REUNION COMMUNE DE LA COMMISSION DE L'INTERIEUR, DES AFFAIRES GENERALES ET DE LA FONCTION PUBLIQUE, DE LA COMMISSION DE LA DEFENSE NATIONALE, DE LA COMMISSION DE L'INFRASTRUCTURE, DES COMMUNICATIONS ET DES ENTREPRISES PUBLIQUES ET DE LA COMMISSION DE LA JUSTICE

du

MARDI 4 FEVRIER 2014

Après-midi

_____

GEMEENSCHAPPELIJKE VERGADERING VAN DE COMMISSIE VOOR DE BINNENLANDSE ZAKEN, DE ALGEMENE ZAKEN EN HET OPENBAAR AMBT, DE COMMISSIE VOOR DE LANDSVERDEDIGING, DE COMMISSIE VOOR DE INFRASTRUCTUUR, HET VERKEER EN DE OVERHEIDSBEDRIJVEN EN DE COMMISSIE VOOR DE JUSTITIE

van

DINSDAG 4 FEBRUARI 2014

Namiddag

_____

De vergadering wordt geopend om 14.15 uur en voorgezeten door de heer Siegfried Bracke en de dames Sabien Lahaye-Battheu en Kristien Van Vaerenbergh.
La séance est ouverte à 14.15 heures et présidée par M. Siegfried Bracke et Mmes Sabien Lahaye-Battheu et Kristien Van Vaerenbergh.

01 Échange de vues avec le premier ministre sur la cybersécurité et questions jointes de
- M. Georges Dallemagne au premier ministre sur "les attaques des hackers 'Anonymous Belgium' sur le web belge le 15 juin" (n° 18080)
- Mme Jacqueline Galant au premier ministre sur "la stratégie belge en matière de cybersécurité" (n° 19454)
- M. Ben Weyts à la vice-première ministre et ministre de l'Intérieur et de l'Égalité des chances sur "l'espionnage chez Belgacom" (n° 19696)
- M. Roel Deseyn au premier ministre sur "la cyberstratégie" (n° 19722)
- Mme Marie-Christine Marghem au premier ministre sur "la mise en oeuvre de la cyberstratégie belge" (n° 19822)
- Mme Jacqueline Galant à la vice-première ministre et ministre de l'Intérieur et de l'Égalité des chances sur "la hausse du nombre de cas de hacking et de cybercriminalité" (n° 20033)
- Mme Isabelle Emmery au premier ministre sur "la cybercriminalité internationale" (n° 20840)
- M. Georges Dallemagne au premier ministre sur "la cybersécurité en Belgique et en Europe" (n° 21941)
- M. Ronny Balcaen au premier ministre sur "la cybersécurité" (n° 21977)
01 Gedachtewisseling met de eerste minister over cyberveiligheid en toegevoegde vragen van
- de heer Georges Dallemagne aan de eerste minister over "de aangekondigde aanval op het internet in ons land op 15 juni door hackers onder de noemer 'Anonymous Belgium'" (nr. 18080)
- mevrouw Jacqueline Galant aan de eerste minister over "de Belgische strategie inzake cyberveiligheid" (nr. 19454)
- de heer Ben Weyts aan de vice-eersteminister en minister van Binnenlandse Zaken en Gelijke Kansen over "de spionage bij Belgacom" (nr. 19696)
- de heer Roel Deseyn aan de eerste minister over "de cyberstrategie" (nr. 19722)
- mevrouw Marie-Christine Marghem aan de eerste minister over "de uitvoering van de Belgische cyberstrategie" (nr. 19822)

- mevrouw Jacqueline Galant aan de vice-eersteminister en minister van Binnenlandse Zaken en Gelijke Kansen over "de stijging van het aantal gevallen van hacking en cybercriminaliteit" (nr. 20033)
- mevrouw Isabelle Emmery aan de eerste minister over "de internationale cybercriminaliteit" (nr. 20840)
- de heer Georges Dallemagne aan de eerste minister over "cybersecurity in België en Europa" (nr. 21941)
- de heer Ronny Balcaen aan de eerste minister over "cybersecurity" (nr. 21977)

De **voorzitter**: In overleg met de andere voorzitters hebben wij afgesproken dat wij eerst naar de eerste minister zullen luisteren. Daarna kunnen zij die een vraag hebben ingediend, aan het woord komen en vervolgens kunnen andere leden zich daarbij aansluiten.

01.01 Eerste minister **Elio Di Rupo:** Mijnheer de voorzitter, beste collega's, ik dank u voor de interesse die u stelt in dit belangrijk onderwerp, cyberveiligheid en de bescherming van de Belgische cyberspace. Het is een ruim onderwerp. De vragen die eraan gekoppeld zijn, evolueren bovendien zeer snel. Ze omvatten ook informatie die onder het geheim van het gerechtelijk onderzoek valt of betreffen soms geclassificeerde informatie. Mijn uiteenzetting zal rekening houden met die beperkingen en bestaan uit drie delen.

Allereerst zal ik de weg schetsen die wij sinds de jaren '90 hebben afgelegd. Vervolgens zal ik u informeren over de incidenten en de aanvallen die zich de laatste twee jaar in België hebben voorgedaan. Ten slotte zal ik de Belgische initiatieven toelichten die we hebben genomen. Ik zal een overzicht geven van onze reacties op die incidenten. Ik zal ook de antwoorden van onze buitenlandse partners ter sprake brengen en de vragen die aan België werden gesteld.

D'où venons-nous? La plate-forme BelNIS (Belgian Network Information Security) a été créée par une décision du Conseil des ministres en 2005 à l'initiative du SPF ICT, actuellement Fedict. Cet organe de concertation réunit mensuellement les institutions fédérales jouant un rôle dans la politique de sécurité de l'information du pays. BelNIS ne dispose pas de ressources propres ni d'autorité en matière de sécurité de l'information. Chaque institution membre garde son autonomie et sa responsabilité.

En 2007, la plate-forme BelNIS a publié un livre blanc relatif à la politique nationale en matière de sécurité de l'information. À la suite de cette publication, une série de propositions concrètes ont été élaborées en 2008 et ce, à la demande du Collège du renseignement et de la sécurité. Il s'agit notamment de la création d'un centre capable de réagir aux incidents de sécurité, de la nécessaire coordination de la sécurité de l'information dans les services publics fédéraux, de la nécessité d'un inventaire des systèmes d'information critiques, de la certification de produits informatiques, de la formation relative à la sécurité et de la collaboration du service public avec le secteur privé.

BelNIS werd aldus de afspiegeling van het Vast Comité van Toezicht op de Inlichtingen- en Veiligheidsdiensten of het Comité I.

Het Comité I vestigt sinds 1994 de aandacht van het Parlement op het belang van de veiligheid van officiële informatiesystemen. Het raadde aan een officiële instantie verantwoordelijk te maken voor de ontwikkeling en toepassing van een globaal veiligheidsbeleid voor informatiesystemen voor het hele openbaar ambt. Het comité heeft zich in 2006 en 2011 meerdere malen streng opgesteld ten opzichte van het federale beleid inzake informatiebescherming.

Un pas a été franchi en 2011, avec la création du CERT.be (Computer Emergency Response Team). L'équipe du CERT a pour mission d'aider les ressources clefs belges, les fournisseurs d'informations critiques et le public belge en général, à protéger leur infrastructure ICT.

Le 10 décembre 2011, j'ai intégré dans l'accord de gouvernement les recommandations du Comité R: "Afin de donner suite aux recommandations du Comité R, le gouvernement élaborera une stratégie fédérale de sécurité des réseaux et systèmes d'information dans le respect de la protection de la vie privée."

Début 2012, j'ai invité le groupe de travail BelNIS à plancher sur ce projet de stratégie fédérale. Un texte a ainsi été finalisé en octobre. Il a été examiné en groupe de travail le 12 décembre et a été soumis au Conseil des ministres le 21 décembre 2012.

In oktober 2013 heeft de regering, ondanks grote besparingen ten bedrage van 22 miljard euro, 10 miljoen

euro vrijgemaakt om onze strategie voor cyberveiligheid versneld uit te voeren. Op 19 december jongstleden heeft de Ministerraad de oprichting goedgekeurd van een Centrum voor Cybersecurity België.

Le 19 décembre, le Conseil des ministres a approuvé la création d'un Centre de cybersécurité belge (CCB).

Dat centrum wil niet het zoveelste instrument zijn, maar wel een hulpmiddel om de bestaande capaciteiten en kennis in die materie te integreren en coördineren.

La répartition des 10 millions s'opèrera entre différents services actifs dans la cybersécurité. Le dossier est actuellement à l'examen au SPF Budget et sera discuté encore cette semaine en groupe de travail intercabinet.

En décidant la création d'un Centre autorité nationale de cybersécurité, la Belgique développe une stratégie et renforce ainsi les effectifs et les moyens d'action des services impliqués dans la lutte contre les cyberincidents.

Pour être clair sur le plan de la procédure légale, nous travaillons pour le moment par arrêté royal, sur la base des pouvoirs conférés à la Chancellerie. Cela permet de travailler dans des délais courts et de ne pas être pris par la fin de la législature. Nous préparerons en parallèle un projet de loi qui permettra d'inclure le contenu de l'arrêté royal mais nous ne connaissons pas la longueur de la procédure requise. Une loi sera en effet nécessaire pour définir les missions du Centre pour la cybersécurité. Il faudra par ailleurs modifier et compléter les lois existantes qui concernent tantôt la police fédérale, tantôt la Sûreté de l'État, tantôt la Sûreté militaire, CERT.be, le SPF Économie et l'IBPT, pour que tous ces services soient légalement tenus de fournir automatiquement les informations demandées par le Centre pour la cybersécurité sur un certain nombre de sujets.

Il s'agit d'actions concrètes pour lesquelles nous sommes cités en exemple, me dit-on, par des pays voisins, dont la France.

Nu kom ik tot de incidenten.

Net als tal van andere Europese landen, is België met Brussel het doelwit van aanvallen, pogingen tot indringing of cyberincidenten. Ze richten zich, om het eenvoudig te stellen, op onze informaticasystemen en onze computernetwerken met het oog op het verkrijgen van informatie uit die systemen. Er zijn verschillende categorieën van incidenten. Soms gaat het enkel om cyberprotesten, soms is er sprake van politieke en economische spionage. Dat is de realiteit.

Brussel is uiteraard een belangrijk doelwit van dat soort activiteiten, aangezien het de hoofdstad is van Europa, de hoofdzetel van de NAVO en gastland van heel wat internationale missies.

Nos institutions en font également les frais. Le SPF Affaires étrangères et mon administration, la Chancellerie, ont fait l'objet d'intrusions informatiques.

Tout aussi interpellante est l'intrusion subie par Belgacom, fin de l'été dernier. L'entreprise a déposé une plainte contre X. Elle se réserve le droit de réclamer des dommages et intérêts à l'auteur de l'intrusion. À ce stade, l'enquête est toujours en cours.

Le 12 décembre 2013, le conseil d'administration de Belgacom a approuvé un plan de cybersécurité permettant à l'entreprise de sécuriser, à l'avenir, au plus haut niveau ses systèmes télécoms et informatiques. Les leçons que l'entreprise a tirées du *hacking* dont elle a été victime sont évidemment intégrées dans ce plan. Il s'agit d'un programme pluriannuel pour lequel un investissement supplémentaire de 15 millions d'euros sera libéré.

Bovendien heeft het BIPT de virussignatuur van het bij Belgacom ontdekte virus ter beschikking gesteld van de internetproviders.

Chers collègues, tous les pays font face à des défis de cybersécurité. Certains pays européens connaissent des situations plus problématiques que nous. Nous ne déplorons jusqu'à présent pas d'actions de sabotage ou de cyberterrorisme.

En 2007, par exemple, l'Estonie, pays parmi les plus connectés, fut l'objet d'une série d'attaques sans précédent à l'échelle d'un pays. Les sites gouvernementaux furent les premiers visés; puis vint le tour des banques, des médias et des partis politiques. Le numéro des urgences est même resté indisponible pendant plus d'une heure.

Chez nos voisins des Pays-Bas, en avril 2013, près de 10 millions de Néerlandais ont été privés de l'utilisation de leur signature électronique officielle, qui permet notamment de payer ses impôts en ligne. La plate-forme internet de gestion des comptes de ING a également été inaccessible pendant plusieurs heures suite à une attaque, tout comme le site internet de la compagnie aérienne KLM, pour ne citer que quelques exemples.

Plus proche de nous encore, le 21 janvier dernier, l'Office fédéral allemand pour la sécurité dans les technologies de l'information lançait une alerte concernant un piratage de très grande envergure portant sur 16 millions de comptes email, avec leur adresse et mot de passe. Je peux bien entendu multiplier les exemples.

J'imagine que nous reviendrons sur la question des écoutes attribuées à la National Security Agency des États-Unis ou à son pendant britannique The Government Communications Headquarters.

Beste collega's, onze maatschappij en onze economie zijn enorm afhankelijk geworden van informatie- en communicatietechnologieën. Die liggen aan de basis van de werking van heel wat professionele procedures, met inbegrip van de vitale sectoren.

Je le répète, la Belgique et Bruxelles en particulier, de par leur rôle de capitale, siège d'institutions européennes et internationales, sont évidemment des cibles de cyberattaques diverses et variées. Combien? De quels types? Quelles en sont les victimes? Malheureusement, je n'ai pas les informations pour répondre à toutes ces questions. Je constate, comme vous, que les statistiques de CERT.be ou de la police fédérale traduisent malheureusement en augmentation. Les faits augmentent mais leur signalement également, ce qui est en soi une bonne chose. Nous ne sommes pas naïfs; loin s'en faut! Nous devons agir avec méthode pour nous préserver de ces cyberincidents. Nous devons bien entendu associer l'ensemble des acteurs impliqués pour lutter contre cette réalité, sans oublier nos citoyens, victimes au quotidien de cybercriminalité.

Les services et institutions publics doivent y être préparés. Pour ce faire, ils doivent se mobiliser et s'associer avec le secteur privé, le secteur universitaire et le monde de la recherche car - ne l'oublions pas non plus -, la Belgique doit investir dans le cyberespace. Il est source de développement économique également.

Onze nationale strategie inzake cyberveiligheid richt zich op die doelstellingen. Bovendien is zij gericht op de ontwikkeling van een veilige en betrouwbare cyberspace die de fundamentele waarden en rechten respecteert.

Ce cyberespace doit respecter les droits fondamentaux. Notre stratégie en la matière vise également à développer nos propres capacités de cybersécurité pour une politique de sécurité autonome et une réaction aux incidents sécuritaires adaptée. C'est au sein du Centre belge pour la cybersécurité qu'elle sera mise en œuvre.

De même, la capacité de nos services doit être renforcée et notre ambition est de pouvoir engager entre 50 et 55 experts en la matière en 2014. Ce ne sera pas simple, les experts dans ce secteur étant très convoités. La Belgique veut aussi promouvoir une réflexion internationale en la matière.

Alle veiligheidsaspecten moeten worden aangekaart met het oog op een optimale nationale en internationale samenwerking.

Certes, le défi est important, car nous touchons à la souveraineté des États. Même au sein de l'Europe, nous sommes parfois concurrents entre nous. Il est nécessaire de trouver un équilibre qui permette tant la lutte contre le terrorisme que le développement d'un cyberespace respectueux des droits individuels et de la démocratie.

C'est pour ces raisons qu'à plusieurs reprises, j'ai soutenu les initiatives de la présidente brésilienne,

Dilma Rousseff plaidant pour un traité international qui permettrait de protéger la vie privée des citoyens contre l'espionnage sur internet.

J'ai également soutenu et pris part, par un courrier, aux initiatives de mes collègues Hollande et Merkel en vue d'établir un code de bonne conduite entre alliés américains et européens en matière d'espionnage. "La voix de la Belgique et de Bruxelles est remontée jusqu'à Washington", me dit-on, notamment lors de l'International Strategic Dialogue on Cybersecurity, les 16 et 18 décembre 2013.

Le 17 janvier dernier, le président Obama a prononcé un discours sur la réforme du système américain de surveillance des communications. Il y a souligné la nécessité d'un équilibre entre efforts de renseignements et garanties des droits individuels.

Je pense que nous, Européens, avons été entendus, modestement, mais entendus!

Uiteraard is er nog een hele weg te gaan. De Amerikanen zijn ook vragende partij voor synergie met Europa.

Il faut veiller à ce que les révélations de Snowden au sujet de la NSA n'entraînent pas la cyberbalkanisation, un repli sur soi ou la réduction des libertés d'expression sur la toile, sous des prétextes sécuritaires.

Monsieur le président, chers collègues, voilà une introduction que vous jugerez peut-être un peu longue, mais le sujet est d'importance.

De **voorzitter**: Zoals afgesproken krijgen eerst de vraagstellers het woord, waarna de andere leden kunnen interveniëren.

01.02 **Georges Dallemagne** (cdH): Monsieur le premier ministre, merci pour ces informations attendues de longue date par notre parlement: ma première question sur le sujet date en effet du 15 juin dernier.

Évidemment, j'apprécie les efforts menés par vous-même et votre gouvernement à l'égard de cet enjeu considérable. En effet, en quelques mois, nous avons basculé d'un monde à l'autre: d'un monde où chacun conservait sa vie privée, où les entreprises pouvaient préserver leur savoir-faire, où nos gouvernements menaient des actions qui n'étaient pas continuellement épiées sur la place publique, à un monde où tout cela est mis en danger. Cette évolution est extrêmement grave et il faut en saisir toute l'importance et la gravité. Ce problème restera présent encore pour de nombreuses années.

Autant j'apprécie les efforts menés par le gouvernement, autant je déplore que les choses n'avancent pas au rythme auquel progressent ces menaces et ces attaques contre nos entreprises, notre gouvernement, vous-même et la vie privée de nos citoyens.

J'entends que nos services de renseignement avaient déjà repéré diverses défaillances depuis de nombreuses années, puisque vous parlez de la période 2006-2011. En 2008, j'avais interrogé le ministre des Affaires étrangères qui signalait alors que son département était déjà l'objet d'espionnage. L'accord de gouvernement comprend d'ailleurs cet élément. Il s'agit donc d'une stratégie définie voilà 14 mois, mais nous n'avons pas encore pu la mettre réellement en œuvre, du moins dans son pôle le plus important, c'est-à-dire un centre contre la cybercriminalité.

Je souhaiterais donc obtenir des informations supplémentaires sur le timing. De fait, nous sommes confrontés à une course contre la montre par rapport à des personnes ou des gouvernements qui ne veulent pas du bien ni à notre économie ni à notre vie privée; par le biais de divers dispositifs, elles cherchent à nous affaiblir, à nous instrumentaliser, à nous utiliser ou à modifier nos comportements, par exemple, sur le plan économique.

Peut-être suis-je trop direct en le disant, mais je pense que notre réponse est en deça de ce qu'elle devrait être face à un problème aussi grave, tant sur le timing que sur les ressources mises à disposition et sur le dispositif installé. Il est temps d'accélérer le mouvement.

Vous avez rappelé l'intérêt de disposer d'un cadre législatif; cet élément était déjà sur la table depuis de nombreuses années et il a été rappelé dans votre stratégie il y a 14 mois. Il m'apparaît important que, sur le plan législatif, nous avancions, non seulement sur la collaboration entre les services – soit une quinzaine –, mais également sur une neutralisation des ordinateurs des groupes qui nuiraient à nos intérêts.

Actuellement, nous ne pouvons pas agir, car la loi ne nous y autorise pas. Nous devons nous contenter de créer des boucliers suffisamment efficaces: sur un champ de bataille, nous ne serions armés que de boucliers face à des ennemis nettement plus agressifs et mieux équipés. Je pense qu'il est important que nous puissions avancer aussi sur ce point.

J'aurais donc voulu en savoir un peu plus sur ce que contiendra cette loi, notamment sur cette question-là. Pas seulement sur la coordination mais aussi sur la manière dont nous pourrons mieux nous défendre par rapport à des activités hostiles à nos intérêts, nos entreprises, nos citoyens, notre gouvernement.

Le deuxième élément sur lequel je voudrais insister et avoir des détails complémentaires de votre part concerne la coopération internationale. Vous avez dit que chacun en fait une matière de souveraineté nationale. Je vois qu'une série de gouvernements – qui nous sont proches, des gouvernements amis de l'Union européenne – se sont équipés, parfois substantiellement, pour mieux se défendre, beaucoup plus que nous. Je vois des budgets, des chiffres très importants, des ressources très importantes, des dispositions législatives qui ont changé depuis plusieurs années: 2009, 2010 pour l'Allemagne ou la Grande-Bretagne. J'aurais aimé que l'on puisse avoir rapidement cette discussion au niveau européen parce que ces dispositions qui ont été prises par des gouvernements qui nous sont proches sont non seulement des dispositions de défense, ce qui est évidemment tout à fait légitime, mais celles-ci peuvent aussi avoir des conséquences sur nous-mêmes et peuvent, le cas échéant, se retourner ou avoir des possibilités plus offensives.

J'aurais aimé qu'on ait d'urgence non seulement ce code de bonne conduite transatlantique dont vous avez parlé mais qu'il y ait aussi au niveau européen des dispositions très claires sur le plan de ce qu'on peut ou ne peut pas faire entre États membres de l'Union européenne. C'est extrêmement important et très perturbant d'appendre que et la France et la Grande-Bretagne s'autorisent aujourd'hui des activités d'espionnage, y compris sur notre propre territoire. C'est le genre de choses qui me paraît totalement inadmissible.

Le troisième élément concerne les États-Unis. Je me réjouis de votre démarche, mais j'ai entendu le discours de M. Obama et permettez-moi par conséquent d'être un peu moins optimiste que vous. J'ai entendu que M. Obama continue à considérer que les citoyens européens ont moins de droits que les citoyens américains en matière de protection de la vie privée. Nous ne pouvons pas ester en justice aux États-Unis sur ces questions-là alors que les citoyens américains peuvent le faire. Il est extrêmement important de rappeler aux États-Unis, qui sont un partenaire stratégique et commercial très important de la Belgique et de l'Europe, qu'il y a des choses qui ne se font pas et qui ne seront pas tolérées par la Belgique. Il est important de rappeler que ce que les États-Unis ont fait en Belgique est illégal au regard du droit belge. Nous ne pouvons pas, en Belgique, espionner des industries, des départements ou des individus sans l'autorisation préalable d'un juge d'instruction. Les États-Unis ont pu le faire.

Monsieur le ministre, pourriez-vous nous dire si tout cela est maintenant définitivement derrière nous ou si ces activités illégales se perpétuent? Les États-Unis s'autorisent-ils encore à s'adonner à des activités qui sont illégales au sens du droit belge? Il en va de même pour des pays qui ne sont pas des alliés ou qui ont des intérêts encore plus éloignés des nôtres, comme la Chine ou d'autres grandes puissances qui se sont aussi fait connaître par leurs activités d'espionnage.

Cela dit, sur le plan international, au-delà d'un traité, il est important de disposer d'un dispositif permanent pour ce qui concerne un problème aussi grave qui touche aux libertés fondamentales, au cyberespace, à la communication entre les individus, les gouvernements, les entreprises. Il est ici question d'un univers qui est apparu il y a quelques décennies, qui a accompagné notre prospérité, le progrès social économique, mais qui pourrait être, aujourd'hui, utilisé contre les citoyens, contre les États et les entreprises. Il est donc important de se doter d'une organisation internationale qui aurait pour objectif de faire fonctionner correctement cet espace.

Il s'agit d'un enjeu au moins aussi important que celui qui a été à l'origine d'autres organisations internationales des Nations unies. Dans ce domaine, nous devrions également faire en sorte d'assurer, à l'avenir, un regard international, de mettre sur pied une assemblée qui nous permette ainsi qu'aux autres États de vérifier que les droits, les libertés, la protection de la vie privée, la protection des données des entreprises et des gouvernements font bien l'objet d'une protection. Le cas échéant, des sanctions pourraient également être prévues pour ceux qui dérogeraient aux règles.

Voilà, pour l'essentiel, ce que je souhaitais dire au nom de mon groupe. Nous ne devons pas sous-estimer l'importance de l'enjeu. Il ne se passe pas un jour sans que ne soient révélées des atteintes graves à la protection des données de nos citoyens et de nos entreprises. Il est extrêmement important de mettre à la disposition d'un Centre pour la cybersécurité, des ressources, un dispositif légal et un mandat à la hauteur des intrusions dont nous faisons l'objet.

01.03 **Isabelle Emmery** (PS): Monsieur le président, monsieur le premier ministre, au nom de mon groupe, je tiens à vous remercier pour l'exposé clair et précis que vous nous avez livré. Il nous donne les premiers éléments de compréhension et de réaction au sujet de cette problématique importante. Au-delà du détail des mesures qui ont été prises, je voudrais souligner que le déblocage d'un montant aussi conséquent dans une période d'économies budgétaires n'est pas anodin. Cela démontre à quel point le gouvernement, sous votre impulsion, a pleinement pris conscience des enjeux de la cybersécurité, tant pour nos citoyens que pour nos infrastructures et notre économie.

Cela nous rappelle également qu'une politique de cybersécurité ne peut pas être une somme de mesures ponctuelles et improvisées. Elle demande des mesures de fond, des mesures choc, un cadre de réflexion qui soit large tant par ses acteurs qu'au regard des libertés qu'elle doit protéger. Il n'est en effet pas question de brider ou de restreindre l'internet, qui reste un espace formidable de liberté.

Nous ne viderons pas ce débat important aujourd'hui mais afin d'affiner ma compréhension du dossier, je souhaite vous poser quelques questions.

Monsieur le premier ministre, dans quel délai pourra-t-on voir concrétisées les mesures que vous avez évoquées? Les sociétés possédant de larges infrastructures de télécommunications seront-elles directement concernées par ces mesures? Dans l'inventaire des mesures que vous avez précisées, une analyse a-t-elle été faite sur base d'exemples étrangers?

Vous l'avez rappelé, vous avez fait un appel commun avec la présidente de l'État brésilien pour aller vers un traité, vers une prise de conscience plus internationale du phénomène. Quel est votre sentiment sur la suite qui sera réservée à cet appel international?

01.04 **Ronny Balcaen** (Ecolo-Groen): Monsieur le président, monsieur le premier ministre, je vous remercie pour vos explications et votre exposé qui apportent une série de réponses aux questions que nous nous posons. Ceci dit, le sujet que nous traitons aujourd'hui et qui s'impose à nous depuis plusieurs mois est d'une importance capitale pour le respect de nos droits privés, du droit à la vie privée et le respect de notre souveraineté économique et politique. Vous l'avez d'ailleurs reconnu comme d'autres collègues.

À ce sujet, on ne peut que constater avec le grand public que ce qui est découvert depuis plusieurs mois est particulièrement choquant. Je me rallie à ce que M. Dallemagne a dit sur l'illégalité et le cynisme de certains pays aujourd'hui en matière d'espionnage, un cynisme qui ne semble pas décroître malgré les protestations qui se sont fait jour un peu partout.

En Belgique, toutes ces annonces et informations que nous avons reçues sur les attaques, l'espionnage, le *hacking*, etc., auront sans doute été le déclic pour enfin tenter de mettre en œuvre une politique de cybersécurité plus cohérente. J'ai néanmoins, moi aussi, certains doutes quant à l'efficacité des moyens qui sont dégagés aujourd'hui. Dans la période de disette budgétaire et de crise économique que nous vivons actuellement, il n'est pas simple de dégager 10 millions d'euros du budget fédéral. C'est un montant important. Toutefois, comparé au budget de la NSA qui est de 10,8 milliards de dollars, on se demande ce que l'on va pouvoir faire avec ces 10 millions d'euros, à la fois pour nous protéger, pour protéger nos citoyens et nos entreprises.

Monsieur le premier ministre, j'hésite à vous poser la question mais je la pose quand même. Pourriez-vous être un peu plus précis dans la manière dont ces moyens seront utilisés? Vous avez évoqué le fait que le gouvernement va travailler par arrêté royal, en parallèle avec une proposition de loi. Pouvez-vous déjà être un peu plus précis sur ces questions-là? Comme nous sommes d'accord de dire qu'il faut avancer vite, d'autant plus que nous sommes en fin de législature, les différentes commissions pourraient-elles disposer du contenu des arrêtés royaux en discussion? Ce serait une bonne chose.

Voilà pour les points d'avenir pour lesquels je suis en attente de plus d'informations. Il conviendrait de ne pas passer trop rapidement au bleu tout ce qui s'est passé ces derniers mois et qui se déroule depuis des

années sans doute.

Mes questions touchent aussi aux initiatives prises au niveau judiciaire pour tenter d'en savoir plus, tant sur Belgacom que sur les autres incidents que vous avez évoqués.

Aujourd'hui, des initiatives nettes ont-elles été prises par la Justice pour faire la lumière sur ces incidents?

Vous avez évoqué les initiatives diplomatiques prises notamment au niveau belge ou au niveau européen. Peut-on aujourd'hui se contenter des faibles signaux envoyés par les États-Unis assurant de leur attention accrue et de davantage de respect des droits? On n'y trouve nulle trace de remise en question fondamentale de leur stratégie.

Vu les faibles moyens dont nous disposons, sans remise en cause fondamentale de la stratégie des États-Unis et, sans doute, de la Grande-Bretagne, je vois mal comment nous pourrions lutter avec efficacité contre le phénomène.

J'ai évoqué Belgacom. Est-il possible de nous apporter des réponses sur la chronologie des faits et sur ce qui s'est vraiment passé au sein de l'entreprise? Quel a été l'impact de l'événement sur la clientèle? En effet, à ce jour, nous disposons de peu d'informations à ce sujet.

Vous parlez de 15 millions d'euros dégagés pour résoudre quelques problèmes et les failles déjà identifiées. Nous supposons que les actions à entreprendre sont d'un niveau très technique, mais nous aimerions néanmoins recevoir des renseignements sur la répartition de ce montant.

Enfin, des activités illégales d'espionnage, de *hacking* et autres ont été perpétrées sur notre territoire et nous aimerions savoir par qui, comment, dans quel but et à cause de quelles failles dans nos systèmes. Elles impliquent certaines relations au niveau international et mettent en cause des droits essentiels, comme le droit à la vie privée.

C'est pourquoi le groupe Ecolo-Groen proposera que, pour la prochaine législature, notre parlement puisse travailler sur cette question de manière sérieuse pour identifier les responsabilités et découvrir ce qui s'est passé sur le terrain au quotidien. Il demandera la mise sur pied d'une commission d'enquête à la prochaine rentrée parlementaire.

01.05 **Karolien Grosemans** (N-VA): Mijnheer de voorzitter, mijnheer de eerste minister, ik dank u voor de toelichting. Ik heb enkele vragen ter zake.

Generaal Testelmans, hoofd van de ADIV, verklaarde in augustus 2013 dat zijn dienst het slachtoffer was van een cyberincident. De ADIV moest constateren dat er onvoldoende capaciteit was om die malware te verwijderen, wat vrij wrang is als men bedenkt dat vijfentwintig jaar geleden al voor dergelijke cyberaanvallen werd gewaarschuwd.

De ADIV moest een beroep doen op het Amerikaanse Army Cyber Command. De dienst moest dus op buitenlandse instanties een beroep doen, wat ons natuurlijk erg kwetsbaar maakt. Wij zijn sowieso al een kwetsbaar land met de NAVO en de diplomatie hier. Ook internationaal expert Jonathan Holslag, professor aan de VUB, wees er al op dat wij een van de slechtst beveiligde landen op het vlak van cyberaanvallen zijn.

Het is natuurlijk goed te horen dat 50 tot 75 cyberpersoneelsleden zouden worden aangeworven, wat tot nu toe een mooie, weliswaar aangekondigde, versterking is. Hoeveel personen zullen aan de militaire inlichtingendienst ADIV worden toegevoegd, om het operationeel aspect te verhogen? Nog belangrijker is te weten hoe men dat personeel in dienst zal houden, als men weet dat werken in de privésector veel lucratiever is. Zal er een samenwerking met de bedrijfswereld zijn?

Er zijn ideeën in Nederland en Groot-Brittannië, waar met cyberreservisten wordt gewerkt. Bijvoorbeeld, medewerkers zouden bij de ADIV een militaire opleiding kunnen krijgen. Zij zouden er expertise kunnen opbouwen, maar wel hun baan in de burgermaatschappij behouden. Zij zouden een aantal keer worden opgeroepen voor een training van militaire basisvaardigheden. Zij kunnen ook als cyberdeskundige werken en meegaan op oefeningen en missies. Dat is misschien een interessante piste. Is het een denkpiste waaraan eventueel nu al wordt gewerkt?

De ADIV is wettelijk bevoegd om op cyberaanvallen te reageren. Ik citeer even uit de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Artikel 11, § 2, bepaalt het volgende: “Het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert, de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen en in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheerst, de aanval neutraliseren en er de daders van identificeren” — nu volgt het belangrijke deel — “onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren, overeenkomstig de bepalingen van het recht van de gewapende conflicten.” Hoe vaak maakte de ADIV al gebruik van dit recht?

Vervolgens heb ik een vraag over wat op 2 oktober 2013 in *Knack* is verschenen. Aan het woord is Eddy Willems van het European Institute for Computer Antivirusresearch. Hij zegt: “Zolang de aanvallen op onze bedrijven of overheidsbedrijven beperkt blijven tot buitenlandse inlichtingendiensten die informatie verzamelen, is er geen man overboord. De grootste vrees van de regering zou moeten zijn dat op een dag dezelfde gaten in de beveiliging zullen worden gebruikt om ons elektriciteitsnetwerk uit te schakelen of meerdere overheidssites tegelijk lam te leggen. Daar zijn wij totaal niet op voorbereid.” Liggen daarvoor scenario’s klaar? Wordt hier ook aan gewerkt? Dit is zeker niet onbelangrijk.

Het Comité I beveelt aan te voorzien in de mogelijkheid om systemen in het buitenland te neutraliseren in geval van aanvallen tegen de informatiesystemen van andere overheidsdiensten dan die van Defensie, de diensten van de eerste minister, de FOD Buitenlandse Zaken, VSSE enzovoort, of tegen de nationale kritieke infrastructuur. De VSSE zou met die opdracht kunnen worden belast. Wat is uw standpunt, mijnheer de premier?

Ten slotte, kreeg ik nog graag een antwoord op de volgende vragen. Quid met de uitwerking van een cyberstrategie? Wat is de huidige stand van zaken in verband met het CCSB? Hiervoor werd advies gevraagd aan de Raad van State in december. Ik zou daar graag meer toelichting over willen.

Wordt de beveiliging van de FOD’s gecontroleerd? Wordt er gebruikgemaakt van *mystery hackers* in dit kader? Wat zijn hiervan de resultaten?

Welke initiatieven werden genomen na het hacken van Buitenlandse Zaken en van de Kanselarij? Kunt u daar meer toelichting bij geven? Is er intussen ook een overzicht van de gestolen gegevens? China zou achter die aanval zitten; wordt er gesproken met de Chinezen? Kunt u daar iets meer over vertellen?

Ten slotte, welke federale overheidsdiensten werden gehackt?

01.06 **Denis Ducarme** (MR): Monsieur le président, c'est un débat difficile!

Je voudrais, tout d'abord, remercier le premier ministre d'être présent aujourd'hui pour débattre avec le parlement – et plus précisément quatre de ses commissions – de cette question importante que nous souhaitions aborder avec lui depuis les mois de septembre et octobre de l'année passée. C'est une bonne chose que nous puissions, quatorze mois après la note et la décision du gouvernement, vous confier, monsieur le premier ministre, ce dossier et avoir un échange de vues avec vous.

La problématique dont il est question est extrêmement compliquée. Comme la note du gouvernement l'indique, nous sommes vulnérables. Le directeur du Renseignement indiquait même publiquement que le monde politique se désintéressait complètement de la problématique de la cybersécurité, du cyberterrorisme ou de la cybercriminalité. Peut-être tournons-nous donc aujourd'hui la page de ce désintérêt général, comme il l'exprimait, pour avancer.

Monsieur le premier ministre, dans votre exposé introductif, vous avez rappelé les différentes attaques dont nous avons été victimes et vous êtes revenu sur la stratégie à mettre en place. Malheureusement, je rejoindrai mon collègue Dallemagne qui soulignait – il me corrigera, si nécessaire – une forme de lenteur que nous mettons à nous concentrer sur ce dossier pour sortir des effets concrets. Je me demande – et j'ai la franchise de vous le dire – si nous n'avons pas perdu une législature dans ce dossier. Vous indiquiez qu'un certain nombre de réunions intercabinet devaient avoir lieu pour produire prochainement et rapidement, par arrêté royal, des effets concrets, sans doute avant la dissolution très prochaine des Chambres.

Je suis un peu interrogatif. En effet, monsieur le premier ministre, votre exposé introductif utile au débat qui va suivre ne m'a pas appris grand-chose. Bien entendu, le parlement a salué unanimement, je pense, la décision prise par le gouvernement d'investir 10 millions d'euros dans ce qui m'apparaît être une forme de coordination de nos services qui pourront travailler ensemble de manière concertée face à la cybermenace.

Pour un certain nombre d'entre nous et la majorité des Belges, cette cybermenace n'est peut-être pas encore très concrète. On ne la voit pas, comme on peut voir les images d'un terroriste. Pourtant, il faut l'admettre - et ce n'est pas attiser les peurs que de le dire -, la cybermenace est aujourd'hui aussi dangereuse que le terrorisme pour notre société, pour la sécurité des Belges, de nos entreprises et de nos infrastructures. Clairement, la cybermenace est aussi dangereuse qu'une bombe.

Le gouvernement a le mérite d'avoir ouvert une perspective sans doute intéressante. Je tiens ici à souligner que ce dossier est porté par le premier ministre. Ce n'est en effet pas rien, monsieur le premier ministre, que vous soyez là pour défendre ce dossier. Le fait que vous soyez aux manettes est un élément dont nous reconnaissons l'importance.

Nous avons cependant aussi un devoir critique par rapport aux priorités aujourd'hui. Mme Jaqueline Galant m'a demandé de revenir sur la nécessité de voir le premier ministre nous expliquer quelles étaient notre stratégie et nos priorités. Nous attendons, il est vrai, ce débat à la Chambre avec impatience depuis un certain nombre de mois. Je vous avoue, monsieur le premier ministre, que je m'attendais à recevoir un document expliquant, dans le cadre de la cybermenace, les stratégies du gouvernement pour les mois qui viennent, les objectifs auxquels nous devons tendre et précisant à quoi vont servir ces 10 millions d'euros qui comparés à un certain nombre d'investissements de pays européens, …. Oui, c'est la crise mais il ne s'agit pas de comparer des pommes et des poires! Nous ne sommes pas les États-Unis ni la NSA, Dieu nous en préserve!

Cependant, ce ne sont pas dix millions d'euros qui vont solutionner la problématique et qui vont nous rendre moins vulnérables aujourd'hui en Belgique, quand on voit les montants qui sont investis par un certain nombre de pays européens, même de grands pays. Ceux-là savent très bien que cela ne sera pas suffisant et qu'il faudra remettre le couvert et de plus en plus chaque année, à chaque budget.

Dix millions d'euros, c'est un signal important: nous nous mettons au travail. Mais quels sont nos objectifs précis? Bien sûr, nous ne sommes pas des techniciens et vous n'êtes pas non plus, monsieur le premier ministre, un technicien de la cybermenace. Il nous faudra donc voir dans les mois prochains comment nous allons travailler pour pouvoir juger de ces avancées et tendre vers ces objectifs.

Il y a un élément que vous avez souligné et qui me semble extrêmement important. D'autres pays européens ont pu produire des collaborations en vue de faire des progrès plus conséquents en matière de cyberprotection. Il faut envisager des collaborations fortes avec des universités mais également avec le privé, vous l'avez dit. En France, 600 entreprises travaillent sur la question de la cyberprotection; cela représente un gisement évalué à 50 000 emplois. Le privé doit être le partenaire pour atteindre les objectifs que nous devons nous fixer et que sans doute vous préciserez dans la deuxième partie du débat.

Monsieur le premier ministre, je souhaiterais que vous puissiez nous tracer une ligne, que vous nous montriez l'objectif que nous devons atteindre dans un dossier aussi important et menaçant. À ce moment-là, nous aurons fait ensemble le premier pas essentiel en la matière.

Par ailleurs, j'ai écouté tout du long votre intervention devant les Nations unies cet été. Vous avez eu raison de le faire ainsi. Les pays amis doivent s'entendre dire certaines vérités. Vous l'avez fait! Mais je ne vous cacherai pas que la NSA, que les États-Unis, je ne les considère pas comme la menace la plus importante à notre encontre et qu'il ne faudrait pas que l'espionnage américain soit finalement le nuage de fumée que l'on place devant les vrais problèmes pour peut-être les évacuer.

Naturellement, ce n'est pas le problème le plus important. Vous avez bien fait de mettre les choses au point, comme d'autres pays européens l'ont fait, mais ce n'est pas l'essentiel.

Enfin, vous avez parlé du code de bonne conduite et de la collaboration avec un certain nombre de pays européens. Par rapport à la question de la NSA, c'est évidemment un élément important, mais j'ignore si un code de bonne conduite constituera une arme suffisante pour nous protéger comme nous le devons.

En cela, les initiatives qui peuvent être prises en collaboration avec l'agence européenne qui se consacre à la question de la cybermenace, les collaborations qui peuvent être mises en place et accentuées avec l'agence dépendant de l'OTAN me semblent, en effet, essentielles.

Eu égard à cet élément, j'ignore si les dix millions d'euros en question serviront à accentuer les collaborations nécessaires. Nous ne pouvons pas envisager, face à cette menace mondiale qu'est la cybermenace, de nous protéger seuls. Nous ne sommes pas une île numérique. Dans ce cadre, il sera nécessaire, à l'avenir, de projeter davantage de collaboration avec les amis européens et les amis de l'OTAN pour améliorer notre protection.

Une annonce a été faite, cet été, du renforcement du SGRS à hauteur d'un budget de six millions. Monsieur le premier ministre, ces six millions d'euros affectés cet été au SGRS sont-ils à ajouter aux dix millions annoncés dans le cadre du travail de la coordination de nos services? Ou, au contraire, ces six millions d'euros font-ils partie de ces dix millions. Je parle du SGRS, car nous savons qu'il collabore avec un certain nombre de services au niveau international, comme l'OTAN.

01.07 **Jef Van den Bergh** (CD&V): Mijnheer de voorzitter, mijnheer de premier, bedankt voor uw inleiding.

Ik houd mijn uiteenzetting met enige schroom, want onze 'cyberspecialist,' Roel Deseyn, bevindt zich voor de Raad van Europa in het buitenland. Zelf zou ik mij geen specialist durven noemen. Ik zou mijzelf eerder plaatsen in het kamp van de naïeve gebruikers van alle mogelijke cybertoepassingen.

Het bewustzijn moet elke dag groeien en het groeit ook bij ons. Wij mogen niet meer naïef zijn en na de onthullingen van Snowden en andere incidenten de jongste maanden is het trouwens moeilijk om daarin nog naïef te blijven.

Die onthullingen geven de indruk dat de gebeurtenissen allemaal erg groots zijn en dat alles boven onze hoofden gebeurt. Toch mag dat er niet toe leiden dat wij als overheid van een klein land de handdoek in de ring gooien. Ook met beperkte middelen denk ik dat wij weerwerk moeten en kunnen bieden, onder andere door het opdrijven van de strijd tegen economische spionage, door een snellere uitvoering van de cyberstrategie, door een versterking van de bestaande expertisepolen.

Op 4 december raakte bekend dat het NSA honderden miljoenen gsm's permanent lokaliseert. Het NSA voegde daar in een reactie onmiddellijk aan toe dat het niet om Amerikaanse burgers gaat. Dat vond ik toch een wat vreemde reactie, alsof er een dubbele moraal wordt gehanteerd met verschillende regels voor Amerikaanse dan wel Europese burgers. Het lijkt ons onaanvaardbaar dat de Verenigde Staten aan Europese burgers grondrechten ontzeggen die blijkbaar wel aan Amerikaanse burgers toegezegd worden. Dat lijkt mij al een fundamentele beschouwing om nog even bij te blijven stilstaan.

Vlaanderen is een kenniseconomie. Het internet is omnipresent in iedere onderneming en in ieder huishouden. Meer dan ooit moet de overheid ondernemingen en ook burgers sensibiliseren omtrent spionage, industriële spionage en zo verder. Meer dan ooit moet iedere inwoner doordrongen zijn van de noodzaak van internetveiligheid. Dat geldt, zoals ik al zei, zeker ook voor mijzelf.

Op 5 september jongstleden deed Rudi Thomaes nog een opvallende uitspraak. Op een studiedag van het ICRI over internetveiligheid stelde hij dat Franse, Amerikaanse en Chinese inlichtingendiensten ook bij ons aan industriële spionage doen. Als iemand van zijn kaliber dat stelt op een studiedag, dan mogen we daar volgens mij ook niet zomaar aan voorbijgaan.

Bij die spionage wordt ook gebruikgemaakt van technologie die bijna iedereen op zijn toestellen heeft staan. Het NSA maakt bijvoorbeeld gebruik van specifieke onderdelen van Microsoftsoftware en het Chinees bedrijf Huawei, waarop onze mobiele telecomnetwerken trouwens zijn gebouwd, geeft publiek toe dat er achterpoorten ingebouwd worden.

Dit zijn allemaal verontrustende berichten. In diezelfde periode stelde Belgacom nochtans dat er geen probleem was met de beveiliging van haar netwerken.

Ondertussen, u heeft dit daarstraks ook aangehaald, is Belgacom van koers veranderd en heeft het klacht ingediend tegen onbekenden wegens de incidenten van eind augustus. Al die incidenten hebben ons ertoe

gebracht om alvast een wetsvoorstel klaar te stomen om de meldingsplicht van veiligheidsincidenten uit te breiden tot alle sectoren en het toezicht hierop te verstrengen.

Wanneer iemand zijn privacy te grabbel werd gegooid, heeft hij immers het recht om zo snel mogelijk te worden geïnformeerd zodat hij maatregelen kan nemen. Wanneer bijvoorbeeld paswoorden of pincodes worden gestolen via cybercriminaliteit is het goed dat de betrokkenen dat zo snel mogelijk weten. Vandaag is enkel de telecomsector verplicht om dergelijke incidenten te melden. Wij willen dit met ons wetsvoorstel uitbreiden tot andere sectoren.

Internetveiligheid gaat ook niet alleen over spionage door staten of veiligheidsdiensten. Het gaat over het bestrijden van diefstal van persoonsgegevens, identiteitsdiefstal, malafide privé-detectives, fraudeurs, georganiseerde misdaad enzovoort.

Is er de voorbije jaren niets gebeurd? In 2009 werd, onder andere op vraag van onze fractie, het CERT, het Computer Emergency Response Team in het leven geroepen. In 2011 bespraken we hier de wetgeving inzake kritische infrastructuur. In 2012 werd daarenboven een cyberstrategie afgesproken. U heeft hier ook naar verwezen.

De uitwerking van een cyberstrategie staat ondertussen bijna twee jaar in de steigers. Wij menen dat ter zake toch wel een versnelling mogelijk en noodzakelijk is. In Nederland is men ondertussen al aan zijn tweede cybersecurity strategie. Wij pleiten ervoor om de private sector hierbij te betrekken.

Wij hebben de indruk dat de uitwerking van de strategie en het overleg ter zake via BelNIS hoofdzakelijk een overheidsgebeuren blijft. Wij menen dat de private sector, naar analogie van wat er gebeurt in de buurlanden, ook moet participeren met mensen en vooral ook met knowhow.

U kondigde ook aan om een nieuw agentschap, het CCSB, op te richten en hiervoor een directeur en een adjunct-directeur te zullen benoemen. Ik meen dat wij de voor- en nadelen goed moeten afwegen alvorens te kiezen voor een nieuwe aparte structuur.

Als wij bekijken wie er vandaag allemaal bezig is met cybersecurity dan is dat een hele waslijst. Er is de Federal Computer Crime Unit bij de internetpolitie. Daarnaast zijn er ook nog de privacycommissie, de telecomregulator, het CERT, Fedict, Belnet, het Belgian Cybercrime Centre, het Crisiscentrum, de Veiligheid van de Staat, de militaire inlichtingendienst ADIV, de Belgische accreditatie-instelling BELAC en BeSaCC.

Kortom, een hele waslijst aan instellingen die met dit thema bezig zijn. De vraag is dan ook of daar nog eens een nieuwe instelling bij moet komen, dan wel of wij naar manieren moeten zoeken om de bestaande expertise te versterken en samen te voegen? Ik denk dat daar voldoende zal moeten worden over nagedacht.

Mijnheer de voorzitter, naast deze beschouwingen en commentaren heb ik nog twee meer specifieke vragen naar aanleiding van het incident met het NSA.

Duitsland heeft erg fel gereageerd naar aanleiding van die spionageberichtgeving. De eerste minister heeft toen gezegd dat er in dialoog moet worden getreden met de VS over die spionage tussen bondgenoten. Mijnheer de eerste minister, heeft die dialoog ondertussen ook plaatsgevonden? Wat is de stand van zaken? Wat zijn de mogelijke conclusies?

Een tweede vraag gaat over de aangekondigde cyberstrategie. Hoe ziet het tijdschema van die cyberstrategie eruit? Wanneer mogen wij daar concrete elementen verwachten?Waaraan zullen de extra middelen die in het vooruitzicht werden gesteld, precies worden besteed?

01.08 **Bruno Tuybens** (sp.a): Mijnheer de voorzitter, er is door de collega's al heel wat gezegd. Ik zal mij dan ook beperken tot één opmerking en één vraag.

Mijnheer de eerste minister, wij waren gechoqueerd door de mediaberichten. Wij zijn niet allemaal grote experten ter zake, maar het is evident dat wij allemaal aanvoelen dat die problematiek moet worden aangepakt. Nadat wij de berichten van Edward Snowden hoorden over de acties van het NSA, bleek Amerika zich zeer cynisch op te stellen, tot er vanuit Duitsland een snauw kwam, toen werd bekendgemaakt dat de gsm van uw collega Merkel werd afgeluisterd. De Amerikaanse overheid heeft daarop wat

ingebonden. Ik het gevoel dat sindsdien de Amerikaanse president de nodige maatregelen heeft genomen om de overdrijvingen – want dat zijn het uiteraard – in te perken.

Ik wil echter waarschuwen voor een aspect dat misschien onvoldoende naar voren is gekomen. Een vergelijking met 9/11 is misschien oneerbiedig omdat bij die aanslag 3 000 doden vielen, wat uiteraard een gruwel was, maar de administratie van Bush heeft er na 9/11 wel voor gekozen om in de strijd tegen het terrorisme bijzonder veel grondrechten uit te hollen en de burgerrechten in te perken. Dat had zeer veel impact op vele miljoenen mensen. Het belang van het recht op privacy komt te weinig aan bod. De waarde ervan wordt onderschat. Het is voor de vrijheid van de burgers en de bedrijven heel erg belangrijk om op die privacy te kunnen rekenen. Wij moeten ongehinderd kunnen blijven werken.

Voor mij, mijnheer de eerste minister, is er geen verschil tussen privacy en veiligheid. Privacy moet niet tegenover veiligheid geplaatst worden. Iedereen heeft het recht op privacy, maar evenzeer op veiligheid. Dat wil dus zeggen dat wij onze samenleving moeten organiseren op een zodanige wijze dat iedereen zich veilig voelt en zich tegelijkertijd toch vrij kan voelen. Dat betekent ook dat wij daarin sterk moeten investeren.

Zoals door collega's gezegd is 10 miljoen euro misschien een eerste start, maar onze inspanningen moeten verder reiken, niet als dusdanig budgettair, maar wel wat de uitkomst en timing betreft. Die vragen zijn gesteld.

Er is sprake van spionage ten aanzien van publieke overheden, alsook van industriële spionage. Mijn vraag is dus ook op welke wijze het bedrijfsleven hierbij wordt betrokken? Het bedrijfsleven is zelf vragende partij. Ik kan mij niet anders indenken dan dat het bedrijfsleven zelf vragende partij is om mee dat veiligheidscordon op te zetten. Indien ons land onvoldoende vooruitgang boekt of misschien niet makkelijk de vooropgestelde timing kan realiseren, moet er misschien een tandje worden bijgestoken.

Ik ben ervan overtuigd dat het bedrijfsleven zelf daar ook vragende partij voor is, wellicht zelfs om daarin mee te investeren. Het kan dat het bedrijfsleven mee wil investeren in een grotere oefening waarbij overheid en bedrijfsleven samen zoeken naar oplossingen op het vlak van cyberveiligheid.

De overheid moet verschillende rollen spelen, niet alleen moet ze een bewustzijnsbevorderende rol spelen ten aanzien van bedrijven en ondernemingen op het vlak van cyberveiligheid, ze moet ook de verdediger zijn van de cyberveiligheid en een coördinerende rol spelen. Dit laatste dan niet alleen intern ten aanzien van de diverse instellingen die momenteel rond deze problematiek werken, maar ook extern met een coördinerende rol ten opzichte van het bedrijfsleven om zo een sterkere vooruitgang te boeken. Anders zullen wij effectief het slachtoffer blijven van deze aanvallen.

Mijn pleidooi is heel erg duidelijk: in alle maatregelen die worden genomen mogen wij niet dezelfde weg opgaan als Bush na de 9/11-aanslagen door bijzonder sterk in te binden in de grondrechten en de uitholling van de burgerrechten. Dit moeten wij juist niet doen, wij moeten ervoor zorgen dat in alle maatregelen die worden genomen, het zo belangrijke recht op privacy in onze samenleving sterk in het oog wordt gehouden.

01.09 **Tanguy Veys** (VB): Mijnheer de eerste minister, natuurlijk zijn wij blij dat ook de federale regering inspanningen levert, onder andere in het kader van de begrotingsopmaak en de relancemaatregelen. De vraag rijst echter in hoeverre die 10 miljoen euro, die nu naar voren wordt geschoven, volstaat. Ik heb veeleer de indruk dat het hier gaat om een inhaaloperatie, een inhaaloperatie die in feite reeds jaren geleden had moeten gebeuren.

Als ik naar de cijfers kijk, valt het mij toch wel op dat de voorbije jaren het aantal gevallen van cybercriminaliteit in België enorm gestegen is. Wat niet enorm gestegen is, zijn de inspanningen van de overheid om daartegen op te treden. In feite moet men het optreden in drie delen opdelen: ten eerste, preventie; ten tweede, de beveiliging van de infrastructuur, en, ten derde, bestraffing.

Laten wij dan eens kijken naar de cijfers. Er is een hoorzitting geweest in de Senaat over het aantal incidenten. Het was toch wel opvallend dat zowel de vertegenwoordiger van de Federal Computer Crime Unit als de vertegenwoordiger van het CERT onomwonden stelden dat er meer middelen en meer mensen nodig zijn om deze strijd naar behoren te kunnen voeren. Mijnheer de eerste minister, zij stelden dat begin dit jaar, dus nadat uw regering die 10 miljoen ter beschikking had gesteld. Neen, nu nog steeds, anno 2014, kampen zij met tekorten.

Dat gaat over de effectieve strijd tegen cybercriminaliteit. De cijfers spreken daar boekdelen. In september 2013 raakte bekend dat elke maand gemiddeld 334 bedrijven en non-profitorganisaties af te rekenen hebben met cybercriminaliteit. Volgens het CERT liggen die cijfers wellicht nog hoger, omdat veel gevallen nooit worden aangegeven bij het CERT. Opvallend, het CERT zegt dat zijn succes als meldpunt komt door het feit dat het vertrouwelijker werkt dan de politie, dat het laagdrempeliger is. Blijkbaar stapt men sneller naar het CERT dan naar de politie. Er schort dan toch iets aan de werking van de politiediensten. Ook daar moet opnieuw aan de vertrouwensband tussen het bedrijfsleven en de non-profitorganisaties worden gewerkt.

Naast de bedrijven worden ook de individuen zelf met internetfraude en cybercriminaliteit geconfronteerd. Op Europees vlak gaat het over een bedrag van 9,5 miljard euro. Ik vermoed dat België daarin ook een belangrijk aandeel heeft. Het bedrag van 10 miljoen euro is dus een peulschil.

Ik laat in het midden of Belgacom zelf in de mailboxen van kritische journalisten of politici zat te snuffelen, dan wel of het NSA in de mailboxen van Belgacom zat te snuffelen, maar dat bedrijf alleen al trekt in 2014 een bedrag van 15 miljoen euro uit om haar eigen netwerken te beveiligen. De federale overheid trekt slechts 10 miljoen euro uit en dan nog gefaseerd, voor het aanwerven van een aantal mensen in 2014 en de komende jaren. Dat is een druppel op een hete plaat, premier.

De inspanningen die u hier thans komt verdedigen en waarvoor sommigen applaudisseren, zijn totaal ontoereikend. In feite is het een lachertje. Ik betreur het dat de regering zo zwaar tekortschiet in de inspanningen met betrekking tot een problematiek die zo pijnlijk aanwezig was als het hacken onder meer van Belgacom, en met grote financiële gevolgen.

Ik kom tot mijn laatste bedenking.

Wij hebben het over beveiliging, preventie, sensibilisatie, enerzijds, en over bestraffing, anderzijds, en op dat laatste schiet ook Justitie zwaar tekort. Minister Turtelboom heeft in diverse antwoorden op vragen duidelijk laten verstaan dat de meeste gevallen van seponering precies gebeuren in dossiers van internetcriminaliteit en cybercriminaliteit. Ik ken meerdere gevallen waarbij personen die van het parket gewoon een brief krijgen met de mededeling dat men niet kan optreden wegens een gebrek aan capaciteit.

Premier, er moet veel meer gebeuren dan het uittrekken van 10 miljoen euro. Zo is bijvoorbeeld ook bij Justitie bijkomend personeel noodzakelijk. Dat heeft ook uw collega Turtelboom begin januari zeer duidelijk gezegd in de commissie. Ik citeer haar: “Gelet op het toenemend belang van het gebruik van internet en de opkomst van nieuwe technologieën stellen de opsporings- en vervolgingsdiensten evenwel duidelijk dat ze op heden ter zake nog over onvoldoende mogelijkheden beschikken, zowel op technisch als op juridisch vlak, inzonderheid om de identificatie, lokalisatie en kennisname van privécommunicatie mogelijk te maken.” Uw eigen regeringsleden zeggen duidelijk dat al wat u hier vandaag komt vertellen ontoereikend is en dat er bijkomende inspanningen moeten gebeuren. Er zijn misschien al inspanningen geleverd, door samenwerking, ook op het vlak van Justitie, zoals in de provincie Oost-Vlaanderen waar alles inzake informaticacriminaliteit wordt doorgeschoven naar het parket van Dendermonde en in de provincie West-Vlaanderen waar die zaken naar het parket van Veurne gaan. Ook die maatregelen zijn echter ontoereikend.

Het is tijd dat u ingrijpt, mijnheer de premier, en met veel meer over de brug komt dan met 10 miljoen euro.

01.10 **Sabien Lahaye-Battheu** (Open Vld): Mijnheer de premier, ik kom nog kort even tussen namens mijn fractie. Uit de vele tussenkomsten blijkt volgens mij toch wel dat velen zich vragen stellen bij de werkmethode en pleiten voor een zeer efficiënte en meer geïntegreerde aanpak, en voor het opdrijven van het tempo van de werkzaamheden in dit dossier.

Misschien namen wij bij de werkzaamheden in dit huis enigszins een valse start, in die zin dat de hoorzitting vandaag zeer laat komt. Bovendien leveren wij dubbel werk, aangezien in de Senaat al een aantal vergaderingen heeft plaatsgevonden over dit thema. De werkzaamheden staan daar al veel verder dan hier. Dat wou ik toch even opmerken.

Het is bovendien niet de eerste keer dat wij over dit thema een grondig onderzoek willen voeren. Ik verwijs naar het Echelonschandaal van 1998. Daar heeft de Belgische politiek zich destijds ook over gebogen heeft er in 2002 een verslag over opgesteld. Het zou misschien interessant zijn dat verslag van onder het stof te halen en na te gaan welke lessen wij toen hebben getrokken en welke aanbevelingen toen zijn uitgevoerd.

Een aantal leden heeft het al gezegd, de scoop van cybercriminaliteit is te beperkt. Het gaat ook over privacy en over het commercieel aspect. Wij hebben het ter zake bijvoorbeeld over de digitale economie. Persoonsgegevens zijn erg waardevol geworden. In dat verband wil ik toch vermelden dat bepaalde bronnen de waarde van de gegevens van de Europese burgers tegen 2020, dus over zes jaar, op een waarde van één biljoen euro schatten. Het is dus ook een zeer commercieel thema geworden.

Mijnheer de eerste minister, hoe ziet u de wisselwerking tussen het werk binnen de regering en in het Parlement? Volgens mij hebben wij strengere privacywetten nodig die de rechtspositie van de burger beter beschermen tegen de nieuwe technologische mogelijkheden waarover niet alleen de inlichtingen- en de veiligheidsdiensten maar evenzeer de commerciële ondernemingen beschikken. Het wordt dus een delicate evenwichtsoefening.

Mijnheer de eerste minister, u had het over de oprichting van een centrum voor cybersecurity waarvoor de regering een bedrag van 10 miljoen euro heeft uitgetrokken. Als ik het goed heb begrepen, zou het centrum zelf 1,3 miljoen euro kosten. Kunt u specificeren waaraan het resterend bedrag van 8,7 miljoen euro dan zal worden besteed?

Ik sluit mij aan bij de vragen van andere leden over het al dan niet samensporen van de Belgische cyberstrategie met de strategie van Europa en van de NAVO. Wij zijn geen eiland. Het is dan ook belangrijk dat wij op dit punt hetzelfde spoor als Europa en de NAVO bewandelen. Is zulks het geval of moet daaraan nog worden gewerkt? Zijn er ter zake nog veel verschillen?

Last but not least is er het feit dat met de privésector zeer nuttig, efficiënt en kostenbesparend zou kunnen worden samengewerkt. Wat is uw mening over deze piste? Wat zult u op dat vlak ondernemen?

01.11 **Bert Schoofs** (VB): Mijnheer de eerste minister, ik sluit mij aan bij de vragen van collega Veys en herinner eraan dat ik er destijds al bij was toen minister Verwilghen hier zijn *magnum opus* inzake cybercriminaliteit presenteerde. Dat was een zeer goede wet, die vandaag trouwens nog een zeer nuttig instrument is. Zij is zeker geen juridisch archaïsme.

Gelet op de vlucht die de technologie intussen heeft genomen, weten wij echter dat het instrument zeker niet voldoende is om alles aan te pakken wat op ons afkomt via de elektronische snelweg.

De problematiek van het NSA is maar het topje van de ijsberg, meen ik. In de Verenigde Staten zijn veel meer *intelligence agencies* werkzaam, die gelijkaardige operaties uitvoeren als het NSA. Soms vraag ik mij af of de president van de Verenigde Staten zelf wel weet wat er allemaal gebeurt binnen zijn diensten. Zo zijn er National Geospatial Intelligence Agency, National Reconnaissance Office, National Security Agency, Defense Intelligence Agency. Een twintigtal instanties ziet toe op alle Amerikaanse belangen in de wereld, die beschermd moeten worden.

Met de Verenigde Staten valt toch nog enigszins te onderhandelen. Maar ook criminele en terroristische organisaties proberen het web te gebruiken om hun activiteiten te ontplooien. Er is dus reden tot ongerustheid.

De Belgacomintrusie was zoals gezegd maar één punt. Ik vraag mij af wat het *dark number* is en welke pogingen men doet om dat *dark number* bloot te leggen. Sommige firma's die aangevallen werden, durven dat namelijk met het oog op hun eer en goede naam niet wereldkundig te maken.

Is er nood aan een betere meldingsplicht? Misschien wel, op dat vlak. Doen onze inlichtingendiensten regelmatig audits in samenwerking met gevoelige bedrijven? Doen zij onderzoek naar aanvallen op hun cyberveiligheid? Ik denk dan uiteraard aan de economisch belangrijke spelers, maar ook aan de overheidsdiensten. Hoe systematisch gebeuren onderzoeken naar dergelijke aanvallen?

In elk geval is het vooral belangrijk om criminele en terroristische organisaties aan te pakken. Vandaag schrijft *The Wall Street Journal* dat Amerikaanse bedrijven hinder ondervinden van de acties ondernomen door het NSA. In Frankrijk, Duitsland, Canada en Brazilië wordt gewerkt aan wetgeving en maatregelen die het Amerikaanse bedrijven onrechtstreeks moeilijk maken om handel te drijven en economische activiteiten te ontplooien. Criminele organisaties en terroristen ontsnappen daar natuurlijk aan.

Het is dan ook van belang dat de EU-lidstaten en -instellingen zich niet uit elkaar laten spelen. Ik lees dat Frankrijk en Duitsland maatregelen nemen, maar waar blijft België? Waar blijft België in het hele plaatje, dat samen met de 27 andere EU-lidstaten een virtueel rakettenschild moet opbouwen om ervoor te zorgen dat onze belangen in Europa gevrijwaard blijven?

01.12 **Elio Di Rupo,** premier ministre: Chers collègues, tout d'abord, je voudrais vous remercier pour l'intérêt que vous portez au sujet et pour le fait que vous ayez souhaité m'entendre, ce qui m'honore. Je le fais avec beaucoup de plaisir mais, jusqu'à présent, le premier ministre n'est en aucun cas ministre de tutelle directe d'aucun service concerné. Il pourrait le devenir si le Centre de cybersécurité se met en place ainsi que nous le souhaitons. Dans un deuxième temps, j'estime nécessaire d'adopter une loi générale en la matière et de modifier ou compléter toutes les lois qui concernent les différents départements pour les forcer à fournir les informations nécessaires et répondre aux questions du Centre.

Pour votre information, actuellement, le ministre de la Défense a la responsabilité des services de sûreté militaire avec la défense des intérêts belges à l'étranger et tout ce qui concerne la dimension militaire des cyberattaques ou de défense. La ministre de l'Intérieur est responsable de la police fédérale, sauf pour la partie qui relève de la ministre de la Justice, avec toute une série de tâches spécifiques en termes de cybersécurité. La ministre de la Justice a sous sa responsabilité la Commission de la Protection de la vie privée, la Sûreté de l'État et la partie de la police fédérale chargée des enquêtes. Aux Affaires étrangères, on a le positionnement de la Belgique et l'interaction au niveau de l'OTAN, l'OSCE et la CEE et le ministre de l'Économie s'occupe de l'IBPT, cité par certains membres.

Quoi qu'il en soit, j'imagine que vous avez déjà interpellé chacun des ministres mais il est bon que nous puissions avoir une vue d'ensemble.

Avant de poursuivre dans mes réponses, il va sans dire, mes chers collègues, qu'il n'y a pas de bons espions, d'un côté, et des mauvais, de l'autre. Je ne voudrais pas laisser croire qu'un pays procéderait à de bons espionnages et d'autres à de mauvais espionnages. L'espionnage, c'est l'espionnage; et si on porte atteinte à la vie privée, il va sans dire que c'est inacceptable. Ça me permet de répondre à une question qui apparaît en filigrane de tout ce que vous avez dit: pourquoi certains pays se sont-ils lancés dans ce type d'opérations? Il est clair que la lutte contre le terrorisme reste une priorité absolue. Ne nous voilons pas la face, c'est le danger le plus important que nous courons et il doit rester une priorité absolue. Mais comme l'a dit un honorable membre, on doit trouver le juste équilibre entre la nécessité de combattre le terrorisme par tous les moyens et la protection de la vie privée, dans un pays comme le nôtre, fondamentalement attaché à une telle valeur.

On m'a demandé si j'avais une ligne de conduite ou une stratégie. Bien entendu! Il serait assez dramatique de ne pas en avoir. Mais la question m'a étonné simplement parce que, le 23 novembre 2012, a été mis en ligne, sur le site de la Chancellerie, un document connu de tous qui s'appelle *Cybersecurity Strategy* (la stratégie de cybersécurité). Le ministre du Budget de l'époque avait d'ailleurs, à juste titre, indiqué qu'il n'y avait pas de moyens financiers complémentaires. Ce sont les difficultés budgétaires auxquelles le gouvernement doit faire face qui font qu'il faut parfois des heures de discussion pour économiser un million. Les membres de la majorité le savent parfaitement. Dix millions, ça peut paraître comme une goutte dans l'océan; mais pour ceux qui doivent calculer à cent mille euros près, c'est beaucoup d'argent.

En tout cas, c'est un premier pas, et j'ai beaucoup apprécié d'entendre que j'avais le mérite d'avoir ouvert des perspectives, car c'est vrai.

Ik kom nu tot de vragen over de Kanselarij.

In juli 2012 heb ik een integriteitsanalyse van het IT-netwerk van de Kanselarij gevraagd. Ter herinnering, het kabinet van de eerste minister gebruikt hetzelfde netwerk als zijn administratie, de Kanselarij. Na die analyse hebben wij inbraaksporen en actieve virussen vastgesteld op het netwerk van de Kanselarij, maar niet op dat van het kabinet. Samen met mijn diensten en de diensten van de militaire veiligheid hebben wij de vereiste maatregelen genomen. Dit betekent een verwijdering van de besmette computers, het schoonmaken van het netwerk en het verhogen van het veiligheidsniveau. Ook werd een sensor geïnstalleerd die als alarmsysteem dient. Dat systeem kan het tijdstip van de uitwisselingen op het netwerk controleren.

Destijds heb ik geen klacht ingediend bij de privacycommissie en dat was ik ook niet verplicht. Ik ben echter

van mening veranderd en op 21 oktober 2013 hebben wij een klacht ingediend bij het federaal parket. Die klacht omvat twee IT-aanvallen waarvan de Kanselarij het slachtoffer is geworden. Het gaat om een daad van piraterij die plaatsvond op 16 oktober 2013 en het incident van de zomer van 2013, waarover ik het net had.

De virussen die werden teruggevonden binnen de Kanselarij vertonen grote gelijkenissen met die op het netwerk van Buitenlandse Zaken en zij maken trouwens ook het voorwerp uit van een juridisch onderzoek. Meer bepaald waren de aanvallen van 16 oktober 2013 niet rechtstreeks tegen onze netwerken gericht, maar wel tegen een website die door de ICT-diensten van de Kanselarij wordt gehost.

Ten slotte heb ik ook een klacht ingediend tegen de inbreuk op mijn Facebookaccount. Cybercriminaliteit heeft vele facetten.

Gelet op de aangehaalde elementen heb ik eind oktober 2013 de regeringsleden per brief gevraagd om zelf ook ad-hocmaatregelen te treffen om de integriteit van hun IT-systeem te onderzoeken.

Quant à Belgacom, l'entreprise a identifié un problème dans ses systèmes le 19 juin 2013. Le 20 juin, en fin de journée, Microsoft a alors confirmé l'hypothèse de la présence d'un *malware*, virus de type cheval de Troie.

Des spécialistes externes néerlandais ont été sollicités. Ils sont arrivés sur site le 25 juin pour aider à analyser cette intrusion et déterminer son type, voire son extension.

Vu la complexité de l'attaque, l'analyse s'est déroulée pendant plusieurs semaines avec l'aide des experts belges qui étaient assignés par le parquet fédéral. L'IBPT a été informé le 6 août, alors même que la question du problème de sécurité du réseau de Belgacom n'était toujours pas résolue. J'ai été averti moi-même à la fin du mois d'août. Finalement le travail ainsi réalisé a permis d'opérer un nettoyage du réseau lors du week-end des 14 et 15 septembre 2013. La Commission de la Protection de la vie privée a été informée le 16 septembre.

À ma connaissance, il n'y a pas eu d'effet préjudiciable pour les clients. Je dis bien "à ma connaissance".

Quant aux 15 millions qui ont été cités pour Belgacom, cette somme concerne la gouvernance, l'éducation du personnel, le renforcement de l'architecture IT, le renforcement du système télécoms et la création d'un centre permanent de cyberdéfense interne à l'entreprise.

La question, tout à fait légitime, de savoir ce que l'on faisait avec les 10 millions et avec les personnes engagées, a été posée. En ce qui concerne le recrutement, dix personnes sont engagées pour le centre, dix pour le CERT.be (Computer Security Incident Response Team), dix personnes pour la police fédérale (plus spécifiquement dans la Federal Computer Crime Unit), dix personnes pour la Sûreté militaire, dix personnes pour la Sûreté de l'État, deux pour le SPF Économie et cinq à l'IBPT sur la sécurité des réseaux, l'idée étant que toutes ces personnes travaillent sur une plate-forme commune en synergie avec le Centre belge pour la cybersécurité.

Quelques éléments de réponse encore.

Pour le timing de l'arrêté royal, nous comptons franchir une étape importante d'ici la fin de la législature. Le texte devra passer devant le Conseil d'État; à son retour, il pourra être avalisé par le Conseil des ministres.

Quant à l'aspect législatif, je vous ai fait part de mon sentiment. Comme vous, je pense qu'il conviendra de légiférer; vous en avez déjà longuement débattu d'ailleurs. À cet égard, le débat sera particulièrement vaste.

Certains se sont demandé s'il ne suffisait pas d'améliorer une loi existante, comme celle sur la protection de la vie privée, par exemple. Il est tout à fait légitime de se poser cette question dans le cadre d'une telle discussion. Je m'attends donc à ce que, tout naturellement, le débat parlementaire soit très ouvert pour permettre de prendre diverses dispositions. Il conviendra, selon moi, de travailler à la fois sur des dispositions nouvelles, mais aussi sur les dispositions existantes, ce qui prendra du temps.

Vous l'avez souligné, je suis intervenu avec force aux Nations unies sur ce sujet. De fait, je pense, comme la présidente du Brésil, que l'idéal serait la création d'un traité international, vu le sujet. Je comprends l'émotion

qu'il suscite dans notre pays, qui connaît d'autres problèmes, mais la Belgique n'est pas le seul pays concerné. Or l'horizon prévu pour l'avancement d'un traité aux Nations unies est toujours éloigné: cela prendra du temps, mais nous continuerons à le revendiquer.

En revanche, je puis rassurer davantage sur les capacités au niveau européen: en théorie, l'Union européenne pourrait agir avec efficacité. Dans la pratique, d'après mon expérience des sommets européens, il serait exagéré de dénoncer 28 points de vue, mais au moins le fait que pas un seul point de vue n'est partagé.

J'ai assisté, lors de la discussion sur le sujet, à des déclarations exprimant plus que des nuances d'un pays à l'autre. D'une manière générale, ce sont des sujets sur lesquels les responsables parlent à *mezza voce* – il n'est pas nécessaire de vous traduire cette expression. Je ne crois donc pas que nous aurons demain ou dans des délais courts une attitude européenne.

En revanche, il existe une initiative allemande et française à laquelle j'ai demandé que nos services soient associés. Les services travaillent entre eux. Il est vrai que par rapport aux services du renseignement américain comme par rapport à tous les autres services alliés, l'idéal est d'avoir une collaboration pour lutter contre le terrorisme et bien entendu protéger la vie privée de tout un chacun sur le sol américain ou européen.

Pourquoi n'ai-je jamais désigné les Américains, les Chinois, les Britanniques ou je ne sais quel service? Simplement parce que je lis, j'écoute, j'entends, mais je ne dispose d'aucune information de source belge et indiscutable qui me permettrait de dire avec certitude que tel service d'intelligence est à la base de ceci.

Si j'en avais la certitude, je ne me gênerais bien sûr pas pour le dire. Tant que je ne l'ai pas, il me semble que, dans mon rôle de chef de gouvernement, je dois faire preuve de prudence. Nous avons bien quelques idées, mais si je devais vous raconter toutes mes idées, je vous tiendrais plusieurs jours d'affilée, jour et nuit! Ce n'est pas l'objet de nos discussions. Pour le moment, nous n'avons pas de certitudes sur qui fait quoi.

Plusieurs membres ont demandé: quid du privé? Il y a des collaborations avec le privé. Le CERT.be travaille déjà avec le privé. Mais d'une manière générale, le secteur privé n'aime pas du tout être cité et demande la discrétion, voire le secret. Il y a déjà actuellement un travail en collaboration.

Compte tenu de la complexité du niveau d'expertise, je crois que le travail en synergie avec le privé s'impose de lui-même.

Nous n'aurons pas les moyens d'engager tous les experts nécessaires. Il faudra travailler en synergie avec le secteur privé. Des questions concernaient également les simulations en cas de crise. Les services actuels essaient de voir ce que cela peut donner en cas de crise. Les responsables privés et les grandes sociétés privées, elles-mêmes, disposent déjà de simulations à cet égard. Là aussi, si nous avions un centre de coordination …

Een coördinatiecentrum van alle diensten zou een simulatie gemakkelijker maken.

Monsieur le président, il me semble avoir répondu à l'essentiel des questions. Je reste bien entendu à votre disposition.

De **voorzitter**: Zijn er collega's die nog iets willen toevoegen?

Monsieur Dallemagne, vous avez la parole.

01.13 **Georges Dallemagne** (cdH): Monsieur le premier ministre, je vous remercie pour ces informations complémentaires qui donnent une vision plus précise des moyens qui seront affectés à ce travail extrêmement important. Je partage évidemment l'objectif de lutte contre le terrorisme. De nombreuses actions menées contre des citoyens et des entreprises sont évidemment totalement en dehors de cet objectif et ne répondent absolument pas à ces préoccupations. Même dans le cadre de la lutte contre le terrorisme, il faut continuer à se battre pour un État de droit. J'estime qu'il y a eu des atteintes à cet État de droit.

Pour ce qui est des moyens, je suis un peu inquiet de voir des moyens qui ont l'air de répondre davantage à une préoccupation de répartition politique plutôt qu'à des besoins réels dans chacun des départements. Une

quinzaine d'organes travaillent aujourd'hui. Il est important d'avoir un centre très fort qui puisse recevoir toutes les informations, les coordonner et donner les impulsions nécessaires. Cela me paraît extrêmement important. Or, j'ai parfois l'impression qu'on se partage un peu la pénurie. C'est pourquoi c'est difficile aujourd'hui sur le plan des ressources financières. Finalement, chaque département aurait probablement des besoins beaucoup plus importants, surtout ce centre pour la cybersécurité.

Comme vous l'avez souligné, il est important que notre parlement continue à se saisir de ce dossier de manière régulière. J'ai déposé une résolution et j'entends que d'autres collègues ont également pris des initiatives.

Madame la présidente, monsieur le président, il sera très important de voir quelles suites nous pouvons donner à ces travaux. Je ne suis pas tout à fait rassuré sur les nouvelles dispositions américaines. J'aurais trouvé intéressant que nous puissions rencontrer l'ambassadrice des États-Unis pour qu'elle puisse nous dire ce qu'elle a fait et ce qu'elle ne fera plus à l'égard des intérêts de notre pays.

01.14 **Karolien Grosemans** (N-VA): Mijnheer de premier, ik dank u voor uw antwoorden, al heb ik weinig antwoorden gekregen op mijn concrete vragen en vragen van militaire aard in verband met de staatsveiligheid. Ik zal uiteraard niet al mijn vragen herhalen in de hoop alsnog een antwoord te krijgen.

Ik wil wel nog even ingaan op een drietal elementen.

Ten eerste, ik dank u voor het overzicht van het personeelsverloop. Wat echter veel belangrijker is, is de vraag hoe u dit personeel zult houden. Wij weten immers allemaal dat betrokkenen een zeer goede opleiding krijgen bij Defensie, maar dat zij daarna weggaan omdat het veel winstgevender is om in de privésector te werken. U zult betrokkenen als het ware aan de ketting moeten leggen om hen daar te houden. Dat is de realiteit. U kunt dan wel 50 tot 75 personen aannemen, maar ik geef u op een blaadje dat zij binnen de kortste keren verdwenen zijn. Ik hoop dat er wordt nagedacht over een manier om die mensen ter plaatse te houden. Om die reden verwees ik ook naar een samenwerking met de bedrijfswereld.

Ten tweede, de ADIV is wettelijk bevoegd om te reageren op een cyberaanval. Als de dienst een cyberaanval ontdekt, mag hij zelf een cyberaanval lanceren. Hoe vaak heeft de dienst dit recht als aangewend? Het is belangrijk dat u op die vraag antwoordt en ik hoop dat u het antwoord kent.

Ten derde, wat is er al in het werk is gesteld om te voorkomen dat bijvoorbeeld een elektriciteitsnetwerk wordt uitgeschakeld? U had het over simulatieoefeningen en dat zou ons dan moeten geruststellen.

Mijnheer de premier, de uitdagingen op het vlak van de cyberveiligheid zijn enorm, maar ik heb de indruk dat er voornamelijk op papier een aantal maatregelen wordt genomen. Er zijn allerhande overlegplatformen, er is een witboek Informatieveiligheid, er zijn een aantal strategieën en er wordt vooral heel veel gepraat. Ik zie een heel zelfgenoegzame regering die het eigen beleid bejubelt. Ik meen echter dat dit getuigt van een enorme wereldvreemdheid.

Het doet mij denken aan collega Landuyt die een jaar geleden zei dat spionnetje spelen een spielerei was van de staatsveiligheid en dat dit niet meer van deze tijd is. Maanden later kaartte Edward Snowdon de problematiek aan met zijn onthulling, en werden wij op de hoogte gebracht.

De problematiek is veel te belangrijk om enkel op papier maatregelen te nemen. Het is belangrijk om meer operationeel te worden en om nu te handelen. Wij moeten dringend gas geven op twee vlakken.

Ten eerste, er moet worden gewerkt aan de creativiteit en de samenwerking tussen de privésector en het publiek. Alleen kunnen wij het niet. Ik verwijs opnieuw naar de 150 cyberreservisten die Nederland heel gericht kan inzetten. Ik vroeg of dat een denkpiste was, maar ik heb daar geen antwoord op gekregen.

Ten tweede, 10 miljoen euro is echt een druppel op een hete plaat.

01.15 **Denis Ducarme** (MR): Je voudrais vraiment remercier le premier ministre pour sa présence et le temps consacré à cet échange sur ce dossier extrêmement important.

Monsieur le premier ministre, vous parliez des ministres responsables dans ce dossier mais ce n'est pas un hasard si le 17 décembre 2012, le Conseil vous chargeait de coordonner la mise en œuvre de cette

stratégie.

Si vous coordonnez cette stratégie, il était naturellement utile que ce soit avec vous que nous ayons ce débat. Si j'ai bien compris, la stratégie est celle de ce document publié le 18 décembre 2012. Nous dégageons 10 millions d'euros qui nous permettent de prendre un certain nombre d'engagements. Des dispositions nouvelles seront prises dans le cadre d'arrêtés royaux actuellement débattus en réunions intercabinet. Voilà où nous en sommes dans ce dossier. Nous restons sur la même ligne que celle décrite en 2012, et tout cela est très bien.

Il est important que nous puissions utiliser les outils qui existent à l'échelle internationale. Je pense que l'Agence européenne de cybersécurité peut vraiment être une source d'impulsion nouvelle en la matière. L'agence de l'OTAN qui traite de la question de la cybermenace et du cyberespionnage peut aussi nous voir davantage travailler collectivement pour, solidairement, nous protéger.

J'ai entendu M. Dallemagne nous indiquer qu'il prendrait un certain nombre d'initiatives au sujet de la coopération internationale. Nous nous permettrons également d'en prendre, pour étoffer cette stratégie déterminée en 2012.

01.16 **Isabelle Emmery** (PS): Monsieur le président, pour ma part, à ce stade du débat qui est intéressant mais dont les détails doivent encore être précisés, je pense qu'il serait nécessaire de dessiner le contour de nos futurs travaux. Dans ce cadre, je formulerai la proposition suivante. Il existe, au sein de cette assemblée, un comité chargé des questions scientifiques et technologiques. Je vous proposerai de le transformer en une sous-commission chargée de cybersécurité, d'économie numérique et de protection de la vie privée. Le comité auquel je fais référence a, sous cette législature, énormément traité de questions de vie privée liées aux nouvelles technologies. Je pense qu'il serait l'outil et l'instrument adéquat pour le futur de nos travaux. Ma proposition est de soumettre cela le plus rapidement possible à la Conférence des présidents.

01.17 **Ronny Balcaen** (Ecolo-Groen): Monsieur le président, bien sûr il y a la menace terroriste et il faut la prendre en compte. Dans la recherche d'un équilibre entre la lutte contre le terrorisme et le respect de la vie privée et de toute une série de droits fondamentaux, il y a évidemment un principe de proportionnalité qui doit jouer. Aujourd'hui, ce principe ne joue absolument pas. En raison d'une lutte justifiée contre la menace terroriste ou sous prétexte de cette lutte, on assiste aujourd'hui à une remise en cause fondamentale de nos droits et de notre droit à la vie privée. Il y a aussi une préoccupation d'efficacité. J'ai lu des rapports disant qu'à ce stade, la NSA était incapable de justifier les mesures prises en regard de résultats dans la lutte contre le terrorisme. Je pense que nous devons être particulièrement attentifs à ce point-là.

Monsieur le premier ministre, vous avez dit que pour le moment, nous n'avons pas de certitude sur qui a fait quoi en matière d'attaque, d'intrusion. Je pense qu'on ne peut pas rester sur ce constat. Il est peut-être justifié aujourd'hui mais il serait tout à fait insupportable de ne jamais connaître ceux qui ont perpétré les actes dont nous avons parlé aujourd'hui.

Je suis donc tout à fait d'accord avec l'ensemble des collègues sur le fait qu'il faille continuer à investiguer sur des atteintes à notre souveraineté nationale, au respect de la vie privée, notamment par les puissances étrangères, et qui concernent aussi nos intérêts économiques et ceux de nos entreprises. Le Parlement doit travailler et il nous semble que c'est au travers d'une prochaine commission d'enquête que nous pourrons faire la lumière sur ce qui s'est passé et rédiger des recommandations utiles pour l'avenir.

De **voorzitter**: Misschien kunnen wij het hierbij laten. Ik meen trouwens te weten dat u elders naartoe moet, mijnheer de eerste minister, al wil ik niemand beletten om nog iets toe te voegen.

Mijnheer Schoofs, u hebt het woord.

01.18 **Bert Schoofs** (VB): Mijnheer de eerste minister, er ontbrak vandaag misschien nog een commissie, met name de commissie voor de Buitenlandse Betrekkingen, want wij hebben relatief weinig gehoord over wat er binnen de EU gaande is en hoe de EU kan repliceren.

Als men weet dat het NSA werkt met 75 000 personeelsleden en een budget van 48 miljard dollar, als ik mij niet vergis, dan blijkt dat Europa op dat vlak ontstellend zwak staat. Wij kunnen daarop weinig riposteren. Dat is — naast de reeds genoemde pijnpunten — zeker een nog pijnpunt, niet alleen in dit land, maar in de

hele EU.

Dat debat moeten wij misschien een andere keer voeren.

Het incident is gesloten.
L'incident est clos.

De openbare commissievergadering wordt gesloten om 16.14 uur.
La réunion publique de commission est levée à 16.14 heures.