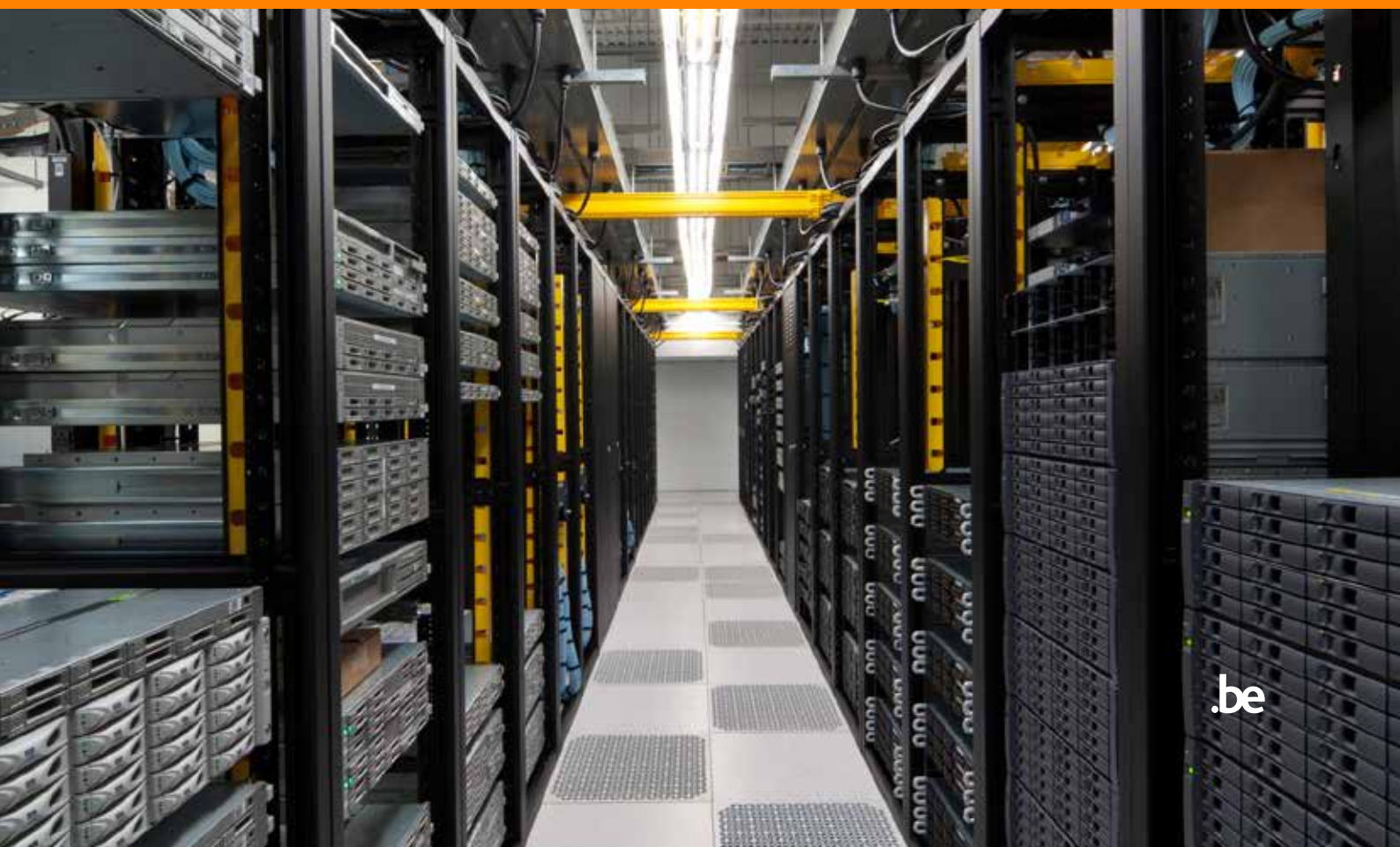
CENTRE FOR
CYBER SECURITY
BELGIUM

CHANCELLERY OF
THE PRIME MINISTER

CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE

/ RAPPORT ANNUEL 2015



INTRODUCTION

2015 fut une année phare pour le Centre pour la Cybersécurité Belgique (CCB) puisque ce fut celle de sa naissance !

L'arrêté royal du 10/10/2014 a ancré la création du CCB sur papier. Cependant, il a fallu attendre le mois d'août 2015 pour que le CCB puisse effectivement s'atteler à l'exercice de ses missions. En effet, c'est en août 2015 que le directeur, Miguel De Bruycker, et la directrice adjointe, Phédra Clouner, ont été nommés pour un mandat de cinq ans.

Ces missions imposées par voie d'arrêté royal sont à la fois ambitieuses et variées : en qualité d'autorité nationale, le CCB est tenu de superviser et de coordonner la politique belge en la matière. Il doit en outre veiller à sa mise en œuvre. Par ailleurs, il sera amené à gérer divers projets en matière de cybersécurité selon une approche intégrée et centralisée, à assurer la coordination entre les services concernés ainsi que les autorités publiques, le secteur privé et le monde scientifique. Le CCB doit formuler des propositions d'adaptation du cadre réglementaire en matière de cybersécurité et assurer la gestion de crise en cas de cyberincidents, en collaboration avec le Centre de coordination et de crise.

Mais ce n'est pas tout : les missions du CCB intègrent aussi l'élaboration, la diffusion et le contrôle de la mise en œuvre de standards, directives et normes de sécurité pour les différents systèmes informatiques des administrations et organismes publics, la coordination de la représentation belge sur les forums internationaux dédiés à la cybersécurité, du suivi des obligations internationales et des propositions relatives à la position nationale en cette matière. Enfin, le CCB coordonne également l'évaluation et la certification de la sécurité des systèmes d'information et de communication et informe les utilisateurs finaux quant aux systèmes d'information et de communication, tout en les y sensibilisant.

C'est pour mener à bien ces missions qu'un plan stratégique a été rédigé. Il servira de fil rouge au fonctionnement du CCB pour les cinq prochaines années. Le plan stratégique épingle des priorités, énumère des objectifs et esquisse un calendrier pour le lancement de projets. Trois grandes phases sont identifiées : une phase de lancement de six mois (octobre 2015-mars 2016), suivie d'une phase de consolidation de trois ans et enfin, une phase de maturité de cinq années. Chacune de ces trois phases est associée à un plan opérationnel distinct, soumis à approbation et sujet à adaptation le cas échéant. Les objectifs liés à ces phases ont aussi été formulés dans le plan stratégique.

Lors de la phase de lancement, le CCB recrutera du personnel et se concentrera sur l'organisation de ses ressources propres. Il dressera aussi un aperçu des cybercapacités existantes en Belgique et élaborera une procédure nationale en cas de cyberattaque, en étroite collaboration avec le Centre de coordination et de crise.

À l'échelle internationale, les premiers contacts ont été pris avec les pays voisins : France, Luxembourg et Pays-Bas. Et ce, en vue d'une collaboration étroite inscrite sur le long terme. La Computer Emergency Response Team (CERT) nationale est placée sous l'administration du CCB et les éventuels chevauchements au niveau des responsabilités des services publics sont supprimés.

C'est au cours de la phase de consolidation consécutive que les projets seront lancés et supervisés. La phase de maturité sera, enfin, l'occasion pour le CCB de tenter de rassembler toutes les pièces lui permettant d'atteindre ses objectifs stratégiques.

Dans ce rapport, nous revenons sur la phase de lancement du CCB. Sept collaborateurs sur les dix prévus ont été recrutés.

Les cyberservices concernés ont été officiellement sondés quant aux capacités existantes en Belgique en matière de cybersécurité. Nous sommes ainsi en mesure de correctement répertorier les capacités actuelles dont dispose la Belgique.

En décembre 2015, le CCB a entamé l'élaboration d'un Cyberplan d'urgence national avec l'ensemble des services concernés. Ce plan d'urgence poursuit comme objectif principal l'organisation d'une structure de réponse aux crises et aux incidents de cybersécurité qui requièrent une coordination ou une gestion au niveau national.

Dans le même temps, les premiers contacts avec les cybercentres étrangers ont été pris. Nous avons présenté le CCB devant les membres du Nationaal Cyber Security Centrum (NCSC) aux Pays-Bas, de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France et du govCERT au Luxembourg ; le but étant de discuter de l'intensification de la coopération à l'avenir.

Pour conclure, nous portons également notre regard sur la phase suivante, à savoir la phase de consolidation. Dans la suite du rapport, le lecteur découvre les futurs projets que le CCB prévoit de lancer. Tandis que le recrutement du personnel touche à sa fin, nombre de projets prévus pour la phase de consolidation sont déjà en chantier. Avec ces projets en ligne de mire, le CCB remplit non seulement les missions qui lui ont été confiées par arrêté royal mais il contribue aussi à la réalisation de l'objectif qu'il s'est lui-même fixé : à l'horizon 2020, faire de la Belgique une sphère de sécurité numérique pour les citoyens et les entreprises.

Bonne lecture !

Miguel De Bruycker

01

INTERVIEW

01

LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE A ÉTÉ FONDÉ PAR L'ARRÊTÉ ROYAL DU 10 OCTOBRE 2014 PORTANT CRÉATION DU CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE. LE 10 AOÛT 2015, MIGUEL DE BRUYCKER ET PHÉDRA CLOUNER ONT RESPECTIVEMENT ÉTÉ DÉSIGNÉS DIRECTEUR ET DIRECTRICE ADJOINTE. DANS CET ENTRETIEN, LES JEUNES DIRECTEURS FONT LE POINT SUR LES SIX PREMIERS MOIS DE VIE DU CENTRE.

AVANT TOUTE CHOSE, FÉLICITATIONS POUR VOTRE NOMINATION ! VOUS AVEZ ÉTÉ INVESTIS D'UNE LOURDE TÂCHE, LA CRÉATION ET LA DIRECTION D'UN NOUVEAU CENTRE N'ÉTANT PAS CHOSE AISÉE. QUELLE A ÉTÉ VOTRE RÉACTION LORSQUE VOUS AVEZ ÉTÉ NOMMÉS POUR PORTER CET AMBITIEUX PROJET ?

Miguel : J'étais avant tout très content de pouvoir m'atteler à cette ambitieuse mission. La cybersécurité est un domaine extrêmement intéressant et je suis donc honoré de pouvoir œuvrer à davantage de cybersécurité en Belgique.

Phédra : Fonder un nouveau centre de A à Z est un défi des plus prenants. Je savais que ce ne serait pas une mince affaire mais j'étais, et je suis toujours, très motivée à l'idée de mener ce projet à bien. La cybersécurité est en effet un domaine vaste en perpétuel changement. De plus, l'intérêt pour la cybersécurité ne fera qu'augmenter ; nous avons donc fort intérêt à pouvoir rapidement anticiper.

AU COURS DES DEUX PREMIERS MOIS, LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE NE COMPTAIT QUE DEUX EMPLOYÉS : VOUS DEUX.

- **Vous connaissiez-vous ?**
  Phédra : le monde du cyber n'est pas très grand en Belgique et j'avais déjà rencontré Miguel plusieurs fois à l'occasion de conférences sur la cybersécurité.
- **Comment s'est passée la collaboration ?**
  Miguel : très bien ! L'une de nos premières missions consistait en l'élaboration du plan stratégique. Nous avons rédigé un plan stratégique ambitieux et l'avons soumis pour approbation au Conseil des ministres. Cette collaboration s'est super bien déroulée !

LA PREMIÈRE MISSION ÉTAIT DE LANCER LES RECRUTEMENTS AFIN DE COMPLÉTER L'ÉQUIPE. ÊTES-VOUS AU COMPLET DÉSORMAIS ?

Miguel : nous avons recruté 7 des 10 collaborateurs prévus. En octobre 2015, nous avons accueilli notre responsable communication et en février 2016 ce sont un chef de projet et un conseiller qui nous ont rejoints. Enfin, en mars 2016, le deuxième chef de projet est arrivé, suivi quelques semaines plus tard par un collaborateur en charge de la coordination de la collaboration académique. La procédure de sélection pour deux offices managers est également clôturée et en juin, un office manager francophone et un office manager

néerlandophone viendront renforcer nos rangs. Dans les mois à venir, nous allons également organiser le recrutement d'un chef de projet en charge de la rédaction et de la diffusion auprès des entreprises des best practices et de *whitepapers*.

LE CCB N'EST PAS UNIQUE EN SON GENRE, PUISQUE D'AUTRES PAYS EUROPÉENS DISPOSENT DÉJÀ DEPUIS QUELQUE TEMPS D'UN CENTRE NATIONAL POUR LA CYBERSÉCURITÉ.

- **La Belgique est-elle en retard par rapport à ses pays voisins en matière de cybersécurité ?**
  Miguel : Il est vrai que les centres nationaux pour la cybersécurité existent depuis plus longtemps déjà chez nos voisins. Mais il serait trop facile de dire que, de ce fait, la Belgique accuse un retard. En effet, plusieurs services publics comme la police, l'armée, la justice et le centre de crise disposent depuis longtemps de départements consacrés à la cybersécurité et qui mènent une politique efficace. Et sans parler de CERT.be, la Cyber Emergency Response Team qui existe depuis un bout de temps. C'est pour cela que le CCB entreprendra des actions en collaboration avec ces services. Les capacités existantes sont pleinement utilisées et nous accorderons nos violons pour ce qui est des projets.

L'ARRÊTÉ ROYAL DE CRÉATION DU CCB STIPULE QUE LA COLLABORATION INTERNATIONALE FIGURE ÉGALEMENT PARMI LES PREMIERS POINTS DE L'ORDRE DU JOUR. COMMENT LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE ENTEND-T-IL COLLABORER AVEC LES CYBERCENTRES ÉTRANGERS ?

Phédra : Miguel et moi avons déjà présenté le CCB au Nationaal Cyber Security Centrum (NCSC) aux Pays-Bas, à l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) en France et à govCERT au Luxembourg. Nous avons en avons profité pour évoquer notre souhait de davantage collaborer avec les pays du Benelux et la France. Ces visites de travail se sont par ailleurs avérées très importantes pour notre organisation interne. En effet, comme ces organisations existent depuis longtemps, nous avons pu tirer des enseignements de leurs parcours de création et des choix faits alors.

LE 26 OCTOBRE, LE PREMIER MINISTRE A PRÉSENTÉ LE PLAN STRATÉGIQUE DU CCB À LA PRESSE. QUEL SOUVENIR GARDEZ-VOUS DE CETTE JOURNÉE ?

Miguel : Une journée très importante ! Tout d'abord parce que nous étions contents de présenter notre plan stratégique au grand public et ensuite parce que cette présentation nous donnait le feu vert officiel pour nous atteler à la réalisation de nos plans ambitieux.

Phédra : J'étais à la fois nerveuse et excitée des réactions qu'allait susciter notre plan stratégique. Mais elles ont été très positives en général !

EN DÉCEMBRE, VOUS AVEZ REJOINT LES RANGS DU CONSEIL D'ADMINISTRATION DE LA CYBER SECURITY COALITION BELGIUM. QUEL SERA LE RÔLE DU CCB DANS CETTE COALITION ?

Miguel : La collaboration entre les secteurs public et le privé est primordiale, et le monde du cyber ne fait pas exception à la règle. La cybersécurité est en effet une responsabilité partagée. Nous essayons de réunir un maximum de partenaires afin d'entreprendre, ensemble, les étapes nous menant vers une stratégie qui sera adoptée par les organisations qui s'intéressent à la cybersécurité. La relation de confiance au sein de la coalition est établie, les concurrents sont assis côte-à-côte afin d'échanger des solutions aux problèmes de sécurité. Personnellement je trouve ça très beau. Seule la collaboration nous permettra de faire front contre la cybercriminalité.

Le CCB a été lancé entre septembre 2015 et mars 2016. Au cours de cette phase de lancement, le CCB n'était pas pleinement opérationnel et il s'attelait avant tout à réaliser et à organiser ses ressources propres.

01

QUELLE FUT LA PLUS IMPORTANTE RÉALISATION DU CCB PENDANT SA PHASE DE LANCEMENT ?

Miguel : En avril 2016, nous avons présenté une première version du cyberplan d'urgence à tous les partenaires concernés. On peut dire que les réactions étaient majoritairement positives. Nous nous attendons dès lors à ce que ce plan devienne rapidement opérationnel.

Phédra : Le recrutement du personnel du CCB s'est lui aussi déroulé sans problème. Grâce à la précieuse aide que nous avons reçue de la Chancellerie, les sélections et les engagements sont presque terminés. Il est en effet crucial de disposer d'une équipe motivée afin de réaliser les nombreuses missions du CCB.

L'UN DES OBJECTIFS DE LA PHASE DE LANCEMENT CONSISTAIT À DRESSER LES CONTOURS DU PAYSAGE ACTUEL DE LA CYBERSÉCURITÉ EN BELGIQUE. QUELLE FUT VOTRE MÉTHODE DE TRAVAIL ?

Miguel : En octobre 2015, nous avons envoyé un courrier à tous les services concernés en Belgique en leur demandant de nous faire parvenir leurs capacités actuelles en termes de cybersécurité. Forts de ces informations, nous avons obtenu un aperçu clair des capacités actuelles en Belgique, afin d'être en mesure de mener une politique ciblée, tournée vers l'avenir.

À L'ISSUE DE LA PHASE DE LANCEMENT (SIX MOIS), LE CCB PRÉVOIT UNE PHASE DE CONSOLIDATION DE TROIS ANS. QUELS SONT LES DÉFIS QUI VOUS ATTENDENT CES TROIS PROCHAINES ANNÉES ?

Phédra : Pendant la phase de consolidation, nous allons créer les fondements qui nous permettront d'atteindre l'objectif ultime du CCB, à savoir faire de la Belgique une sphère de sécurité numérique pour les organisations et les entreprises d'ici 2020. Plus concrètement, ces fondements se traduisent par des projets que nos gestionnaires de projets lanceront et accompagneront.

Un grand merci pour cette interview et bonne chance pour votre mission !
(Andries Bomans)

LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE ET SES COLLABORATEURS

De gauche à droite : **Andries Bomans :** responsable communication
Jo De Muynck : chef de projet
Nathalie Van Raemdonck : collaboratrice stratégique collaboration académique
Valéry Vander Geeten : conseiller juridique
Phédra Clouner : directrice adjointe
Miguel De Bruycker : directeur
Philippe Moisse : chef de projet

02

CYBER SECURITY COALITION

02

DEPUIS 2015, LA CYBER SECURITY COALITION RASSEMBLE LES RESPONSABLES DU SECTEUR PUBLIC, DU SECTEUR PRIVÉ ET DU MONDE ACADÉMIQUE AU SEIN D'UNE SEULE ET UNIQUE ORGANISATION. IL S'AGIT D'UNE APPROCHE UNIQUE EN BELGIQUE QUI PERMET, D'UNE PART, L'ÉCHANGE D'EXPÉRIENCES, DE BEST PRACTICES, D'OPPORTUNIES AND THREATS ET, D'AUTRE PART, D'ÉLABORER UNE POLITIQUE DE SENSIBILISATION EN MATIÈRE DE CYBERSÉCURITÉ.

VOICI LES QUELQUES CONTRIBUTIONS À LA POLITIQUE BELGE DE CYBERSÉCURITÉ DONT LA COALITION PEUT DÉJÀ SE TARGUER :

- **échange d'expériences et de connaissances entre les experts en matière de cybersécurité depuis 2015 ;**
- **campagne nationale de sensibilisation en collaboration avec CERT.be sur l'utilisation de phrases de passe au lieu de mots de passe. Cette campagne nationale bénéficiait du soutien du site Internet www.safeonweb.be et a rencontré un franc succès ;**
- **publication de « Cybersécurité – Guide de gestion des incidents », un guide qui adopte une approche intégrale et pragmatique de la manière dont les organisations doivent réagir face à des cyberincidents ;**
- **la mise en place d'une réelle collaboration avec le Centre pour la Cybersécurité Belgique.**

En sa qualité de directeur du Centre pour la Cybersécurité Belgique, Miguel De Bruycker a été désigné le 7 décembre 2015 membre du conseil d'administration de la Coalition. La Cyber Security Coalition a rédigé le guide « Cybersécurité – Guide de gestion des incidents » en collaboration avec le Centre pour la Cybersécurité Belgique.

En 2016, la Coalition continuera de travailler à quatre niveaux :

- **sensibilisation, essentielle en matière de cybersécurité ;**
- **échange de connaissances ;**
- **coopération inter-CSIRT ;**
- **recommandations et mesures.**

Le CCB apportera une contribution dans chacun de ces quatre domaines et appuiera la Coalition dans son ensemble.

03

PLATFORM CYBER SECURITY

03

LE COMITÉ STRATÉGIQUE ET LE COMITÉ DE COORDINATION DU RENSEIGNEMENT ET DE LA SÉCURITÉ (CCRS) ONT ÉTÉ CRÉÉS EN JUIN 2015 PAR VOIE D'AR (2/06/2015). LES DEUX ORGANES DOIVENT ASSURER LA MISE EN ŒUVRE COORDONNÉE DES DÉCISIONS DU CONSEIL NATIONAL DE SÉCURITÉ.

LE COMITÉ STRATÉGIQUE EST CHARGÉ D'ÉTUDIER CHAQUE PROPOSITION DANS LE CADRE DE LA POLITIQUE DE RENSEIGNEMENT ET DE SÉCURITÉ QUE DOIT DÉTERMINER LE CONSEIL NATIONAL DE SÉCURITÉ. LE COMITÉ DE COORDINATION EST INVITÉ À FORMULER DES PROPOSITIONS COORDONNÉES AU CONSEIL NATIONAL DE SÉCURITÉ RELATIVES À :

- **la politique générale de renseignement et de sécurité ;**
- **la coordination de la lutte contre le financement du terrorisme et la propagation d'armes de destruction massive ;**
- **la politique de protection des informations sensibles.**

Il doit en outre développer des plans d'action pour chaque priorité fixée par le Conseil national de sécurité et en assurer le suivi ou proposer de nouvelles priorités ; promouvoir la collaboration et l'échange d'informations efficaces entre les services de renseignements et de sécurité ; et assurer la mise en œuvre coordonnée des décisions du Conseil national de sécurité. Les membres du Comité de coordination du renseignement et de la sécurité sont tous des dirigeants des services et autorités associés à la politique du renseignement et de la sécurité.

Le CCRS compte huit membres permanents : l'administrateur général de la Sûreté de l'Etat, le chef du Service général du renseignement et de la sécurité des Forces armées, le directeur de l'Organe de coordination pour l'analyse de la menace, le commissaire général de la Police fédérale,
le directeur général de la Direction générale Centre de crise du service public fédéral Intérieur, le président du comité de direction du service public fédéral Affaires étrangères (ou un représentant), un membre du Collège des procureurs généraux et le procureur fédéral.

Six autres membres ne siègent que pour les matières qui les concernent : l'administrateur général de l'Administration générale des Douanes et Accises, le directeur du Centre pour la Cybersécurité Belgique, le président de la Cellule de traitement des informations financières, le directeur général de la Direction générale Transport aérien, le directeur général de la Direction générale Transport maritime et le président de l'Autorité nationale de Sécurité.

Le directeur du Centre pour la Cybersécurité Belgique est un membre non permanent et n'assiste donc aux réunions du CCRS que lorsqu'y sont abordés des dossiers liés à la cybersécurité.

Le Comité de coordination du renseignement et de la sécurité a créé un certain nombre de plateformes dont deux concernent la cybersécurité : la plateforme Cyber Security et la sous-plateforme Cyber Intelligence.

Le CCB est le pilote de la plateforme Cyber Security ; il en assure l'organisation et la coordination. Il fixe en outre l'ordre du jour en concertation avec les membres permanents de cette plateforme.

L'objectif de cette plateforme est de mettre au point, en concertation avec les services publics concernés, une politique nationale en matière de cybersécurité dans le cadre de laquelle ces services fournissent un effort adéquat et constituent ensemble une capacité belge intégrée en matière de cybersécurité. En optimalisant l'échange d'informations, la population, les entreprises, les autorités et les secteurs vitaux bénéficieront d'une protection adaptée.

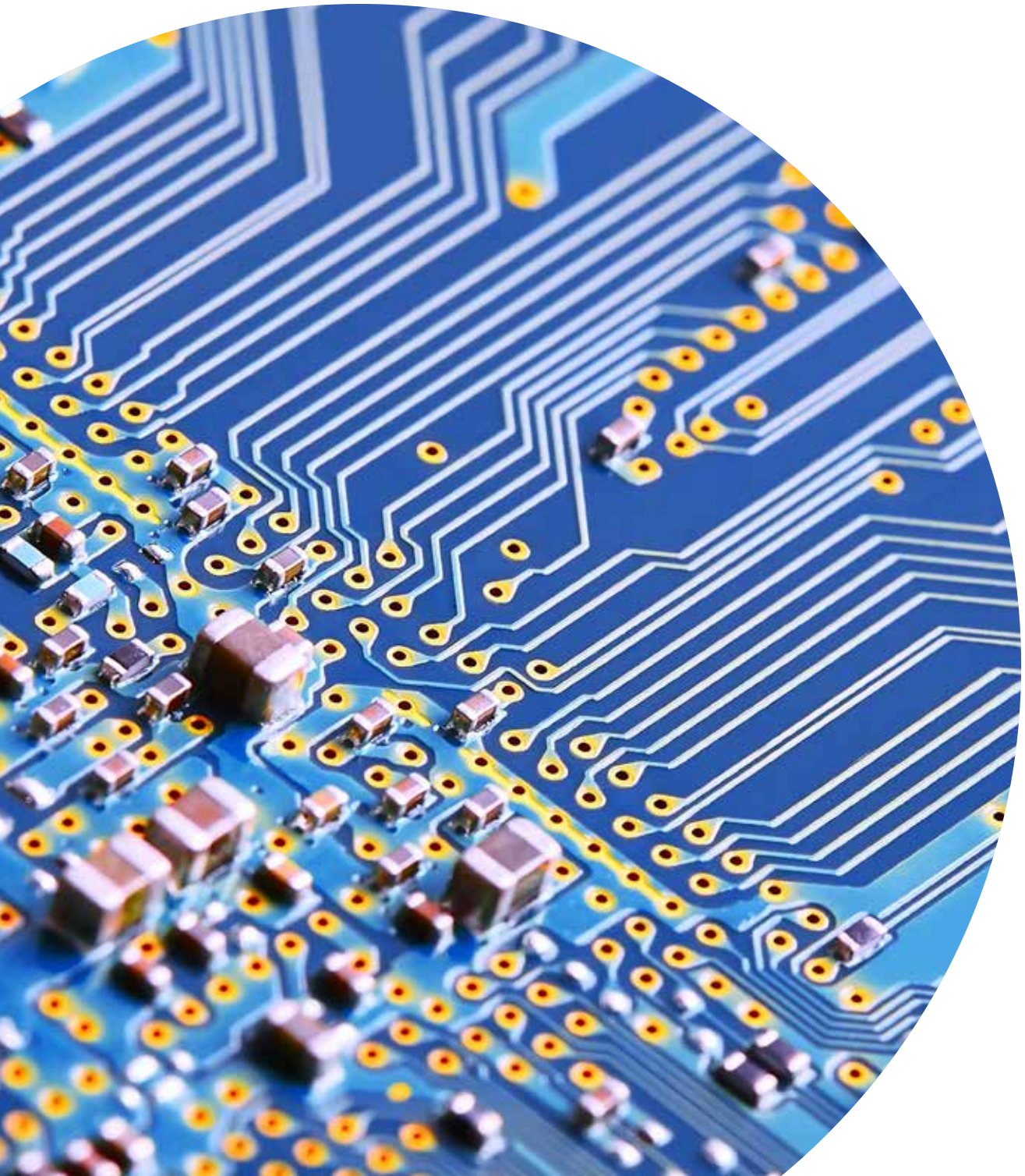
Le CCB entend engranger des résultats concrets via cette plateforme. Dans un premier temps, il espère définir une politique belge de cybersécurité claire. Il s'agit dès lors d'élaborer des procédures concrètes et éprouvées pour le traitement d'incidents de cybersécurité graves, d'avoir un aperçu de la situation actuelle des capacités et responsabilités en matière de cybersécurité en Belgique, de formuler des propositions de situation souhaitée des capacités et responsabilités en matière de cybersécurité et de rédiger un plan d'action visant à atteindre la situation souhaitée.

Dans un deuxième temps, le concept de « cyber security situational awareness » est inscrit à l'ordre du jour. C'est à cette fin qu'a été créée la sous-plateforme Cyber Intelligence, laquelle est pilotée par le service général du renseignement et de la sécurité (SGRS).

Enfin, dans un troisième temps, le CCB entend établir des mécanismes de gestion de l'expertise en cybersécurité et définir des plateformes de communication efficaces en matière de cybersécrurité au service des citoyens, des entreprises et des secteurs vitaux.

Le Centre pour la Cybersécurité Belgique établira un rapport final des résultats obtenus et donnera des orientations à la politique. Afin de parvenir à évaluer sur une base permanente les procédures et les capacités de traitement des incidents de cybersécurité graves, la Belgique participera à des exercices nationaux et internationaux de cybersécurité.

Depuis la création du CCB, cette plateforme s'est réunie à sept reprises.



04

CYBERPLAN NATIONAL D'URGENCE

04

QUELQUES PROJETS ONT ÉTÉ ENTAMÉS LORS DE LA PHASE DE LANCEMENT MAIS N'ENTRERONT EN VIGUEUR QU'ENSUITE, DANS LA PHASE DE CONSOLIDATION (MARS 2016-MARS 2019).

En décembre 2015, le CCB entamait l'élaboration d'un Cyberplan national d'urgence. Il est crucial qu'en cas de crise et d'incidents sérieux de cybersécurité, les différents services belges actifs dans le cyberdomaine puissent collaborer efficacement afin de reprendre au plus vite le contrôle de la situation.

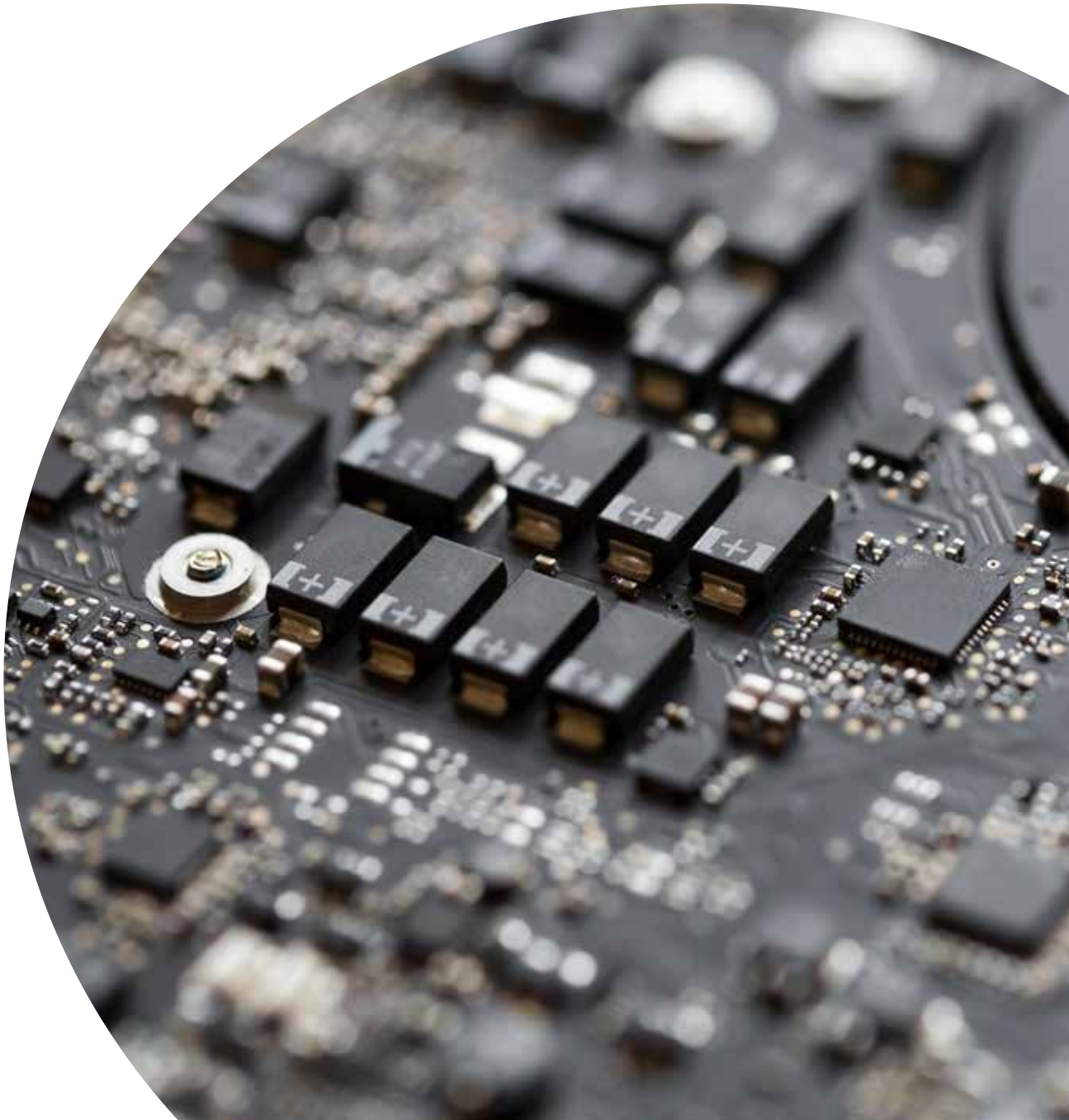
L'objectif principal du Cyberplan national d'urgence belge est de prévoir une structure de réponse aux crises et incidents dans le domaine de la cybersécurité qui exigent une coordination et/ou une gestion à l'échelon national. Le plan établit un ordre de priorité en fonction de l'impact du cyberévènement. Il identifie les Crises nationales de cybersécurité et les Incidents nationaux de cybersécurité. Il prévoit une escalade de base permettant aux différents services actifs dans le cyberdomaine de coordonner leurs actions afin de faire face aux cyberincidents au niveau national. L'accent est nettement placé sur l'échange rapide et correct d'informations entre les services.

Le plan se veut un fil rouge pour les procédures à suivre et les mesures de protection à prendre lors de crises et d'incidents nationaux de cybersécurité et ce, dès que le besoin se fait sentir. Il décrit les missions que doivent éventuellement exécuter les divers organismes et services, chacun dans les limites de ses compétences légales et réglementaires, dans le cadre du processus général de traitement des incidents et crises de cybersécurité.

Ce plan s'intègre dans une matrice plus vaste. Tout service concerné peut utiliser ce document comme base pour les aspects opérationnels de la gestion de crise et d'incident, dans les limites de ses compétences.

S'agissant de l'élaboration de ce Cyberplan d'urgence, le CCB peut compter sur l'expertise et les connaissances du Centre national de Crise. Les différents services actifs dans le cyberdomaine se réunissent afin de donner une image correcte de l'ensemble des capacités actuelles permettant de traiter de tels incidents.

D'ici le mois de juin 2016, le CCB espère disposer d'une première version de ce plan. Des exercices seront organisés afin d'éprouver cette première version et, si nécessaire, de procéder à des ajustements.




CODI
CLICK
CLICK HERE FOR MORE INFOR

05

BOTNET ERADICATION SYSTEM

05

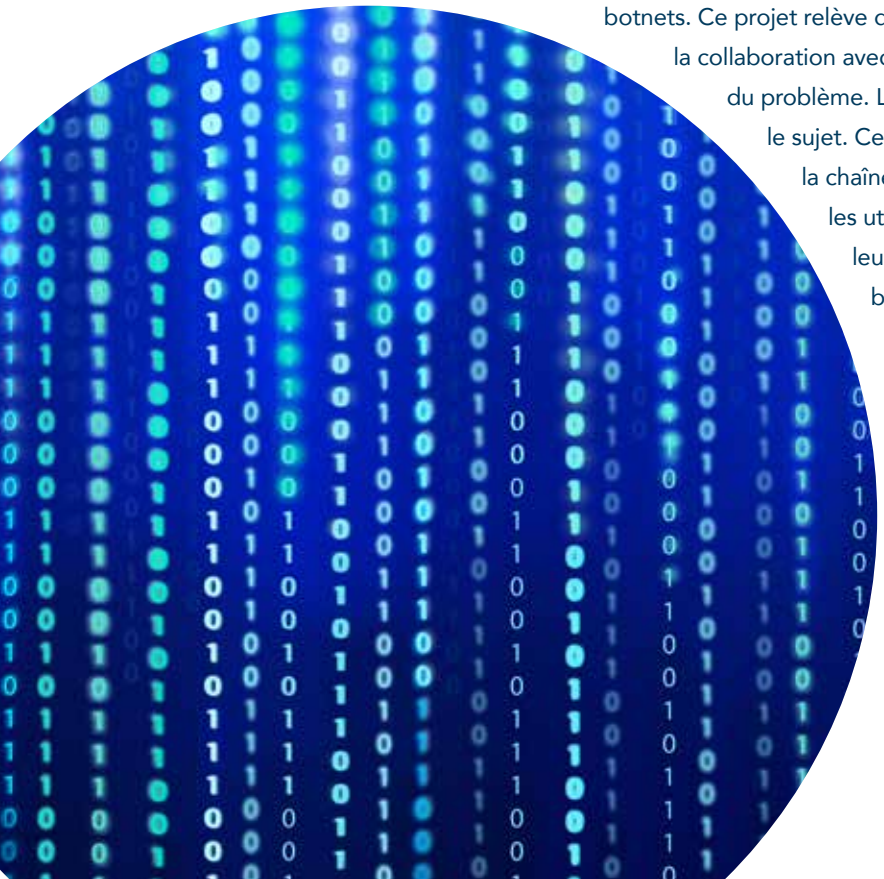
EN NOVEMBRE 2015, LE CENTRE POUR LA CYBERSÉCURITÉ BELGIQUE A CONNU SON BAPTÊME DU FEU. DES MENACES ONT ÉTÉ PUBLIÉES SUR YOUTUBE, AVERTISSANT QUE DES SITES INTERNET DE POUVOIRS PUBLICS BELGES SERAIENT LA CIBLE D'ATTAQUES DDOS. LORS D'UNE ATTAQUE DDOS, OU ATTAQUE « DISTRIBUTED DENIAL OF SERVICE », LES CYBERCRIMINELS TENTENT DE SABOTER UN SERVEUR EN LE SURCHARGEANT DE REQUÊTES DE PAGES. LE SERVEUR EST ALORS DANS L'INCAPACITÉ DE TRAITER CETTE QUANTITÉ DE DEMANDES, À UN POINT TEL QUE LE SITE INTERNET N'EST PLUS ACCESSIBLE JUSQU'À CE QUE L'ATTAQUE CESSE OU QU'ELLE SOIT CONTRÉE.

Le CCB a pris les menaces au sérieux et a envoyé un avertissement aux services concernés. À la demande du CCB, CERT.be a publié en novembre 2015 un *whitepaper* reprenant les mesures proactives et réactives pour lutter contre les attaques DDoS. Ce document aide celui qui le veut à prendre des mesures en cas d'attaque de ce type.

Le Centre pour la Cybersécurité Belgique entend néanmoins aller plus loin que la simple protection de sites des pouvoirs publics contre des attaques DDoS. Il y a lieu de restreindre la possibilité de les réaliser.

Les attaques DDoS sont effectuées à l'aide de botnets. Il s'agit de réseaux étendus d'ordinateurs contaminés qui sont pilotés par le cybercriminel lors de l'attaque. Il s'agit de détecter les botnets et de nettoyer les ordinateurs contaminés.

Le CCB a lancé un projet de Botnet Eradication System visant l'élimination de ces botnets. Ce projet relève d'une responsabilité partagée et exige dès lors la collaboration avec différents partenaires afin de s'attaquer aux racines du problème. Le CCB a mis sur pied un groupe de travail sur le sujet. Ce projet constituera un maillon important de la chaîne d'élimination des botnets. L'objectif est d'informer les utilisateurs (tant les privés que les entreprises) que leurs ordinateurs sont infectés et font partie d'un botnet. En plus de ces informations, les utilisateurs apprendront comment ils peuvent désinfecter leur ordinateur. La Commission pour la protection de la vie privée collaborera étroitement au projet afin d'assurer une information correcte des utilisateurs d'ordinateurs infectés.



Ce projet a été lancé en mars 2016.

06

LA DIRECTIVE NIS

06

PROJET DE DIRECTIVE EUROPEENNE CONCERNANT DES MESURES DESTINEES A ASSURER UN NIVEAU ELEVE COMMUN DE SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION (NIS)

Fin 2015, un projet de directive concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information (« Network and Information systems Security » - en abrégé NIS) a été finalisé au sein des institutions européennes. L'objectif de la directive est d'assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information au sein de l'Union Européenne afin d'améliorer le fonctionnement du marché intérieur.

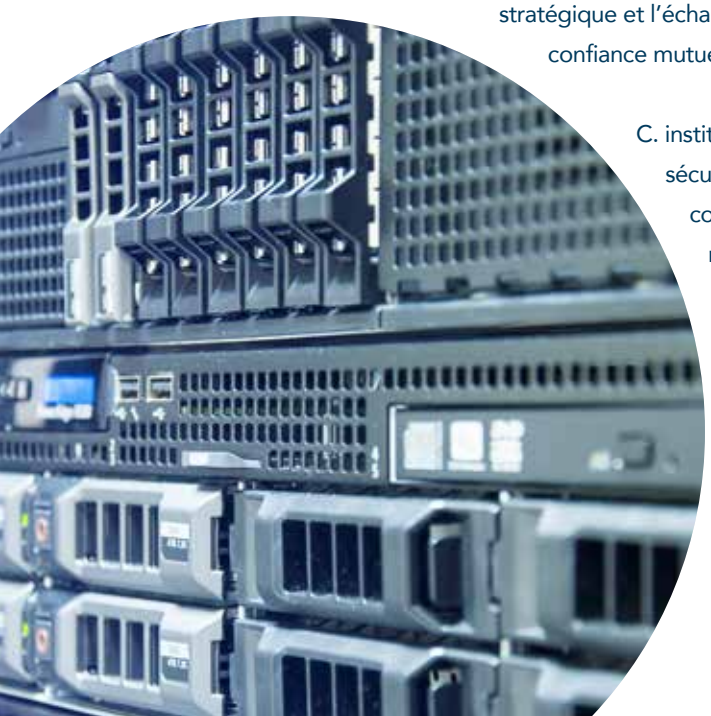
Les mesures prévues visent à améliorer l'efficacité des systèmes informatiques numériques, à combattre la cybercriminalité et à renforcer la politique internationale de cybersécurité et la cyberdéfense de l'UE.

La directive proposée en matière de sécurité des réseaux et des systèmes d'information constitue un volet important de la mise en œuvre de la cyberstratégie européenne (adoptée le 7.02.2013) et impose à tous les États membres, aux opérateurs de services essentiels (les acteurs dans les domaines de l'énergie, des transports, des banques, des soins de santé et de l'eau potable) et aux fournisseurs de services numériques (place de marché en ligne, moteurs de recherche en ligne, service d'informatique en nuage) de veiller sur l'ensemble du territoire de l'UE à un environnement numérique sûr et fiable.

Pour ce faire, la directive :

A. fixe des obligations à tous les États membres en ce qui concerne l'adoption d'une stratégie nationale en matière de sécurité des systèmes de réseaux et d'information ;

B. institue un groupe de coopération afin de favoriser et faciliter la coopération stratégique et l'échange d'informations entre les États membres et de renforcer la confiance mutuelle ;



C. institue un réseau des équipes de réaction aux incidents touchant la sécurité informatique (CSIRT) afin de contribuer au renforcement de la confiance entre les États membres et de promouvoir une coopération rapide et effective au niveau opérationnel ;

D. établit des exigences en matière de sécurité et de notification pour les opérateurs de services essentiels et pour les fournisseurs de services numériques ;

E. fixe des obligations aux États membres pour la désignation d'autorités compétentes nationales, de guichets uniques et de CSIRT chargés de tâches liées à la sécurité des systèmes de réseaux et d'information.

La stratégie de cybersécurité et la directive qui l'accompagne posent un jalon important sur la voie d'un environnement numérique sûr en Europe. La cybersécurité est non seulement une affaire de collaboration entre nombreux acteurs des secteurs public et privé et au sein des États membres. Il s'agit aussi de s'intéresser de plus en plus à ce qu'il se passe de l'autre côté de nos frontières pour y chercher des solutions et prévenir les perturbations ICT et les cyberattaques.

Le CCB a suivi attentivement le processus d'élaboration de cet projet de directive et va coordonner, dès l'adoption de celui-ci, la rédaction des projets de textes légaux nécessaires à la transposition de cette directive en droit belge.

07

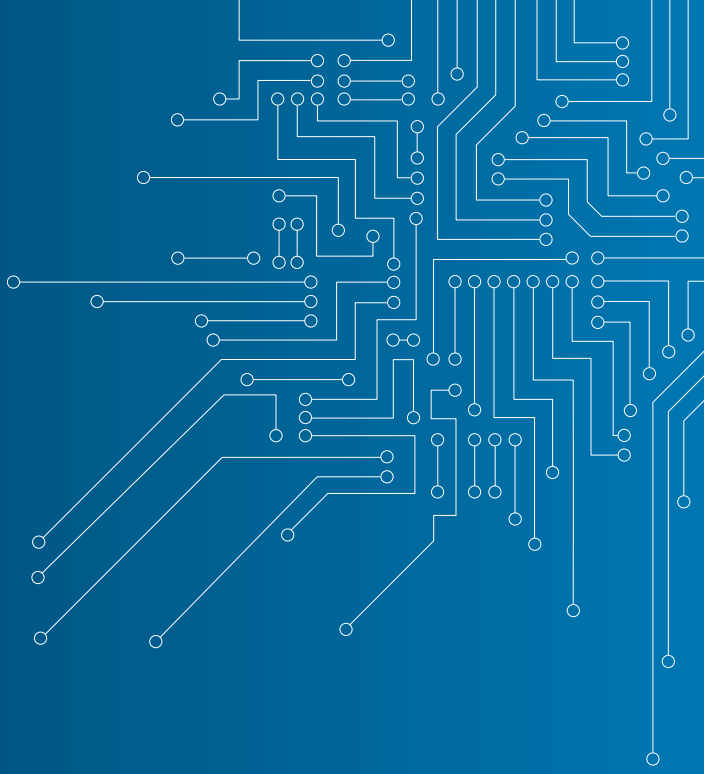
EARLY WARNING SYSTEM

AFIN DE PRÉVENIR LES SECTEURS VITAUX BELGES DE MANIÈRE RAPIDE ET STANDARDISÉE QUANT AUX NOUVELLES CYBERMENACES ET CYBERATTAQUES, LE CCB A CRÉÉ UN SYSTÈME « EARLY WARNING ».

Les secteurs vitaux ont ainsi accès, par le biais d'une plateforme partagée, aux avertissements filtrés faisant état d'intrusions ou de cybermenaces. Grâce à cela, ils reçoivent rapidement des informations de la part d'une source fiable et peuvent très rapidement prendre des mesures.

Le système « Early Warning » devrait selon toute vraisemblance être opérationnel dans le courant de l'automne.

CENTRE FOR
CYBER SECURITY
BELGIUM



CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 - 1000 Brussels

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be