Art. 2
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
Für Annahme des Entwurfes ... 30 Stimmen
Dagegen ... 1 Stimme
(2 Enthaltungen)

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
Bericht SiK-SR 11.01.11
Rapport CPS-CE 11.01.11
Ständerat/Conseil des Etats 15.03.11

Präsident (Inderkum Hansheiri, Präsident): Sie haben einen schriftlichen Bericht der Kommission erhalten. Die Kommission beantragt einstimmig – mit 12 Stimmen –, die Motion anzunehmen. Der Bundesrat beantragt ebenfalls die Annahme der Motion.

Recordon Luc (G, VD), pour la commission: D'emblée, et je le souligne, la commission vous propose, à l'unanimité, d'adopter cette motion. Je crois qu'il importe tout de même de souligner certains points.
D'abord, la cyberguerre, qu'est-ce que c'est? La notion de «guerre», de toute façon, n'est pas extrêmement bien définie; mais, au sens général, il s'agit d'une menée imputable à un Etat et dirigée contre un autre Etat ou par plusieurs Etats contre plusieurs Etats. Dans son acception moderne toutefois, on tend à qualifier de «guerre» des actions qui mettent aussi en présence des groupes non étatiques, par exemple des groupes terroristes, des mouvements de libération ou des éléments de ce genre; donc la notion s'est un peu étendue.
Dans le domaine de la cybernétique, on peut craindre que ce type d'extension de sens mérite d'être pris en considération, c'est-à-dire que des groupes hostiles, et non pas seulement des Etats, voire des groupes hostiles plus ou moins dirigés en sous-main par des Etats, mènent des actions d'une telle ampleur et d'une telle gravité qu'on puisse les qualifier de «cyberguerre». A ce titre, il convient de les distinguer de simples cyberattaques, par exemple menées à titre économique, voire à titre ludique par des pirates qu'on appelle en franglais des «hackers». Je crois que nous devons bien faire la distinction.
En effet, les cyberattaques auxquelles on a pu assister sont restées encore assez limitées. Il y a eu, pour prendre la plus grave connue, celle qui a pour ainsi dire paralysé à un moment donné les réseaux informatiques d'un petit pays comme l'Estonie, qui semble avoir été menée à partir de serveurs qui étaient placés en Russie et qui semble aussi avoir eu pour motivation, pour origine, le mécontentement de tenants de l'ancien système soviétique à l'égard de mesures de «désoviétisation» de l'Estonie. Nous avons aussi subi – il faut le savoir – des attaques qui ne méritent peut-être pas encore le qualificatif d'actions de guerre mais qui sont assez graves et qui ont frappé certains départements de l'administration fédérale, en particulier le Département fédéral des affaires étrangères.
Nous ne sommes donc pas à l'abri, ni par nature, ni du fait de nos prises de position sur le plan politique. Mais ce qui pourrait être véritablement grave, ce serait si des groupes – ou des Etats – qui nous sont hostiles s'en prenaient carrément à des réseaux vitaux pour nous, comme ceux de transport, de communication, d'énergie, en les attaquant par le truchement des télécommunications afin de bloquer leur système de régulation informatique.
Et à ce titre-là, la commission prend le danger très au sérieux. Elle estime que c'est un danger nouveau et d'importance croissante à prendre en considération. Elle reconnaît que le Conseil fédéral a fait un effort et constate qu'il a nommé un responsable. Je ne crois pas qu'elle soit entièrement convaincue que la mesure qui a été prise par le gouvernement, vu l'importance et la gravité du problème, soit encore suffisante.
C'est dans cet esprit que la commission a décidé de vous proposer d'adopter la motion, même si un effort a déjà été fait. Je vous rappelle que la motion vise à ce que le Conseil fédéral crée des bases légales pour 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.
On soulignera encore ici les notions de défense active et de défense passive. Il faut bien sûr se protéger contre les attaques, mais il peut être nécessaire de lancer des contre-attaques pour paralyser à notre tour ceux qu'on aurait pu identifier – ce qui est toujours très difficile en l'état actuel des connaissances techniques en informatique et en télécommunications – comme nous étant hostiles. On ne doit donc pas non plus exclure une activité offensive.

Maurer Ueli, Bundesrat: Der Bundesrat beantragt die Annahme der Motion. Sie wurde auch vom Nationalrat angenommen. Der Kommissionssprecher hat ausgeführt, in welchen Dimensionen wir hier denken müssen, was in den nächsten Jahren alles passieren könnte. Wir sind bereits konkret an der Arbeit. Wir haben innerhalb der Bundesverwaltung das Projekt Cyber Defence gestartet, mit einer Projektleitung und mit entsprechenden Arbeitsgruppen aus den Departementen. Es geht darum, einmal eine Auslegeordnung dazu zu machen, was bereits vorhanden ist. Das ist ja alles noch etwas dunkel, nicht erhellt. Man spürt eine Attacke in der Regel erst, wenn sie bereits passiert ist. Es geht darum, nicht nur die Verwaltung als solche einmal zu analysieren, sondern auch Schnittstellen mit den Kantonen zu bilden, allenfalls auch mit der Wirtschaft und mit Betreibern von Infrastrukturanlagen, sei das im Bereich Wasser, sei das im Bereich Elektrizität usw. Diese ganzen Bereiche können betroffen sein.
Wir möchten bis Ende dieses Jahres einen Bericht abliefern, aufgrund dessen wir dann entsprechende Gesetzesänderungsvorschläge unterbreiten und sagen, was allenfalls zu tun ist. Wenn diese Auslegeordnung einmal gemacht ist, werden wir auch entscheiden können, wie wir konkret weitergehen können. Das Ganze steckt noch in den Kinderschuhen. Kürzlich hat das jemand an einem Vortrag mit der Fliegerei vor hundert Jahren verglichen. Da öffnete man die Türe und warf eine Handgranate ab; das war früher die Bombe. Wahrscheinlich sind wir hier auch etwa in diesem Stadium. Das hat sich bereits entwickelt und wird sich sehr rasch weiterentwickeln. Hier den Anschluss nicht zu verpassen bedingt auch, dass man internationale Kontakte pflegt. Was läuft international, was kann man lernen, wie arbeitet man zusammen? Das funktioniert auf Stufe der Nachrichtendienste. Auf Stufe der Armeen gibt es ein entsprechendes Zentrum der Nato in Tallinn.
Insgesamt bewegen wir uns in einem neuen Feld; da wissen wir nicht alles. Wir arbeiten aber intensiv daran und versuchen, die Aufträge, die uns das Parlament mit dieser Motion und anderen Vorstössen erteilt, zu erfüllen. Ich denke, das ist eine Thematik, die uns noch Jahrzehnte beschäftigen wird und die auch entsprechende Mittel binden kann. Es

geht jetzt einmal darum, eine Auslegeordnung zu machen, eine Auflistung, und dann konkret und pragmatisch vorzuschlagen, was mit welchen Mitteln getan werden kann. Daran arbeiten wir. Mit seinen Erläuterungen und Ausführungen hat der Kommissionssprecher eigentlich den ganzen Bereich abgedeckt.
Wir versuchen, dem Anliegen gerecht zu werden, und mit der Annahme der Motion geben Sie uns auch den Auftrag und das Zeichen, hier weiter aktiv zu sein.

Angenommen – Adopté

Schluss der Sitzung um 11.45 Uhr
La séance est levée à 11 h 45