776/1

RAADGEVENDE INTERPARLEMENTAIRE BENELUXRAAD

21 april 2008

CONFERENTIE VAN 29 FEBRUARI 2008 IN TALLIN

Bedreiging van het Internet

CONSEIL INTERPARLEMENTAIRE CONSULTATIF DE BENELUX

21 avril 2008

CONFÉRENCE DU 29 FÉVRIER 2008 À TALLIN

La menace de l'internet

VAST SECRETARIAAT
VAN DE INTERPARLEMENTAIRE BENELUXRAAD
PALEIS DER NATIE — BRUSSEL

SECRETARIAT PERMANENT
DU CONSEIL INTERPARLEMENTAIRE DE BENELUX
PALAIS DE LA NATION — BRUXELLES

Op 29 februari 2008 heeft de Baltische Assemblee in Tallinn, Estland, een conferentie georganiseerd onder de titel Bedreiging van het internet *(Threat from the net)*. Aan de conferentie werd deelgenomen door de heren Weekers, Braz en Verougstraete, respectievelijk voorzitter en leden van de Commissie voor Justitie en Openbare Orde. Zij werden bijgestaan door de heren Michiels, secretaris-generaal, en Van Waasbergen, secretaris van de Commissie. Aan de conferentie is ook deelgenomen door een delegatie van de Noordse Raad.

Le 29 février 2008, l'Assemblée balte a organisé à Tallinn (Estonie), une conférence sous le titre «La menace de l'internet» *(Threat from the net)*. Ont participé à la conférence MM. Weekers, Braz et Verougstraete, respectivement président et membres de la commission de la Jstice et de l'Ordre public. Ils ont été assistés de MM. Michiels, secrétaire général, et Van Waasbergen, secrétaire de la commission. Une délégation du Conseil nordique était également présente à la conférence.

Inleiding

Het internet voegt een dimensie aan de wereld toe. De informatiesamenleving is wereldwijd, al zijn de implicaties ervan lokaal. De meeste mensen zijn geneigd de invloed van de informatie- en communicatietechnologie in het algemeen te overschatten en de invloed op henzelf te onderschatten. De dreigingen op het net zijn groot zijn, aanvallen kunnen van velerlei bronnen afkomstig zijn.

In het voorjaar van 2007 vond een aanval via het internet op Estland plaats. Dagen achtereen werden vanuit het buitenland gecoördineerde aanvallen op de computersystemen van ministeries, banken en communicatiemedia uitgevoerd. De aanvallen hebben deze computersystemen platgelegd.

Dergelijke aanvallen zijn niet nieuw. In 1997-1999, ten tijde van de vrijheidsstrijd op Oost-Timor, werd de in Ierland gevestigde webstek van de onafhankelijkheidsbeweging van Oost-Timor platgelegd, naar wordt aangenomen door de Indonesische inlichtingendienst. In 2000-2001 vond waarschijnlijk van Palestijnse zijde een aanval via Berlijn en Londen plaats op het Israelische kadaster, de zogenaamde e-Jihad.

Aanvallen via het internet kunnen ook als aanvulling op andere machtsinstrumenten dienen. Bijvoorbeeld in geval van economische sancties of andere non-militaire middelen zoals in het geval van Estland. Ook als verlengstuk van militair optreden, bij voorbeeld door noodsystemen na bomaanvallen plat te leggen. Gebleken is dat een

Introduction

L'internet ajoute une dimension au monde. La société de l'information est à l'échelle mondiale, même si ses implications sont locales. La plupart des personnes ont tendance à surestimer l'influence des technologies de l'information et de la communication sur le plan général mais à sous-estimer l'influence qu'elles exercent sur eux-mêmes. Les menaces sur le net sont nombreuses et les attaques peuvent venir de sources très diverses

L'Estonie a été victime d'une attaque par l'internet au printemps 2007. Des jours durant, des attaques coordonnées ont été menées depuis l'étranger contre les systèmes informatiques des ministères, des banques et des médias de communication. Ces attaques ont entièrement paralysé ces systèmes informatiques.

De telles attaques ne sont pas une nouveauté. En 1997-1999, à l'époque du combat pour la liberté au Timor oriental, le site internet du mouvement d'indépendance du Timor oriental, hébergé en Irlande, a été détruit semble-t-il par les services de renseignement indonésiens. En 2000-2001, le cadastre israélien, l'e-Jihad, a fait l'objet d'une attaque sans doute menée par des milieux palestiniens, par le biais de Berlin et de Londres.

Les attaques par l'internet peuvent aussi être menées en complément d'autres instruments de pouvoir tels le recours à des sanctions économiques ou à d'autres moyens non militaires, comme pour l'Estonie. Elles peuvent l'être aussi dans le prolongement d'une opération militaire, par exemple pour annihiler les systèmes de secours après une

staat internetaanvallen kan uitvoeren, maar zijn betrokkenheid daarbij kan verhullen.

Probleemstelling

Aanvallen op internet plegen anoniem te zijn. De oorsprong van dreigingen op het net is vaak asymmetrisch. De dreiging kan uitgaan van en zich richten op Staten, organisaties, individuen en samenwerkingsverbanden daartussen.

Grote aanvallen, zoals in het geval van Estland zijn niet talrijk. Kleine aanvallen zijn dat wel en vinden overal en elke dag plaats. De samenleving is niet in staat deze dreigingen het hoofd te bieden. Het internet is letterlijk grenzeloos. Een aanval via het internet kan worden opgezet in land A, gebruik maken van computers in landen B, C en D, en gericht zijn op een doel in land E.

Dergelijke gebeurtenissen roepen vragen op, zoals wie verantwoordelijk is voor wat er op het net gebeurt: is het de Staat, een internetaanbieder, een bedrijf of organisatie, of kan het een individu zijn, misschien zelfs een minderjarige? Wat is als een oorlogshandeling op het internet te beschouwen? Wat is de rol van de Regering? Is die rol gecoördineerd met anderen? Wiens regels gelden? Wie mag «wapens» ontwikkelen en inzetten?

Andere problemen zijn het overbruggen van de kloof tussen politieke en technische deskundigheid, en de weg van onderzoek en analyse naar beleid en actie. Technische experts overheersen bij het onderzoek en de ontwikkeling op het gebied van de internetveiligheid, en de communicatie tussen hun en de politici en beleidsmakers is niet altijd gemakkelijk.

Oplossingsrichting

Enerzijds werd veel verwacht van de verdere ontwikkeling van beveiligingssystemen van netwerken, computers en gebruikers.

attaque au moyen de bombes. Il s'est avéré qu'un Etat peut mener des attaques sur l'internet tout en occultant sa participation.

Problématique

Les attaques sur l'internet sont généralement anonymes. L'origine des menaces sur le net est souvent asymétrique. Les attaques peuvent émaner d'un Etat, d'une organisation, d'individus ou de structures de coopération entre ces acteurs, ou être dirigées contre eux.

Les attaques de grande envergure comme celle menée contre l'Estonie ne sont pas fréquentes. Les petites attaques le sont: elles sont perpétrées quotidiennement et partout. La société n'est pas en mesure de faire face à ces menaces. L'internet ne connaît littéralement pas de frontières. Une attaque par l'internet peut être menée à partir d'un pays A au moyens d'ordinateurs se trouvant dans des pays B, C et D, et viser un objectif dans un pays E.

De tels événements appellent des questions: qui est responsable de ce qui se passe sur le net? Est-ce l'Etat, un hébergeur, une entreprise ou une organisation? Cela peut-il être un individu, éventuellement même un mineur? Que faut-il considérer comme un acte de guerre sur l'internet? Quel est le rôle du gouvernement? Ce rôle est-il coordonné avec d'autres? Quelles règles sont d'application? Qui peut développer et utiliser des «armes»?

Parmi les autres problèmes, il y a le comblement de la fracture entre l'expertise politique et technique, et le trajet qui va de l'étude et de l'analayse à la politique et à l'action. Les experts techniques dominent dans le domaine de l'étude et du développement dans le domaine de la sécurité internet, et la communication entre eux et les politiciens et les décideurs n'est pas toujours facile.

Vers une solution

D'une part, le développement de systèmes de sécurisation de réseaux, d'ordinateurs et d'utilisateurs a suscité de grands espoirs.

Anderzijds wezen velen erop dat oplossingen internationale samenwerking vereisen. Wet- en regelgeving hebben het beginsel van territorialiteit als uitgangspunt. Evenals het internet zelf gaan doelstellingen en instrumenten met het oog op internetveiligheid over de landsgrenzen heen. Om te komen tot een gemeenschappelijke basis voor veiligheidsmaatregelen voor het internet zijn overeenkomsten tussen Staten nodig.

Internetveiligheid is een nieuw terrein voor wet- en regelgeving. Hoewel er al enige jaren internationaal actief en veelomvattend wordt samen gewerkt, is een internationale consensus over de regelgeving die nodig is, nog niet bereikt.

Er waren op de conferentie ook sceptische geluiden te horen i.v.m. de internationale samenwerking met het oog op de bestrijding van internetmisdaad. Die samenwerking zou in veel gevallen niet effectief zijn en in de praktijk weinig opleveren.

Wat doen internationale organisaties?

Verenigde Naties

De Algemene Vergadering van de VN heeft resoluties aangenomen over:

– ontwikkelingen op het gebied van informatie en telecommunicatie in de context van internationale veiligheid;

– het bestrijden van crimineel misbruik van informatietechnologie;

– de creatie van een wereldwijde cultuur van internetveiligheid;

– de creatie van een wereldwijde cultuur van internetveiligheid en de bescherming van cruciale informatie-infrastructuren.

Raad van Europa

De Raad heeft in 2001 een conventie inzake internetcriminaliteit uitgewerkt, die in 2004 van kracht is geworden.

D'autre part, nombreux sont ceux qui estiment que les solutions passeraient par la coopération internationale. La législation et la réglementation sont fondées sur le principe de la territorialité. Comme l'internet lui-même, les objectifs et les instruments tendant à la sécurisation de l'internet ignorent les frontières des pays. Des conventions devraient être conclues entre les Etats pour créer une base commune aux mesures de sécurité.

La sécurité internet est un nouveau terrain pour la législation et la réglementation. Même si une coopération internationale large et active existe depuis quelques années déjà, cette réglementation ne fait pas encore l'objet d'un consensus international.

On a entendu aussi lors de la conférence des manifestations de scepticisme à propos de la coopération internationale dans la lutte contre la criminalité sur l'internet. Dans bien des cas, cette coopération serait inefficace et ne produirait guère de résultats.

Que font les organisation internationales?

Nations Unies

L'Assemblée générale des Nations Unie a adopté des résolutions concernant:

– les développements en matière d'information et de télécommunication dans le contexte de la sécurité internationale;

– la répression de l'usage abusif criminel de la technologie de l'information;

– la création d'une culture mondiale de la sécurité internet;

– la création d'une culture mondiale de la sécurité internet et la protection d'infrastructures de protection cruciales.

Conseil de l'Europe

Le Conseil a rédigé en 2001 une convention sur la criminalité internet qui est entrée en vigueur en 2004.

Europese Unie

De Europese Raad heeft in juni 2004 besloten een beleid te ontwikkelen gericht op de bescherming van de cruciale informatie-infrastructuur. In november 2005 heeft de Europese Commissie een Groenboek met beleidsopties aangenomen. Aan dat boek is bijgedragen door 22 lidstaten en meer dan 100 organisaties van bedrijfstakken. De Europese Commissie heeft in december 2006 een ontwerp-richtlijn inzake de vaststelling van een Europese cruciale informatie-infrastructuur gepubliceerd.

NAVO

Bij de NAVO staat de bestrijding van internetcriminaliteit al 5 jaar op agenda, maar pas sinds de aanval op Estland wordt er echt goed naar gekeken. Men ziet een zekere parallel met de aanvallen van 11 september 2001: een probleem van één NAVO-lidstaat wordt een probleem voor alle lidstaten, en daarenboven zijn zowel de aanvallen van 11 september 2001 als de aanval op Estland problemen sui generis. De bestrijding van internetcriminaliteit leent zich niet voor actie door één organisatie alleen, er is een gezamenlijke actie nodig. Bij de NAVO leeft niet het idee oplossingen aan de lidstaten te kunnen opdringen. Wel is er sinds begin 2008 een internetbeleid, met als doelstelling het ontwikkelen van een gemeenschappelijke benadering van de verdediging tegen aanvallen via het internet en het vergroten van het vermogen van de NAVO systemen van cruciaal belang te beschermen. Overigens is het niet gemakkelijk tot een omschrijving van het begrip cruciaal belang te komen, die door alle 26 lidstaten wordt onderschreven. Hierbij speelt het verschil tussen nationale en collectieve verantwoordelijkheden een rol. De beginselen van subsidiariteit (welk niveau doet wat het beste) en van non-duplicatie zijn daarbij leidend.

Andere organisaties

Ook andere internationale organisaties zijn bezig met de bestrijding van internetcriminaliteit. Genoemd werden de International Telecommunication Union, Interpol, de G8 High Tech Group, en de Organisatie voor Economische Samenwerking en Ontwikkeling.

Union européenne

Le Conseil européen a décidé, en juin 2004, de développer une politique axée sur la protection de l'infrastructure de l'information cruciale. En novembre 2005, la Commission européenne a adopté un Livre vert comportant des options politiques. Ont contribué à ce Livre 22 Etats membres et plus de 100 organisations de branches industrielles. La Commission européenne a publié en décembre 2006 un projet de directive sur la mise en place d'une information de l'infrastructure européenne cruciale.

OTAN

La lutte contre la criminalité internet figure depuis 5 ans déjà à l'ordre du jour de l'OTAN mais ne retient vraiment l'intérêt que depuis l'attaque contre l'Estonie. Un certain parallèle est établi avec les attaques du 11 septembre 2001: un problème rencontré par un membre de l'OTAN devient un problème pour tous les membres et, en outre, tant les attaques du 11 septembre 2001 que l'attaque contre l'Estonie génèrent des problèmes sui generis. La lutte contre la criminalité internet ne se prête pas à des actions mises sur pied par une seule organisation. Il faut une action commune. On ne pense pas, dans le cadre de l'OTAN, pouvoir imposer des solutions aux Etats membres. Il existe toutefois depuis 2008 une politique internet qui vise à développer une approche commune de la protection contre les attaques par le biais de l'internet et du renforcement de la capacité de l'OTAN à protéger les systèmes d'importance cruciale. Il n'est par ailleurs pas facile de fournir de la notion d'importance cruciale une définition qui agrée les 26 Etats membres. La distinction entre les responsabilités nationale et collective joue un rôle à cet égard. Les principes de la subsidiarité, du niveau le plus approprié et de la non-duplication sont à cet égard déterminants.

Autres organisations

D'autres organisation internationales aussi s'occupent de la lutte contre la criminalité internet, tels la International Telecommunication Union, Interpol, le G8 High Tech Group et l'Organisation de coopération et de développement économiques.

Centrale drukkerij – Deze publicatie wordt uitsluitend gedrukt op volledig gerecycleerd papier
Imprimerie centrale – Cette publication est imprimée exclusivement sur du papier entièrement recyclé