Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

Pacte Défense Cyber
50 mesures pour changer d'échelle

E.M.A

DGA

COMMANDEMENT OPÉRATIONNEL DE CYBERDÉFENSE

Sommaire

Préambule

Le Livre Blanc sur la Défense et la Sécurité Nationale approuvé par le Président de la République en avril 2013 élève la cyberdéfense au rang de priorité nationale. En effet, la part croissante prise par le cyberespace dans nos moyens de défense, notre économie et plus généralement notre mode de vie engendre des risques qui peuvent se révéler stratégiques. En particulier, les menaces contre nos systèmes d'information, qu'ils soient civils ou militaires, y compris ceux qui sont indispensables à la vie de la Nation, sont déjà une réalité et ne peuvent que croître avec l'utilisation massive, par tous et partout, des moyens d'information et de communications.

Pour faire face à ces menaces, le Livre Blanc sur la Défense et la Sécurité Nationale a donné un cap, a énoncé une doctrine nationale de cyberdéfense et a fixé des objectifs ambitieux :

- rechercher systématiquement un haut niveau de sécurité et de résilience des systèmes critiques de l'État et des entreprises d'importance vitale,
- développer une capacité globale de réponse aux crises cybernétiques,
- mettre en place une organisation bien coordonnée de tous les acteurs publics sous l'autorité du Premier ministre, par l'implication du secteur privé dans la posture globale de sécurité, par la maîtrise des équipements critiques des réseaux et par le soutien au développement d'une industrie nationale et européenne de la cybersécurité.

Si beaucoup de progrès ont été accomplis depuis le Livre Blanc de 2008, beaucoup reste à faire.

Pour sa part, le ministère de la Défense a une exigence d'excellence dans ce domaine. Il met en œuvre les moyens correspondants aux différentes postures de dissuasion nucléaire, de sauvegarde maritime et aérienne, et de conduite des interventions militaires. Il développe et opère des systèmes d'information et de communications particulièrement complexes tant en France qu'à l'extérieur du territoire national, supports essentiels des opérations militaires. Il est responsable des systèmes les plus stratégiques, ceux liés à la dissuasion nucléaire mais également des systèmes d'armes sophistiqués : aéronefs de combat ou de transport, navires de surface ou sous-marins, véhicules de combat terrestres. Le ministère de la Défense est par conséquent très fortement concerné par la menace cyber et doit durcir sa posture de vigilance et d'action dans le domaine. À titre d'illustration, les attaques significatives contre les systèmes du ministère ont approché les 800 en 2013, ce qui représente un doublement chaque année.

De plus, si l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est globalement en charge de la défense des systèmes d'information de l'État, le ministère de la Défense doit continuer à opérer en toutes circonstances, même et surtout lorsque beaucoup d'autres organisations voient leur fonctionnement dégradé ou entravé par des cyberattaques.

Pour assurer ses missions, le ministère de la Défense a développé et renforce des compétences de pointe et une expertise tant opérationnelle que technique reconnue en cyberdéfense. Il peut et doit placer ses capacités uniques au service de la posture nationale de cyberdéfense et appuyer l'ANSSI dans sa mission interministérielle de sécurité des systèmes d'information, en pleine concertation et complémentarité avec les autres ministères régaliens, et en premier lieu avec celui de l'Intérieur en charge de la lutte contre la cybercriminalité et particulièrement impliqué dans la gestion des crises sur le territoire national.

C'est pourquoi, en cohérence avec les principes et la doctrine nationale de cyberdéfense énoncés dans le Livre Blanc, j'ai décidé de mettre en place un plan d'action cyberdéfense à la hauteur des défis que nous devons affronter collectivement. Ce plan d'action cadrera toutes les actions à conduire sur la première période de la Loi de Programmation Militaire (LPM), soit les années 2014, 2015 et 2016. 2016 étant l'année où la LPM arrivera à mi-période et devra être réactualisée, un second plan sera alors mis en place.

Pour mobiliser l'ensemble de mon ministère et mettre en perspective de façon très claire les objectifs que j'ai assignés à mes grands adjoints, j'ai donc décidé de les formaliser au sein du « Pacte Défense Cyber » dont je suivrai l'exécution au travers d'indicateurs précis. Ce plan est également destiné à mobiliser les énergies de toute la communauté de la défense. Cette communauté dépasse le seul ministère et rassemble aussi bien nos grands maîtres d'œuvre industriels que nos Petites et Moyennes Entreprises ou Industries (PME/PMI), les organismes de recherche académique et technologique, mais aussi les organismes de formation. En effet, les défis auxquels nous devons faire face appellent à la constitution d'une véritable communauté nationale pour constituer les ressources humaines et les compétences dont toute la Nation va avoir besoin pour innover et se défendre.

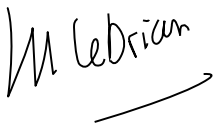
Ce plan embrasse tous les aspects de la cyberdéfense : il comprend des mesures internes au ministère, mais aussi des mesures destinées à créer ou soutenir des dynamiques extérieures en apportant un socle sur lequel des initiatives des collectivités locales,

des grands groupes ou des opérateurs de formation pourront s'appuyer. Il s'attache en particulier à :

- durcir notre posture préventive en amplifiant la réorganisation de la cyberprotection sous l'égide de la Direction Générale des Systèmes d'Information et de Communication (DGSIC) en lien avec mes grands subordonnés ;
- élever le niveau de préparation des forces et des emprises du ministère face à ces menaces par la mise en place d'indicateurs de qualification opérationnelle et d'exercices ;
- durcir notre posture réactive en amplifiant la mise en place des capacités du commandement opérationnel de cyberdéfense créé en 2011 au sein du Centre de Planification et de Conduite des Opérations (CPCO) et son irrigation au sein de toutes les unités des armées et des entités du ministère ;
- contribuer au développement d'une base industrielle et technologique de défense en cybersécurité, capable notamment d'offrir une nouvelle génération d'équipements, de systèmes et de logiciels, fortement maîtrisés et aptes à être mieux défendus, soutenue notamment par les études amont et les programmes d'équipement des forces ;
- soutenir les PMI/PME via l'emploi et le renforcement dans le domaine de la cybersécurité du dispositif RAPID (Régime d'Appui Pour l'Innovation Duale) porté par la Direction Générale de l'Armement (DGA) ;
- participer à la stimulation de la recherche et de la formation avec la création d'un pôle d'excellence cyberdéfense en Bretagne, où le ministère dispose déjà d'un réseau important d'expertise technique et de centres de formation. Un pilier opérationnel est présent dans cette région et appelé à se renforcer. Par ailleurs, plusieurs chaires ont déjà été créées à Paris et à Coëtquidan ; d'autres devront suivre, notamment pour couvrir les domaines aérospatial et maritime où nous disposons d'une industrie d'excellence ;
- consolider l'expertise technologique du pôle d'excellence Bretagne en s'appuyant sur le centre DGA Maîtrise de l'Information ainsi que son expertise opérationnelle en s'appuyant sur l'antenne Bretagne du Centre d'Analyse en Lutte Informatique Défensive (CALID), qui y délocalisera ses capacités d'entraînement et d'exercice ;
- poursuivre, en lien avec ce pôle d'excellence, la mise en place d'un réseau de simulation distribuée conçu pour entraîner et former à la défense informatique face à des attaques mais aussi à la gestion d'une crise cybernétique et qui pourra aussi être utilisé au-delà du seul ministère ;
- contribuer au renforcement de la communauté nationale de cyberdéfense en multipliant les liens et les échanges entre les différents services. À titre d'exemple, le centre de cyberdéfense du ministère de la Défense, le CALID, est déjà colocalisé avec celui de l'ANSSI ;
- soutenir l'ANSSI dans l'assistance à nos grands industriels de défense en cas d'attaque informatique, avec un rôle renforcé pour la Direction de la Protection et de la Sécurité de la Défense (DPSD). En effet, la cybersécurité de mon ministère commence avec celle de ses partenaires de confiance et grands fournisseurs ;
- développer l'expertise juridique en cyberdéfense pour donner aux forces armées un cadre consolidé sur le plan national comme international, en particulier en cas de conflit ;
- promouvoir l'esprit de cyberdéfense avec la montée en puissance du réseau Cyberdéfense de la réserve citoyenne en partenariat entre les armées, l'ANSSI, la DGA et la Direction Générale de la Gendarmerie Nationale (DGGN), et poursuivre son déploiement en province ;
- poursuivre l'étude de la mise en place d'une réserve à vocation opérationnelle selon une démarche pragmatique et l'utiliser de façon expérimentale lors d'un exercice interministériel ;
- approfondir les partenariats avec nos principaux alliés, mais aussi être force de proposition au sein de l'Organisation du Traité de l'Atlantique Nord (OTAN) et des structures de sécurité et de défense de l'Union Européenne pour renforcer notre cybersécurité collective.

Vous le voyez, ce pacte met en perspective l'ensemble des travaux menés par mon ministère ; il se fonde sur une démarche pragmatique et des projets concrets. L'une des preuves tangibles de cette volonté est l'effort significatif de près d'un milliard d'euros que mon ministère investira pour la cybersécurité d'ici 2019. L'autre preuve de cet engagement est la création d'un tableau d'indicateurs quantifiés ou de tendance que chacune des autorités pilote devra me proposer et qui sera systématiquement présenté lors du Comité ministériel des SIC que je préside. Il me permettra de suivre globalement l'évolution des actions de ce plan et d'en mesurer les progrès.

Jean-Yves Le Drian,
ministre de la Défense



Axe 1

Durcir le niveau de sécurité des systèmes d'information et les moyens de défense et d'intervention du ministère et de ses grands partenaires de confiance

Les principes exposés par le Livre Blanc sur la Défense et la Sécurité Nationale visent à une plus grande robustesse et à une plus grande résilience des systèmes d'information de l'État mais aussi des opérateurs d'importance vitale. Le ministère de la Défense doit assumer ses responsabilités en garantissant le fonctionnement et la défense des systèmes dont il a la responsabilité tant sur le territoire national qu'en dehors de nos frontières, et en assistant si besoin les autres administrations de l'État, et en particulier l'ANSSI, ainsi que les partenaires auxquels nous sommes liés par des accords de défense.

1.1 ACCENTUER LE DÉVELOPPEMENT ET L'USAGE DES MOYENS TECHNIQUES CONTRIBUANT À L'AUTONOMIE DE NOS ACTIONS SOUVERAINES

Face à une menace grandissante et aux doutes sur certains équipements et logiciels d'origine étrangère, la maîtrise nationale de certains produits clés est indispensable.

Action 1

-> renforcer le niveau de cyberdéfense du ministère par l'utilisation d'équipements et de logiciels souverains partout où cela est nécessaire

L'analyse de risque menée lors de l'analyse des systèmes (démarche d'homologation) doit conduire à privilégier pour les systèmes les plus critiques pour l'action du ministère l'acquisition et l'utilisation de produits développés ou bien maîtrisés nationalement.
La DGSIC étudiera en lien avec le SGDSN la politique d'acquisition à adopter au sein du ministère.
Indicateur : prise en compte dans la politique d'acquisition (Pilote : DGSIC).

Action 2

-> créer, maintenir et utiliser des outils de cybersécurité d'un niveau de sécurité élevé

L'action du ministère en matière de réalisation et d'emploi de produits de haut niveau de sécurité à usage gouvernemental (ECHINOPS, TEOREM…) doit être poursuivie, en étroite coopération avec l'ANSSI et les industriels.
En particulier, une tablette hautement sécurisée devra être disponible à l'échéance 2017.
Indicateur : suivi de la feuille de route des produits de sécurité en Comité ministériel des SIC (Pilote : EMA/DGA).

Action 3

-> développer et déployer des capacités avancées de détection et d'intervention

La défense de nos systèmes dépend étroitement de la qualité et de la maîtrise de nos outils de détection des menaces et d'intervention. En complément d'outils commerciaux, le développement autonome de moyens spécifiques et souverains est donc indispensable. Ces moyens spécifiques seront développés par l'industrie nationale ou directement par les services de l'État. Ce point sera intégré à la feuille de route des produits de sécurité.
Indicateur : suivi des outils spécifiques cyber en Comité ministériel des SIC (Pilote : EMA/DGA).

Action 4

-> renforcer l'emploi de la cryptographie pour la sécurité des échanges

Conformément à la Stratégie de la France pour la défense et la sécurité des systèmes d'information, la protection cryptographique des informations demeure un des piliers essentiels de la cybersécurité. Le ministère veillera à maintenir cette primauté en poursuivant ses investissements humains et financiers dans ce domaine.
Indicateur : maintien des investissements humains et financiers (Pilote : DGA et EMA).

Action 5

-> achever la mise en place d'une identité numérique des agents du ministère

En complément d'une plus grande sensibilisation des agents du ministère, l'utilisation de moyens plus sécurisés d'accès aux systèmes est indispensable. En particulier, le déploiement en cours de la Carte d'Identité Professionnelle Multi-services Sécurisée (CIMS) doit être poursuivi et achevé pour 2015, sous la direction de projet de la Direction Générale de l'Armement (DGA), avec le soutien de l'État-Major des Armées (EMA) et de la Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information (DIRISI).
Indicateur : déploiement de 10 000 cartes pour le nouveau site du ministère en 2015 et le reste des Bases de défense avant 2017 (Pilote : DGA).

1.2 AMÉLIORER L'ORGANISATION INTERNE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DU MINISTÈRE

Action 6

-> faire évoluer la chaîne fonctionnelle SSI des armées vers une chaîne de cyberprotection qui sera créée dès 2014

Indicateur : création de la chaîne dès 2014 puis atteinte de la cible définie (Pilote : EMA).

Action 7

-> poursuivre l'adaptation de la cyberprotection selon les orientations du schéma directeur cybersécurité

Sous l'égide de la DGSIC, l'adaptation de la cyberprotection sera suivie grâce à la mise en œuvre d'indicateurs d'avancement du plan d'action de cybersécurité, qui découle du schéma directeur cybersécurité de juillet 2011, avec le soutien des grands subordonnés du ministre.
Indicateur : suivi de ces indicateurs en Comité ministériel des SIC dès le deuxième semestre 2014 (Pilote : DGSIC).

Action 8

-> renforcer la cyberprotection en accentuant la prévention et en mettant en place un retour d'expérience

La chaîne de cyberprotection des armées mène en particulier les actions de prévention nécessaires à l'ensemble des entités des armées et veille à l'homologation et au Maintien en Condition de Sécurité (MCS) de l'ensemble des systèmes d'information associés. Les indicateurs de suivi des homologations et du MCS renouvelés seront mis en place et intégrés au rapport annuel de la sécurité des systèmes d'information de 2015.
Le niveau de préparation du ministère sera élevé en concevant systématiquement des plans de continuité d'activité informatique des sites et des systèmes critiques.
Par ailleurs, sous l'égide de la DGSIC, un processus de retour d'expérience en matière de cybersécurité sera mis en place pour l'été 2014.
Indicateur : intégration des indicateurs de suivi des homologations et du MCS au rapport annuel de la sécurité des systèmes d'information de 2015, mise en place de la structure RETEX avant l'été 2014 (Pilote : DGSIC).

Action 9

-> suivre l'évolution de la posture de cybersécurité des fournisseurs du ministère

L'expérience montre que certains cyberincidents surviennent malgré les défenses du ministère *via* des entreprises qui fournissent des produits ou services ou interviennent sur nos systèmes. Il s'agit donc d'augmenter notre vigilance en partenariat avec nos fournisseurs et dans le respect des dispositions légales, notamment des articles 21 à 24 de la LPM.
Indicateurs : suivre la mise en œuvre des directives articles 21 à 24 de la LPM et dresser un bilan du nombre de cyberincidents et de leur gravité (Pilote : DPSD).

Action 10

-> promouvoir dans chaque armée des réflexions pour améliorer la prise en compte de ses spécificités en matière de cybersécurité

Chaque armée dispose d'une expertise technico-opérationnelle de milieu qu'elle doit mettre à profit pour améliorer avec la DGA la sécurisation de ses systèmes spécifiques face aux menaces cyber. Cela passe tout d'abord par l'intégration de la problématique cyber à ses réflexions sur l'emploi des systèmes, en particulier, mais pas seulement, de ses systèmes d'armes.
Cela conduit ensuite à prendre en compte les menaces cyber dans toutes les étapes du cycle de vie des systèmes spécifiques et à concevoir un MCS adapté. Chaque armée développera un processus mixte avec la DGA afin de guider cette prise en compte.
Chaque armée organisera une journée de la cybersécurité propre à son milieu.
Indicateur : vérification de l'existence du processus mixte avec la DGA et de la journée de la cybersécurité (Pilote : EMA avec EMAT, EMM et EMAA).

1.3 DURCIR LA POSTURE RÉACTIVE EN RENFORÇANT LA CHAÎNE MILITAIRE DE CYBERDÉFENSE ET LES MOYENS TECHNIQUES ASSOCIÉS

Sous l'autorité du Commandement Opérationnel de Cyberdéfense créé en 2011 au sein du CPCO et qui a compétence sur l'ensemble du ministère, les différents services et au premier chef les forces armées doivent accroître leur niveau de préparation face aux cybermenaces. Cette chaîne de commandement est unifiée, centralisée et spécialisée.

Les investissements dans les moyens techniques et humains seront poursuivis pour assurer une surveillance constante et approfondie de nos systèmes et renforcer nos capacités d'intervention pendant toutes les phases d'une crise cyber. Pour cela, la LPM prévoit une augmentation de 350 spécialistes en cybersécurité pour les armées et la poursuite de l'opération MTLID (Moyens Techniques de Lutte Informatique Défensive).

Action 11

-> poursuivre la mise en place de la cyberdéfense du ministère de la Défense, autour du commandement opérationnel de cyberdéfense et du CALID

Dans le cadre de l'exécution de la LPM qui prévoit l'augmentation des effectifs dédiés à la cyberdéfense, le ministère de la Défense poursuivra la mise en place de la chaîne de cyberdéfense, son intégration à la planification et à la conduite des opérations militaires et ses relations étroites avec les autres acteurs de la cybersécurité du ministère.
Dans ce cadre, l'intégration d'un volet cyber à toutes les directives liées au dialogue organique et aux contrats opérationnels est impérative.
Une doctrine de cyberdéfense rénovée et les documents associés seront publiés en 2014.
Indicateur : publication des documents en 2014 (Pilote : EMA).

Action 12

-> doter les forces d'une capacité projetable de cyberdéfense permettant d'élargir le périmètre de surveillance et de détection du CALID aux opérations extérieures

Une nouvelle unité projetable d'une centaine de spécialistes sera constituée et permettra d'assurer une véritable bulle de cyberdéfense au profit des états-majors déployés sur les théâtres, comme en ce moment à Serval ou Sangaris. Il s'agira d'une capacité interarmées mise en œuvre par une unité spécifique qui aura pour mission de se déployer sur les théâtres d'opération pour assurer au plus près la surveillance et la défense des états-majors et des systèmes. Elle s'appuiera notamment sur une capacité initiale de surveillance projetable connectée au CALID, qui sera utilisée en condition opérationnelle dès la fin de l'année 2014, puis étendue pour atteindre une pleine capacité opérationnelle en 2018.
Indicateur : existence de cette pleine capacité opérationnelle projetée (Pilote : EMA).

Action 13

-> poursuivre dans les armées, directions et services la mise en place d'une chaîne de cyberdéfense pour la surveillance de leurs systèmes métiers spécifiques et le maintien de leur expertise sur ces systèmes

Les directives et la doctrine de cyberdéfense devront être déclinées dans les documents de chacune des armées, directions et services en 2014.
Indicateur : prise en compte dans les documents en 2014 (Pilote : EMA avec EMAT, EMM et EMAA).

Action 14

-> inclure systématiquement un volet cyberdéfense dans tous les niveaux des exercices des forces armées

L'effort fait par les armées en matière de préparation opérationnelle des forces se poursuivra en intégrant systématiquement un volet cyber dans les exercices de différents niveaux. Il s'agira de vérifier la capacité des armées à tous les échelons à opérer malgré les cybermenaces et à intégrer les problématiques liées au cyberespace dans leur espace de manœuvre.
Le ministère participera à l'exercice national Piranet 2014 en relation avec l'ANSSI.
De plus, la participation aux exercices internationaux avec les alliés, et notamment ceux organisés par le centre d'excellence en cyberdéfense de Tallinn, sera recherchée.
Un bilan annuel des exercices réalisés sera effectué par l'EMA pour recenser la participation aux exercices de cyberdéfense (ex. : Cyber Coalition) et au volet cyber des exercices conventionnels (ex. : Piranet), tant nationaux qu'internationaux.
Indicateur : bilan annuel des exercices (Pilote : EMA avec EMAT, EMM et EMAA).

1.4 DÉVELOPPER UN RENSEIGNEMENT D'INTÉRÊT CYBER NOURRI PAR TOUS LES ACTEURS DU RENSEIGNEMENT DU MINISTÈRE

Action 15

-> animer au bénéfice du commandement opérationnel de cyberdéfense le renseignement d'intérêt cyber avec les différents acteurs concernés

Pour anticiper les menaces, évaluer les capacités offensives des adversaires potentiels et identifier l'origine des attaques, le Renseignement d'Intérêt Cyber (RIC) est nécessaire. Chaque acteur du renseignement du ministère doit y apporter son expertise propre sous la coordination du commandement opérationnel de cyberdéfense.
Un processus *ad hoc* sera mis en place en cohérence avec le processus d'anticipation opérationnelle.
Indicateur : existence du processus RIC (Pilote : EMA).

1.5 PRÉCISER LE CADRE JURIDIQUE DE LA CYBERDÉFENSE SPÉCIFIQUE AUX ARMÉES POUR GARANTIR L'EFFICACITÉ DES FORCES

Le cadre juridique de la cyberdéfense ressort à la fois du droit international et du droit national. Au plan international, si certains textes s'appliquent explicitement au cyberespace, beaucoup sont encore à interpréter ou à créer et font l'objet de discussions dans les enceintes internationales et notamment à l'Organisation des Nations Unies. En particulier, la façon de respecter le droit des conflits armés lors d'opérations cyber reste à préciser. Au plan national, le code pénal et le code de la défense encadrent les actions possibles de forces armées dans le cyberespace. L'adaptation régulière de ces textes est une obligation pour ne pas créer un fossé entre la réalité des menaces et la liberté de manœuvre des forces armées.
Le cadre juridique de la cyberdéfense doit donc devenir un axe d'excellence des services du ministère de la Défense. Les travaux engagés par la Direction des Affaires Juridiques (DAJ) et l'EMA doivent permettre de définir un cadre solide face à la complexité de ce milieu civilo-militaire et international, et contribuer à définir la position de la France dans les instances internationales, en lien avec l'ANSSI et le ministère des Affaires Étrangères.

Action 16

-> renforcer l'expertise juridique du ministère de la Défense en matière de cyberdéfense pour consolider les règles d'engagement en cohérence du droit national et international

La DAJ et les juristes opérationnels (JUROPS) de l'EMA travailleront ensemble sur ces questions. Sous l'égide de la DAJ, un vivier de conseillers juridiques (LEGAD) formés aux enjeux de la cyberdéfense sera constitué.
Indicateur : nombre de LEGAD dans le vivier (Pilote : DAJ).

Axe 2

Préparer l'avenir en intensifiant l'effort de recherche tant technique et académique qu'opérationnel, tout en soutenant la base industrielle

Le cyberespace est en constante évolution : technologies, usages, stratégies des différents acteurs… Pour que la France soit parmi les nations qui comptent dans le cyberespace, un soutien résolu à la recherche est indispensable. Je veux que le ministère de la Défense participe significativement aux efforts en la matière.

2.1 ENCOURAGER ET SOUTENIR LES ÉTUDIANTS ET LES CENTRES DE RECHERCHE À S'INVESTIR DANS LE DOMAINE DE LA CYBERDÉFENSE

Action 17

-> augmenter le nombre de thèses de doctorat approfondissant l'expertise en cyberdéfense

Concernant les aspects techniques, la DGA met à profit son centre d'expertise DGA-Maîtrise de l'Information et soutient la recherche et développement avec des crédits considérablement augmentés. De même, l'IRSEM soutiendra les études en cyberdéfense dans le domaine des sciences humaines et sociales. Un nombre croissant de thèses de doctorat va être financé et co-encadré au travers de conventions de recherche avec les laboratoires académiques. Cet axe sera en particulier développé au travers du volet « recherche » du pôle d'excellence Bretagne.
Le nombre de thèses consacrées à la cyberdéfense soutenues par le ministère sera doublé entre 2014 et 2019.
Indicateur :évolution du nombre de thèses (Pilote : DGA en relation avec le chef du projet pôle d'excellence cyber Bretagne).

Action 18

-> développer dans les écoles d'officiers, en partenariat avec les industriels nationaux, des chaires de cyberdéfense

La création en 2013 de la chaire de cyberdéfense en partenariat avec les Écoles de Saint-Cyr Coëtquidan et des entreprises privées marque la volonté du ministère de soutenir également la recherche académique. D'autres chaires devront se développer d'ici 2015 notamment dans les écoles d'officiers de l'armée de l'air à Salon-de-Provence, de la Marine Nationale à Brest (Lanvéoc-Poulmic) et de l'ENSTA Bretagne (École Nationale Supérieure des techniques Avancées) à Brest pour mieux appréhender la cybersécurité dans l'ensemble des espaces terrestres, maritime et aérospatial.
Indicateur :création des chaires avant 2015 (Pilote : EMAT, EMM, EMAA et DGA).

Action 19

-> soutenir les organismes publics et privés qui contribuent à la réflexion sur la cyberdéfense

Les organismes liés à la recherche stratégique, en particulier la Direction Générale des Relations Internationales (DGRI) et l'Institut pour la Recherche Stratégique de l'École Militaire (IRSEM) accroîtront leurs efforts pour soutenir les *think tanks*, écoles, universités et doctorants qui souhaitent apporter leur contribution à la réflexion sur la cyberdéfense. La part des financements consacrés à la cyberdéfense devra être progressivement portée à 10 %.
Indicateur : part des études financées portée à 10 % (Pilote : DGRI).

2.2 FORGER UNE PENSÉE STRATÉGIQUE ET OPÉRATIONNELLE FRANÇAISE EN CYBERDÉFENSE

Action 20

-> développer à tous les niveaux de la réflexion stratégique et opérationnelle une réflexion croisée sur la cyberdéfense

Les écoles d'officiers, les centres de doctrine d'armée, le Centre de doctrine interarmées, l'État-major interarmées de force et d'entraînement ainsi que l'École de guerre doivent développer, chacun à son niveau mais aussi en échangeant leurs travaux, une réflexion sur les aspects stratégiques et opérationnels de la cyberdéfense.
La rédaction d'ouvrages sur la cyberdéfense par des officiers et des personnels civils de la défense sera encouragée et soutenue. Les meilleurs devront être traduits et diffusés pour faire rayonner la pensée française à l'international.
Le Centre de documentation de l'École militaire soutiendra cette démarche en créant et alimentant un rayon cyber.
Les échanges avec les partenaires de cette réflexion extérieurs au ministère seront encouragés, en particulier avec l'Institut des Hautes Études de la Défense Nationale, le Centre des Hautes Études Militaires et le Centre des Hautes Études du Ministère de l'Intérieur.
Indicateur : nombre d'ouvrages publiés (Pilotes : DGRI et EMA).

Action 21

-> mieux appréhender le contexte géopolitique de la cyber en accroissant les échanges avec nos partenaires étrangers pour confronter avec eux nos idées et ainsi progresser dans la constitution d'une pensée stratégique française

Pour stimuler cette pensée stratégique française que je souhaite voir émerger en cyberdéfense comme elle a émergé dans les autres milieux, les échanges avec nos partenaires étrangers sont indispensables. Ils concernent bien entendu au premier chef nos alliés proches et je rappelle notre adhésion au Centre d'Excellence en cyberdéfense de l'OTAN à Tallinn. Mais nous devons également mieux comprendre les autres acteurs du cyberespace et discuter, échanger et partager notre vision avec les États de toutes les régions du monde – je pense en particulier aux grands acteurs comme la Russie et la Chine, mais aussi aux puissances cyber montantes comme l'Inde et le Brésil.
Le domaine de la cyberdéfense doit être inclus au niveau adapté dans les dialogues stratégiques et les plans de coopération avec nos partenaires étrangers. Un indicateur sera établi par la DGRI pour les dialogues stratégiques et l'EMA pour les coopérations.
Indicateur : bilan des relations et coopérations incluant un volet cyber (Pilotes : DGRI et EMA).

2.3 RENFORCER LA BASE INDUSTRIELLE ET TECHNOLOGIQUE EN PORTANT UNE ATTENTION TOUTE PARTICULIÈRE AUX PME/PMI

Pour maintenir et étendre notre capacité souveraine d'action dans le cyberespace, il est indispensable de renforcer une véritable base industrielle et technologique de défense en cybersécurité, capable notamment d'offrir une nouvelle génération d'équipements et de logiciels, fortement maîtrisés, soutenue en premier lieu par les Projets d'Étude Amont (PEA) et les programmes d'équipement des forces, à côté d'autres modes de financements publics et en cohérence avec le Comité de la Filière des Industries de la Sécurité (COFIS) et en appui des plans de reconquête de la Nouvelle France Industrielle.

Action 22

-> élaborer et entretenir une feuille de route pour orienter la recherche et le développement sur la cyberdéfense et anticiper les futurs besoins

Sur la base du rapport d'orientation de la R&D publié par l'ANSSI, le ministère de la Défense cherchera à consolider avec l'ANSSI la feuille de route de produits de sécurité pour guider les financements des PEA et les appels à projets.
L'avancement de cette feuille de route sera suivi en Comité Ministériel des SIC
Indicateur : suivi de l'avancement de cette feuille de route en Comité ministériel des SIC (Pilote : DGA).

Action 23

-> consolider la structuration de la filière cybersécurité

Pour disposer d'une industrie nationale innovante et compétitive, la structuration de la filière de cybersécurité est impérative. En cohérence avec le COFIS et les démarches comme le plan cybersécurité pour une nouvelle France industrielle, le ministère de la Défense poursuivra sa cartographie des acteurs du milieu, et en particulier des PME/PMI innovantes et l'identification des entreprises stratégiques. Il mènera une politique active de soutien de leurs activités de recherche et développement, veillera à mettre en œuvre les moyens nécessaires à la pérennité des acteurs contribuant aux travaux de souveraineté et valorisera les projets à l'export. Il s'assurera enfin, en particulier grâce à des actions de sensibilisation renforcées, à ce qu'ils veillent à leur propre cybersécurité.
Indicateur : émergence de la filière cybersécurité (Pilote : DGA).

Action 24

-> augmenter et pérenniser le niveau de budget consacré aux études amont sur la cybersécurité

Les études amont en cybersécurité conduites par la DGA, en coopération avec l'EMA mais également l'ANSSI, verront leurs moyens considérablement augmentés avec un triplement qui les porte ainsi à au moins 30 millions d'euros par an. Ils visent à structurer la recherche et développement au sein des acteurs industriels afin de consolider une offre nationale de produits et de systèmes de haut niveau de sécurité. Ces moyens devront être pérennisés sur toute la période 2014-2019.
Indicateur : pérennisation des moyens alloués (Pilote : DGA).

Action 25

-> mieux informer les PME/PMI sur le dispositif RAPID et le renforcer au profit des projets de cybersécurité

Le dispositif RAPID de soutien à l'innovation des PME/PMI a fait la preuve de sa souplesse et de son efficacité. Focalisé sur les projets dont les retombées seront à la fois civiles et militaires, RAPID est naturellement ouvert aux projets de cyberdéfense. Afin de donner toute leur chance aux projets de cybersécurité, la DGA renforcera son accompagnement en amont de ces projets auprès des PME/PMI. RAPID contribuera ainsi à la maturation de projets innovants et au développement d'offres nationales compétitives. Un indicateur des projets bénéficiant du dispositif RAPID concernant la cybersécurité sera établi par la DGA.
Indicateur : nombre de projets RAPID dédiés à la cyber (Pilote : DGA).

Action 26

-> renforcer les capacités d'expertise technique étatique et industrielle

Disposer d'une capacité d'expertise technique cohérente et de haut niveau, à la fois chez les acteurs étatiques (DGA et ANSSI) et industriels, est indispensable afin de développer la cybersécurité. Elle doit permettre de développer les solutions de souveraineté tout en mutualisant au niveau européen la R&D qui peut l'être, par exemple dans le domaine de la sécurité des systèmes industriels.
À cette fin, un effort important de recrutement d'ingénieurs de haut niveau sera consenti pour porter l'effectif d'experts en cybersécurité du centre DGA Maîtrise de l'Information (DGA-MI) à 400 personnes en 2017.
Indicateurs : effectifs et expertises disponibles dans le centre DGA-MI (Pilote : DGA).

Axe 3

Renforcer les ressources humaines dédiées à la cyberdéfense et construire les parcours professionnels associés

Le Livre Blanc sur la Sécurité et la Défense Nationale prévoit l'accroissement des ressources humaines dans le domaine cyber. Nous sommes donc face à un besoin de formation de tout le personnel, du simple utilisateur aux spécialistes techniques et tous les opérationnels qui doivent prendre en compte le cyberespace comme nouveau domaine des opérations militaires. Cette diversité des compétences nécessaires à l'exercice des métiers de la cyberdéfense et la rareté de la ressource humaine correspondante appellent une coordination active des politiques de gestion, d'emploi et de formation.
La DRH-MD, les organismes spécialisés dans les SIC et la cyberdéfense doivent donc travailler à améliorer la Gestion Prévisionnelle des Emplois, des Effectifs et des Compétences (GPEEC) cybersécurité du ministère.

Action 27

-> coordonner plus étroitement les politiques de gestion, d'emploi et de formation dans le domaine de la cybersécurité

Les actions initiées par le comité de pilotage des ressources humaines de la filière « sécurité des systèmes d'information » seront pérennisées, sous la coprésidence du directeur général des SIC et du DRH-MD. Ce comité établira une vision partagée des enjeux RH relatifs à la cybersécurité (fiabilisation de la description de la ressource spécialisée, identification des écarts entre ressources et besoins, attractivité des parcours professionnels, mobilité interne ou externe des experts…).
La Commission Spécialisée de la Formation (CSF) Cybersécurité appuiera cette démarche pour garantir la meilleure adéquation entre les formations dispensées et le besoin des employeurs du ministère.
Les comptes-rendus du Comité de Pilotage (COPIL) des RH SSI et de la CSF permettront de mesurer les progrès en la matière.
Indicateurs : comptes-rendus du COPIL RH SSI et de la CSF (Pilotes : DGSIC et DRH-MD).

Action 28

-> prendre en compte dans chaque armée, service et direction ces filières pour disposer du personnel formé en nombre suffisant, dans les domaines techniques comme opérationnels.

Les armées, directions et services doivent mettre en place dans leurs écoles de formation un enseignement sur la cyberdéfense adapté aux différents profils de leur personnel : simple utilisateur, spécialiste technique, expert confirmé, ingénieur, chef militaire. Dans les écoles d'officiers, cet enseignement peut s'appuyer sur les centres de recherche pour délivrer un enseignement de haut niveau.
Dans la gestion de leur personnel, ils veilleront au développement et au maintien d'une expertise technique en cyberdéfense pour un nombre suffisant de spécialistes et à la diffusion auprès de tous les opérationnels d'une formation généraliste en cyberdéfense.
Indicateurs : comptes-rendus du COPIL RH SSI (Pilotes : DGSIC et DRH-MD).

Action 29

-> optimiser et mutualiser au plan interarmées et ministériel les formations à la cyberdéfense au sein du ministère

Dans un souci de cohérence dans la mise en œuvre opérationnelle des procédures de cybersécurité, il est primordial que les actions de formation des armées et services soient partagées par l'ensemble des acteurs de la cybersécurité, au sein du ministère et avec nos partenaires de confiance. L'identification de modules communs de formation pour tout ce qui ne relève pas de la partie métier des systèmes d'information ainsi que la mise en place de centres de référence de formation sur ces modules doivent être recherchées, notamment dans le cadre de la CSF, en synergie avec le pôle d'excellence cyberdéfense.
Indicateurs : comptes-rendus du COPIL RH SSI (Pilotes : DGSIC et DRH-MD).

Action 30

-> participer à la construction d'une filière nationale des RH en cybersécurité en facilitant la mobilité des agents du ministère

La mobilité interne et externe des agents civils et militaires du ministère de la Défense doit être facilitée pour participer aux partages des expériences et à la constitution d'une véritable communauté nationale de cyberdéfense.
La DRH-MD mettra en place un indicateur adapté.
Indicateurs : taux de mobilité interne et externe (Pilote : DRH-MD).

Axe 4

Développer le Pôle d'excellence en cyberdéfense en Bretagne au profit du ministère de la Défense et de la communauté nationale de cyberdéfense

Le Pôle d'excellence en cyberdéfense en Bretagne se structure autour de deux composantes indissociables. La première est consacrée à la formation initiale, la formation continue et l'enseignement supérieur. L'autre concerne la recherche, garante d'un enseignement supérieur de qualité, et le développement d'un tissu industriel avec une attention particulière pour les PME/PMI. Il doit également s'appuyer sur l'organisation technico-opérationnelle pour mettre en place les plates-formes nécessaires à la formation, l'entraînement à la gestion de cyberattaques et l'expérimentation de nouveaux produits de sécurité informatique

Action 31

-> optimiser l'utilisation des moyens et le développement des compétences cyber du ministère présents en Bretagne en y concentrant les unités

La présence de nombreuses implantations du ministère de la Défense, stimulée par la création du Pôle Bretagne, doit permettre la constitution d'un véritable bassin d'emplois « défense » en matière de cybersécurité. Ce bassin doit servir de support à la construction des parcours professionnels qualifiants et cohérents alliant la satisfaction des besoins en compétence du ministère et les contraintes de mobilités des agents civils et militaires. En lien avec la DRH-MD, la DGSIC mettra en place un indicateur des RH cyber présentes dans la zone du Pôle.

Indicateurs : pourcentage des ressources humaines présent dans le périmètre du pôle, pourcentage de rotation annuelle (Pilotes : DRH-MD et DGSIC, en relation avec le chef de projet pôle d'excellence cyber de Bretagne).

4.1 DÉVELOPPER UNE OFFRE DE FORMATION ADAPTÉE QUI S'APPUIE SUR LE TISSU DE CENTRES DE FORMATION, D'EXPERTISE OPÉRATIONNELLE, UNIVERSITAIRES OU TECHNIQUES DE LA RÉGION BRETAGNE

Action 32

-> stimuler la recherche, la formation et l'innovation avec la création du pôle d'excellence cyberdéfense en Bretagne, où le ministère dispose déjà d'un réseau important d'expertise technique et de centres de formation

La défense doit capitaliser sur ses écoles et ses centres d'expertise, dont la plupart sont en Bretagne : les Écoles de Saint-Cyr Coëtquidan (ESCC), la DGA MI, le CALID Bretagne, l'École des Transmissions (ETRS), les centres de la DIRISI en Bretagne, l'ENSTA Bretagne, l'École Navale... Elle peut aussi établir des partenariats et des synergies avec les écoles civiles et les universités (Supelec, ENST Bretagne, Rennes I, Sciences Po Rennes, IUT Lannion et Saint-Malo, Université de Bretagne Sud, Université de Bretagne Occidentale, l'Université Européenne de Bretagne…) et les centres techniques des entreprises privées de la région (Orange, DCNS…).

Le plan d'action et de suivi du Pôle Bretagne permettra de mesurer les progrès en la matière.
Indicateur : plan d'action et de suivi du Pôle Bretagne (Pilote : chargé de mission Pôle Bretagne).

Action 33

->créer un cursus de formation à la conduite des opérations et à la gestion des crises cyber qui sera ouvert aux partenaires publics ou étrangers, avec une première session en 2015

En complément de ces possibilités de formation et d'entraînement dispensés dans les écoles, un nouveau cursus de formation à la gestion des crises cyber va être créé avec les partenaires du pôle Bretagne. Résolument tourné vers une approche globale, il apportera une compréhension des phénomènes techniques et comprendra des modules de droit, d'éthique, de relations internationales et de gestion civilo-militaire des crises.
D'ici 2015, des modules adaptés seront mis en place. Dès 2015, à partir d'un noyau opéré par les ESCC et l'ETRS, il sera ouvert aux officiers de toutes les armées et également aux agents d'autres ministères et à des partenaires étrangers.
Indicateur : plan d'action et de suivi du Pôle Bretagne (Pilote : chef de projet Pôle d'excellence cyber de Bretagne).

4.2 RENFORCER L'INTÉGRATION DE LA CYBERDÉFENSE DANS LA PRÉPARATION OPÉRATIONNELLE DES FORCES EN S'APPUYANT SUR DE NOUVEAUX MOYENS D'ENTRAÎNEMENT ET DE SIMULATION DISTRIBUÉE DÈS LA RENTRÉE 2015

Action 34

-> déployer et exploiter une capacité de formation, d'entraînement et de perfectionnement simulée en cyberdéfense, sous la coordination opérationnelle du CALID Bretagne et avec l'expertise technique de DGA-MI

Pour appuyer la formation, l'entraînement et le perfectionnement des forces armées et des spécialistes de la cyberdéfense, une plate-forme distribuée de simulation et d'entraînement sera constituée. Soutenue par l'expertise technique de DGA-MI et sous la coordination opérationnelle du CALID Bretagne, cette capacité sera déployée et mise en œuvre en fonction des besoins des différentes armées, directions et services pour former et entraîner à la défense contre des agressions informatiques comme à la gestion de crise cybernétique et pourra aussi être utilisée au-delà du seul ministère. Cette plate-forme devra être capable de soutenir le pôle d'excellence et notamment le cursus de formation à la gestion des crises cyber dès septembre 2015
Indicateurs : capacités de la plate-forme en 2015 (Pilote : EMA/DGA).

Axe 5

Cultiver un réseau de partenaires étrangers, tant en Europe qu'au sein de l'Alliance Atlantique et dans les zones d'intérêt stratégique

La France a des intérêts à défendre partout dans le monde, que ce soit grâce à ses départements ou collectivités ultramarines, ses accords de défense avec de nombreux pays ou ses intérêts stratégiques. Pour assurer la cyberdéfense de son territoire et de ses forces face aux menaces mondiales et provenant d'acteurs étatiques ou non, elle doit bâtir des coopérations pour échanger des informations et éventuellement coordonner ses actions dans le cyberespace.

Au premier rang de ses partenaires se trouvent naturellement les États membres de l'Union Européenne et les États alliés de l'OTAN. Mais d'autres États des zones d'intérêt stratégique – notamment au Moyen-Orient ou dans le Pacifique – sont également des partenaires à rechercher. Toutefois, les coopérations les plus approfondies imposent un haut degré de confiance et des capacités techniques développées qui restreignent le cercle des partenaires potentiels.

Action 35

-> contribuer, avec l'ANSSI et le ministère des Affaires Étrangères, à la définition et à la défense de positions françaises contribuant à la stabilité du cyberespace

Le cyberespace est un domaine où, par essence, les distinctions entre sécurité et défense sont plus difficiles à établir. Il s'agit d'un véritable continuum sécurité défense, dans lequel les problématiques militaires doivent être prises en compte. Aussi, dans toutes les négociations internationales dans ce domaine, le ministère de la Défense apportera son expertise spécialisée aux autres acteurs.

Indicateur : participation d'experts du ministère à la préparation et à la conduite des négociations internationales (Pilote : DGRI).

5.1 ENGAGER ET APPROFONDIR DES COOPÉRATIONS BILATÉRALES MUTUELLEMENT PROFITABLES AVEC NOS ALLIÉS DANS LES DOMAINES OPÉRATIONNELS, TECHNIQUES ET INDUSTRIELS

Nous devons être capables de bâtir jour après jour une confiance mutuelle avec nos alliés dans l'intérêt de tous. Ainsi, je veux qu'avec ses partenaires les plus proches le ministère de la Défense développe des coopérations opérationnelles, techniques et industrielles étroites qui assurent une vraie supériorité dans le cyberespace. Avec les partenaires moins avancés, nous serons dans une démarche de progrès pour élever le niveau général de cybersécurité et contribuer ainsi indirectement à sécuriser le cyberespace

Action 36

-> approfondir les coopérations opérationnelles et techniques en cyberdéfense avec les partenaires engagés dans les mêmes opérations militaires afin d'en développer l'interopérabilité

Indicateur : tableau de suivi des coopérations dans ce domaine (Pilote : EMA).

Action 37

-> approfondir les coopérations avec les alliés les plus présents dans le cyberespace pour améliorer notre vision commune des menaces, anticiper les attaques et travailler en commun à leur solution

Indicateur : tableau de suivi des coopérations dans ce domaine (Pilote : EMA).

Action 38

-> ajouter un volet cyberdéfense dans les relations de défense que nous avons établies avec nos partenaires, en cohérence avec la profondeur de nos relations et le niveau de menaces

Indicateur : tableau de suivi des coopérations dans ce domaine (Pilote : DGRI).

5.2 PROMOUVOIR LA PRISE EN COMPTE CONCRÈTE DE LA CYBERDÉFENSE DANS LA POLITIQUE DE SÉCURITÉ ET DE DÉFENSE COMMUNE DE L'UNION EUROPÉENNE

L'Union Européenne reste quant à elle le cadre naturel du développement de la cybersécurité collective de nos infrastructures critiques. Le ministère de la Défense, en lien avec l'ANSSI et le ministère des Affaires Étrangères, s'attachera à renforcer la prise en compte de la cyberdéfense de toutes les organisations militaires de l'Union Européenne et des opérations militaires sous commandement européen.

Action 39

-> soutenir la prise en compte de la cybersécurité comme priorité européenne d'abord pour les institutions elles-mêmes et également pour les États membres

Pour appuyer l'action de l'ANSSI et du ministère des Affaires Étrangères, le ministère sera force de proposition et mettra à profit les relations de confiance qu'il a établies avec ses partenaires.
Indicateur : avancement de la cybersécurité européenne (Pilote : DGRI).

Action 40

-> promouvoir les solutions européennes de cybersécurité dans les domaines où une capacité nationale souveraine n'est pas accessible ou nécessaire

Une base industrielle européenne doit progressivement être élaborée afin d'assurer à terme la cybersécurité des programmes conduits par l'Union Européenne, et en particulier par l'Agence Européenne de Défense. Cette construction complexe s'appuiera à court terme sur la mutualisation de certaines des actions de recherche et de formation présentées par ailleurs dans ce pacte.
Indicateur : développement d'initiatives de recherche, de formation et des projets industriels européens en cybersécurité (Pilote : DGA).

Action 41

-> s'engager résolument pour promouvoir la cyberdéfense militaire dans l'Union Européenne

Ainsi, la France cherchera dans tous les organismes militaires européens auxquels elle participe à améliorer la prise en compte de la cyberdéfense pour la protection de ces organismes mais aussi dans la planification et la conduite de leurs opérations. À cette fin, le soutien de nos partenaires européens proches comme le Royaume Uni et l'Allemagne sera recherché, mais aussi celui des nations comme l'Estonie et la Belgique.
Par ailleurs, l'expertise et l'expérience opérationnelle françaises seront mises à la disposition de l'État-major de l'Union Européenne pour partager nos savoirs faire et contribuer à construire une cyberdéfense militaire européenne concrète et efficace.
Indicateur : avancement des aspects militaires de la cyberdéfense européenne (Pilote : EMA).

5.3 S'ENGAGER À L'OTAN POUR GARANTIR LA RÉSILIENCE DE L'ORGANISATION EN CAS DE CRISE CYBER ET LES CAPACITÉS OPÉRATIONNELLES DES FORCES ALLIÉES EN OPÉRATION

S'agissant de l'Alliance Atlantique, le soutien de la France à la prise en compte de la cyberdéfense comme enjeu stratégique est total. La protection des infrastructures de l'OTAN elle-même et la cyberdéfense des forces en opération sont les deux objectifs majeurs. En cas de crise cyber particulièrement grave qui affecterait un de nos Alliés, nous assumerions naturellement nos responsabilités en l'assistant de notre mieux.

Action 42

-> promouvoir à l'OTAN les priorités de l'organisation de cyberdéfense et d'interopérabilité des forces

Ainsi, l'organisation de la cyberdéfense de l'OTAN doit être orientée vers la prévention des cybermenaces, vers la gestion de crises cyber et vers la prise en compte de la cyberdéfense des forces en opération. Elle s'appuiera essentiellement sur le développement des capacités de cyberdéfense des Alliés et une coopération accrue avec l'Union Européenne.
Indicateur : avancement de la cyberdéfense de l'OTAN (Pilote : EMA).

Action 43

-> contribuer à la défense de nos Alliés en partageant avec l'OTAN les informations sur les menaces qui pourraient nuire à leur sécurité et en leur portant assistance en cas de crise cybernétique majeure

e ministère de la Défense donnera notamment une nouvelle impulsion au Memorandum of Understanding (MOU) avec l'OTAN.
Indicateur : intensification des échanges avec l'OTAN (Pilote : EMA).

Axe 6

Favoriser l'émergence d'une communauté nationale Défense de cyberdéfense en s'appuyant sur un cercle de partenaires et les réseaux de la réserve

Le Livre Blanc sur la Sécurité et la Défense Nationale appelle à une coopération étroite des services de l'État pour faire face aux cybermenaces. Le défi posé par le caractère global du cyberespace impose aussi d'échanger et de partager avec tous les acteurs non étatiques concernés.

6.1 SE DOTER DES OUTILS ET MOYENS DE CONSTITUER ET FIDÉLISER UNE COMMUNAUTÉ NATIONALE DÉFENSE DE CYBERDÉFENSE

Action 44

-> Valoriser et reconnaître l'engagement au service de la Nation dans la cyberdéfense

La cyberdéfense fera l'objet d'un plan de communication spécifique pour faire connaître les enjeux, promouvoir les différentes formes d'action au service de la Nation, et en particulier les réserves cyber, et valoriser l'engagement de tous les acteurs civils ou militaires. Dans ce cadre, une politique de reconnaissance sera mise en place au sein du ministère au profit du personnel d'active ou de réserve servant dans la cyberdéfense (logo, insigne, récompenses, agrafe, etc.).
Indicateur : motivation des personnels de la cyberdéfense (Pilote : DICOD).

Action 45

-> organiser l'évaluation des mesures prises, des attentes et de la notoriété du Pacte Défense Cyber et le suivi du tableau de bord « Cyber Mindef »

Le suivi des mesures prises sera assuré grâce aux différents indicateurs définis qui montreront les progrès effectués, soit quantitativement, soit tendanciellement, et qui seront rassemblés dans un tableau de bord destiné au ministre.
Indicateur : tableau des indicateurs définis dans le Pacte Défense Cyber (Pilote : EMA).

Action 46

-> en relation avec le Pôle d'excellence, contribuer à fédérer dans le cadre régional des grandes implantations de la défense tous les acteurs publics ou privés en lien avec le ministère

Le cercle des partenaires régionaux, animé par le commandant de l'ETRS de Rennes, vise à fédérer les énergies, mutualiser les capacités et permettre une fertilisation croisée entre experts, enseignants et opérationnels, militaires comme civils, du public comme du privé. Il poursuivra son action en lien avec le développement du pôle d'excellence de Bretagne.
D'autres cercles régionaux sont à développer autour des grands pôles d'acteurs que sont les zones de Toulon et Brest pour la marine, Lille pour les forces terrestres et la région Bordeaux/Toulouse ou Aix/Marseille pour le domaine aérospatial, tout en garantissant un lien fort avec les activités du pôle d'excellence de Bretagne
Indicateur : développement des projets dans le cadre des cercles régionaux (Pilotes : EMAT, EMM et EMAA).

6.2 CONTRIBUER À RAPPROCHER LES DIFFÉRENTS ACTEURS NATIONAUX DE LA CYBERDÉFENSE AU TRAVERS DU DÉVELOPPEMENT DE LA RÉSERVE CITOYENNE

La Défense a développé le concept de réserve citoyenne pour renforcer le lien armée-Nation en bénéficiant de l'expertise et des compétences des réservistes issus de la société civile qui sont également autant de relais pour diffuser l'esprit de défense dans leur milieu.
Appliqué à la cyberdéfense, ce concept a permis, grâce à ses réservistes citoyens de toutes les armées et de tous horizons (entrepreneurs, juristes, communicants, parlementaires, jeunes professionnels), de partager largement le constat des enjeux et des défis du cyberespace, d'aider à définir les voies de progrès et de contribuer à convaincre les acteurs nationaux des enjeux dans ce domaine.

Action 47

-> développer la réserve citoyenne de cyberdéfense en approfondissant les réflexions de la réserve parisienne et en l'étendant dans les régions françaises

La création d'antennes de la réserve citoyenne dans les régions permettra de diffuser les bonnes pratiques auprès de tous, de bénéficier des bonnes idées d'où qu'elles viennent et de créer un réseau d'acteurs impliqués qui permettra de soutenir localement l'action des acteurs qui sont la Gendarmerie Nationale, la DPSD, la Direction Centrale du Renseignement Intérieur (DCRI) ou encore les Observatoires zonaux de la sécurité des systèmes d'information qui agissent au profit de l'ANSSI.
Indicateurs : nombre de régions dans lesquelles la réserve citoyenne se déploie et nombre d'actions menées (Pilote : EMA).

Action 48

-> consolider et approfondir la Réserve citoyenne cyber

En lien avec la DGRI et la DICOD qui soutiendront concrètement les actions de la RCC, il s'agit de garantir la pérennité de cette structure en lui apportant un soutien humain et financier au travers d'actes de communication (supports, insignes…) et d'événements de réflexion stratégique (séminaires). Entre autres, il s'agira d'évaluer le besoin en frais de fonctionnement et d'affecter les ressources correspondantes.
Indicateurs : moyens affectés à la RCC et nombre d'actions menées (Pilote : EMA).

6.3 CONTRIBUER À LA GESTION DES CRISES CYBERNÉTIQUES ET À LA RÉSILIENCE DE LA NATION EN DÉVELOPPANT EN PARTICULIER UNE RÉSERVE DE CYBERDÉFENSE À VOCATION OPÉRATIONNELLE

Les crises cyber sont particulièrement complexes à traiter. Selon leur nature, elles peuvent par exemple nécessiter, pendant une phase d'évaluation, une équipe réduite disposant d'un haut degré d'expertise que l'ANSSI ou les armées développent et entretiennent et, pendant une phase de restauration, une ressource humaine moins qualifiée mais nombreuse que les opérateurs pourraient avoir des difficultés à réunir, notamment si la crise touche de nombreux systèmes.

Action 49

-> développer une réserve de cyberdéfense à vocation opérationnelle pour assister l'État et les armées en cas de crise majeure

Constituée de jeunes professionnels ou d'étudiants, elle pourrait intervenir, encadrée par des spécialistes du ministère de la Défense, du ministère de l'Intérieur et de l'ANSSI, pour rétablir les systèmes attaqués. Les jeunes impliqués dans cette réserve cultiveraient de façon pratique le lien armée-Nation en servant directement les intérêts de la Nation et bénéficieraient d'une formation et d'une expérience uniques.
Ce projet sera développé en coopération étroite avec l'ANSSI et la Gendarmerie Nationale. Il s'inspirera des exemples de nos partenaires étrangers et devra pouvoir être expérimenté d'ici fin 2014.
Indicateur : projet à expérimenter avant la fin de l'année 2014 (Pilote : EMA).

Action 50

-> consolider une vision globale des différents types de réserve cyber

En lien avec l'ANSSI, l'EMA préparera une instruction globale cadrant les deux volets de la réserve cyber et organisant leur complémentarité.
Indicateur : projet d'instruction établi en 2015 (Pilote : EMA).

DICoD

Délégation à l'information et
à la communication de la Défense