contre les Etats membres en général. C'est pour cette raison que l'OTAN a lancé certains travaux, mais tous les Etats se rendent compte que c'est un sujet extrêmement complexe.
Nous nous posons les mêmes questions. Nous ne voulons surtout pas nous précipiter sans avoir fait un état des lieux,

AB 2016 S 735 / BO 2016 E 735

sans avoir vraiment établi une stratégie afin d'être au clair sur ce que nous voulons faire, ni défini les nouvelles structures à mettre en place. Mais, avant tout, nous devons définir quel concept de défense nous voulons mettre en oeuvre en cas de cyberattaque.
Dans le cadre du nouveau rapport sur la politique de sécurité, nous constatons qu'il peut être nécessaire de recourir à des mesures de défense non seulement lors d'une attaque militaire conventionnelle qui viendrait de l'extérieur, mais aussi et surtout quand ces menaces sont particulièrement intenses et étendues. Dans ce contexte, la problématique des cyberattaques prend toutes son importance. Pour nous, c'est un sujet extrêmement stratégique, mais, comme nous le rappelons dans le rapport sur la politique de sécurité, elles doivent avoir une certaine ampleur.
Je répète que, d'ici la fin de l'année, nous serons à peu près prêts au sein du département pour dire comment nous voyons la chose, quelle sera notre stratégie. Dans le cadre de l'examen du rapport sur la politique de sécurité, nous aurons l'occasion de revenir sur tous ces aspects.
Je suppose que cette réponse vous satisfait. Si ce n'est pas le cas, vous aurez l'occasion de me le dire au moment où nous aborderons ce sujet.