854/3

Benelux Interparlementaire Assemblee

13 juni 2015

ANTWOORD

van het Comité van Ministers op de aanbeveling over cybersecurity (doc. 854/2)

Assemblée Interparlementaire Benelux

13 juin 2015

RÉPONSE

du Comité de Ministres à la recommandation concernant la cybersécurité (doc. 854/2)

VAST SECRETARIAAT
VAN DE BENELUX INTERPARLEMENTAIRE
ASSEMBLEE — PALEIS DER NATIE — BRUSSEL

SECRETARIAT PERMANENT
DE L' ASSEMBLÉE INTERPARLEMENTAIRE
BENELUX — PALAIS DE LA NATION — BRUXELLES

Het Comité van Ministers is verheugd over de belangstelling van uw Raad voor het cyberveiligheidsvraagstuk en acht uw Aanbeveling volstrekt relevant.

Immers, cyberspace levert weliswaar ontzettend veel voordelen op, maar maakt ons ook kwetsbaar voor cybercriminaliteit. Welnu, deze criminaliteit, die zeer vaak het werk is van aanvallers van buitenaf, is aan een spectaculaire opmars bezig en treft zowel economische, financiële, maatschappelijke als militaire belangen.

Bijgevolg vormen de beveiliging van informatie- en communicatietechnologie en vitale infrastructuur, alsook de bescherming van persoonsgegevens één van de grootste uitdagingen van deze tijd.

Het is aan ieder land om daar zo snel mogelijk op in te spelen en beslissingen te nemen over het adequate veiligheidsniveau.

De landen ontwikkelen daartoe een algemene strategie inzake cyberveiligheid, richten *Cyber Security Boards* op en stellen *Computer Emergency Response Teams* (CERT's) in:

— In Luxemburg ressorteert cyberveiligheid onder het *Ministère d'État* en het ministerie van Economische Zaken. Dienaangaande heeft de regering in 2011 besloten om een landelijke strategie op te zetten waarvan de totstandbrenging, uitvoering en opvolging behoren tot de taken van een comité, de *Cyber Security Board*, dat onder het gezag van de premier opereert en uit vertegenwoordigers van de betrokken ministeries bestaat.

— In Nederland steunt de strategie inzake cybercriminaliteit op een integrale aanpak, met de medewerking van een brede waaier van publieke en private actoren, kennisinstellingen en maatschappelijke organisaties. Het Nationaal Cyber Security Centrum (NCSC), dat op 1 januari 2012 de deuren opende, vormt een centraal onderdeel van deze strategie. Het centrum opereert onder het gezag van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), die onder de minister van Veiligheid en Justitie ressorteert.

Le Comité de Ministres se félicite de l'intérêt que votre Conseil porte à la problématique de la cybersécurité et juge votre Recommandation tout à fait pertinente.

En effet, si le cyberespace offre énormément d'avantages, il rend aussi fort vulnérable face à la criminalité électronique. Or celle-ci, bien souvent portée par des assaillants externes, connait un essor spectaculaire et touche des intérêts tant économiques, financiers, sociaux que militaires.

Dès lors, la sécurité des technologies de l'information et de la communication, la protection des infrastructures vitales ainsi que la protection des données à caractère personnel représentent un des défis actuels majeurs.

Il appartient à chaque pays d'y réagir le plus vite possible et de décider du niveau adéquat de sécurité.

À cet effet, les pays développent des stratégies globales en matière de cybersécurité, mettent en place des *Cyber Security Board* et créent des *Computer Emergency Response Teams* (CERT):

— Au Luxembourg, la cybersécurité relève de la compétence du Minsitère d'État ainsi que du Ministère de l'Économie. Dans ce domaine, le gouvernement a décidé en 2011 de la mise en place d'une stratégie nationale dont l'élaboration, la mise en œuvre ainsi que son suivi relèvent d'un comité, le *Cyber Security Board*, fonctionnant sous l'autorité du Premier ministre et composé de représentants des ministères concernés.

— Aux Pays-Bas, la stratégie en matière de cybercriminalité est fondée sur une approche intégrale, avec le concours d'un vaste éventail d'acteurs publics et privés, d'organismes de connaissances et d'organisations sociales. Le "*Nationaal Cyber Security Centrum* (NCSC)" qui a ouvert ses portes au 1er janvier 2012 constitue un élément central de cette stratégie. Le centre fonctionne sous l'autorité du Coordinateur national de lutte contre le terrorisme et la sécurité (NCTV) qui dépend du ministre de la Justice et de la Sécurité.

— In België is de regering momenteel doende met het instellen van het Centrum voor Cybersecurity België, dat onder meer wordt belast met het concretiseren, onder de auspiciën van de eerste minister, van de Belgische cyberstrategie.

Bovendien worden er in Europees en internationaal verband heel wat initiatieven ontplooid.

Het spreekt evenwel voor zich dat onze landen, die fysieke grenzen en tal van gemeenschappelijke belangen met elkaar delen, er goed aan doen om nog hechter samen te werken.

In die geest werd op 5 april 2011 een Benelux ministeriële intentieverklaring inzake cyberveiligheid "*Success through Cooperation*" getekend.

Sindsdien kwam er met name een operationele samenwerking tot stand tussen de nationale CERT's van de drie landen. Concreet hebben de hoofden van de nationale CERT's (*Computer Emergency Response Teams*) van de Benelux elkaar begin juni en begin december 2014 ontmoet en afspraken gemaakt over nauwere samenwerking. Eén van de afspraken is betere communicatie en samenwerking tussen de drie overheids-CERT's van de Benelux-landen te bewerkstelligen.

Voorts hebben onze regeringen andermaal te kennen gegeven dat ze op dit terrein willen samenwerken en hebben zij de bestrijding van cybercriminaliteit en de samenwerking op het gebied van cyberveiligheid als specifieke doelstelling opgenomen in het Benelux-jaarplan voor 2015, waarbij het thema veiligheid tevens een van de drie grote prioriteiten is van het huidige Belgische voorzitterschap van de Benelux. In dit verband hechten onze regeringen veel belang aan een publiek-private samenwerkingsaanpak en de medewerking van de academische kringen. Evenzo moedigen zij elk initiatief aan om synergie-effecten te sorteren op het gebied van het operationeel onderzoek voor cyberveiligheid. Uitwisselingen tussen de drie landen in het kader van de nodige updating van cyberstrategieën, met name via gemeenschappelijke analyses van best practices, zullen van pas komen.

— En Belgique, le gouvernement met actuellement en place le "Centre pour la Cybersécurité Belgique" qui aura entre autres pour mission de concrétiser, sous les auspices du Premier ministre, la Cyberstratégie belge.

En outre, de nombreuses initiatives sont prises au niveau européen et international.

Il est néanmoins évident que nos pays qui partagent des frontières physiques et bon nombre d'intérêts communs ont tout intérêt à travailler encore plus étroitement ensemble.

C'est dans cet esprit qu'une Déclaration d'intention ministérielle Benelux sur la cybersécurité fut signée le 5 avril 2011 "*Succes through Cooperation*".

Depuis lors, une coopération opérationnelle s'est notamment nouée entre les CERT nationaux des trois pays. C'est ainsi que les chefs des CERT nationaux (*Computer Emergency Response Teams*) du Benelux se sont rencontrés début juin et début décembre 2014 et ont passé des accords en vue d'une coopération plus étroite. L'un des accords consiste à établir une meilleure communication et coopération entre les trois autorités CERT des pays du Benelux.

Par ailleurs, nos gouvernements ont une nouvelle fois affiché leur volonté de travailler conjointement en la matière en inscrivant la lutte contre la cybercriminalité et la coopération dans le domaine de la cybersécurité comme objectif spécifique du plan annuel Benelux pour 2015, le thème de la sécurité étant aussi l'une des trois priorités majeures de l'actuelle présidence belge du Benelux. À cet égard, nos gouvernements attachent une grande importance à l'approche d'une coopération public-privé et à la collaboration du secteur académique, de même qu'ils encouragent toute initiative favorisant le développement de synergies en matière de recherche opérationnelle pour la cybersécurité. Des échanges entre les trois pays dans le cadre des nécessaires mises à jour des cyberstratégies seront les bienvenus notamment par le biais d'analyses communes des meilleures pratiques.

In die gedachtegang menen wij dat de oprichting van een werkgroep met als doel de Aanbeveling van uw Raad concrete invulling te geven, beslist zinvol is. Wij zullen ook aan de betrokken diensten van onze landen vragen er bijzondere aandacht aan te schenken en een start te maken met de verwezenlijking ervan.

Deze samenwerking, waarbij vooral voorrang moet worden gegeven aan bestaande werkgroepen en diensten, valt volgens ons met name op de volgende thema's te overwegen:

— identificatie van gedeelde risico's/dreigingen;

— inventarisatie en assessment van de infrastructuur en ingezette tools ten behoeve van IT-beveiliging;

— ervaring delen over lacunes in nationale wetgeving;

— analyse van de uitdagingen tussen CERT's en politie;

— informatie-uitwisseling op het gebied van vitale infrastructuur (bedrijven) die een belangrijke positie hebben in de drie Benelux-landen.

Hiermee krijgt de samenwerking die uw Raad voor ogen heeft, stap voor stap invulling. Vanwege de complexiteit van cyberveiligheid, zowel juridisch, als operationeel, beleidsmatig en tactisch, is dit echter een proces van de lange adem. Daarom wordt om uw begrip gevraagd voor het feit dat hier meer tijd voor nodig zal zijn. Niet in de laatste plaats door de Brusselse werkelijkheid en de hoeveelheid werk die vanuit de EU op de Benelux-landen afkomt.

Dans cette logique, nous estimons qu'un groupe de travail peut certainement être mis en place dans le but de concrétiser la Recommandation de votre Conseil. Nous demanderons aussi aux services concernés de nos pays d'y être particulièrement attentifs et de s'atteler à sa réalisation.

Il nous semble que cette coopération, qui doit surtout privilégier les groupes de travail et services existants, peut notamment être envisagée sur les thèmes suivants:

— l'identification des risques et menaces partagés;

— l'inventaire et l'évaluation des infrastructures et des outils mis en place pour sécuriser l'informatique;

— le partage d'expériences sur les lacunes dans les législations nationales;

— l'analyse des défis entre les CERT et la police.

— l'échange d'informations dans le domaine des infrastructures vitales (entreprises) qui occupent une place importante dans les trois pays du Benelux.

De cette manière, la coopération voulue par votre Conseil se concrétisera pas à pas. Vu la complexité de la cybersécurité, que ce soit au niveau juridique comme opérationnel, stratégique et tactique, c'est toutefois un processus de longue haleine. C'est pourquoi il convient de vous montrer compréhensif pour le fait qu'un temps plus long sera nécessaire à cette fin, sans oublier la réalité de Bruxelles et la quantité de travail que l'UE déverse sur les pays du Benelux.